Hindawi
Security and Communication Networks
Volume 2022, Article ID 9569703, 10 pages
https://doi.org/10.1155/2022/9569703

Research Article

CAN Signal Extinction-based DoS Attack on In-Vehicle Network

Yousik Lee[1] **and Samuel Woo**[2]

[1]*ETAS Korea, Gyeonggi 13494, Republic of Korea*
[2]*Department of Software Science, Dankook University, Gyeonggi 16891, Republic of Korea*

Correspondence should be addressed to Samuel Woo; samuelwoo@dankook.ac.kr

Received 2 July 2022; Revised 12 August 2022; Accepted 24 August 2022; Published 26 September 2022

Academic Editor: Hao Peng

As automobiles become more electrified, more and more Electronic Control Units (ECU) are installed in vehicles. ECUs communicate with each other through dedicated protocols such as a controller area network (CAN), but these protocols do not have their own security measures. Many cyberattacks have exploited this weakness, but an intrusion detection system (IDS) is emerging as an effective countermeasure. In this study, we introduce a new attack method that existing IDS cannot detect. CAN signal extinction-based DoS attack (CEDA) is a new attack method that uses a voltage drop to erase the CAN signal. When the target ECU transmits a signal, adding a resister that lowers the differential voltage to an undefined gray zone causes the other ECU to ignore the signal being sent from the target ECU. In cybersecurity, denial of service (DoS) is defined as restricting an authorized entity from accessing a resource or delaying a time-critical system. This attack is a kind of a DoS attack since the adversary can make the target ECU bus-off through a CEDA. CEDA could be a serious problem as it has not been detected by any known IDS to date. In this study, we use laboratory and vehicle tests to detail the attack methods and introduce appropriate security measures.

1. Introduction

Modern vehicles are developing into huge information technology (IT) systems of software as the convergence of vehicles and information & communication technology (ICT), represented by connected cars and autonomous vehicles, becomes active [1, 2]. However, more software means more potential for cyberattacks on the vehicle [3–5]. After the first recall of vehicles due to a cyberattack in 2015, manufacturers began to equip security functions in their vehicles [6, 7]. And related organizations such as governments, associations, and societies have implemented standards, guidelines, and regulations related to automotive security.

One of the most notable security measures is the intrusion detection system (IDS) because it is effective against cyberattacks on vehicles, and many regulations recommend the installation of IDS [8–10]. Recently, artificial Intelligence and machine learning technologies have been actively introduced into the latest IDS research [11–13]. They will soon be adopted for automotive IDS as well. An electronic control units (ECUs) communicate with each other through an in-vehicle network using a protocol such as a controller area network (CAN). An application of the ECU generates data and sends it to the CAN controller. Then, the CAN controller hands the data to the CAN transceiver, and it transforms the data to an electrical signal and sends it to the CAN bus. Conversely, the CAN transceiver of the receiving ECU receives the signal to convert into logical bits, which the CAN controller further converts into a message that the application can recognize.

After that, an application reads the converted message. Figure 1 shows the architecture of the CAN compared with an open systems interconnection reference model (OSI) layer. Since most cyberattacks are performed in the application layer, an IDS is installed on the application layer. However, if the attack is conducted on the physical layer, IDS cannot detect it.

In this paper, we introduce CAN signal extinction-based DoS attack (CEDA) that erases messages by using a voltage drop by increasing the resistance. The differential voltage must be within the range defined by the standard so that the

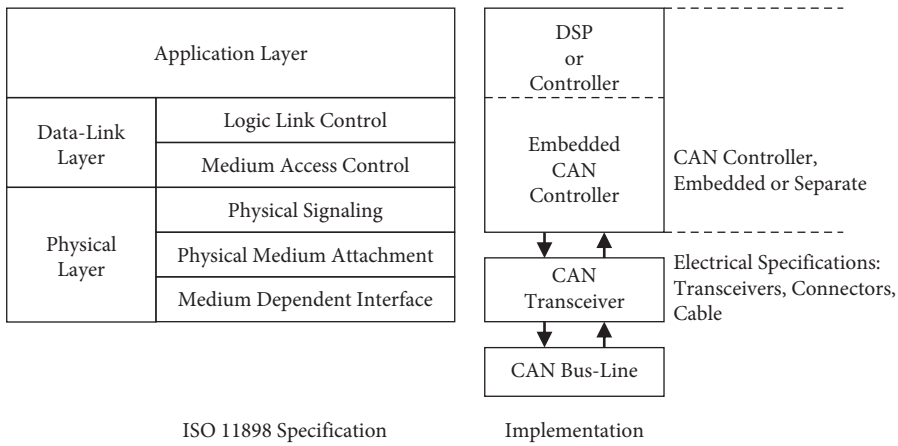


Figure 1: The layered ISO 11898 standard architecture [14].

receiving ECU can recognize the signal as a 0 or 1, but it can be made outside this range by simply adding a resistor. We propose to call the area outside the range defined in the standard a "gray zone." The gray zone is not defined in the standard, so other ECUs will ignore the signal if the differential voltage is in this zone. Therefore, if an adversary lowers the differential voltage to the gray zone by adding a resistor when the target message is transmitted, all ECUs in the in-vehicle network will ignore the signal. No existing IDS can detect the CEDA because:

(1) It is a signal-based attack, not a message-based attack, and it is ignored by the CAN transceiver, so no message is passed to the application layer where the IDS is installed.

(2) Attack device does not send messages and does not communicate with other ECUs.

In addition, since the attack device we proposed can be manufactured for less than 20 US dollars, this attack is quite realistic with the catastrophic consequences. We prove the proposed attack technique through the following three experiments.

(1) Feasibility check in the laboratory.

(2) Simulation test in the laboratory.

(3) Attack on a real vehicle.

This paper is structured as follows. "Background" reviews the background of the in-vehicle network architecture, CAN protocol, and related studies. We explain the mechanism of CEDA and attack model in "Proposed attack technique." We then describe the test on the laboratory and the real vehicle, and respective countermeasures in "Practical attack experiment." "Conclusion" concludes the paper and proposes future work area.

2. Background

2.1. Communication Protocols for In-Vehicle Networks. As vehicles evolve into connected cars and autonomous vehicles, more and more components are required to communicate with each other. Information is collected through sensors or other components and processed by the respective electronic control unit (ECU). The processed data is then transmitted to other ECUs. The ECUs that require data control the vehicle through an actuator or display the information on the devices. The ECUs that do not require data ignore the data. This is the reason why the in-vehicle network (IVN) is essential to the vehicle. Modern cars carry about 150 ECUs [15]. ECUs are classified into domains according to their functions or physical configurations, and communicate with each other via protocols such as CAN, CAN flexible data rate (CAN FD), local interconnect network (LIN), media oriented systems transport (MOST), FlexRay, and Ethernet. Figure 2 shows the traditional IVN architecture.

2.2. Controller Area Network. A CAN is a serial data communications bus developed by Robert Bosch GmbH for the vehicular embedded system in the early 1980s. CAN is a multi-master broadcast protocol based on sender IDs. It allows ECUs to communicate with data rates up to 1 Megabit per second. CAN is divided according to the communication speed into high-speed CAN and low-speed CAN. This paper provides all explanations based on the high-speed CAN. In the CAN bus system, each ECU uses a data frame to transfer information to other ECUs.

All ECUs are connected to each other through two dedicated wires. The wires are called CAN high (CANH) and CAN low (CANL). The CAN bus system must have bus Termination resistors 120 Ω at both endpoints of the physical network wires. The CAN Bus topology is shown in Figure 3(a).

ECUs generate a dominant bit (0) and a recessive bit (1) using a CAN transceiver to transmit the data frame. In the recessive state, both CANH and CANL are at the same level of 2.5 voltage potential (V), while CANH is at 3.5 V and CANL is at 1.5 V in the dominant state. The bit representation of the CAN transceiver is shown in Figure 3(b).

2.3. Related Work. Although CAN is the most widely used communication protocol for an in-vehicle network, it does not have its own security measures. For this reason, many attack techniques have been introduced since CAN was

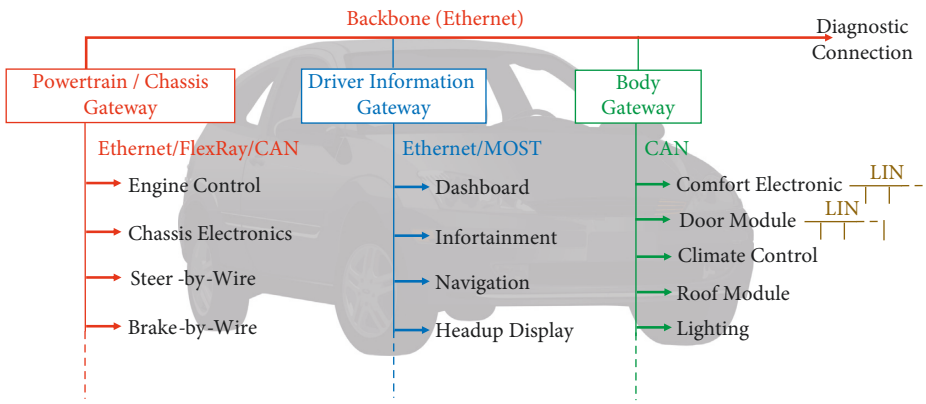


Figure 2: Traditional topology of in-vehicle network.

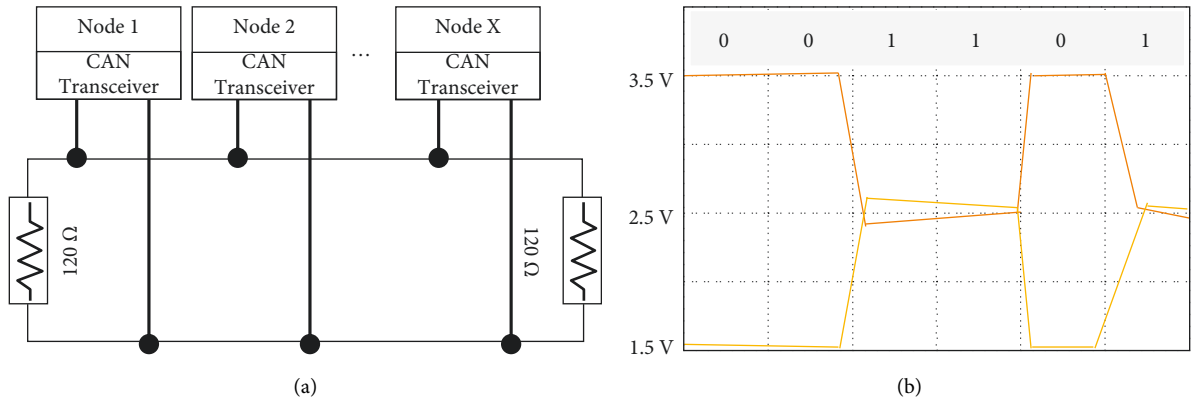


Figure 3: CAN BUS topology and nominal bus levels. (a) CAN BUS topology, (b) normal bus levels.

invented. In the early days of automotive cybersecurity research, system hackers from the traditional IT environment entered the automotive field, and there were a lot of SW-based attacks like in the IT environment. As cybersecurity became one of the important factors in the automotive industry, researchers have begun to use the characteristics of vehicles to expose their weaknesses, especially in-vehicle network protocols.

Miller and Valasek hacked a vehicle running on the highway with only a laptop and a smartphone [7]. They used the vulnerability of the head unit, which communicates with the outside to obtain administrator rights. Then, they replaced the firmware of the head unit with theirs and sent an attack message to the vehicle. As a result of this attack, the vehicle manufacturer recalled 1.4 million related vehicles, which was the first recall case due to a cyberattack [6]. The importance of the automotive cybersecurity increased due to this attack, and vehicle manufacturers began to implement countermeasures against cyberattacks on their vehicles. Government and related organizations started to enforce regulations, guidelines, and standards.

Palanca et al. proposed a new attack technique using a weakness of the CAN protocol [16]. In order to cause an error, they modulated a recessive bit into a dominant bit when a sender transmits a data frame. CAN is a carrier sense multiple access/collision detection (CSMA/CD) protocol, which means every node on the network can send a message. If two nodes start transmitting at the same time, the nodes will detect the collision and perform a nondestructive bitwise arbitration. If the attacker injects the dominant bit when the legitimate ECU sends the recessive bit, the recessive bit can be changed to the dominant bit.

Lee et al. introduced the app repackaging attack [17]. The researchers attacked the vehicle with OBD-II dongle and an app for operating it. The attack was made with a device that can be easily purchased in the market and downloaded apps from Google Play that can operate the device, which shows that the attack is realistic. They demonstrated unauthorized vehicle control such as opening a locked door and halting the engine. As countermeasures, they proposed obfuscation to prevent app tampering and message filtering to prevent receiving messages that control the vehicle from the outside.

To protect CAN-based network against cyberattacks, an intrusion detection system (IDS) was proposed [18]. An IDS is effective in detecting malicious messages since most messages in a CAN protocol have a fixed length and sending frequency. But as IDS has become more sophisticated, they are looking for ways to circumvent it. Attackers have begun to exploit software-based IDS by using the physical characteristics of the CAN protocol. Accordingly, IDS has also evolved to search for malicious messages using physical characteristics of the CAN protocol.

Cho and Shin proposed a mechanism for detecting an attack and identifying the specific ECU using clock skew that reflects the hardware characteristics of the clock source constituting the ECU [19]. Even if two ECUs transmit messages in the same period, they have different clock skew due to the characteristics of the hardware. The authors introduced a technique for detecting this clock skew as an attack if it fluctuates beyond a critical value while monitoring it. In addition, they proposed a voltage-based attacker identification (VIDEN), which is based on the characteristic of CAN signals transmitted by ECUs [20]. This characteristic is unique due to the difference in voltage supplied to each ECU, but it has limitations in mass-produced vehicles because an oscilloscope is required for the detection.

Sagong et al. introduced the hardware-based intrusion response system (IRS) [21]. They demonstrated vulnerabilities of the voltage-based IDS with three types of attacks:

(1) Overcurrent attack: supplying a current that exceeds the range the microcontroller can accommodate.

(2) Denial-of-service attack: letting CAN bus be in the idle state in a way that zeroes all signal and causes an error frame.

(3) Forced retransmission attack: forcing the ECU to send the message repeatedly.

An IRS is proposed to defend the attack which can circumvent the voltage-based IDS. In order for IDS to detect a malicious message or an attack device, it must receive a message or signal from the device. But, since the CAN signal extinction attack we proposed simply lowers the differential voltage of the signal transmitted from the target device, it is not detected by the existing IDS.

3. Proposed Attack Technique

3.1. Attack Mechanism. As described in section above, CAN has two logical states-a recessive state and a dominant state. In the recessive state, both CANH and CANL are at the same level of 2.5 voltage potential (V), while CANH is at 3.5 V and CANL is at 1.5 V in the dominant state [22]. The logical state of the bus can be determined by subtracting the voltage potential of CANH and CANL, which is called the differential voltage. However, since the differential voltage of each state can change according to various variables such as device characteristics, wire length and location, and vehicle driving conditions, it is not always possible to pinpoint 2.5 V and 0 V. Therefore, the CAN standard tolerates a certain amount of margin of error.

If the differential voltage is less than 0.5 V, the bus will be considered as the recessive state, and the bus will be regarded as the dominant state when the differential voltage is greater than 0.9 V.

However, if the differential voltage is between 0.5 V and 0.9 V, it is neither a dominant state nor a recessive state. In this case, the bus state is not defined according to the CAN standard [22]. It means that ECUs do not take any actions if they receive an undefined state. We propose to call this area the gray zone. Thus, if attackers can place the differential voltage in the gray zone when the target ECU sends a message, other ECUs ignore the message from the target ECU, and the target ECU generates an error frame. When attackers conduct this attack to a specific ECU distinguished by ID, the ECU continuously generates an error frame. And when the number of an error frame reaches the threshold, the ECU becomes a "bus-off" state and the ECU in the bus-off state cannot be operated normally. This is a DoS attack that can be conducted on the CAN-based in-vehicle network.

According to formula (1) and (2), the differential voltage is inversely proportional to the resistance, so increasing the resistance can decrease the differential voltage. Therefore, if an appropriate resistance can be calculated according to the in-vehicle network characteristics of the target vehicle and the corresponding resistor can be installed in the vehicle so that the differential voltage is located in the gray zone, the specific message of the vehicle can be erased. In other words, while monitoring messages in the CAN-based in-vehicle network, if a message with target ID appears, the resistance is increased so that the differential voltage is located in the gray zone. This can cause other ECUs to ignore the message and lead to disable certain functions.

3.2. Attack Model. The idea of the attack we propose comes from the structural architecture of the CAN-based in-vehicle network. This attack method is a kind of a DoS attack. The goal of a DoS attack is to make the target system unusable. We chose this method to remove the target system from the network instead of making the target system unavailable by sending a large amount of traffic to the system. When the ID of the target system appears while monitoring the CAN-based in-vehicle network, attackers make the message invalid by adjusting the voltage. We propose the following attack model and make a few assumptions that are required for the attack to be successful.

3.2.1. Attacker's Ability. Attackers can create the monitoring device and monitor messages in the CAN-based in-vehicle network. Based on this, attackers can find the CAN ID of the target function or device and add the resistance to prevent other ECUs from receiving messages from the target ECU. Attack that needs additional devices requires the attacker to equip the attack device to the target vehicle. Thus, it is assumed that the attackers can equip their device to the vehicle.

3.2.2. Target Vehicle. It is assumed that the in-vehicle network of the target vehicle includes a CAN. It is also assumed that the target vehicle is equipped with an ECU with the function that the attacker wants to exploit.

3.2.3. Attack Model. The attack method we propose can consider two attack models. The first attack model is the supply chain attack. The supply chain is very complex and layered. Most vehicle manufacturers cannot produce the cars by themselves and are provided parts, systems, and services

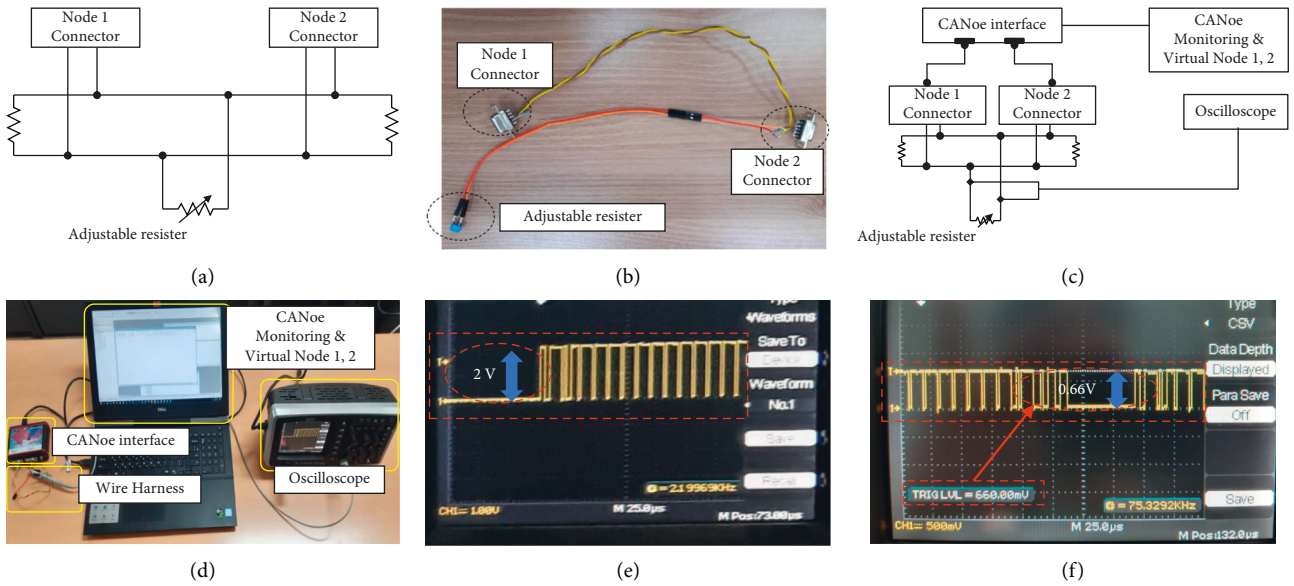


FIGURE 4: Experiment structures and environments for feasibility testing. (a) Block diagram of wire harness, (b) wire harness, (c) block diagram of testbed, (d) testbed, (e) normal state, (f) attack case.

from various suppliers. Suppliers also purchase parts and systems from other partners. Securing the entire supply chain is difficult because attackers can exploit any part of the complex supply chain. Attackers may add features or devices to enable our proposed attack method in certain parts of the supply chain, or even some vendors can be the attackers in this model. The second attack model is terrorism. Attack devices can be attached to a specific vehicle to compromise the safety of specific targets.

4. Practical Attack Experiment

In this chapter, we describe the attack experiment in laboratory environments and in a real vehicle. The following three experiments were conducted to prove our proposal.

(1) Feasibility test in a laboratory environment
(2) Attack simulation in laboratory environment
(3) Attack on a real vehicle

Finally, we describe the countermeasures against the attack we proposed.

4.1. Feasibility Test. In this section, we prove our idea through a simple device and facilities in a laboratory environment. We only need two nodes of CAN network for this attack. One node is a victim node that sends messages to another node. Since messages coming from the victim node will be erased by adjusting the resister, the contents of the messages are not important. Figure 4(a) shows the concept of a wire harness schematic, and Figure 4(b) shows the actual wire harness according to the schema in Figure 4(a). The nodes are created virtually on the laptop using CANoe that is an ECU simulation and test tool made by Vector Informatik GmbH, and they transmit the data through each node connector. Therefore, each node connector may be regarded as an individual node in order to simplify the system.

We assume that the "Node 1" is the victim system. Communicated messages can be monitored via a "Monitoring laptop" that is connected with a wire harness using a "CAN interface." Also, an "Oscilloscope" is used to check the voltage potential and the difference between them. We sent messages from "Node 1" to "Node 2" and monitored the transmitted messages to see whether "Node 2" could receive the messages. Figures 4(c) and 4(d) show the testbed environment. Without the proposed attack, the difference of the voltage potential is 2 V in the dominant state as shown in Figure 4(e). To simulate the attack, we gradually increased the resistance by controlling the adjustable register. The communication failed when 12.1 Ω was applied to the testing environment and the value of voltage potential was 0.66 V (Figure 4(f)), which means that the value was greater than 0.5 V and less than 0.9 V. Through this experiment, we proved that the CEDA is possible to attack an in-vehicle network. If attackers remove the signal regarding the brake system, the vehicle cannot slowdown, which could seriously endanger the safety of passengers and pedestrians.

4.2. Attack Simulation in a Laboratory Environment. In this section, we introduce a vehicle simulation test in a laboratory environment. The laboratory testing was performed at the automotive security living lab that was established by the Korea Internet & Security Agency (KISA) [23]. We confirmed in previous experiments that our idea is feasible. Our next step was to check whether the CEDA is possible in a vehicle simulator. In order to conduct the test, we need to consider the following procedures.

(1) Find the CAN ID of a target function
(2) Find out the voltage drop due to turn-on resistance of field effect transistor (FET) switches (3) Calculate

additional resistance to place the differential voltage between CANH and CANL in the gray zone so that the CAN signals dissipate

(3) Add the resistance calculated above to the CAN BUS

To accomplish the 4th step, we developed new device that can add a resistor programmable.

4.2.1. Reversing to Find CAN IDs. As described in "Attack Mechanism," we perform an attack that removes data when a specific message appears on the in-vehicle network. We selected a function that controls the motor-driven power steering (MDPS). In order to attack, we need to identify the CAN ID of the related message. In general, CAN specification includes CAN IDs and the data frame structures is one of the intellectual properties of respective vehicle manufacturers. Thus, we should reverse engineer the data frame structure to find the CAN ID of the message. The process is as follows:

(1) To monitor messages on the in-vehicle network, connect the monitoring tool to the vehicle. CANoe TM of Vector was used in this study.

(2) After turning on the ignition, leave the vehicle alone for a while so that the vehicle is in a stable state.

(3) A stable state means the ECUs in the vehicle send the same value or send a repeating predictable value periodically.

(4) Look for the message whose value changes significantly by manipulating the handle.

(5) Fixing the ID of the found message in the monitoring tool, and verify the CAN ID by checking the values when the steering wheel is being operated and not.

The CAN ID of the MDPS control message analyzed by the above process is shown in the following Table 1. Since the target messages are removed, we do not analyze the contents of the message.

4.2.2. Calculating the Voltage Drop due to Turn-On Resistance of FET Switches. To calculate the proper resistance to place the differential voltage in the gray zone, we must calculate the voltage drop due to turn-on resistance of FET switches. In order to make this calculation, we also need to know the structure of the CAN transceiver. Figure 5(a) shows the structure of the transceiver. According to Ohm's law, we can calculate the differential voltage between CANH and CANL using the following formula: formula,

$$V_{\text{diff}} = \frac{R_r}{R_r + R_1 + R_2} * V_{in}, \tag{1}$$

where, R_{r} = resultant resistance. R_1, R_2 = voltage drop due to turn-on resistance in FET switches, (B) in Figure 5(a). V_{diff} = a differential voltage between CANH and CANL. V_{in} = input voltage, (A) in Figure 5(a).

In the case of in-vehicle network, a terminating resistance is 120 Ω in general [22].

Table 1: CAN ID of MDPS functions found by reversing.

CAN ID	Description
0x381	MDPS (Motor-driven power steering)

Thus, a resultant resistance can be calculated by the formula.

$$R_r = \frac{1}{1/R_a + 1/R_b}, \tag{2}$$

where, R_a, R_b = resistances which are in parallel connection in a circuit, in this experiments 120 Ω.

A terminating resistance R_r is 60 Ω in the normal state (not the attacked state), and can be changed if an attacker puts additional resistance. We calculate the input voltage (V_{in}) to be 3.3 V through the data sheet of VP230 transceiver which is used in this study [24]. The differential voltage between CANH and CANL (V_{diff}) can be checked using an oscilloscope at the automotive security living lab; and we calculated the value to be 2.44 V as shown in Figure 5(b). Now, we can calculate $R_1 + R_2$ and the value is 21.15 Ω. As you can see in Figure 5(a), R_1 , R_2 are only affected by the input voltage. Since the input voltage is a constant value fixed at 3.3 V in this study, it is meaningless to figure out each value.

4.2.3. Calculating Additional Resistance to Attack the Vehicle. Again, our goal is to place the differential voltage (V_{diff}) between 0.5 V and 0.9 V so that other ECUs cannot recognize the message from the target ECU. To do this, we must calculate the additional resistance using Formula (1).

Since V_{diff}, V_{in}, and $R_1 + R_2$ are known values, we can calculate R_r. And the resistance we want to know can be calculated from R_r using Formula (2). The calculated additional resistance that places the differential voltage in the gray zone was $3.55\ \Omega \le R_{\text{b}} \le 7.00\ \Omega$. Thus, we chose 6 Ω as the additional resistance. To attack the CAN-based network, we developed a device as shown in Figure 5. Figure 5(d) shows the overall appearance of the KISA's automotive security living lab, and Figure 5(e) shows how to connect the vehicle simulator and the device. Figure 5(c) is the schematic of the device structure.

The device consists of an additional resistance to attack the target and a field programmable gate array (FPGA), which gives the additional resistance to the network if the received ID is the target ID. Details of each part are shown in Table 2.

When the FPGA receives signals through the CAN transceiver, it checks whether the received ID is the target ID or not. If the received ID is the target ID, the FPGA approves the attack resistance to the network by turning on the switch.

Figure 6(a) shows the screen capture of the oscilloscope after an attack, and Figure 6(b) is the chart used to find the exact value. To check the exact value, we downloaded the data from the oscilloscope and drew a chart with time and voltage. As you can see Figure 6(b), if 22 Ω resistance is added to the network, the differential voltage is 0.72 V, which is in the range of the gray area. This means that the

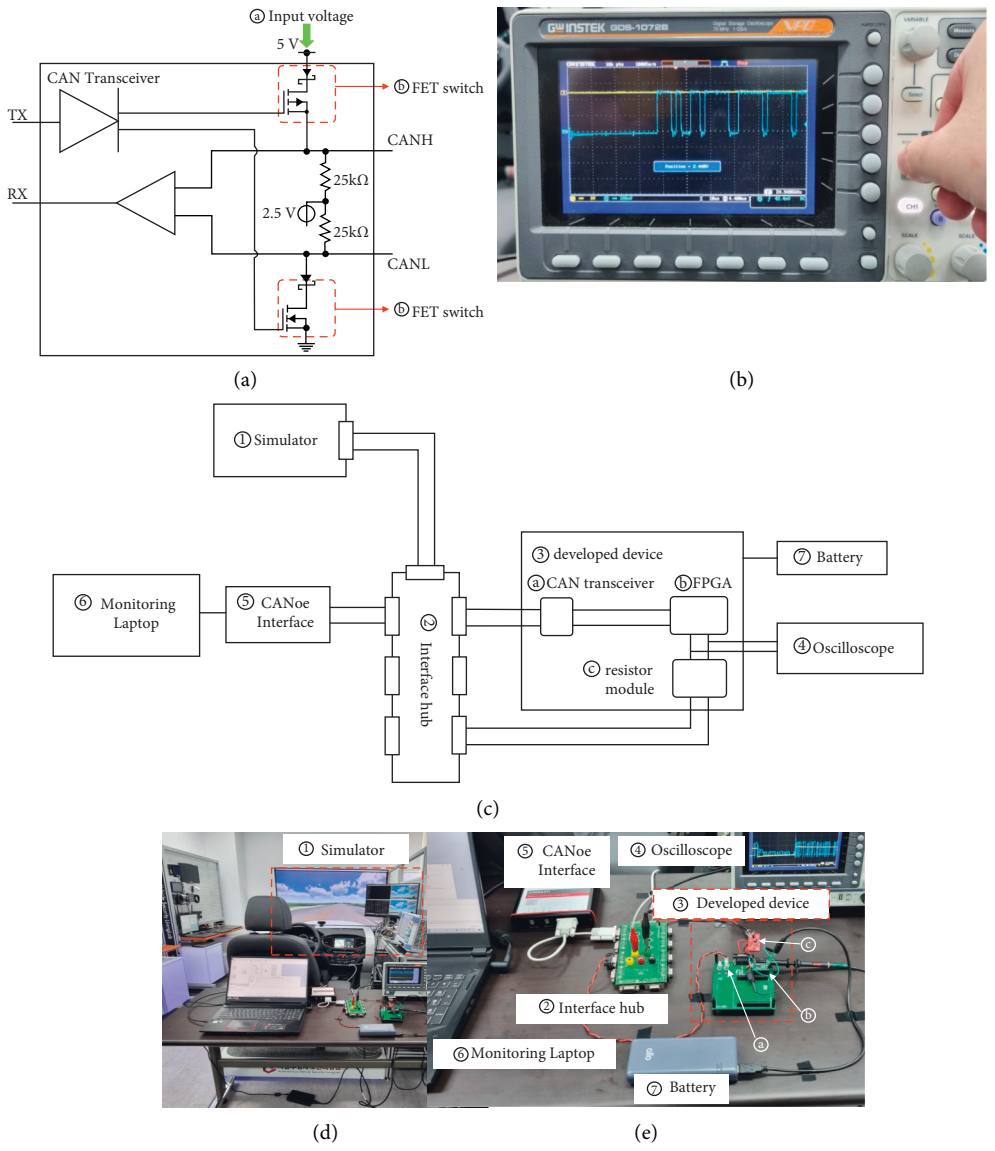


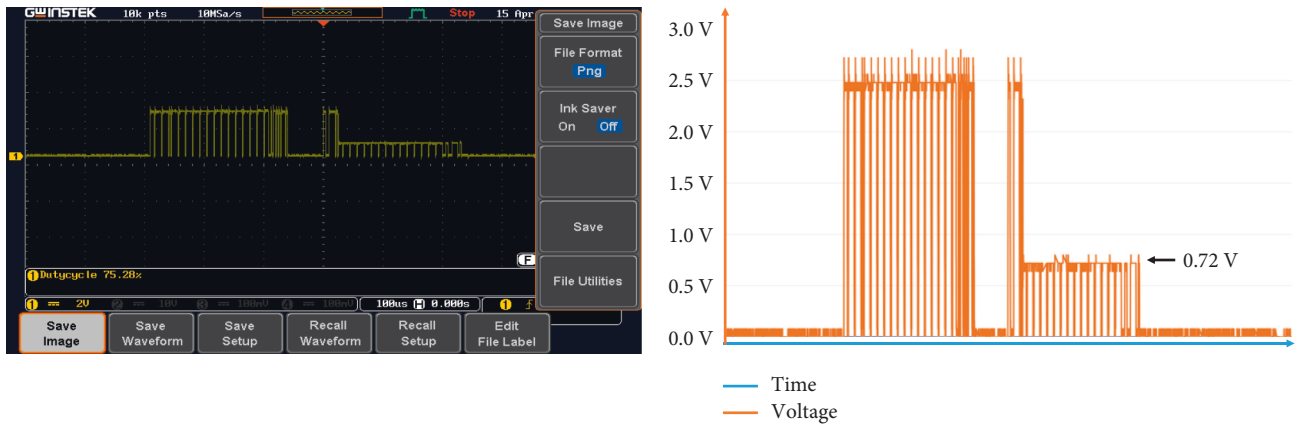
Figure 5: Experiment structures and environments for laboratory simulation testing. (a) CAN transceiver structure, (b) The differential voltage between CANH and CANL, (c) Detailed structure of the device, (d) Overall appearance of the lab, (e) The Developed device.

Table 2: Tools used for the attack experiment.

Tool	Product info
Adjustable resister	P080 3590S
Oscilloscope	GDS-1072B, 70 MHz
CAN interface	CANcaseXL CANoe to CAN BUS
Monitoring and data transmission	CANoe (for CAN BUS)
Simulator	Automotive security living lab [23]
Developed device	CAN transceiver resistor module FPGA
CAN transceiver	SN65HVD230 TEXAS Instruments
Resistor module	2N3904
FPGA	TinyFPGA AX2
Interface hub	CAN BUS terminal
Vehicle	Midsize car (2021 model)

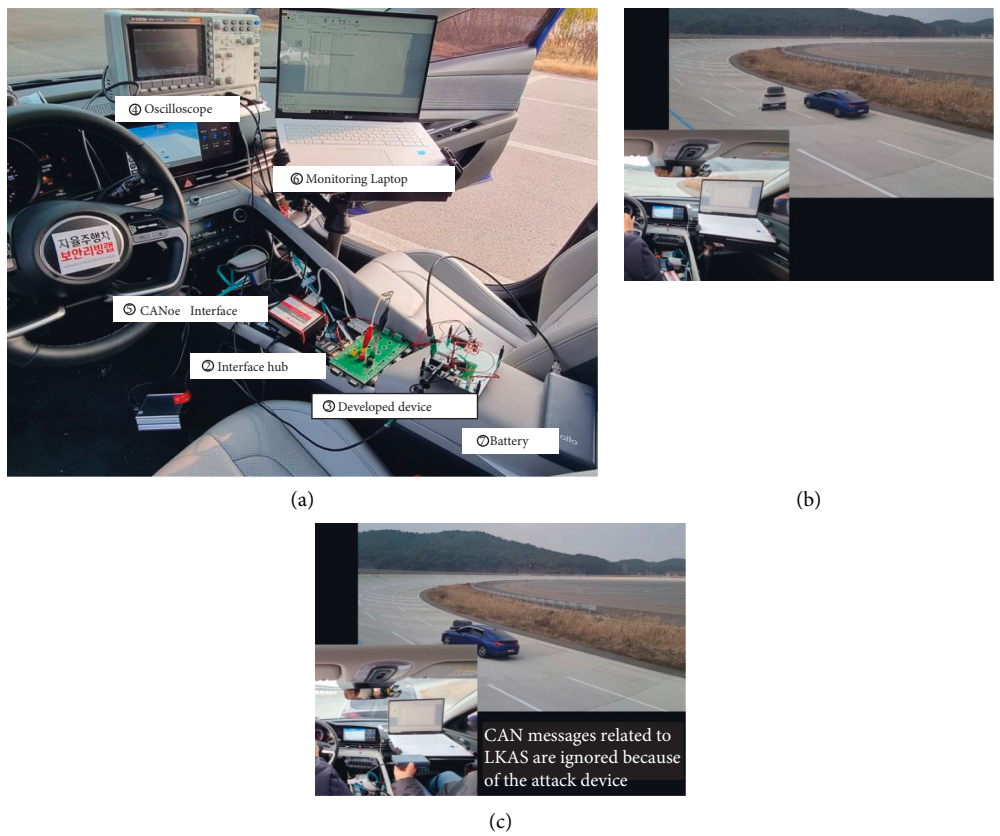
MDPS function is invalidated, and we confirmed that a lane keeping assist system (LKAS) does not work even though it is activated through the simulator.

4.3. Attack on Real Vehicle. In the "Attack simulation in a laboratory environment" section, we showed that the proposed attack is feasible in a simulator that simulates a real vehicle. In this section, we show that the attack we proposed is possible in a real-life setting and therefore dangerous. We applied the device developed in the laboratory environment to a real vehicle. Hyundai Avante (Code name CN7) was used for this experiment. According to the manufacturer, the vehicle has a LKAS named Lane Maintenance Assist function that helps keep the vehicle within the chosen driving lane [25]. The vehicle was supported by KISA living lab [23]. This attack we proposed does not use the weakness of the specific vehicle. It will affect all



(a) (b)

Figure 6: Experimental result of laboratory simulation testing. (a) oscilloscope view, (b) detailed waveform created based on recorded data.



(a) (b)

(c)

Figure 7: Attack on real vehicle. (a) overall view of the vehicle with attack device installed, (b) normal driving, (c) driving under attack.

vehicles that use the CAN-based in-vehicle network. We installed our device in the vehicle (Figure 7(a)). Then, we compared driving in normal and attack situations and recorded the video [26]. The video data used to support the findings of this study have been deposited in the GitHub repository (https://github.com/team-aegis/ceda). As you can see in the video, the first part is driving under normal conditions with the driver's hands off the steering wheel, and the vehicle is driving well between the lanes with the LKAS (Figure 7(b)). In the second part, after the attack starts (by connecting the battery and supplying power), the LKAS related message is not recognized in the in-vehicle network. The vehicle ignores the lane and collides with another vehicle driving in the next lane (Figure 7(c)).

4.4. Countermeasures. As discussed in section 3. B, CEDA can be realized through a supply chain attack or terrorism. In the case of a supply chain attack, MITRE tries to address it by generating a catalog of attack patterns that provides a structure for maturing aspects of supply chain risk

management [27]. Potential countermeasures against supply chain attacks are a good illustration of the catalog. The attack with ID CM-2 is named Prevent or Detect Critical Component Tempering, and the mitigation approach is to prevent or detect tampering with critical hardware or firmware components while in transit, across all lifecycle phases, through use of state-of-the-art anti-tamper devices [27]. In addition, the attack with ID CM-11 is named Multiple Suppliers, and the mitigation approach is Use multiple suppliers for key critical components [27]. As you can see examples in the catalog, almost all countermeasures are managerial measures rather than technical ones. The United Nations (UN) recently enacted a regulation related to vehicle security, UN Regulation No.155, and ISO/SAE 21434 supported the regulation [28, 29]. This regulation consists of two certification programs—Cyber security management system (CSMS) and Vehicle type approval (VTA). The CSMS is a regulation for the security governance and all countries under the 1958 agreement of the UN must enact and follow the relevant laws. You can see why the regulation focuses on supply chain management through security governance, which is consistent with the countermeasures against supply chain attacks proposed by MITRE, are consistent.

In the case of terrorism, the attack is much more difficult to detect. Since the attack device we developed just inspects the received message and increases the resistance in the network, it cannot be detected by a function such as component identification [30]. The IDS also cannot detect it because the device does not send the message to the other ECUs. Therefore, a practical countermeasure is to continuously monitor the voltage in the network and notify the IDS when a voltage is in the gray zone. In this case, a false positive must be considered and additional investigation is needed.

5. Conclusion

In this study, we have shown that it is easy to attack a CAN-based in-vehicle by controlling the resistance and eliminating specific and/or whole messages on the network. As described in Table 2, the attack device can be manufactured at a low cost of less than 20 US dollars. Also since this attack uses the weak point of the CAN-based network protocol, it is hard to detect. It means the attack we proposed can have a huge ripple effect in the real world. Therefore, to protect vehicles from this kind of attack, we need to consider designs based on "security by design" and "defense in depth" and carefully select the security features through security risk assessment [31]. In addition, we need to consider the supply chain management that is required by UN regulation No. 155 and ISO/SAE 21434 to mitigate the risk that comes from supply chain attacks. Furthermore, we believe the monitoring resistance of the network is an appropriate countermeasure against the CAN signal extinction-based DoS attack.

In the future, we will study this attack as an intrusion protection system (IPS). If the IDS can perfectly detect the attack message, the attack message can be completely removed using the CAN signal extinction mechanism we proposed. In the case of a firewall, only the ECUs are located.

Data Availability

The video data used to support the findings of this study have been deposited in the GitHub repository (https://github.com/team-aegis/ceda).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The present research was supported by the research fund of Dankook University in 2019.

References

[1] A. Saad and U. Weinmann, "Automotive software engineering and concepts," *GI. Jahrestagung*, vol. 34, pp. 318-319, 2003.

[2] M. Arfizurrahmanl, M. S. H. Ahmad, M. S. Hossain, M. A. Haque, and K. Andersson, "Real-time non-intrusive driver fatigue detection system using belief rule-based expert system," *J. Internet Serv. Inf. Secur.*, pp. 44–60, 2021.

[3] K. Koscher, A. Czeskis, F. Roesner et al., "Experimental security analysis of a modern automobile," in *Proceeding of the. 2010 IEEE Symposium on Security and Privacy*, pp. 447–462, IEEE, Oakland, CA, USA United Syate of America, May 2010.

[4] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Comprehensive experimental analyses of automotive attack surfaces," in *Proceeding of the. 20th USENIX Security Symposium*, San Francisco, CA, August 2011.

[5] G. Lacava, A. Marotta, F. Martinelli et al., "Cybsersecurity issues in robotics," in *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl*Springer, Berlin/Heidelberg, Germany, 2022.

[6] FCA US LLC, "safety recall R40/NHTSA 15V-461 radio security vulnerability," 2015, https://static.nhtsa.gov/odi/rcl/2015/RCRIT-15V461-7681.pdf.

[7] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," in *Proceeding of the. Black Hat USA*, Black Hat USA, United state of america, August 2015.

[8] H.R.3711, "safely ensuring lives future deployment and research in vehicle evolution act," 2019, https://www.congress.gov/bill/117th-congress/house-bill/3711.

[9] S.2182, "security and privacy in your car act of 2019," 2019.

[10] M. Komisarek, M. Pawlicki, R. Kozik, and M. Choras, "Machine learning based approach to anomaly and cyber-attack detection in streamed network traffic data," *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl*, pp. 3–19, 2021.

[11] M. Elshrkawey, M. Alalfi, and H. Al-Mahdi, "An enhanced intrusion detection system based on multi-layer feature reduction for probe and DoS attacks," *J. Internet Serv. Inf. Secur.*, pp. 61–78, 2021.

[12] P. Nowakowski, P. Zórawski, K. Cabaj, and W. Mazurczyk, "Detecting network covert channels using machine learning, data mining and hierarchical organisation of frequent sets,"

Mob. Networks Ubiquitous Comput. Dependable Appl, vol. 12, pp. 20–43, 2021.

[13] D. Bae and J. Ha, "Performance metric for differential deep learning analysis," *J. Internet Serv. Inf. Secur.*, pp. 22–33, 2021.

[14] S. C. Hpl, "Introduction to the Controller Area Network (CAN)," *Application Report SLOA101*, pp. 1–17, 2002.

[15] J. Deichmann, B. Klein, G. Scherf, and R. Stützle, "The Race for Cybersecurity: Protecting the Connected Car in the Era of New Regulation," 2019, https://mck.co/2xcXm4G.

[16] A. Palanca, E. Evenchick, F. Maggi, and S. Zanero, "A stealth, selective, link-layer denial-of-service attack against automotive networks, Detection of Intrusions and Malware, and Vulnerability Assessment," in *Proceeding of the. International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pp. 185–206, Bonn, Germany, June 2017.

[17] Y. Lee, S. Woo, J. Lee, Y. Song, H. Moon, and D. Lee, "Enhanced Android app-repackaging attack on in-vehicle network," *Wireless Communications and Mobile Computing*, pp. 185–206, 2019.

[18] P. S. Groza and B. Groza, "Source identification using signal characteristics in controller area networks," *IEEE Signal Processing Letters*, vol. 21, no. 4, pp. 395–399, 2014.

[19] K. T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in *Proceeding of the 25th USENIX Security Symposium*, pp. 911–927, ktcho, kgshin, August 2016.

[20] K. T. Cho and K. G. Shin, "VIDEN: attacker identification on in-vehicle networks," in *Proceeding of the. 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1109–1123, New York, NY, United States, October 2017.

[21] S. U. Sagong, X. Ying, R. Poovendran, and L. Bushnell, "Exploring attack surfaces of voltage-based intrusion detection systems in controller area networks," *SAVE Proceedings. 2018 ESCAR Europe*, pp. 1–13, 2018.

[22] ISO, *ISO11898-2:2016, Road Vehicles - Controller Area Network (CAN) - Part 2: High-Speed Medium Access Unit*, International Organization for Standardization, Geneva, Switzerland, 2003.

[23] KISA, "the automotive security living lab," https://www.kisa.or.kr/1040404, 2020.

[24] TI, VP230 datasheet - 3.3-v CAN transceivers, 2022, https://www.digchip.com/datasheets/parts/datasheet/477/vp230.php.

[25] Hyundai, "avante catalog," 2022, https://www.hyundai.com/kr/en/sedan/avante/20fc/price.

[26] Team-AEGIS, "CEDA: can signal extinction-based DoS attack," 2022, https://github.com/team-aegis/ceda.

[27] J. F. Miller, *Supply Chain Attack Framework and Attack Patterns*, MITRE CORP MCLEAN VA, Colshire Dr, McLean, VA 22102, USA, 2013.

[28] UN Regulation, No.155, *Uniform Provisions Concerning the Approval of Vehicles with Regards to Cyber Security and Cyber Security Management System*, UN, New York, 2021.

[29] ISO, *Road Vehicles — Cybersecurity Engineering*, International Organization for Standardization, Geneva, 2021.

[30] A Weimerskirch, C Paar, and M Wolf, "Cryptographic component identification: enabler for secure vehicles," in *Proceeding of the. IEEE Vehicular Technology Conference*, vol. 62, no. 2, p. 1227, September 2005.

[31] S. R. Ronald, M. Michael, and C. O. Janet, "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," *NIST Special Publication*, pp. 800–160, 2016.