LETTER *Special Section on Next-generation Security Applications and Practice*

SOME/IP Intrusion Detection System Using Machine Learning*

Jaewoong HEO[†a)], **Hyunghoon KIM**[†], ***and*** **Hyo Jin JO**[†b)], ***Nonmembers***

SUMMARY With the development of in-vehicle network technologies, Automotive Ethernet is being applied to modern vehicles. Scalable service-Oriented MiddlewarE over IP (SOME/IP) is an automotive middleware solution that is used for communications of the infotainment domain as well as that of other domains in the vehicle. However, since SOME/IP lacks security, it is vulnerable to a variety of network-based attacks. In this paper, we introduce a new type of intrusion detection system (IDS) leveraging on SOME/IP packet's header information and packet reception time to deal with SOME/IP related network attacks.

key words: *Automotive Ethernet, SOME/IP, intrusion detection system*

1. Introduction

As an autonomous driving technology is now widely utilized in modern vehicles, Automotive Ethernet is being adopted as in-vehicle network technology.

In light of this, AUTomotive Open System ARchitecture (AUTOSAR) consortium developed Scalable service-Oriented MiddlewarE over IP (SOME/IP) that is the Automotive Ethernet middleware [1]. However, since SOME/IP does not consider security, it is vulnerable to cyber-attacks. Even though there are many security works for SOME/IP [2], [3], these works cannot deal with the new attack scenarios such as a masquerade attack that mimics the frequency of SOME/IP packet transmission. In this paper, we introduce three SOME/IP-based attacks and propose a machine learning-based intrusion detection system (IDS) [4] that can detect the SOME/IP-based attacks better than exiting IDSs.

2. Background and Related Works

2.1 SOME/IP

SOME/IP as a communication middleware in Automotive Ethernet was developed by the AUTOSAR consortium. SOME/IP provides three communication models: Request/Response, Fire&Forget (Request w/o response) and Notification (a general Publish/Subscribe-Concept).

Manuscript received February 10, 2022.
Manuscript revised May 23, 2022.
Manuscript publicized July 13, 2022.

[†]The authors are with the Graduate School of Software, Soongsil University, Seoul, Republic of Korea.

*This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2021R1A4A1029650).

a) E-mail: wkdgjwodnd26@gmail.com
b) E-mail: hyojin.jo@ssu.ac.kr (Corresponding author)

DOI: 10.1587/transinf.2022NGL0007

2.2 Intrusion Detection System for SOME/IP

Since SOME/IP lacks security, many studies have been conducted to add security features in SOME/IP. [3] proposed Recurrent Neural Network (RNN)-based [5] SOME/IP IDS. In this work, SOME/IP packets are converted to binary vectors by using one-hot encoding, then they are grouped into sequences to be used for RNN's input. This work can detect several types of SOME/IP attacks such as Request without Response, Response without Request, Error on Error, and Error on Event that are defined in [3].

3. Proposed IDS

3.1 Attack Model and Attack Scenario

Figure 1 shows an adversary model in an Automotive Ethernet environment. In Fig. 1, the publisher ECU acts as a server and the subscriber acts as a client. We assume that the attacker can remotely access Automotive Ethernet by compromising an ECU such as a telematics ECU [6]. The attacker can perform cyber-attacks such as Denial-of-Service (DoS) Attack, Message Frequency-Aware (MFA) Attack, and Replay Attack.

- DoS Attack: It aims to consume network bandwidth by sending a massive number of SOME/IP packets.
- MFA Attack: It injects SOME/IP packets by mimicking the message transmission cycle of a publisher ECU.
- Replay Attack: A stream of SOME/IP packets is copied, and that stream is replayed on Automotive Ethernet.

3.2 Feature Extraction

To improve the performance of the IDS, 10 features were ex-

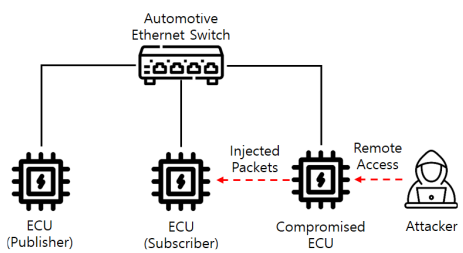

Fig. 1 Adversary model.

Table 1 Features for intrusion detection system.

Features	Description
Timestamp	Reception time of a SOME/IP packet
Session ID	A unique identifier for the session
Return Code	A signal whether a request was successfully been processed
Source Port	The port number of a source device.
Destination Port	The port number of a destination device
Source MAC	The MAC address of a source device
Destination MAC	The MAC address of a destination device
Service ID	A service identifier
Method ID	A method, event or field identifier
Client ID	A unique identifier for the calling client inside the ECU

Fig. 2 Experimental setup.

tracted by using Recursive Features Elimination with Cross-Validation (RFECV) [7]. Table 1 shows the selected features for detection of DoS, MFA and Replay attacks. These features are composed of the selected information from the header of SOME/IP packets and the timestamp that indicates the reception time of SOME/IP packets.

3.3 Intrusion Detection System

The proposed IDS adopts two machine learning models, a Random Forest (RF) model and a RNN model.

4. Evaluation

4.1 Environment Setup

Figure 2 shows our experimental setup. We used two Raspberry Pi 3B devices (Ubuntu MATE 16.04) as a server and a client, respectively. Raspberry Pi 4 device (Kali Linux) was used as an attacker, and a virtual machine (Ubuntu 16.04) was used to generate normal SOME/IP traffic. We implemented an attack tool supporting DoS, MFA, and Replay attack modules and evaluated the proposed IDS against these attacks. The attack detection results were validated by using K-fold cross-validation.

4.2 Experiment Results

To compare the accuracy between the existing SOME/IP IDS [3] and the proposed IDS, we measured the F1-score of each model by using the attack dataset generated from our experiment environment. The experimental results are

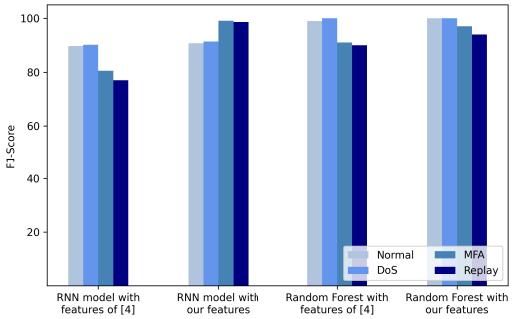

Fig. 3 Comparison between [3] and our model.

as shown in Fig. 3. Compared with the RNN-based IDS using 15 features of [3], it was confirmed that the detection rate of the proposed RNN-based IDS using 10 features is high by about 10%, 11%, and 13% for the three attacks, respectively.

Likewise, in the comparison of RF-based IDSs, the proposed 10 features-based IDS showed higher F1-scores than the RF-based IDS using 15 features of [3] for MFA and replay attacks. However, for the DoS attack, the F1-score of ours was about 4% lower than that of the existing method. With this experiment, we confirmed that our features are more useful for dealing with the proposed attacks.

5. Conclusion

In this paper, we introduce three SOME/IP attacks and propose 10 features used for SOME/IP IDS.

References

[1] AUTOSAR, "SOME/IP protocol specification," 2016. https://www.autosar.org/fileadmin/user_upload/standards/foundation/21-11/AUTOSAR_PRS_SOMEIPProtocol.pdf
[2] M. Iorio, M. Reineri, F. Risso, R. Sisto, and F. Valenza, "Securing SOME/IP for in-vehicle service protection," IEEE Trans. Veh. Technol., vol.69, no.11, pp.13450–13466, 2020.
[3] N. Alkhatib, H. Ghauch, and J.-L. Danger, "SOME/IP intrusion detection using deep learning-based sequential models in automotive ethernet networks," 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp.0954–0962, IEEE, 2021.
[4] M. Komisarek, M. Pawlicki, R. Kozik, and M. Choraś, "Machine learning based approach to anomaly and cyberattack detection in streamed network traffic data.," J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., vol.12, no.1, pp.3–19, 2021.
[5] J.J. Hopfield, "Neural networks and physical systems with emergent collective computational abilities," Proc. National Academy of Sciences, vol.79, no.8, pp.2554–2558, 1982.
[6] S. Jeong, B. Jeon, B. Chung, and H.K. Kim, "Convolutional neural network-based intrusion detection system for AVTP streams in automotive Ethernet-based networks," Vehicular Communications, vol.29, 100338, 2021.
[7] I. Guyon, J. Weston, S. Barnhill, and V. Vapnik, "Gene selection for cancer classification using support vector machines," Machine Learning, vol.46, no.1, pp.389–422, 2002.