Review of PhD Dissertation “New Methods for Security and Privacy of CAN Bus Communication”by András Gazdag

Dr. Zhendong Ma

Luxoft/DXC Technology, Munich, Germany
zhendong.drma@dxc.com
December 11, 2023

Review comments

CAN bus is a 40 years old technology and is still widely used in the automotive industry today. As a matter of fact, CAN bus will be continually used in next generation vehicle architecture designs, which gives it at least another 10 to 20 years of shelf time. CAN bus was designed for robustness and simplicity of wiring in mind. Security was never a “by-design” consideration. With the emergence of connected and software-defined vehicle as well as autonomous driving, security of CAN communication becomes a very relevant and critical issue of modern vehicles. András' research has looked into some of the possibilities to address the security and privacy challenges related to CAN bus communication.

The author gives motivation of his work on security and privacy of CAN communication in Chapter “Introduction” and states that the focus of the work is for “a retrospective communication data analysis for future cyber attack analysis” and “track the movement of vehicles” using data from CAN communication. This gives a clear definition of the scope of the dissertation. The chapter ends with an overview of the structure of the dissertation, which helps a reader to get oriented for the rest of the dissertation.

The introduction has described the problem space. I think as the first chapter, it is important to also consider the following points:

- With all the cybersecurity challenges of automotive systems, why the author chose CAN communication as the focus area?
- What are the research questions of the dissertation?
- What are the expected outcome of this research? In other words, what are the research goals?
- What research methodology has been used to carry out this work?

Chapter 1 “CAN bus” and Chapter 2 “Attack against the CAN bus” define the system and threat model of CAN communication, which give a clear picture of the target to be protected and threats considered in the following work. The threats against CAN communication include DoS attack (CAN ID based DoS and physical DoS by forcing CAN_H and CAN_L into dominant state), message injection attack, and message modification attack. Particularly, Chapter 2.3 “Message modification attacks” goes into details of the design and implementation of a CAN Gateway device to launch Man-in-the-Middle (MitM) attack on the payload of CAN messages. Chapter 2.4 “CrySyS dataset of CAN traffic logs” describes the collection and the method for modifying CAN data to generate simulated attack data set. The Proof-of-concept of attacks on CAN bus and realistic dataset can be a great contribution to enable the research community to develop and test solutions to secure CAN communication.

For Chapter 1 and 2, I have the following comments:

- Is the work presented in Chapter 2.3 and Chapter 2.4 the author's own contribution? From the description, it is not clear. If so, why it is not included in the “Summary of new results”?
- The statement “the CAN bus does not support any kind of cryptographic message authentication” in Chapter 2.2 is not consistent with the description of CAN security measures in Chapter 4.1. Besides, Secure On-board Communication (SecOC) is a technical standard defined by AUTOSAR and it is implemented in some vehicle types.

- The E/E architecture of modern vehicles are typically divided into domains, e.g. powertrain, chassis, body, connectivity, infotainment, ADAS etc. ECUs within the same domain share and communicate on the same CAN bus. A central gateway ECU filters and routes CAN communication among ECUs across different domains. Because central gateway "routes" CAN messages, many CAN messages do not appear on OBD-II port, which is connected to the gateway for diagnostics or emission reading. I would consider this fact as a limitation of the CAN data captured from OBD port. The implication is that some of the critical CAN messages generated during vehicle operation cannot be captured by an OBD dongle, which limits the coverage of the proposed approaches in this research. Although academic research might not have the access to industry proprietary or internal knowledge of automotive systems, this limitation can be mentioned in the dissertation to give a reader a complete picture.

- CAN signals are date points encoded in CAN payload. DBC files are typically used to define how the CAN signals are encoded. DBC are often required in the implementation of commercial in-vehicle IDS solution to interpret the meaning and value of signals. This industry specific topic might not be obvious to academic research. However, additional information can be added to explain the concept of CAN signal (Cf. `https://docs.openvehicles.com/en/latest/components/vehicle_dbc/docs/dbc-primer.html`).

- One minor comment. Reference [SEC15] and [SEC16] should include the number and edition of the ISO standard, e.g. ISO 11898-1:2015. "ISO Central Secretary" is not the right way to refer a international standard.

Chapter 3 "Semantic compression of CAN traffic" presents a semantic compression algorithm on CAN communication data and shows a 10% compression rate in binary format or up to around 5% if syntactic compression is combined. The approach is evaluated on the criteria of run-time complexity, compression ratio, and correctness. As CAN communication is largely periodic in nature, I think the proposed approach might be plugged into the automotive Intrusion Detection System (IDS) or forensic analysis workflow to reduce the storage and transmission overhead.

Chapter 4 "Anomaly detection" contains the main contribution of this dissertation on the detection of cyber attacks on CAN bus. The focus of the author's work is on the detection of CAN message injection and modification attacks. The author proposed three approaches for detecting attacks based on compressed CAN data: message frequency based, signal correlation based, and anomaly detection of signals using neural network algorithm TCN. For detection based on message frequency, the evaluation shows that it is effective to identify injected CAN messages. As for the next step, the author proposes to use a model-based anomaly detection algorithm to correlate the signals in CAN message payload. This is a more interesting approach comparing to counting CAN message with same IDs because it goes one step further to inspect the message payload. The author defines seven signal modification scenarios and evaluates the proposed algorithm on synthesized data. The result shows that the detection rate is above 55% and in some case, 100%. The TCN-based anomaly detection is an extension of anomaly detection without the need of fully understanding the CAN payload semantics. Applying TCN algorithms to anomaly detection of CAN communication is an interesting experiment. The main evaluation of this approach is based on the comparison to the INDRA model published by Kukkala *et al.* The author shows that his approach has slight improvement in terms of accuracy and false positive.

- In recent years, a large amount of papers have been published on the topic of detection of cyber attacks in and to vehicles, e.g. "Fingerprinting Electronic Control Units for Vehicle Intrusion Detection" by Cho and Shin (cited as [CS16] for attacks but not for detection), "Context-aware Intrusion Detection in Automotive Control Systems" by Wasicek *et al.*, or "A Structured Approach to Anomaly Detection for In-Vehicle Networks" by Mueter *et al.*, just to name a few. Although a systematic literature review might not be a mandatory part of the dissertation, I think it would be good to include more discussions of State-of-the-Art and to have more comparison of the author's approach to existing ones.

Chapter 5 "Privacy problems" addresses privacy of CAN data against location tracking algorithm. The author proposed a microtracking algorithm to reconstruct vehicle trajectories from CAN data, which effective defeats data distortion technique used for protecting user privacy.

- I assume that it is a cumulative dissertation. However, Chapter 5 gives me the impression that it is a little isolated and offbeat from the rest of the dissertation. The author should work on the motivation and transition to ensure that this chapter on privacy is consistent with the overarching research goals of the dissertation.

General comment

In summary, from a positive side, this dissertation is based on a collection of the author's research papers published in security, information and vehicle technology workshops, conference, and journals. Nine out of ten publications have the author as the first author, indicating a significant individual contribution from the author to the research work. The research topic of detection of automotive cyber attacks is relevant and very timely, as cybersecurity monitoring becomes mandatory for all new vehicle type approvals by UNECE R155 (Cf. R155 §7.3.7). The dissertation presents the author's work on cyber attacks and detection, which will benefit the research community to continue the on-going quest to find a cos-effective way to protect the legacy CAN bus communication. Furthermore, evaluations are provided for all the proposed approaches to demonstrate the effectiveness.

For things that I think András can improve on are given in the review comments in each chapter. The most important things from my perspective include: clearly formulated research questions, more discussion of the State-of-the-Art. Last but not least, it would be good to include a discussion and future work section for the whole dissertation to clearly state the limitation of the work and the author's opinion for future research.

With these considerations in mind, I regard the dissertation has reached the level that can proceed to public defense.

Reviewer: ____
Dr. Zhendong Ma