Regular Paper

Automotive Security on Abnormal Vehicle Behavior Using Only Fabricated Informative CAN Messages

Junko Takahashi[1,a)] Masashi Tanaka[1] Hitoshi Fuji[1] Toshio Narita[2] Shunsuke Matsumoto[2] Hiroki Sato[2]

Received: May 21, 2018, Accepted: November 7, 2018

Abstract: We present a method for influencing vehicle behaviors using only informative Controller Area Network (CAN) messages that are used to inform vehicle status. Some recent vehicle attack techniques have been shown to have a significant impact on the automotive industry. Almost all previous studies employ active CAN messages that directly induce actions for the attacks, but there have been no studies that explicitly use only the informative CAN messages. This is the first report of using only informative CAN messages in an attack especially targeting a driving-support system. Through experiments, we show that abrupt acceleration/deceleration is abnormally induced using informative messages regarding the wheel speed while the cruise control system is activated. We also find that the speed limit control of the cruise control system can be disabled and the parking assist system can be canceled using fabricated informative messages. The experimental results reveal that fabricated informative CAN messages can manipulate the vehicle to yield an improper behavior. We evaluate the effectiveness of some countermeasures by applying them to the attacks and clarify the strength and weakness of each countermeasure. We believe that this study will bring a new perspective to the automotive security toward vehicle system design.

Keywords: automotive security, Controller Area Network (CAN), abnormal behavior, spoofing attacks

1. Introduction

Recently, automotive security has attracted attention because abnormal behaviors have been induced in real vehicles and the sophistication of the attack techniques has increased every year. Some researchers have shown that abnormal vehicular actions can be induced by an attacker injecting fabricated messages into a Controller Area Network (CAN) bus such as in Refs. [1], [2], [3], [4]. Thus, the security of real vehicles is an important topic and research on protection against such attacks has become an urgent issue. It is considered that protection methods used in Information Technology (IT) security techniques are useful for ensuring CAN-bus security. As examples, Message Authentication Codes (MACs) [5], [6], [7], anomaly detection [8], [9], [10], and Intrusion Detection Systems (IDSs) [11], [12], [13] were proposed for adoption into in-vehicle networks.

Attacks in real vehicles were previously shown in, for example, Refs. [1], [3], [4]; however, these attacks mostly rely on two types of CAN messages, diagnostic messages used for vehicle maintenance and active messages that can directly cause an action. Examples of active messages are accelerating the vehicle, turning the steering wheel, and locking the door. In Ref. [3], a kind of informative message that only informs the gear position status is used in the attack to change the internal gear status to manipulate the steering wheel. However, these messages play an absolutely subsidiary role and the authors of Ref. [3] could not show that a single informative message explicitly affected critical vehicle controls. Furthermore, because informative messages are considered to only provide information regarding the vehicle status, there are cases in which countermeasures would not be implemented due to a shortage of computational resources of a vehicle control module. From another aspect, we also point out that very few studies can perform successful attacks to manipulate acceleration/deceleration in real vehicles.

In this paper, we first show that the abnormal vehicle behaviors can be induced using only informative CAN messages while the driving support system is activated [*1]. In fact, we precisely show that we are able to actualize an abnormal acceleration/deceleration by injecting the fabricated wheel-speed messages to indicate a much lower/higher speed than the set speed while the cruise control system is used. In the same way, we show that we can disable the speed limit for activating the cruise control system. Furthermore, we show that the parking assist system can be abruptly canceled without driver operation. Based on the experimental results, we show that informative messages as well as active messages should be protected. We evaluate the effectiveness of some countermeasures by applying them to the attacks and clarify the strength and weakness of each counter-

[1] NTT Secure Platform Laboratories, Musashino, Tokyo 180–8585, Japan
[2] NTT DATA MSE CORPORATION, Yokohama, Kanagawa 222–0033, Japan
[a)] junko.takahashi.fc@hco.ntt.co.jp

[*1] A preliminary version of this paper was published in the conference proceedings of HOST 2018 [14]. In this paper, we also describe the details of other attack methods such as deceleration, disabling the speed limit for activating the cruise control system, and canceling the parking assist without driver operation in Section 4. We also describe the details of the countermeasures in Section 5.

measure. We believe that this study will bring a new perspective to developing vehicle systems for improving security.

Hereafter, Section 2 provides background information on the vehicle controls and Section 3 describes previous studies. Section 4 presents the attacks using fabricated informative messages in real vehicles. The evaluation of the countermeasures is described in Section 5. Finally, we conclude the paper in Section 6.

2. Preliminary on Vehicle Controls

We first describe a general mechanism for the vehicle controls that are performed using in-vehicle messages.

2.1 General Mechanism for Vehicle Controls

The general mechanism for a vehicle control is shown in **Fig. 1**. A control unit usually refers to the (i) requests for actions to be performed such as turning the steering wheel and accelerating the vehicle, and the (ii) status of the vehicle based on the captured sensor information such as information of the current speed and the gear position through an in-vehicle network (CAN, Local Interconnect Network (LIN), and FlexRay). Then, the control unit decides whether an action is performed based on that information. In modern systems, a control unit may monitor several kinds of messages to conduct a complicated action [2].

Types of information (i) and (ii) above are usually input into the control unit using in-vehicle messages such as CAN messages. CAN messages can be roughly categorized into three types based on the responsibility for transmitting messages to the control unit: diagnostic, active, and informative messages [4]. We employ these categories in the paper. Each message is used for the appropriate vehicle functions. Example actions induced by these three kinds of CAN messages are given in **Table 1**. We give details on the meanings of each type of message in the next section.

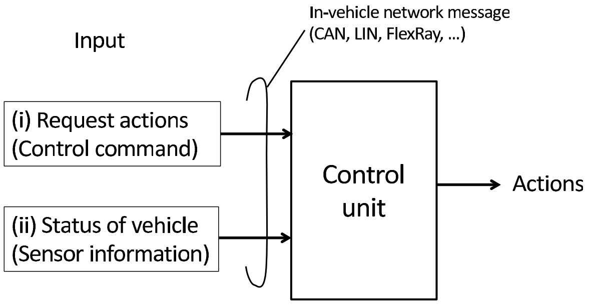

Fig. 1 Mechanism for vehicle control using an in-vehicle message.

Table 1 Example actions induced by CAN Messages.

CAN Message	Contents
Diagnostic Message	- Brakes will not work - Lights On/Off - Fastening of seatbelt - Killing an engine
Active Message	- Engaging brakes - Turning steering wheel - Accelerating vehicle - Locking/Unlocking door
Informative Message	- Informing wheel angle - Informing wheel speed - Informing current speed of vehicle - Informing brake pedal position

2.2 Kinds of CAN Messages

Diagnostic messages are only used for vehicle maintenance. They can be viewed in the communications between the diagnostic tool and the bus for obtaining information on the vehicle and for active tests to confirm the behavior of the vehicle systems. In ISO-TP/ISO 15765-2 [15], the method for sending diagnostic messages in the CAN bus is defined. The message format for the diagnostic messages is defined in ISO 14229 [16] or 14230 [17].

Active messages, which are a type of normal message that is usually sent through the bus, request the control unit to perform actions as shown in Fig. 1 (i). These messages are responsible for performing physical actions of the vehicle related to control systems such as moving the vehicle, engaging brakes, turning the steering wheel, and related to the body control systems such as opening/closing the windows and locking/unlocking the door.

Informative messages, which are a type of normal message, are responsible for informing the control unit of the state of the vehicle from the captured sensors as shown in Fig. 1 (ii). The messages related to the wheel angle and the brake pedal position obtained from each sensor are examples. This type of message does not directly induce any vehicle action.

3. Previous Studies

This section describes previous vehicle attacks using fabricated CAN messages based on the mechanism of vehicle control described in Section 2.

The investigations in Refs. [1], [2], and [3] showed automotive control by injecting attack messages using diagnostic messages in the CAN bus through the on-board diagnostics (OBD)-II port. These studies showed that the attacker can achieve a partial control over the body of the vehicle such as turning on the lights, moving wipers or fastening a seat belt at any time.

In Refs. [1], [3], [4], it was shown that injecting active CAN messages can induce some abnormal behaviors. In Ref. [1], the authors showed that they were able to, for example, tamper with some control over the vehicle body system. The researchers in Refs. [3], [4] showed that a fabricated message can be used to request a control unit to take action (as in Fig. 1 (i)) resulting in engaging the brakes and turning the steering wheel.

All of the above previous papers propose and discuss attacks using diagnostic or active messages that directly indicate actions for a control unit and their countermeasures. Informative messages are utilized to inform the control unit of the vehicle state and it was typically considered that these messages do not affect physical aspects of the vehicle [4].

Although the researchers in Ref. [3] used fabricated informative messages to activate the parking assist system at any gear position, these messages played a subsidiary role and the active messages were still needed for the attacks. So, they could not achieve successful attacks in causing abnormal vehicle behavior by only injecting informative messages. Furthermore, there are few studies that show the vehicle is irregularly accelerated or decelerated by injecting fabricated in-vehicle messages.

4. Method for Influencing Vehicle Behavior Using Fabricated Informative Messages

In this section, we present details on the attack methods and the experimental results.

4.1 How to Find Proposed Attack and Concept Behind Attack

In this section, we describe the objective of the attacks, how to find the attacks and the concept behind the attacks to give the information for reference when someone investigates the attack method and evaluates real vehicles.

We consider that the most serious threat related to the driving the vehicle is to induce the significant accidents to be involved in the human lives. Then, we define the objective of the proposed attacks as inducing the abnormal vehicle behaviors which cause the significant accidents by the attacks, and then, compromising a control unit.

In order to compromise the significant vehicle controls, we focus on the driving support systems in which the functions are electronically controlled and we investigate the attack methods to induce the abnormal behaviors by the irregular controls of the vehicle from the attackers.

At this time, as shown in Fig. 1, the control unit which manages the driving-support-system function is activated using two kinds of messages: those that request action and those that inform the controller of the status of the vehicle. Furthermore, recent vehicle systems such as the driving support systems require complex interactions among several modules including the sensors [1], [18]. From the aspect of the attacks, the fact that messages that request action (active or diagnostic message) could be used was published in the previous studies [1], [3], [4]. However, the attacks using the messages of the status of the vehicle (informative messages) have not been publicly proposed.

Then, we consider that a single informative message can be used in attacks as well as the active or diagnostic message because these complex driving support systems refer to many kinds of information. As a result, we find that we can affect critical vehicle actions only using one type of fabricated informative message. In fact, we show that the driving support systems can be easily compromised by such messages and point out that serious consideration should be given to the security of informative messages.

4.2 Attacker Capabilities and Experimental Conditions

This section describes attacker capabilities needed to achieve the successful attacks and the experimental conditions used in this study.

4.2.1 Attacker Capabilities

We describe the attacker capabilities to achieve the successful attacks.

- The attacker can access the internal CAN-bus. As an example, the paths to access the bus are considered as follows: through the OBD-II port, by tapping the bus directly, or through some other remote attack interfaces such as the infotainment systems.
- The attacker can sniff the CAN messages transmitted in the bus and identify the meaning of the CAN-ID and data because the contents of the data are sometimes proprietary.

  We note that, to identify the meaning of the informative messages is more difficult compared to the active messages in some cases because the attacker cannot easily verify any visible action by injecting informative messages in a normal vehicle situation. Therefore, the attacker tries to identify the contents of the data by focusing on the characteristics of the data structure and the transitions of the data based on the vehicle behaviors.
- The attacker can inject fabricated messages into the vehicle based on the analysis of the CAN messages through paths mentioned in the first item as an example while the driving support system is activated in the vehicle which the attacker targets.

  At this time, the attacker injects the fabricated messages an equal number of times to the original messages or more than the number of the original messages to increase the impact of the attacks.

Considering the attacks against the real vehicles [3], [19], the above attack conditions are general and feasible.

4.2.2 Experimental Conditions

Based on the attacker capabilities, we describe the experimental conditions used in this study.

- We sniff the CAN messages and inject fabricated messages through the OBD-II port or by tapping the bus directly depending on the vehicle.

  The injected messages include the same ID as the original message and data related to the control are different from those in the original message.
- We inject the fabricated messages immediately after the original ones so that they will be overridden by the fabricated messages without the need to reprogram the module. The average timing difference between the original and fabricated message is 0.6 ms.
- We use CANoe software [20] installed on a PC to sniff and inject the fabricated messages and use VN1630A which is the hardware interface of the CAN bus including the CAN transceiver [21].
- In the experiment, we conduct cruise control system tests on a specialized roller that is embedded in the ground.

4.3 Controlling Acceleration/Deceleration by Targeting a Cruise Control System

The cruise control system is used to maintain a constant speed according to a set value selected by the driver. **Figure 2** shows a typical system structure. A module related to the cruise control system monitors physical information signals related to the vehicle status. Based on these signals, the cruise control module requests speed-management actions.

Even though the cruise control system monitors several kinds of signals to control the speed, we find that we can induce abnormal acceleration/deceleration without physically depressing the accelerator by fabricating a CAN message related to the vehicle status. The basic idea is that we create a false state by injecting

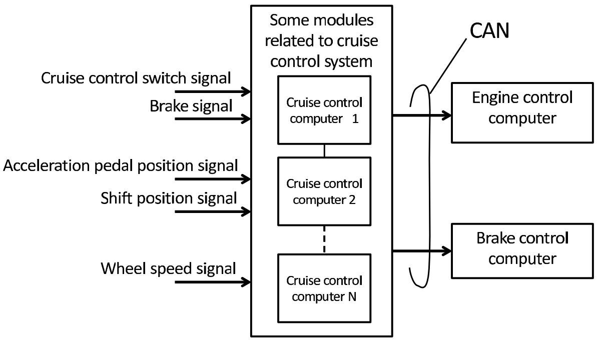
Some modules related to cruise control system
CAN
Cruise control switch signal
Brake signal
Acceleration pedal position signal
Shift position signal
Wheel speed signal
Cruise control computer 1
Cruise control computer 2
Cruise control computer N
Engine control computer
Brake control computer

Fig. 2 Typical cruise control system structures.

the fabricated message and the cruise control system falsely recognizes that it needs to accelerate the vehicle even though it does not actually need to do so.

In the vehicle used in the experiments, the CAN message related to the vehicle status is the current wheel-speed CAN message[*2]. Usually the CAN message related to the current wheel speed is broadcast to the bus to inform each module of the individual wheel speed. We note that injecting the fabricated wheel-speed message does not result in an abnormal physical action when the vehicle is driving as usual. However, we show that the fabricated wheel-speed message affects the vehicle behavior while the cruise control system is used.

4.3.1 Attack Method for Abnormal Acceleration

Here, we present the details of the attack procedure and its implementation in real vehicles. In the experiments, we implement the attack while we drive at a constant speed using the cruise control system.

(A) A driver presses a button to activate the cruise control system and accelerate the vehicle to the desired speed, of 60 km/h as an example.

(B) After the speed of the vehicle exceeds the desired speed, the driver sets the desired constant speed, 60 km/h, by manipulating a lever. The vehicle travels at the set speed for a certain time.

After that time, the attacker starts to inject fabricated wheel-speed messages indicating that the vehicle is at the much lower speed of 40 km/h as an example.

In a real attack situation, the attacker would know when the cruise control system is active by investigating the sniffed CAN messages related to the vehicle speed which is shown as constant.

(C) As a result, the vehicle gradually accelerates and the actual speed eventually reaches approximately 120 km/h on the speedometer display, which far exceeds the set speed[*3].

Figure 3 shows the transition in the vehicle speed described from the captured CAN messages while the attack proceeds. The vehicle speed is represented on the vertical axis and time is represented on the horizontal axis.

In the above case, we surmise that the cruise control module trusts the new messages indicating the wheel speed when the module receives them in sequence. So, the module trusts the fabricated message sent immediately after the genuine one. This induces a misinterpretation of the current speed by its module and results in requests for the engine control computer to increase the engine throttle.

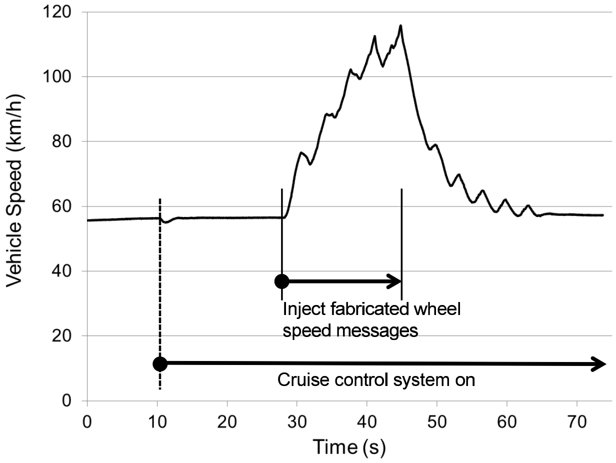

Fig. 3 Transition in vehicle speed described from the captured CAN messages when fabricated wheel-speed messages lower than that for the set speed are injected.

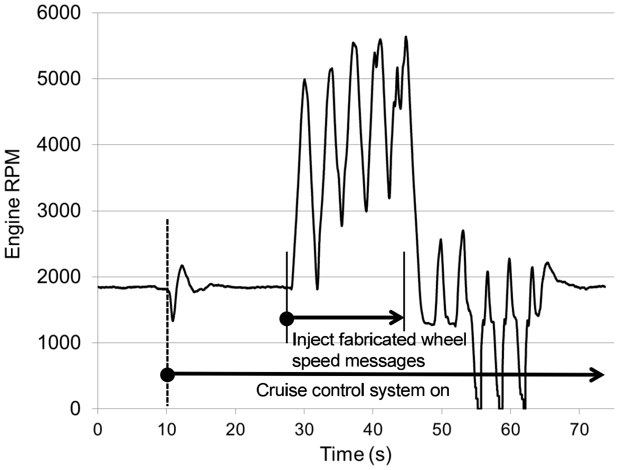

Fig. 4 Transition in the engine RPMs with vehicle speed described from the captured CAN messages for the case in Fig. 3.

For reference, we show in **Fig. 4** the engine revolutions per minute (RPMs) described from the captured CAN messages at that time. The figure from the CAN messages shows that the RPMs exceed 5,500 while the speed is accelerated.

The cruise control system can usually be disengaged when the driver depresses the brake pedal and the driver may mitigate the effects of the above abnormal behavior by performing such handling. However, we consider that this fact may cause the driver to panic when the speed is suddenly accelerated/decelerated without the driver intention and it is still dangerous if the driver does not pay attention to this problem.

4.3.2 Attack Method for Abnormal Deceleration

This mechanism is almost the same as that for the acceleration. Abnormal deceleration can be induced by injecting the fabricated wheel-speed messages indicating a higher speed than that of the original one.

[*2] In another vehicle developed by a different carmaker, the CAN message we used in the attacks is the current-speed message.

[*3] For safety reasons, we stop injecting the fabricated CAN messages when the actual speed reaches approximately 120 km/h in the experiments. The speed will continue to increase to the maximum speed of the vehicle until we stop injecting the fabricated messages.

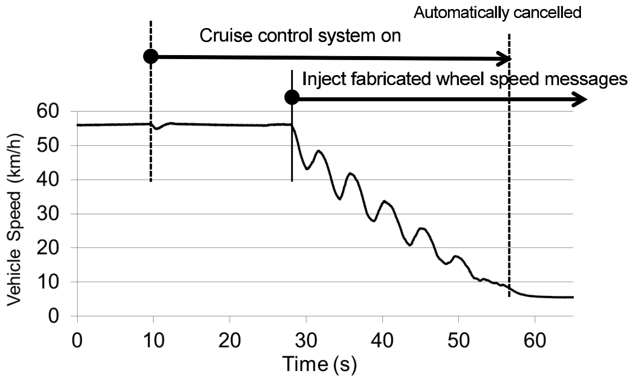

Fig. 5 Transition in vehicle speed when fabricated wheel-speed messages higher than that for the set speed are injected. The cruise control system is automatically canceled around 56 s.

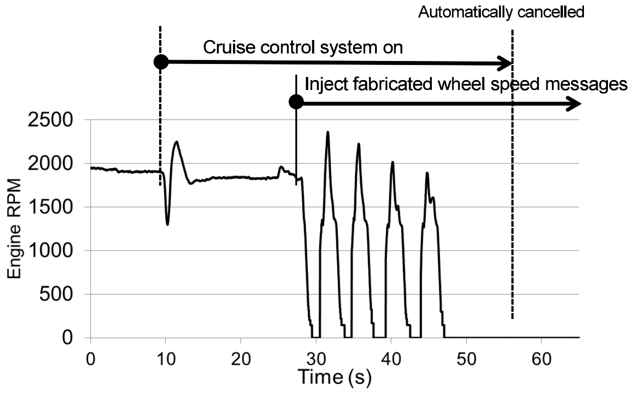

Fig. 6 Transition in engine RPMs with vehicle speed described from the captured CAN messages in the case in Fig. 5.

To start, a driver activates the cruise control system and he sets the speed to 60 km/h as an example. After the actual speed reaches approximately 60 km/h and he sets it as the set speed, the attacker injects fabricated wheel-speed CAN messages that indicate that the vehicle is moving at 70 km/h. Then, the cruise control system misinterprets that the speed has exceeded the set speed and must be reduced to 60 km/h even though the current speed is already 60 km/h. In fact, the speed is gradually reduced to 0 km/h. **Figure 5** shows the transition in the vehicle speed described from the CAN messages when the fabricated wheel-speed messages are injected. The figure shows that the vehicle speed is reduced from 55 km/h to almost 0 km/h.

When the vehicle speed reaches approximately 10 km/h (56 s point), the cruise control system is automatically canceled. In a normal situation, an automatic cancellation occurs at less than 40 km/h which is defined for each vehicle. However, in this case, the automatic cancellation does not occur until the speed reaches 10 km/h. This is because the perceived wheel speed is higher than the actual speed due to injections of the fabricated messages of 70 km/h and the cruise control system verifies that the current vehicle speed is higher than 40 km/h.

For reference, we show in **Fig. 6** the transition in RPMs described from the CAN messages for this case. As shown in the figure, the RPMs drastically change when the vehicle speed is reduced when injecting the fabricated messages and eventually become 0.

4.4 Other Behaviors That Could be Induced by Fabricated Informative Messages

In this section, we describe other aspects of the abnormal behaviors regarding disabling the speed limit of the cruise control system and cancellation of the parking assist system. Although these facts may not directly induce a significant accident, we show that other driving-support-system functions are compromised by the fabricated informative messages.

4.4.1 Disabling Speed Limit of Cruise Control System

Because the cruise control system verifies whether the system is activated based on the vehicle speed, we consider that we can mislead the module related to the control of the activation of the cruise control system.

We can induce an abnormal activation of the system even though the activation conditions are not satisfied. Usually, we can set the set speed in the system when the vehicle speed is higher than the designated speed such as 40 km/h. However, we find that we can activate the cruise control system by injecting a fabricated wheel speed even when the actual speed does not reach the designated speed.

Details of the procedure that improperly affects the system are given below.

(A) We press the cruise control system button and engage the system.

(B) We drives at a very low speed of less than 10 km/h. At this time, we inject a fabricated wheel-speed message indicating that the current wheel speed is higher than the designated speed to activate the cruise control system such as 50 km/h.

(C) Then, we try to set the speed in the same way as when the system is active. We are able to set the constant speed in the system at 48 km/h to 53 km/h even when the actual speed does not reach the designated speed of 40 km/h.

It is interesting that after setting the set speed by injecting the fabricated wheel-speed message, an abnormal acceleration without depressing the accelerator is possible. In fact, the speed is accelerated to approximately the set speed even when the actual vehicle speed is lower than 10 km/h by manipulating the cruise-control speed setting button while the fabricated wheel-speed messages are injected.

4.4.2 Cancellation of Parking Assist Systems

The parking assist is a famous driving support system and it assists drivers when parking their vehicles. When the assist is indicated, the steering wheel is automatically rotated to park the vehicle in the desired location. Generally, the system is used at low speeds of less than 10 km/h. **Figure 7** shows a typical parking-assist-system structure.

We find that we can conduct an abnormal cancellation without the driver depressing any button by injecting fabricated informative CAN messages such as the information of the current vehicle speed, shift position, wheel angle or steering position.

Here, we describe a method using the fabricated current-speed message as an example. Because the parking assist system is activated when the vehicle is moving at a low speed, we consider that the fabricated current speed message indicating 40 km/h results in the interruption of the system. It is well known that a fabricated message of the current speed affects the speedometer display

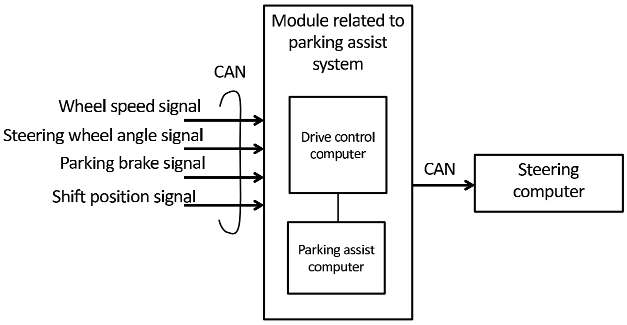

Fig. 7 Typical parking assist structures.

module and we can display incorrect speed values [3]. However, this message could not affect actual acceleration/deceleration actions. We show that the current speed message affects the control of the parking assist system and show that an abrupt cancellation can be induced while the conditions for the activation of its system are still satisfied.

Details of the attack procedure using a real vehicle are given below.

(A) A driver indicates the parking assist by depressing the button on the navigation display.

(B) The parking assist system is activated and automatically rotates the steering wheel to park the vehicle in the desired location while the vehicle speed is less than 10 km/h.
At the same time, the attacker starts to inject a fabricated message indicating 40 km/h as an example.

(C) As a result, the parking assist is suddenly canceled and an error indicating that the speed is too fast appears on the navigation display even when the steering is moving to park the vehicle.
Because the system falsely recognizes that the speed has exceeded the designated parameters, the safety system is activated and the parking assist system stops.

We note that the same results can be induced by injecting other kinds of fabricated informative message such as those regarding shift position, wheel angle or steering position. For safety reasons, the system is abruptly canceled when one of the activated conditions is not satisfied. However, our experimental results show that this fact makes it easier for the attack to disable the system by conducting a denial of service attack.

4.5 Effectiveness of Attacks

We describe a general versatility of the proposed attacks, that is, how the proposed attacks are generally effective to the vehicles.

As described in Fig. 1, in general, the control unit including the driving-support-system module refers the inputs of the vehicle status, that is informative messages, to justify the control of some actions. Then, we consider that the proposed attack to induce the abnormal vehicle behaviors using the informative messages is effective to some kinds of vehicles in which the driving support system is installed and it does not depend on a specific vehicle type. In fact, we perform the attacks against two kinds of vehicles made by different carmakers and in the different years (latest at the moment and the other a few years ago) to verify the effectiveness of the attacks. As a result, we achieve the successful attacks to induce the abnormal behaviors in both kinds of vehicles [*4].

Furthermore, in the latest vehicles, when two kinds of data that largely differ are input to the control unit in a short amount of time, there are some cases where the control unit detects the abrupt change of the values and it may act such that the driving support system is canceled. In this case, the attacker can perform attacks to improve the injected methods of the fabricated messages such as reducing the injected number of fabricated messages or controlling the injected timing of the fabricated messages not to induce the abrupt change of the values in the control unit. At this time, the number of fabricated messages sent by the attacker is less than the original messages. Although the effect of the fabricated messages decreases and the degree of the acceleration/deceleration is reduced as the influence for the attacks, the abnormal acceleration/deceleration is still possible.

5. Countermeasure Evaluations

In this section, we evaluate the effectiveness of countermeasures in the desk study when we apply them to mitigate attacks using informative messages. We describe the countermeasures that are considered to be effective for the proposed attacks and clarify the strength and weakness of each countermeasure for the proposed attacks. Based on the evaluations, we consider that the informative messages as well as the active messages must be protected because the protection methods may not be implemented in the informative messages.

5.1 Implementing Anomaly Detection

Anomaly detection is well known in the IT fields to detect anomalous packets on the Internet [22]. This kind of technique is considered to be effective in detecting fabricated messages in the CAN bus [8], [9], [10]. The basic approach is to compare with the normal situation without the attacks, and then, the data in a normal situation is needed.

We can detect that the proposed attacks have performed by comparing with the normal situation regarding one of the following items: period, number or data transitions of the messages described below. After the fabricated messages are detected, the driving-support-system functions such as the cruise control systems are stopped and only a limited function such as running at a lower speed remains activated. Then, the proposed attacks cannot be proceeded.

- Period of the informative messages:
  In the normal situation, the informative messages such as the wheel-speed or the current-speed messages are periodic about several tens of millisecond (ms) as an example. In the proposed attacks, the attacker injects the fabricated messages immediately after the original one sent from the control unit or he injects the fabricated messages more than the original ones. Then, the period between the wheel-speed or the current-speed messages is shorter than that in the normal situation such as less than 1 ms in the experiments and

[*4] In Section 4, the results using one of the vehicles are described.

Table 2 Summary of effectiveness of countermeasures.

Countermeasures	Strength (+) and Weakness (–)	Example References
Anomaly Detection	(+) Can detect attack when the cycle, number or data transition of the messages is investigated (–) Cannot easily determine which is the fabricated message	Refs. [8], [9], [10]
MAC	(+) Fabricated messages are not accepted in control unit because attacker cannot calculate correct MAC (–) Not effective when module is reprogrammed to calculate and add correct MAC	Refs. [5], [6], [7]
Checking Multiple Sources	(+) Fabricated messages can be detected and rejected so that action is not performed (–) Still can perform attack when attacker can tamper with multiple sources so that there is no consistency	–

it is disturbed. Therefore, when the attacks are performed, the informative-message period differs from that in the normal situation and sending the fabricated messages from the attacker can be detected.

- Number of the informative messages:
  In the proposed attacks, the attacker injects the fabricated messages immediately after the original one sent from the control unit or he injects the fabricated messages more than the original ones. Then, when the attacks are performed, the number of the informative messages of the attack target is more than double compared to a normal situation during a given time interval. Then, in the attack situation, the number of the informative messages differs from that in the normal situation and sending the fabricated messages from the attacker can be detected.
- Data transition of the informative messages:
  In the proposed attacks, the data of the fabricated messages differs from that of the original one. Then, when the attacks are performed, the data of the wheel-speed or the current-speed message approximately takes the two kinds of values alternately in a short time. Therefore, the data transition differs from that in the normal situation and sending the fabricated messages from the attacker can be detected.

Considering the above, the countermeasures of the anomaly detection are effective for the proposed attacks. The behaviors of the informative messages must also be checked in the anomaly detection systems as described above. We note that a more sophisticated analysis is needed to determine which message is the fabricated message. In this case, we also examine which data is not consistent with the vehicle behaviors or the other in-vehicle messages, or we examine the voltage profile of the module to know exactly which message is the fabricated message transmitted from the compromised module.

5.2 Implementing CAN Message Authentication

The way of implementation of a MAC in in-vehicle networks has been proposed [5], [6], [7], [23] and it will be implemented in the CAN bus in the near future. Usually, a MAC is implemented for significant messages directly related to vehicle actions because of the computational resources of the control unit. We consider that MACs must be implemented for the informative CAN messages to prevent the acceptance of fabricated messages.

When we add the MAC to the informative messages transmitted in the bus, the attacker cannot create the fabricated messages with the correct MAC because he does not know the cryptographic secret key to calculate the correct MAC. If the attacker sends the fabricated informative messages with the wrong MAC, it is rejected in the received control unit. Then, the abnormal behaviors in the control unit are not induced and the proposed attacks cannot be proceeded.

We note that, when the implementation of the MAC is improper such as the setting of the short MAC length or multiple use of the same MAC, the attacker may calculate the correct MAC and replay its message [24]. Furthermore, when the attacker can perform re-programing of the module to calculate the correct MAC, the above countermeasure is not effective. However, we consider that it is a difficult task for the attackers in most cases.

5.3 Checking Multiple Sources of Modules

To prevent attacks, reconsidering the driving support system is also needed. We describe a new aspect of the countermeasures that perform checking multiple module inputs in a module related to the driving support system. In contrast to the anomaly detection, this method does not need the data in the normal situation because the different kinds of the multiple inputs that have the same transitions at this time are compared.

We can detect that the proposed attacks have performed by comparing the multiple sources regarding one of the following items, a kind of source on different lines or different kinds of CAN signals described below. After the abnormal behaviors are detected, the driving-support-system functions such as the cruise control systems are stopped and only a limited function such as running at a lower speed remains activated. Then, the proposed attacks cannot be proceeded.

- A kind of source on different lines such as a signal on the in-vehicle network and the physical wiring.
  In general, there are some inputs to the module that have the same signal meaning but on different lines such as the CAN bus and the physical wiring. In the proposed attacks, the attacker only sends the fabricated informative messages in the CAN bus. Then, by comparing the data that has the same meaning such as the current speed of vehicle both in the CAN bus and the physical wiring, sending the fabricated messages from the attacker can be detected when they are different in a short period of time.
- Different kinds of CAN signals calculated from the same sensor values that have the same time-shift transitions.
  In the vehicle systems, there are some kinds of informative CAN messages that have the same time-shift transition cal-

culated by a sensor value such as the current speed of the vehicle and the wheel-speed messages. In the normal situation, they have the same time-shift transition because they are calculated by the same signal source. When the proposed attack is performed, the attacker sends the fabricated messages regarding one kind of CAN messages such as the wheel-speed messages. Then, the time-shift transitions between the wheel-speed and the current speed of the vehicle are obviously different if the attack is proceeded. Therefore, by comparing the time-shift transitions between the multiple CAN messages, sending the fabricated messages from the attacker can be detected.

This countermeasure can also be installed in a central gateway or a domain unit that controls the message flow to each terminal module [25].

From the above, the countermeasures are effective when the attacker sends a kind of fabricated messages. Of course, if the attacker can tamper with multiple sources so as not to create the inconsistency in the multiple inputs of the module, the countermeasure is not effective. However, we consider that tampering the multiple sources to take the same time-shift transitions is difficult for the attackers.

5.4 Comparison of Each Countermeasure

From the above desk study, we show the effectiveness of each countermeasure applied to the attack using the informative messages. A summary is given in **Table 2**. In the table, (+) indicates a strength and (–) indicates a weakness when a countermeasure is implemented. Because each countermeasure itself has weak points based on the attack level, a combination of multiple methods is more effective to completely prevent attacks based on the multilayer detection concepts [26].

6. Conclusions

This paper brought to light a new perspective on fabricated informative CAN messages used to trigger an abnormal behavior that a driver does not intend. The presented methods were able to affect the control of the driving support system through informative messages that were considered only to inform the vehicle status. In fact, by injecting the fabricated wheel-speed messages, we showed that an abrupt acceleration/deceleration to a speed greater/lower than the set speed could occur while the cruise control system was activated. We also showed that we could disable the speed limit to activate the cruise control system. Furthermore, by injecting fabricated current-speed messages, we showed that we could abruptly cancel the parking assist system. These results reveal that such systems can be easily compromised and we must consider that the security of informative messages as well as that of other messages is significant. We evaluated the effectiveness of the countermeasures applied to the proposed attacks and clarified the strength and the weakness of each countermeasure for the attacks. Because the extended automated cruise system has spread all over the world, we believe that this study provides some important information for the design and implementation of the systems and contributes to the development of secure systems.

Acknowledgments The authors thank Mr. Toshinori Fukunaga and Mr. Yoshihito Oshima for their valuable comments on this investigation.

References

[1] Koscher, K., Czeskis A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham H. and Savage, S.: Experimental Security Analysis of a Modern Automobile, *Proc. IEEE Symposium on Security and Privacy* (*SP*), pp.447–462, IEEE Computer Society (2010).

[2] Checkoway, S., Coy, D.M., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F. and Kohno, T.: Comprehensive Experimental Analyses of Automotive Attacks Surfaces, *Proc. USENIX Security Symposium* (2011).

[3] Valasek, C. and Miller, C.: Adventures in Automotive Networks and Control Units, *Proc. DEFCON Hacking Conference* (*DEF CON 21*) (2013).

[4] Miller, C. and Valasek, C.: CAN Message Injection, OG Dynamite Edition June 28, 2016 (online), available from ⟨http://illmatics.com/can message injection.pdf⟩ (accessed 2018-04-25).

[5] Groza B., Murvay, S., Herrewege, A.V. and Verbauwhede, I.: LiBrA-CAN: A Lightweight Broadcast Authentication Protocol for Controller Area Networks, *Proc. CANS 2012*, LNCS 7712, pp.185–200 (2012).

[6] Nilsson, D.K., Larson U.E. and Jonsson, E.: Efficient In-Vehicle Delayed Data Authentication Based on Compound Message Authentication Codes, *Proc. Vehicle Technology Conference fall*, IEEE Computer Society (2008).

[7] Szilagyi, C. and Koopman, P.: Low Cost Multicast Authentication via Validity Voting in Time-Triggered Embedded Control Networks, *Proc. WESS10*, ACM (2010).

[8] Taylor, A., Japkowicz, N. and Leblanc, S.: Frequency-Based Anomaly Detection for the Automotive CAN bus, *Proc. WCICSS*, IEEE Computer Society (2015).

[9] Nair, S., Mittal, S. and Joshi, A.: OBD SecureAlert: An Anomaly Detection System for Vehicles, *Proc. IEEE Workshop on Smart Service Systems* (*SmartSys*), IEEE Computer Society (2016).

[10] Narayanan, S.N., Mittal, S. and Joshi, A.: Using Data Analytics to Detect Anomalous States in Vehicles, arXiv:1512.08048v1 [cs.AI] (Dec. 2015).

[11] Maglaras, L.A.: A Novel Distributed Intrusion Detection System for Vehicular Ad Hoc Networks, *Proc. International Journal of Advanced Computer Science and Applications*, Vol.6, No.4 (2015).

[12] Li, J.: CANsee - An Automobile Intrusion Detection System, HITB-SecConf (2016).

[13] Song, H.M., Kim, H.R. and Kim, H.K.: Intrusion Detection System Based on the Analysis of Time Intervals of CAN Messages for In-Vehicle Network, *Proc. International Conference on Information Networking* (*ICOIN*), IEEE Computer Society (2016).

[14] Takahashi, J., Tanaka, M., Fuji, H., Narita, T., Matsumoto, S. and Sato, H.: Abnormal Vehicle Behavior Induced Using Only Fabricated Informative CAN Messages, *Proc. IEEE International Symposium on Hardware Oriented Security and Trust* (*HOST*), pp.134–137, IEEE Computer Society (2018).

[15] Road vehicles – Diagnostic communication over Controller Area Network (DoCAN) – Part 2: Transport protocol and network layer services, ISO 15765-2:2011 (2011).

[16] ISO 14229-1:2013, Road vehicles – Unified diagnostic services (UDS) – Part 1: Specification and requirements (2013).

[17] ISO 14230-2:2016, Road vehicles – Diagnostic communication over K-Line (DoK-Line) – Part 2: Data link layer (2016).

[18] Intel: Advanced Driver Assistant System Threats, Requirements, Security Solutions, Technical White Paper (2015).

[19] Miller, C. and Valasek, C.: A Survey of Remote Automotive Attack Surfaces, *Proc. DEFCON Hacking Conference* (*DEFCON 22*) (2014).

[20] Vector Informatik: CANoe V9.5, available from ⟨https://vector.com/vi_versionhistory_detail_en,,,1653990,detail.html⟩ (accessed 2018-04-25).

[21] Vector Informatik: VN1630 Interface Family.

[22] Chandola, V., Banerjee, A. and Kumar, V.: Anomaly detection: A survey, *Journal ACM Computing Surveys* (*CSUR*), Vol.41, No.3, Article No.15 (2009).

[23] AUTOSAR: Specification of Module Secure Onboard Communication AUTOSAR Release 4.3.1 (online), available from ⟨https://www.autosar.org/fileadmin/user_upload/standards/classic/4-3/AUTOSAR_SRS_SecureOnboardCommunication.pdf⟩ (accessed 2018-04-25).

[24] Weisglass, Y.: Practical Attacks on CAN Message Authentication, *Proc. Escar Asia* (2017).

[25] Ambroggi, L.D.: Ethernet In car: From Multiplexed network to Service network, IHS Markit Technology (online), available from ⟨https://

technology.ihs.com/590689/ethernet-in-car-from-multiplexed-network-to-service-network⟩ (accessed 2018-04-25).

[26] Birnie, A. and Roermund, T.V.: A Multilayer Vehicle Security Framework, white paper, Date of release: May 2016 (online), available from ⟨https://www.nxp.com/docs/en/white-paper/MULTI-LAYER-VEHICLE-SECURITY-WP.pdf⟩ (accessed 2018-04-25).

Junko Takahashi received her B.S. and M.S. degrees in physics from Waseda University, Japan, in 2004 and 2006, respectively, and her Ph.D. degree in engineering from the University of Electro-Communications, Japan, in 2012. She joined the NTT Information Sharing Platform Laboratories, Nippon Telegraph and Telephone Corporation in 2006. Currently, she is a researcher with the NTT Secure Platform Laboratories, Nippon Telegraph and Telephone Corporation (NTT). At NTT, she has evaluated the resistance of smart cards against side-channel analysis and engaged in basic research of fault analysis attacks and cache timing attacks especially against block ciphers. Recently, she has been studying automotive security evaluations such as in-vehicle devices, protocols, and vehicle services associated with cloud environments. She is a member of the Information and Communication Engineers (IEICE) and Information Processing Society of Japan (IPSJ). She has been a committee member of the hardware security technical committee from 2016 in the IEICE and the IPSJ special interest group on system architecture from 2018. She was awarded the 2008 symposium on cryptography and information security (SCIS) paper prize and her paper in JIP Vol.25 was selected as a specially selected paper in the IPSJ in 2017.

Masashi Tanaka Senior Research Engineer, Cyber Security Project, NTT Secure Platform Laboratories. He received his B.S. and M.S degrees from Osaka Prefecture University in 1999 and 2001, respectively. He is presently engaged in research on IoT cyber security.

Hitoshi Fuji Senior Manager, Planning Section, NTT Secure Platform Laboratories. He received his B.E., and M.E. degrees from Tokyo University of Science in 1991 and 1993, respectively. He also received his Ph.D. degree in informatics. Since joining NTT in 1993, he has been engaged in research on software engineering, network security and information security.

Toshio Narita received his B.E. degree in communications engineering from Shibaura Institute of Technology, Japan, in 1997. He joined the NTT DATA MSE Corporation in 1997. Currently, he is an engineer with NTT DATA MSE Corporation.

Shunsuke Matsumoto received his B.E. degree in electronics and information engineering from Kanagawa University, Japan, in 2015. He joined the NTT DATA MSE Corporation in 2015. Currently, he is an engineer with NTT DATA MSE Corporation.

Hiroki Sato received his B.E. degree in electrical engineering from Yamagata University, Japan, in 1992. He joined the NTT DATA MSE Corporation in 1992. Currently, he is a manager with NTT DATA MSE Corporation.