

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

Dr. Zhendong Ma

Luxoft/DXC Technology, Munich, Germany

zhendong.drma@dxc.com

April 8, 2024

## Open problems

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.

## Summary of novel scientific results

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.

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 can 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 cases, 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 new approach. 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 a slight improvement in terms of accuracy and false positive.

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 effectively defeats data distortion technique used for protecting user privacy.

### **The significance and application of the results**

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) in Europe in 2024. 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 cost-effective way to protect the legacy CAN bus communication in an increasingly open vehicle environment. Furthermore, evaluations are provided for all the proposed approaches to demonstrate the effectiveness.

### **References**

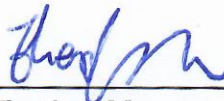
In summary, this dissertation is based on a collection of the author's research papers published in security, information and vehicle technology workshops, conference, and journals. Nine out of ten publications have the author as the first author, indicating a significant individual contribution from the author to the research work.

### **Reviewer's statement**

András has addressed all my questions and comments from the previous review round during and after the department defense and made changes in the final version of the dissertation accordingly.

With the above considerations, I regard the dissertation has reached the level for public defense.

Reviewer: \_\_\_\_\_



Dr. Zhendong Ma