A Proposal for a Method to Detect Malicious Nodes Using CAN ACK-Bit Voltage*

Dongwon Lee[1] and Samuel Woo[1†]

Dankook University, Yongin-si, Gyeonggi-do, South Korea
ldw@dankook.ac.kr

Abstract

This paper presents a physical-layer method to detect unauthorized ECU insertion and wire-harness faults in CAN networks. The method analyzed ACK-bit voltage characteristics and confirmed that the voltage increases with node count. A CAN bus testbed was built, and ACK-bit voltages were measured while incrementally adding nodes. The results confirmed the effectiveness of the proposed method, and future work will focus on developing a low-cost MCU-based voltage measurement tool for in-vehicle implementation.

Keywords— Controller Area Network (CAN), Physical Layer Security, In-Vehicle IDS, ACK-bit Voltage

1 Introduction

The Controller Area Network (CAN) is the most widely used in-vehicle communication protocol for real-time data exchange among Electronic Control Units (ECUs). However, CAN lacks fundamental security mechanisms such as encryption and authentication, making it difficult to detect unauthorized ECU insertion or wire-harness tampering using only the data link layer[**?**]. Since message identifiers (CAN IDs) merely determine frame priority without authenticating the sender, attackers can connect unauthorized ECUs and inject spoofed frames that appear legitimate on the network.[**?**]. To overcome this limitation, this study focuses on the ACK bit in the physical layer—the short interval where all receiving nodes drive a dominant level to acknowledge an error-free frame[**?**]. By analyzing the voltage characteristics of this interval, we aim to leverage physical-layer variations to verify network integrity[**?**].

2 Experiment and Results

A CAN bus testbed was built to emulate a realistic in-vehicle network, as shown in Fig. 1. The setup employed a two-wire twisted pair (CAN_H and CAN_L) with 120 Ω termination resistors at both ends. Each node comprised an Arduino Uno with a CAN Bus Shield V2.0 powered by a 12V battery, and the differential voltage (CAN_H − CAN_L) was measured using an oscilloscope. Starting with two nodes, one was added at a time while measuring the ACK-bit voltage. For each configuration, ten measurements were taken to calculate the mean peak voltage and analyze its variation with node count.

The results showed that the mean ACK-bit voltage increased with the number of nodes (Fig. 2) because multiple receivers drive the bus simultaneously, causing their voltages to overlap. As

*Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-47, December 16-18, 2025, Sapporo, Japan.

†Corresponding author: samuelwoo@dankook.ac.kr

the node count grew, a saturation region appeared where the voltage increases became gradual due to the transceivers' internal resistance and current limits. These findings confirm that the ACK-bit voltage correlates directly with the number of connected nodes and can be used to estimate node count or detect anomalies such as unauthorized ECU insertion.

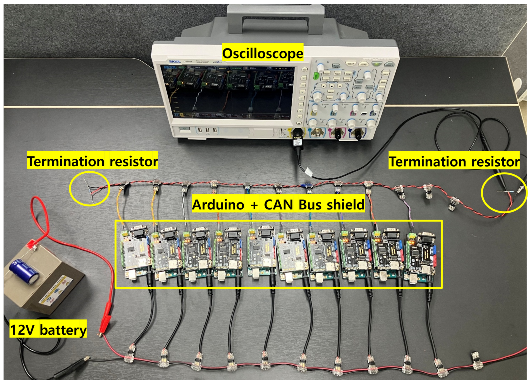

Figure 1: Experimental setup

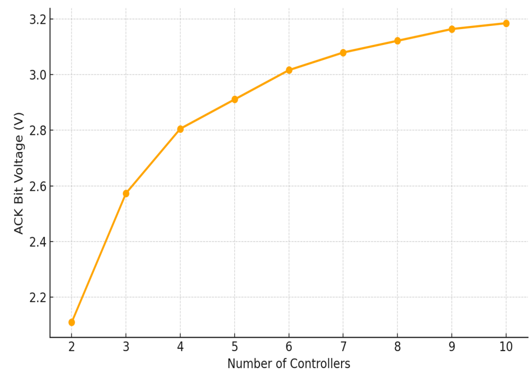

Figure 2: ACK-bit voltage vs. nodes

3 Conclusion and Future Work

A CAN bus testbed emulating a real vehicle environment was constructed, and the ACK-bit voltage was measured according to the number of connected nodes to verify the feasibility of detecting unauthorized ECU insertion and wire-harness faults. The results confirmed that the ACK-bit voltage consistently increased with the number of connected nodes, demonstrating the validity of the proposed detection approach.

Although the measurements were performed using a high-performance oscilloscope, future work will focus on developing a low-cost MCU-based board for real-time in-vehicle implementation. As the ACK-bit voltage converged with an increasing number of nodes, future work will aim to develop a circuit capable of distinguishing subtle voltage differences more precisely and improving detection accuracy.

Acknowledgments

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 and Energy (MOTIE, Korea).

References

[1] Kazuki Iehira, Hiroyuki Inoue, and Kenji Ishida. Spoofing attack using bus-off attacks against a specific ecu of the can bus. In *Proceedings of the 2018 IEEE 15th Annual Consumer Communications and Networking Conference (CCNC)*, pages 1–4. IEEE, 2018.

[2] Hyo Jin Jo and Wonsuk Choi. A survey of attacks on controller area networks and corresponding countermeasures. *IEEE Transactions on Intelligent Transportation Systems*, 23(7):6123–6142, 2022.

[3] Pal-Stefan Murvay and Bogdan Groza. Tidal-can: Differential timing based intrusion detection and localization for controller area network. *IEEE Access*, 8:68895–68912, 2020.

[4] Dominique Paret. *Multiplexed Networks for Embedded Systems: CAN, LIN, Flexray, Safe-by-Wire*. Wiley, may 2007.