Proceedings of 2018 IEMEK Symposium on Embedded Technology (ISET 2018)
MAISON GLAD, JEJU, Korea, 24-*25 May*, *2018*.

SDN Based ARP Spoofing Response Structure for Communication Based Train Control

Sangjun Kim Hyung-Seok Park Kyung-Joon Park

Department of Information and Communication Engineering
Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu, Republic of Korea
E-mail: {sjkim, hyungseok, kjp}@dgist.ac.kr

Abstract

We propose a response structure for ARP spoofing attacks in communication based train control (CBTC) systems. Based on software defined networking (SDN) technology, the proposed structure detects the attack on the switch. Then, a subsystem which is not exposed to attack informs the train of the attack when the control messages from automatic train supervision (ATS) to train are manipulated by the attacker. We carry out experiments to measure the attack response time for the train to detect the attack. Our experimental results show that the proposed structure can effectively inform the train of the attack.

Keywords: CPS, SDN, ARP spoofing, CBTC, security.

1. Introduction

Recently, cyber-physical systems (CPSs) have gained a great interest and there are attempts to apply CPS in many fields [1-2]. One example of CPS is a communication-based train control (CBTC) system, which uses bidirectional radio frequency data communication between the trains and automatic train supervision (ATS) [3]. For the reliable operation of the train, transmission reliability and security for train control and sensing messages between train and ATS are required.

ARP spoofing is one of the cyber-attack, in which malicious attacker intercepts and modifies exchanged messages between the train and ATS. If the messages between the train and the ATS are manipulated by the attacker, the train accidents such as derailment or collision between trains can occur. In order to ensure stable operation of the trains, it is important to detect and cope with ARP spoofing.

In this work, we propose a software defined networking based structure that can detect and cope with ARP spoofing in the network between the ATS and train. Then, we measure the attack response time for ARP spoofing by experiments in an SDN testbed environment.

2. ARP spoofing response structure

We propose a SDN based response structure for ARP spoofing in CBTC. ATS and each switch are connected as shown in Fig. 1. Train uses a wireless technology such as IEEE 802.11 WLAN and LTE to connect to an access point (AP) in S4 in Fig. 1. The subsystem informs the train of the ARP spoofing attack. We assume that the attacker has already entered the network through AP in S4 and selects the ATS and train. In this case, an attacker scans hosts and can detect the train and ATS. However, the subsystem is not detected because this system is disconnected by SDN.

When S1 detects that an IP address matches multiple MAC addresses, S1 determines that a network attack has occurred and informs the SDN controller of the situation. Then, the SDN controller connects between S1 and the subsystem and subsystem can send emergency stop messages to the train.

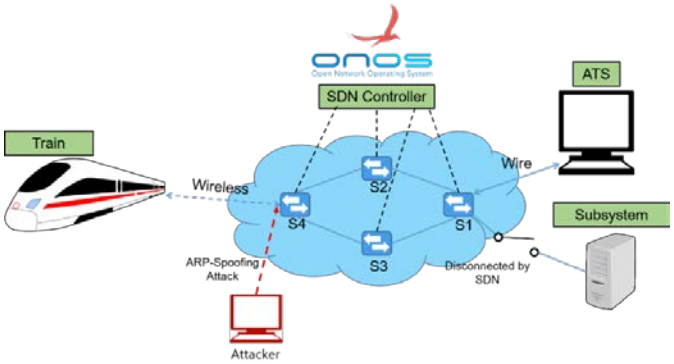

Figure 1. SDN based response structure against ARP Spoofing for CBTC systems.

3. Experiment

To verify this structure, we carry out experiments in our testbed environment. The testbed consists of 4 switches, two host PCs for the ATS and train, an SDN controller, a subsystem and an attacker PC. We use Raspberry Pi3, which acts as a switch, AP and subsystem. The SDN switches are implemented in Raspberry Pi3 and the ONOS SDN controller is installed on the laptop computer and is logically centralized [4]. The train and ATS are replaced by PCs. We use Ettercap tool for ARP spoofing [5].

In order to evaluate the performance of the proposed structure, attack response time is measured when control message periods are 500 ms and 1 s, respectively. The attack response time is calculated as the time interval from the moment the first manipulated packet arrives at the train until the arrival of the train emergency stop packet.

In the median case, when control message periods are 500 ms and 1 s, the respective response time is 589 ms and 552 ms. It should be noted that the response time is zero if the ARP attack is detected and the emergency stop packet arrives before the first manipulated packet arrives at the train. Consequently, the response time tends to decrease due to more zero values with a larger control message period.

In the experimental result, there exists a case when substantial response time occurs. This is a problem, where malicious ARP reply message cannot be detected while S1 monitors legitimate ARP message, when these two ARP messages arrive to S1 during the short time. In our future work, we need to improve the worst-case detection performance of malicious ARP messages.

4. Conclusion

In this work, we have proposed an SDN structure that can cope with ARP spoofing in CBTC. We show that the proposed SDN structure can properly handle the control message manipulation attack through ARP spoofing.

Acknowledgement

This work was supported by the DGIST R&D Program of the Ministry of Science and ICT (18-EE-01).

References

[1] K.-J. Park, R. Zheng, and X. Liu, "Cyber-physical systems: Milestones and research challenges," Computer Communications, vol. 36, issue 1, pp. 1-7, December 2012.

[2] K.-J. Park, J. Kim, H. Lim, and Y. Eun, "Robust path diversity for network quality of service in cyber-physical systems," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2204-2215, November 2014.

[3] Robert D. Pascoe and Thomas N. Eichorn, “What is communication-based train control?,” IEEE Vehicular Technology Magazine, vol. 4, no. 4, pp. 16-21, December 2009.

[4] ONOS website, https://wiki.onosproject.org.

[5] Ettercap website, https://www.ettercap-project.org.