A New Attack Dataset for CAN Intrusion Detection Systems

MinJeong Kang*, Jiwoo Shin, Hyunghoon Kim, Yeongjae Seo, and Hyo Jin Jo

Soongsil University, Seoul, South Korea
{codeliq, sy9254, axolotl0210, hyojinjo86}@gmail.com,ssyyjj1012@naver.com

Abstract

As the automotive industry has evolved in recent years, various IT technologies have been applied to vehicles. Consequently, real-world cyber attacks targeting these systems have emerged. To address these threats, in-vehicle intrusion detection systems (IDS) have been being studied. However, the existing CAN attack datasets have limitations in terms of the variety of attack types they cover, which introduces limitations in evaluating IDS performance. Therefore, in this poster, we propose a new CAN dataset including novel attack types to facilitate the evaluation of IDS for automotive network security.

Keywords: Control Area Network(CAN), Dataset for Intrusion Detection System, Security

1 Introduction

In 1983, the CAN protocol was developed by Bosch in Germany, and it is currently widely used as the communication protocol for internal automotive networks. As vehicle technology has advanced, modern vehicles are equipped with more ECUs, and connected to various telematics devices for efficient communication. This has increased the attack surface of vehicles, leading to various instances of vulnerabilities being exploited in real-world vehicles. Consequently, research into IDS to detect and mitigate threats to vehicles is actively underway. However, the scope of datasets available for IDS development is currently limited.

Representative existing attack datasets include OTIDS[1] and SynCAN[2] which mainly contain periodic CAN message-based attack scenarios. An IDS trained on such limited datasets may face challenges in effectively detecting attacks involving aperiodic messages that could occur in real-world situations.

Therefore, in this poster, we introduce two types of attacks that can occur in vehicles and propose a dataset with new attack scenarios for reliable IDS technology.

2 Our Approach

In a CAN network, there are two types of CAN message transmission: periodic messages and aperiodic messages, which are sent when certain events occur. As shown in Figure 1, the new dataset we propose covers aperiodic message-based attacks known as PE attack and another type of attack called Bus-off attack[3], which can occur in vehicular networks.

Firstly, PE attack utilizes PE(Periodic-and-on-Event) messages, which combine periodic messages and aperiodic event messages. In a PE attack, these PE messages can be spoofed to trigger unintended events like controlling the vehicle's doors or activating emergency signals.

The 7th International Conference on Mobile Internet Security (MobiSec'23), Dec. 19-21, 2023, Okinawa, Japan, Article No.P-5

*Corresponding author: Soongsil University, Seoul, 06978, Republic of Korea, codeliq@gmail.com

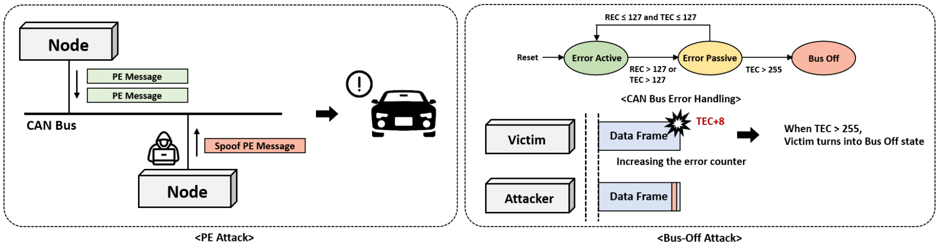

Figure 1: Examples of CAN Attack

Next, Bus-off attack exploits vulnerabilities in the design of the CAN protocol. When errors are continuously detected by the error-handling mechanism of the CAN protocol, the node with the error enters a ”Bus-off” state. Exploiting this, an attacker can intentionally trigger a crash by repeatedly sending data frames. When a crash is detected, the victim node’s TEC(Transmit Error Counter) continues to increment according to their mechanism, transitioning into Bus-off mode when it exceeds a certain threshold, rendering it unable to participate in communication.

This newly collected CAN dataset covers a wider range of attack scenarios compared to existing datasets. Therefore, when utilized in vehicular Intrusion Detection Systems, it contributes to the detection of a wider attack surface.

3 Conclusion

In this poster, we propose a new CAN attack dataset including PE attack and Bus-off attack to evaluate CAN IDS. In our experiments, we evaluated the existing IDS trained based on periodic messages with this dataset and observed low detection rates for new types of attacks. Thus, there is a need for research on IDSs that can detect a wider range of attacks, and we expect that this dataset will help to improve the performance and effectiveness of IDSs, ultimately leading to a higher level of security for vehicles.

Acknowledgement: This work was supported by the Technology Innovation Program (P0023522, HRD Program for Industrial Innovation) funded By the Ministry of Trade, Industry & Energy(MOTIE, Korea)

References

[1] Jeong S.H. Lee, H. and H.K. Kim. Otids: A novel intrusion detection system for in-vehicle network by using remote frame. In *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, pages 55–5709. IEEE, 2017.

[2] Strauss T. Dormann K. Hanselmann, M. and H. Ulmer. Canet: An unsupervised intrusion detection system for high dimensional can bus data. *IEEE Access*, 2020.

[3] K. T. Cho and K. G. Shin. Error handling of in-vehicle networks makes them vulnerable. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1044–1055. ACM, 2016.