Proceedings of 2016 IEMEK Symposium on Embedded Technology
(ISET 2016)
Hotel Inter-Citi Daejeon, Korea, 26-*27 May, 2016*.

An Analysis of Voltage Drop as a Security Feature in Controller Area Network

Ki-Dong Kang[*] Youngmi Baek[**] Seonghun Lee[†] Sang H. Son [*]

[*]Department of Information and Communication Engineering
DGIST, Republic of Korea
E-mail: {kd_kang, son}@dgist.ac.kr
[**]CPS Global Center
DGIST, Republic of Korea
E-mail: ymbaek@dgist.ac.kr
[†]Convergence Research Center for Future Automotive Technology
DGIST, Republic of Korea
E-mail: shunlee@dgist.ac.kr

Abstract

Recently, various technologies of automotive CPS offer excellent potential for road safety and efficiency such as reducing car crashes, fuel consumption, pollution and congestion but are still developing now. On the other hand, they make an automotive system more complicated and the vulnerability of it also increases. In practice, many researchers already demonstrated that a real vehicle could be attacked from anywhere through wire or wireless media by exploiting the various vulnerabilities of automotive CPS. The root of these vulnerabilities comes from a CAN protocol which is de facto standard in in-vehicle network and no consideration of security aspect. In this paper, we show a feasibility of voltage drop among physical layer features in CAN, as a security feature.

Keywords: Security Feature, Controller Area Network, Cyber-physical Systems (CPS)

1. Introduction

As the modern vehicle is designed to support the various functions for safety, convenience and etc., it needs lots of ECUs inside. The various attacks of in-vehicle occur due to high complexity of it and many researchers have shown demonstrations of vehicle attacks in real car [1], [2]. The source of these problems is a vulnerabilities of controller area network (CAN) protocol [3], which is de facto standard in-vehicle network. There is no consideration in terms of security aspects, since CAN protocol was developed in 1983 and in-vehicle network was isolated from outside for a long time. The major vulnerabilities of CAN protocol are: (1) no authentication (2) no address of sender and receiver (3) a small payload size for cryptographic functions.

2. Voltage Drop along the Bus Line

To counteract these problems, we focus on the voltage drop as one of physical features in order to support CAN with enhanced level of security, such as identification of a transmitted CAN node, because it is the difference between sender and receiver voltage, usually due to the wiring resistance which increase with length of wire.

Basic formula of voltage drop has shown in Equation (1), and Equation (2) shows the relationship between the resistance and temperature where R(T) is conductor resistance at temperature T, R_{ref} indicates conductor resistance at reference temperature T_{ref}, α means temperature coefficient of resistance for conductor material, cooper wire is $3.9 \times 10^{-3} \Omega/℃$, T is conductor temperature in degree Celsius, and T_{ref} denotes reference temperature that α is specified at for the conductor material, usually 20℃.

$$V_{drop\ (\mathrm{V})} = I_{wire\ (\mathrm{A})} \times R_{wire(\Omega)} \tag{1}$$

$$R(T) = R_{ref}[1 + \alpha(T - T_{ref})] \tag{2}$$

Figure 1 presents a distribution of the average voltage level of sampled data as a physical distance between two nodes increases. They have the different voltage levels along the length of wire, and the shape follows Gaussian distribution. If we use the specified mean and variance of each individual Gaussian distribution which are taken from our experiment, it could address problems of security in CAN. Note that the measurement of voltage drop along length of wire can help to represent an identification of CAN nodes.

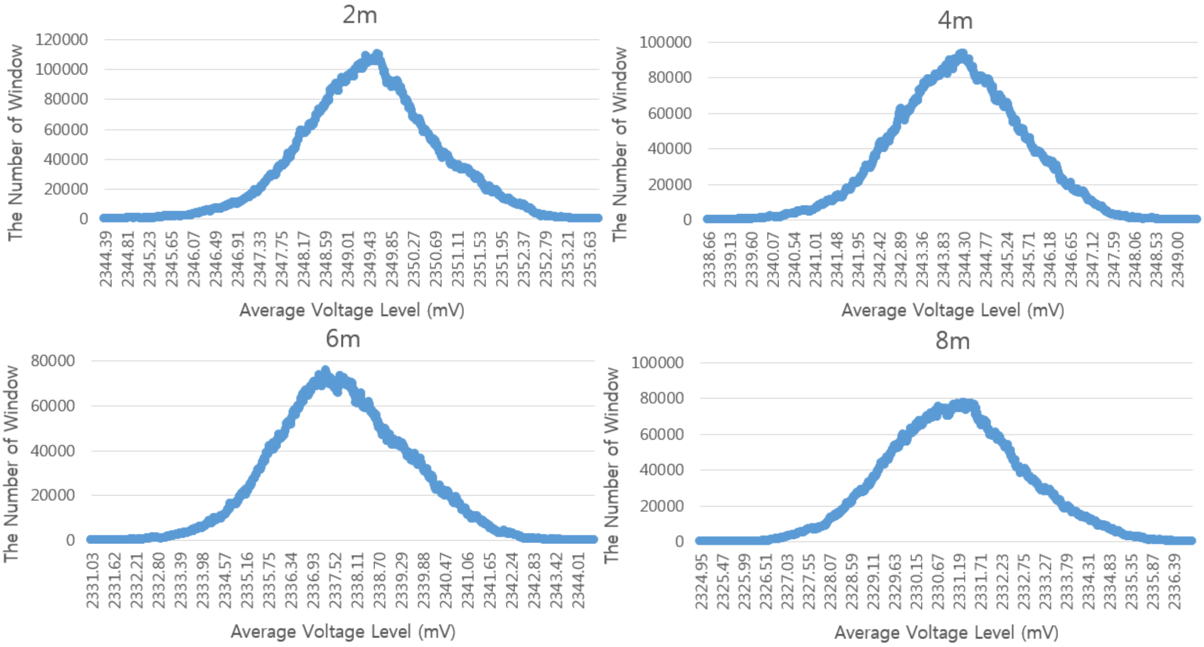

Figure 1. Distribution of average voltage level as 2m, 4m, 6m, and 8m between two nodes, respectively

3. Conclusions and Future Work

In existing research [4], there were various features such as voltage amplitudes and their stability, the shape of clock edges, propagation delays, and signal attenuation due to wire lengths for intrusion detection system in CAN environment. However, they didn't evaluated these features. As the result of this work, we have shown some difference in accordance with wire length. We plan to evaluate other physical features. After that, we will consider combined method using various features together for enhanced level of security in CAN.

Acknowledgement

This research was supported in part by Global Research Laboratory Program (2013K1A1A2A02078326) through NRF, DGIST Research and Development Program (CPS Global Center) funded by the MSIP, and Institute for Information & communications Technology Promotion (IITP) grant funded by the Korean government (MSIP) (No. B0101-15-0557, Resilient Cyber-Physical Systems Research).

References

[1] Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., ... & Kohno, T. (2011, August). Comprehensive Experimental Analyses of Automotive Attack Surfaces. In USENIX Security Symposium.

[2] Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., ... & Savage, S. (2010, May). Experimental security analysis of a modern automobile. In Security and Privacy (SP), 2010 IEEE Symposium on (pp. 447-462). IEEE.

[3] Bosch, R. (1991). CAN specification version 2.0. Rober Bousch GmbH, Postfach, 300240.

[4] Hoppe, T., Kiltz, S., & Dittmann, J. (2011). Security threats to automotive CAN networks—Practical examples and selected short-term countermeasures. Reliability Engineering & System Safety, 96(1), 11-25.