A study on CAN Communication Security Software Design Using Intrusion Alert Messages*

Minyoung Chang and Samuel Woo†
Dankook University, Gyeonggi-do, South Korea
{min311, samuelwoo} @dankook.ac.kr

Abstract

The Controller Area Network (CAN) is essential for in-vehicle communication but remains vulnerable to spoofing attacks. This study proposes a lightweight Alert–Delay mechanism that detects spoofed identifiers and mitigates their effects through intrusion alerts and brief message delays. The method operates entirely in software, requiring no modifications to the CAN protocol or hardware, supporting automotive cybersecurity and enabling simple intrusion detection system (IDS) deployment.

1 Introduction

The Controller Area Network (CAN) serves as the primary communication bus in modern vehicles but lacks built-in authentication and encryption, making it susceptible to spoofing attacks. Existing defenses like cryptographic or hardware-based methods improve security but require protocol or hardware changes, limiting practical use. This study presents a lightweight, software-based defense that preserves CAN compatibility while effectively detecting and mitigating spoofed messages.

2 Mechanism and Research Result

The proposed Alert-Delay mechanism prevents spoofed CAN messages from affecting control variables while maintaining full compatibility with the existing CAN protocol. Operating entirely at the software level, it can be applied to legacy ECUs without any hardware or protocol modification.

Each legitimate node maintains an expected identifier listfor valid messages. When a received frame carries an unexpected or duplicated ID, it is identified as a spoofing attempt. The detecting node immediately sends an intrusion alert frameusing the reserved identifier (ID:0), embedding the spoofed ID in its data field to notify other nodes. Upon receiving the alert, legitimate nodes delay the processing of incoming messages for a short predefined period (microseconds to milliseconds), during which spoofed frames are ignored, effectively isolating the malicious transmission. This cooperative delay mitigates the spoofing impact on control logic while maintaining normal communication flow.

* Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-48, December 16-18, 2025, Sapporo, Japan.
† Corresponding author

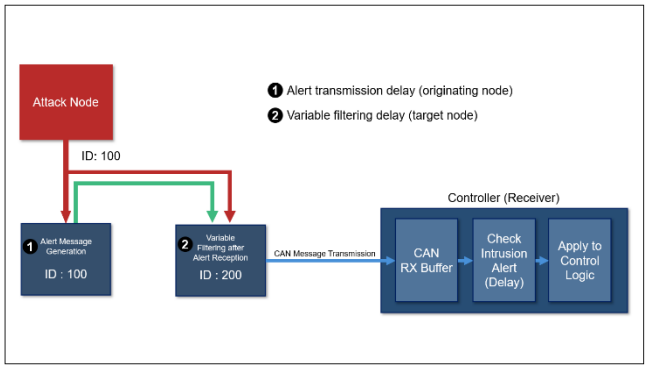

Figure 1: Alert-Delay Mechanism for Spoofing Attack Mitigation

Both Vector CANoe simulations STM32 hardware tests demonstrated stable performance with negligible communication overhead. The measured transmission delays closely matched theoretical values, confirming the method's real-time feasibility across various CAN bitrates.

Bitrate (kbps)	Calculated Delay (ms)	Measure Delay (ms)
125	0.704	0.70
250	0.352	0.35
500	0.176	0.18
1000	0.088	0.09

Table 1: Delay Comparison by Bitrate

3 Conclusion

This paper presented a lightweight spoofing defense mechanism for CAN communication. The proposed approach detects spoofed identifiers and coordinates a brief delay-based response using existing CAN functionalities. Because it requires only minimal software modification and no protocol or hardware changes, it offers a practical and cost-efficient solution for enhancing security in both legacy and next-generation vehicles.

Acknowledgements

This work was supported by the Technology Innovation Program (20022229, Development of security evaluation technology for internal network and wireless software updates of autonomous driving systems) funded by the Ministry of Trade, Industry Energy (MOTIE, Korea)

References

[1] Woo, Samuel, Hyo Jin Jo, and Dong Hoon Lee. "A practical wireless attack on the connected car and security protocol for in-vehicle CAN."IEEE Transactions on intelligent transportation systems16.2 (2014): 993-1006.

[2] Levy, Efrat, et al. "CAN-LOC: Spoofing detection and physical intrusion localization on an in-vehicle CAN bus based on deep features of voltage signals."IEEE Transactions on Information Forensics and Security18 (2023): 4800-4814.
[3] Yang, Yun, Zongtao Duan, and Mark Tehranipoor. "Identify a spoofing attack on an in-vehicle CAN bus based on the deep features of an ECU fingerprint signal."Smart Cities3.1 (2020): 17-30.
[4] Lu, Zhaojun, et al. "LEAP: A lightweight encryption and authentication protocol for in-vehicle communications."2019 IEEE Intelligent Transportation Systems Conference (ITSC). IEEE, 2019.