ISSN 2586-1816
Journal of Convergence for Information Technology e-ISSN 2586-4440
Vol. 8. No. 5, pp. 115-120, 2018 DOI : https://doi.org/10.22156/CS4SMB.2018.8.5.115

Research on Countermeasures of Controller Area Network Vulnerability

Sunghyuck Hong
Associate Professor, Division of Information and Communication, Baekseok University

Controller Area Network 취약점 분석 및 대응 방안 연구

홍성혁
백석대학교 정보통신학부 부교수

Abstract As the number ofconnected cars grows, the security of the connected cars is becoming more important. There are also increasing warnings about the threat of attacks via the CAN bus used for in-vehicle networks. An attack can attack through a vulnerability in the CAN bus because the attacker can access the CAN bus remotely, or directly to the vehicle, without a security certificate on the vehicle, and send a malicious error message to the devices connected to the CAN bus. A large number of error messages put the devices into a 'Bus-Off' state, causing the device to stop functioning. There is a way to detect the error frame, or to manage the power of the devices related to the bus, but eventually the new standard for the CAN bus will be the fundamental solution to the problem. If new standards are adopted in the future, they will need to be studied.

Key Words : Connected vehicles, CAN security, car hacking, communication security, network security

요 약 연결형 자동차의 사용이 늘어나면서 연결형 자동차의 보안이 중요해지고 있다. 그 중 차량 내부 네트워크에 쓰이는 CAN 버스를 통한 공격의 위협성이 증가하고 있다. CAN 버스의 특성상 공격자가 해당 차량에 보안상 인증이 없는 CAN 버스에 원격, 또는 차량에 직접 접근하여 CAN 버스와 연결된 장치들에 악의적인 오류메시지를 전송 가능하다. 따라서 다량의 오류 메시지로 해당 장치들을 'Bus-Off' 상태로 만든 뒤, 해당 장치가 기능을 정지하게 만든다. 이에 대한 대응 방법은 오류 프레임을 감지하는 방법이나 버스와 관련된 장치들의 전원을 관리하는 방법 등이 있으나 결국에는 CAN 버스에 대한 새로운 표준이 문제의 근본적인 해결책이 될 것으로 판단한다. 따라서 본 논문에서는 새로운 연결형 자동차의 보안모델을 제시하여 안전한 연결형 자동차의 이용에 기여하는 것이 본 논문의 목적이다.

주제어 : 연결형 자동차, CAN보안, 자동차 해킹, 통신보안, 네트워크 보안

1. Introduction

1.1 Connected Vehicle

As automobiles are now electronics, modern automobiles are becoming increasingly complex computer network systems. The evolution and development of IOT technology has started the era of Connected Car. Not only major automobile manufacturers like Audi and Jeep work on 'Connected Cars' that offer a variety of features such as location tracking, remote door locking

*This paper was supported by Baekseok University research fund in 2018.
*Corresponding Author : Sunghyuck Hong (shong@bu.ac.kr)
Received September 14, 2018 Revised September 28, 2018
Accepted October 20, 2018 Published October 31, 2018

and unlocking, self parking and navigation, but also, IT companies like Google and Apple work on connected cars. There is also research on autonomous driving there, and it is expected that 'Connected Car' which is capable of full autonomous driving in the near future will be released [1].

In both cases, they succeeded in hacking by exploiting the weaknesses of CAN's internal CAN (automobile standard network protocol). In the meantime, the technology of automobile ECU (automobile electronic control unit) has been developed. However, the control system has been using CAN communication method since 1985 [2]. This communication method is not encrypted, and it is weak and simple to control and manipulate.

This paper describes the structure, form, and vulnerability of CAN in Chapter 2. It describes hacking using CAN vulnerability in Chapter 3, and describes countermeasures against CAN vulnerability in Chapter 4. Chapter 5 concludes the paper with conclusion of this study.

2. What is Controller Area Network (CAN)?

2.1 Background

Modern automobiles have numerous electronic control units (ECUs) for various subsystems. The engine control unit may have transmission, air bags, ABS, cruise control, a power steering device, an audio system, power windows, doors and side mirror adjustment. Some form an independent subsystem, but communication with other subsystems is essential. CAN stands for Controller Area Network. CAN is designed for in-vehicle networking of automotive applications and ECUs communicate with each other via CAN inside the vehicle.

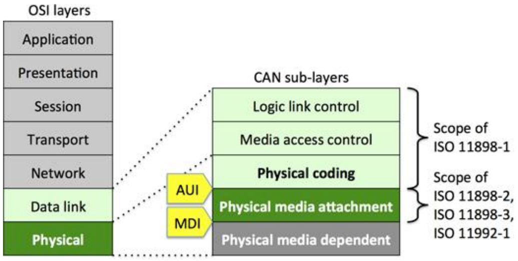

Fig. 1. The OSI model correlates with data link and physical layers [3].

Fig. 1 shows the CAN layer. CAN was first developed in 1983, Bosch Corporation, which was officially launched in 1986 with the GSM protocol which was first used in a production car in 1989. ISO has adopted a standard, and CAN has been published through the ISO11898 and ISO11898. The CAN physical layer for the ISO 11898-1, high-speed CAN deals with the data link layer into two parts: 2012 Bosch has improved the CAN data link layer protocol (CAN FD), an improved standard is added to the ISO 11898-1 and was published in 2014. This standard, CAN, has been used as the standard for virtually all small vehicles [4-6].

CAN does not to have an input from the ECU which is different CAN networks. Therefore, it is economical to reduce the total cost and weight in the automobile network, and the device has intelligent control chip [7-9].

2.2 Structure of CAN

In the CAN standard, there are two wires, CAN High (CANH) and CAN Low (CANL), to which all devices are connected. It is also referred to as the CAN bus because it looks like a shared cable running on all the various subsystems. Fig. 2 shows the basic CAN structure.

Each CAN node can send and receive messages, but it can not both transmit and receive simultaneously. Frames (messages) are transmitted serially on the bus. The pattern of the transmitted signal is encoded in non-return-to-zero (NRZ) and is detected at all nodes [10-13].

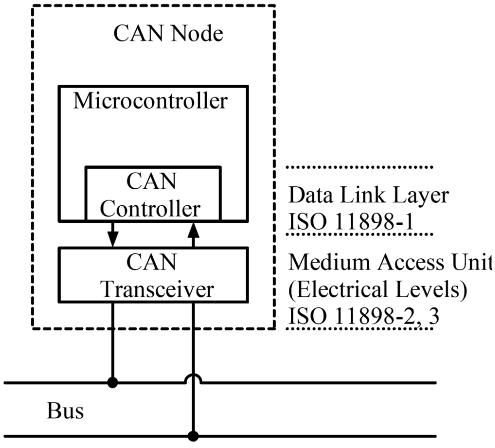

Fig. 2. Typical CAN structure

The function of CAN is that all CAN nodes can send messages when the bus is idle. A multi-master function to send messages, broadcast communication function in which all transmitted messages are received at all nodes, sophisticated error detection. A non-destructive bus arbitration function ensures that the protocol with the highest priority message gets the bus access right immediately if there is a fault isolation mechanism and re-transmission of the problematic message and more than two CAN nodes request the message transmission simultaneously have.

The devices connected to the CAN network are generally sensors, actuators and other control devices. These devices inter-operate in the CAN network, exchanging common commands and status, actuator commands, sensor data obtained from sensors, or requesting information from other nodes that can collect data across the network environment. These devices are not directly connected to the CAN bus, but are also connected via a local host processor, CAN controller, or CAN transceiver.

2.3 Communication method of CAN

If one of the subsystems wants to 'talk', it records a series of 0's and 1's encoded messages (frames) on the CAN bus. All messages circulating through the CAN bus can be read by other devices connected to the bus. If the message relates to a device, the device can perform the task. Since the bus is competitive and bus errors are frequent, any device that writes frames to the CAN bus is responsible for verifying the actual wire values.

If the actual value at a certain time matches the original expected value, but if it does not match, the device calls the previous frame on the CAN bus and informs other devices to ignore the frame [8].

2.4 Vulnerability of CAN

- All devices connected to CAN bus can read and write without any regulations. There is no authentication or access control mechanism.

All data coming through the CAN bus assumes that the attacker can not gain unauthorized access to the CAN bus, so that it can access all the reliable data.

- There is no way to distinguish between well-formed error messages and real error messages. Namely, it can not tell if the device is actually broken or damaged, or if the attacker's command can cause it to go back to 'Bus-Off'.

These vulnerabilities can have serious consequences. All devices on the CAN bus can program messages that can be intercepted from any communication, which is like a Denial of Service (DoS) attack.

If the device sends too many errors, it will be "off" (Bus Off) according to the CAN standard and will be blocked from the CAN, and the device will not be able to read or write data to the CAN and will not be able to operate other modules or systems. This feature is a feature of CAN used in CAN attacks. Attacking triggers this particular function by causing the target device or system on the CAN to be in the Bus Off state and causing enough errors to become inactive or inoperable. In particular, when an essential system such as an airbag system or an ABS system is deactivated, it could endanger the life of the occupant and have a detrimental effect on vehicle performance. Local access reuses frames that are already cycling in CAN rather than attacking the car's CAN with a specialized attacker or a new approach [9]. Fig. 3 shows the states of a CAN node.

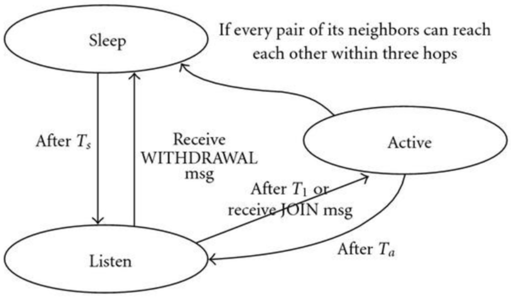
Sleep
If every pair of its neighbors can reach each other within three hops
Active
After T_s
Receive WITHDRAWAL msg
After T_1 or receive JOIN msg
Listen
After T_a

Fig. 3. States of a CAN node

3. CAN attack method

3.1 Active Safety System DoS

The Active Safety System is useful, but it can be dangerous if the driver is overly satisfied with his / her use and relying on it. Attacking hackers can cause certain faults in CAN frames that occur in the Active Safety System, which can cause the Active Safety System to suddenly turn off.

This can cause unexpected accidents for the driver, and it can cause fatal accidents as the driver can not stop the car.

3.2 Throttle DoS

CAN has been used to perform "throttle-by-wire" functions. For example, Toyota's Prius internal combustion engine throttle actuator in 2010 is controlled by the CAN frame sent from the power management control unit to the engine control module.

An attacker can use these frames to attack. It is possible to prevent the driver from controlling the throttle position and moving the vehicle. Though not directly dangerous, an attacker with a money intent can use a covert DoS attack to launch a malicious attack and later display a malicious message on the information display. This causes the owner of the car to repair the car and cause a financial loss to the car owner [14].

4. Response Plan

An important challenge is to detect a leading attack before the DoS is executed. This is because the attacking device may remain hidden from all other CAN devices without participating in the CAN activity.

The following mechanisms can be implemented without significant changes to the internal network of the vehicle without the cost of recalling the vehicle (large-scale recall after the Jeep car hacking incident).

Power drain detection: When a potentially exploitable device is added to the CAN bus network, a system or program that notifies the user of the device will detect anomalous or additional power drain on the bus current (which adds to the power load as more devices are added).

Network Segmentation or Topology Alteration: Create various CAN sub-busses or change the network topology on the bus in a star shape so that the frame can freely circulate to all devices.

Regulated OBD-II Diagnostic Port Access: Requires a special hardware key to open a location where the port is located, or meets software level authentication to allow traffic through the port. This may require changes to the regulations.

Encryption: Encrypts the CAN frame ID field to prevent an attacker from identifying the CAN frame ID, allowing the attacker to have a more aggressive, more perceptible attack pattern.

Error determination: A system or program that can detect as many devices as possible through the nature of the error frame being transmitted. Malicious errors can seem to be the same. This detection approach may in fact indicate that a defective device is maliciously flagged as a malicious device.

The existing CAN bus IDS / IPS technologies are based on abnormal detection of erroneous types of frames because attacks require injection of frames in most cases.

However, attacks send the transmission of the bits at the same time as the transmission of the correct frame. From the viewpoint of the receiving apparatus, the frame transmission may be interrupted due to an error.

Finally, to address the vulnerability of the CAN bus, a new standard is needed to address the vulnerability. In September, the US Road Traffic Safety Commission developed guidelines for autonomous driving, including cyber security and privacy. The European Union executive committee is working to standardize technology such as ensuring smooth communication between connected cars, hardware and software specifications [15].

5. Conclusion

It is now common for a malicious attacker such as a hacker to hack into another user's vehicle. However, only cars parked are not targets of attack. For example, car rentals, car rentals, parking lots, and garages have become new attacks. (Eg, car sharing, autonomous vehicles, widely used automotive app services, used information), and as the automotive computing network evolves and supplementary services evolve, a number of vulnerabilities have been built into devices embedded in in-vehicle systems.

So far, the existence of vulnerabilities has rarely been considered. However, the existence of vulnerabilities in future will be considered deeply. All of these situations and vulnerabilities increase the likelihood of attackers targeting automobiles. Therefore, it is time to establish a standardization body to standardize non-common standards and to design new electronic and mechanical security systems, such as government decision makers and automobile manufacturers, who recognize changes and manage cars of the future.

REFERENCES

[1] Ausflug, Jeep-Safari (2005). *ReiseRechts Aktuell, 13(3).* DOI : 10.1515/rra.2005.13.3.121

[2] C. Bayilmis & E. Kelebekler. (2008). Remote control of a CAN-based mobile model car using a voice activated control system. *2008 IEEE 16th Signal Processing, Communication and Applications Conference.* DOI : 10.1109/siu.2008.4632605

[3] D. J. Arnett. (1987). A High Performance Solution for In-Vehicle Networking - *'Controller Area Network (CAN)'. SAE Technical Paper Series.* DOI : 10.4271/870823

[4] J. Yang, J. Wang, C. Zhao & F. Wang. (2015). Study on Reliability Analysis for Braking System Parts Based on Hybrid Censoring Test under Small Sample Size. *The Open Cybernetics & Systemics Journal, 9(1),* 2530-2535. DOI : 10.2174/1874110x01509012530

[5] P. Song, Y. Zhang, X. Wu, & Y. Lan. (2013). Design and Implementation of the Adaptive Control System for Automotive Headlights Based on CAN/LIN Network. *2013 Third International Conference on Instrumentation, Measurement, Computer, Communication and Control.* DOI : 10.1109/imccc.2013.355

[6] D. Sabolić & Ž. Car. (2013). Stochastic modeling of signal propagation in power-line communication networks. *International Journal of Communication Systems.* DOI : 10.1002/dac.2530.

[7] K. Parnell. (2004.). Telematics Digital Convergence — How to Cope with Emerging Standards and Protocols. *Advanced Microsystems for Automotive Applications VDI-Buch,*335-348. DOI : 10.1007/978-3-540-76989-7_24

[8] J. Espina, T. Falck, A. Panousopoulou, L. Schmitt, O. Mülhens, & G. Yang. (2014). Network Topologies, Communication Protocols, and Standards. *Body Sensor Networks*, 189-236. DOI : 10.1007/978-1-4471-6374-9_5

[9] X. Yang, Z. Yu, M. Xiao, G. Ji & Z. Wang. (2014). Automated test system design based on Tellus for in-vehicle CAN network. *2014 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops* (ICUMT). DOI : 10.1109/icumt.2014.7002089

[10] S. Shivle & A. V. Murthy. (2010). Improvement in Noise Transmission Across Firewall of a Passenger Car. *SAE Technical Paper Series.* DOI : 10.4271/2010-01-0751

[11] S. Hong & K. Han. (2014). Cost-Efficient Routing

Protocol (CERP) on Wireless Sensor Networks. *Wireless Personal Communications, 79(4),* 2517-2530.
DOI : :10.1007/s11277-014-1883-z

[12] S. H. Hong & Y. J. Seo. (2016), Countermeasure of Sning Attack: Survey. *Journal of Convergence Society for SMB (KCI), 6(2),* 31-36

[13] S. Hong. (2014). Analysis of DDoS Attack and Countermeasure: Survey. *The Journal of Digital Policy and Management, 12(1),* 423-429.
DOI : 10.14400/jdpm.2014.12.1.423

[14] S. Hong. (2017). Research on IoT International Strategic Standard Model. *Journal of the Korea Convergence Society, 8(2),* 21-26.
DOI : 10.15207/jkcs.2017.8.2.021

[15] S. Hong. (2014). Vulnerability of Directory List and Countermeasures. *Journal of Digital Convergence, 12(10),* 259-264.
DOI : 10.14400/jdc.2014.12.10.259

홍 성 혁(Sunghyuck Hong) [종신회원]

- 2007년 8월 : Texas Tech University, Computer Science (Ph.D)
- 2007년 9월 ~ 2012년 2월 : Senior Programmer, Texas Tech University, Office of International Affairs
- 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수
- 관심분야 : Blockchain, Network Security, Hacking, Anti-fishing technology
- E-Mail : shong@bu.ac.kr