Poster: Exploring CAN Ringing for ECU Fingerprinting

Ashton McEntarffer*, Kevius Tribble*, Linxi Zhang†, Mert D. Pesé*
*Clemson University †Central Michigan University
{amcenta, jjtribb, mpese}@clemson.edu
zhang15l@cmich.edu

Introduction. In a world where vehicles are increasingly connected, the vulnerability of the Controller Area Network (CAN), crucial for in-vehicle communication yet lacking built-in security, becomes a paramount concern. Detecting an unauthorized Electronic Control Unit (ECU) as early as possible can help in alleviating wide-ranging CAN injection attacks that have the potential to make the vehicle misbehave [1]. This poster introduces a novel method for voltage-based ECU fingerprinting utilizing CAN ringing. It can be usually observed at bit transitions and consists of voltage oscillations which gradually attenuate to a constant level. Unlike other existing methods [2], [3], this method considers low-entropy parts from each CAN frame (*ringing envelope*), striking a balance between reduced computational demands and accuracy. Additionally, this method not only verifies legitimate ECUs, but also effectively identifies intrusions from external devices. We evaluated the proposed method on a prototype testbed with Arduinos, demonstrating its potential for practical application in in-vehicle network security.

CAN Ringing. The ringing envelope of a CAN bit refers to the transient oscillation or resonance that occurs immediately following a transition from one state (e.g., low voltage) to another (e.g., high voltage). This phenomenon is characterized by a series of decaying oscillations around the new steady-state value. It is caused by the physical properties of the electronic circuitry, such as capacitance and inductance, which resist sudden changes in voltage. The ringing envelope typically attenuates to the steady-state value of the bit over a period of time. CAN ringing is depicted in Fig. 1. As summarized in Table I, the ringing envelope has a smaller Shannon entropy compared to the steady state of the bit. This means that the ringing envelope contains *more uniqueness* which can be used for more accurate fingerprinting of the ECU.

TABLE I
ENTROPY DATA FOR ALL ECUS

	CAN_H Ringing	CAN_H Steady	CAN_L Ringing	CAN_L Steady
Mean	10.59	15.69	9.54	15.72

Methodology. The fingerprinting process consists of ringing envelope extraction, followed by feature extraction and model training. Ringing envelope extraction consists of identifying dominant-zero bits, fitting an exponential decay curve from the beginning of the bit to the end, and marking the point from the beginning of the bit to the point where the derivative of the fitted curve reaches below a defined constant. A similar process

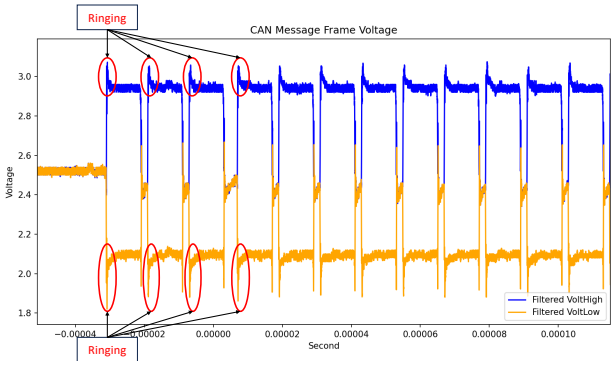

Fig. 1. CAN frame voltage showing CAN ringing at bit transitions

is applied to both CAN-High and CAN-Low voltage readings. After the ringing envelopes of each ECU are extracted, the following six voltage features are extracted: Mean, Standard Deviation, Mean Deviation, Root Mean Square, Maximum, and Minimum. These features are then used to train and test a Random Forest model to identify their source ECUs.

Preliminary Results. In our experiment, we used 9 CAN shield-equipped Arduino Unos, with each Arduino transmitting a unique CAN ID. The voltage data acquisition was performed by a Siglent SDS 1202X-E oscilloscope. Table II summarizes the precision, recall, and F1-Score of our proposed fingerprinting technique for each ECU on the CAN bus.

TABLE II
PRELIMINARY PERFORMANCE RESULTS

ECU	1	2	3	4	5	6	7	8	9
Precision	0.86	0.90	0.77	0.75	0.84	0.72	0.79	0.81	0.82
Recall	0.86	0.83	0.79	0.67	0.82	0.76	0.62	0.83	0.92
F1-Score	0.86	0.87	0.78	0.71	0.83	0.74	0.69	0.82	0.87

Future Work. Machine learning-based classification will be fine-tuned to obtain better performance results comparable to state-of-the-art algorithms. Detection latency will be benchmarked since it is a crucial metric for *online* (i.e., real-time) testing of the algorithm on the Arduinos. If the detection latency is too large, the attack will not be detected in time. Since we are processing less data compared to existing work, the overall detection latency is expected to be smaller.

REFERENCES

[1] M. D. Pese, "Bringing practical security to vehicles," Ph.D. dissertation, 2022.
[2] Y. Xun, Z. Deng, J. Liu, and Y. Zhao, "Side channel analysis: A novel intrusion detection system based on vehicle voltage signals," *IEEE Transactions on Vehicular Technology*, 2023.
[3] Y. Xun, Y. Zhao, and J. Liu, "Vehicleeids: A novel external intrusion detection system based on vehicle voltage signals," *IEEE Internet of Things Journal*, vol. 9, no. 3, pp. 2124–2133, 2021.

Symposium on Vehicles Security and Privacy (VehicleSec) 2024
26 February 2024, San Diego, CA, USA
ISBN 979-8-9894372-7-6
https://dx.doi.org/10.14722/vehiclesec.2024.25023
www.ndss-symposium.org