Perspective
Volume 12:3, 2023

Telecommunication System and Management

ISSN: 2167-0919

Open Access

A System that can Detect Cyberattacks on Powertrain Cyber Physical Systems across Multiple Disciplines

Dario Stabili*

Department of Computing, Macquarie University, Sydney, Australia

Abstract

With the advent of external connectivity in modern automobiles, security experts from academia and the business world grappled with the problem of external communication interfaces exposing internal networks used to control vehicle systems. With the introduction of cellular connectivity, proof-of-concept and demonstrations of remote takeover of the vehicle have been shown, raising awareness about the risks associated with the introduction of external connectivity on the vehicle system, despite the fact that these issues are thought to have little to no impact on the functioning of the vehicle itself due to their requirement of a physical connection. Security researchers demonstrated that a number of flaws in the Controller Area Network (CAN), one of the most widely used in-vehicle communication protocols, could be exploited in all of these remote attacks. In these works, the authors show how to put people inside and outside of modern vehicles in danger by using drive-by-wire features. Several researchers developed algorithms to prevent the injection of malicious CAN messages in order to address this issue. However, these solutions only focus on CAN communication and do not take into account all of the other subsystems that an attacker could use to hijack the vehicle system.

Keywords: Cyberattacks • Powertraincyber • Physical systems • Detection system • Cybersecurity

Introduction

The incorporation of microcontrollers into contemporary automobiles has sparked the development of new safety and comfort-enhancing features by automobile manufacturers. Electronic Control Units, which are connected to the vehicle's mechanical components and communicate with one another through a variety of communication networks, are the microcontrollers that are used to implement these features. The Controller Area Network, developed by Bosch GmbH in the early 1990s, is one of the most widely used communication networks. Although the automotive industry has successfully implemented CAN in vehicular networks to ensure robust communication, the protocol does not provide the fundamental security guarantees required for contemporary applications. Security researchers have already demonstrated this through technical reports and white papers [2, 3] that it is widely acknowledged that vehicles can be hijacked by injecting maliciously forged messages on the CAN bus. Modern automobiles' drive-by-wire capabilities, which let messages sent over the CAN bus control the driving system, are used to carry out these attacks. The speed control, which is activated to maintain the vehicle's speed in order to reduce fuel consumption and, consequently, emissions, is an illustration of the drive-by-wire capabilities of modern automobiles. Despite the fact that these systems were developed for comfort and safety, the fundamentals needed to use them allow for targeted attacks, putting the safety of those inside and outside the vehicle in jeopardy [1].

Description

Numerous researchers and automobile manufacturers have been working to secure the CAN network by implementing intrusion detection systems, encryption, authentication, and other security measures in response to the growing concern about vehicle security. However, these solutions only address a single vehicle domain without taking the entire system into account. In fact, detection methods based on the analysis of the system state are only tested against attacks designed to modify the system state, while detection algorithms designed to detect cyber-attacks targeting the communication network of modern vehicles are only tested against attacks targeting these networks. Since the vehicle is a complicated framework formed by various interconnected frameworks, it is important to address the flexibility of network safety countermeasures against assaults focusing on various spaces to demonstrate their viability. Although the use of a hybrid approach for anomaly detection in complex cyber-physical systems has been the subject of previous research, we point out that its application to the automotive cyber-physical system is, to the best of our knowledge, still a research area that has not been investigated [2].

A multidisciplinary cyberattack detection system for the powertrain cyber physical system is presented in this work. In order to accomplish this, we developed and implemented a generic vehicle's powertrain system, which consists of a speed controller and an internal combustion engine that are connected via the Controller Area Network communication protocol. The implemented system is used to evaluate the effectiveness of selected detection algorithms against various attack scenarios and to analyze the consequences of cyberattacks. This work's contributions to the state of the art are incremental to those of the original work, which served as the foundation for this extension. The original work, in particular, made a contribution by solving the speed controller problem by designing and implementing a controller based on a model of the engine rather than a generic vehicle representation. The second commitment of the first work is the showing of the outcomes of digital assaults to the motor model, taking into account different assault situations focusing on both framework and correspondence level [3].

In addition, we present the evaluation of the performance of various anomaly detection algorithms and techniques derived from control theory and network security against the attacks that make up the threat model in this work. This is, to the best of our knowledge, the first publication to present a multidisciplinary strategy for the cyber security of an automotive CPS and to demonstrate the benefits and drawbacks of employing multiple detection methods to combat the same attacks. In addition, we demonstrate how the output of the detection framework can be used to identify both the ongoing attack and the target of the attack, which can be either the system or the communication network. This makes it possible to develop active defense mechanisms that can withstand a variety of attack scenarios [4].

Control theory and network security serve as inspiration for the various algorithms and methods that make up the detection framework that is presented in this work. We note that these solutions have already undergone independent

***Address for Correspondence:** Dario Stabili, Department of Computing, Macquarie University, Sydney, Australia, E-mail: dariostabili51@gmail.com*

Received: 01 May, 2023, Manuscript No. jtsm-23-104243; **Editor assigned:** 03 May, 2023, PreQC No. P-104243; **Reviewed:** 15 May, 2023, QC No. Q-104243; **Revised:** 22 May, 2023, Manuscript No. R-104243; **Published:** 29 May, 2023, DOI: 10.37421/2167-0919.2023.12.375

testing in their respective fields. The analysis of their behavior in a broader context and the ways in which these complementary solutions can be combined to improve their overall detection performance are the primary focuses of this work. Anomaly detectors make up the framework for detection [5].

Conclusion

A detection framework that enables detection and identification of the source of the attack is presented in this paper, along with an analysis of the consequences of cyberattacks on the powertrain system. The powertrain system consists of a speed controller designed to work with the engine model and a generic model of an internal combustion engine. The speed controller and engine model are set up to exchange can data over. There are three distinct attacks in the threat model examined in this work.

Acknowledgement

None.

Conflict of Interest

None.

References

1. Li, Bo, Ting Wang, Peng Yang and Mingsong Chen, et al. "Rethinking data center networks: Machine learning enables network intelligence." *J Commn Net* 7 (2022): 157-169.
2. Gyamfi, Eric and Anca Jurcut. "Intrusion detection in internet of things systems: A review on design approaches leveraging multi-access edge computing, machine learning, and datasets." *Sens* 22 (2022): 3744.
3. Liu, Xiao, Yuanwei Liu, Yue Chen and Lajos Hanzo. "Trajectory design and power control for multi-UAV assisted wireless networks: A machine learning approach." *IEEE Trans Veh Technol* 68 (2019): 7957-7969.
4. Linjing, Wu, Liu Xinyue and Shu Shihu. "14 Blockchain Application." Security and Trust Issues in Internet of Things: Blockchain to the Rescue (2020): 301.
5. Jhanjhi, N. Z., Mamoona Humayun and Saleh N. Almuayqil. "Cyber security and privacy issues in industrial internet of things." *Comput Syst Sci Eng* 37 (2021).

How to cite this article: Stabili, Dario. “A System that can Detect Cyberattacks on Powertrain Cyber Physical Systems across Multiple Disciplines.” *Telecommun Syst Manage* 12 (2023): 375.