2019

Survey of Automotive Controller Area Network Intrusion Detection Systems

Clinton Young
Iowa State University, cwyoung@iastate.edu

Joseph Zambreno
Iowa State University, zambreno@iastate.edu

Habeeb Olufowobi
Howard University

Gedare Bloom
Howard University

Survey of Automotive Controller Area Network Intrusion Detection Systems

Abstract
Novel attacks continue to appear against in-vehicle networks due to the increasing complexity of heterogeneous software and hardware components used in vehicles. These new components introduce challenges when developing efficient and adaptable security mechanisms. Several intrusion detection systems (IDS) have been proposed to identify and protect in-vehicle networks against malicious activities. We describe the state-of-the-art intrusion detection methods for securing automotive networks, with special focus on the Controller Area Network (CAN). We provide a description of vulnerabilities, highlight threat models, identify known attack vectors present in CAN, and discuss the advantages and disadvantages of suggested solutions.

Keywords
Controller area network, in-vehicle network, intrusion detection system

Disciplines
Electrical and Computer Engineering

Comments
This is a manuscript of an article published as Young, Clinton, Joseph Zambreno, Habeeb Olufowobi, and Gedare Bloom. "Survey of Automotive Controller Area Network Intrusion Detection Systems." *IEEE Design & Test* (2019). DOI: 10.1109/MDAT.2019.2899062. Posted with permission.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/MDAT.2019.2899062, IEEE Design and Test

Survey of Automotive Controller Area Network Intrusion Detection Systems

Clinton Young, Joseph Zambreno
Department of Electrical and Computer Engineering
Iowa State University
Ames, Iowa 50011

Habeeb Olufowobi, Gedare Bloom
Department of Electrical Engineering and Computer Science
Howard University
Washington, D.C. 20059

***Abstract*—Novel attacks continue to appear against in-vehicle networks due to the increasing complexity of heterogeneous software and hardware components used in vehicles. These new components introduce challenges when developing efficient and adaptable security mechanisms. Several intrusion detection systems (IDS) have been proposed to identify and protect in-vehicle networks against malicious activities. We describe the state-of-the-art intrusion detection methods for securing automotive networks, with special focus on the Controller Area Network (CAN). We provide a description of vulnerabilities, highlight threat models, identify known attack vectors present in CAN, and discuss the advantages and disadvantages of suggested solutions.**

I. Introduction

The continued integration of Internet-of-Things technologies and demonstrated cyber attacks on automotive in-vehicle networks [1]–[3] motivate a need for automotive cyber security. Network-based attacks are relatively recent in automobiles; due to the introduction of interconnectivity in modern vehicles. As depicted in Fig. 1, modern vehicles contain multiple interfaces that expose the vehicle to cyber-attacks. With the future emergence of fully autonomous vehicles, the need for securing automobiles will greatly increase. These vehicles must behave securely, predictably, and reliably. Automotive cyber attacks can result in catastrophic consequences, including the loss of human life.

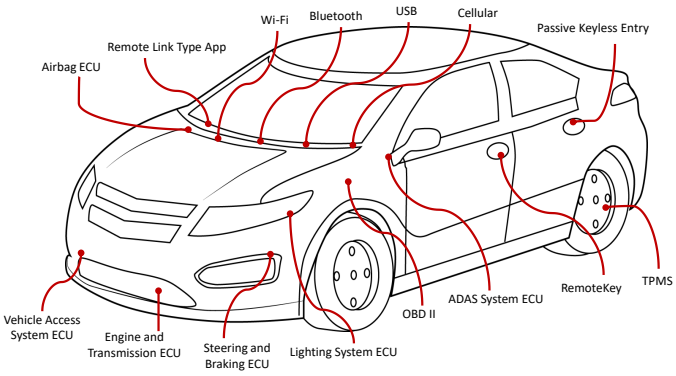

Fig. 1. Automotive attack surfaces.

One option to enhance the security of in-vehicle networks is to adopt intrusion detection and prevention techniques. Intrusion Detection Systems (IDS) are used to mitigate intrusions in computer network systems. However, many traditional techniques in network security cannot be directly applied to vehicular networks. Thus, an effective and efficient IDS that can work for in-vehicle networks is an important need.

In this paper, we explore the methods and approaches researchers have taken to identify threats against vehicles and how to address them with IDS approaches. Our main contribution, is to unify the assumptions, threat models, and terminology used in the research area of automotive IDS.

II. Vulnerabilities and Threats

A. Vulnerabilities of CAN

CAN is an asynchronous, serial, multi-master communication network protocol that connects Electronic Control Units (ECUs) [4]. Vehicles, airplanes, and industrial machinery utilize CAN to reduce network complexity and wiring costs. The CAN architecture was envisioned to be lightweight and robust and designed to be unsegmented, unencrypted, and lacking authentication so that CAN messages could flow freely to and from each ECU. However, these properties directly lead to CAN's security vulnerabilities:

1) Lack of Message Authentication: Each ECU broadcasts and receives all data on the CAN bus then decides whether messages are meant for them. CAN by design is unable to prevent unauthorized devices from joining the bus and broadcasting malicious messages to all the ECUs. By accessing the bus, hackers can send spoofed messages to any ECU on the network. Security in this context is provided only through a lack of open documentation. A hacker needs to dedicate time and resources to reverse engineer the CAN protocol before being able to launch malicious attacks on a particular vehicle.

2) Unsegmented Network: All ECUs are connected to a common network. This is a major reason CAN was adopted in automotive networks, to reduce the needed wiring for point-to-point connections between the various subsystems. However, this reduction means a system component dealing with infotainment can communicate to safety-critical vehicle subsystems. While some manufacturers utilize some network segmentation for safety-critical systems, by design there is still cross-communication between safety-critical and non-critical systems.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/MDAT.2019.2899062, IEEE Design and Test

3) Unencrypted Messages: CAN was designed to be lightweight and robust in the 1980s, when car hacking was not a reality. At the time, the addition of encryption would only slow down CAN messages and clog the network. However, because CAN traffic is unencrypted, it can be easily sniffed, spoofed, modified, and replayed. There is a large area of research in applying encryption to automotive networks [5]–[7].

B. Threats and Attacks

Recent interest in CAN bus security has grown due to several demonstrations of security breaches in automotive systems. Koscher et al. [8] were the first to implement and demonstrate that an attacker who can infiltrate virtually any ECU can circumvent a broad array of safety-critical systems by directly interfacing with the OBD-II port. By sniffing the CAN bus network and reverse engineering ECU code, they demonstrated complete control of a wide range of functions: disabling the brakes, stopping the engine, and controlling other vehicle functions.

Checkoway et al. [1] later demonstrated that a vehicle can be exploited remotely. Previous research had shown that internal networks within vehicles are insecure, however the requirement of physical access was viewed as unrealistic. They gained access without having physical access, and attacked the vehicle over a broad range of attack vectors, including Bluetooth and infotainment systems. The authors concluded that security practices in vehicles should use similar methods as traditional networks to restrict access and improve code security.

Valasek and Miller [9] demonstrated real-world attacks on multiple vehicles via the CAN bus. The authors remotely engaged the brakes of a Jeep Cherokee while it was on a live highway and ran the vehicle into a ditch. They accomplished their attacks without having prior access to the vehicle. In response, Chrysler recalled 1.4 million vehicles.

III. Background on Intrusion Detection Systems

Intrusion Detection Systems (IDS) are software or hardware systems that automate the attack detection process, usually through the use of sensors and reporting systems. Most modern IDS monitor either the host computers or networks to capture intrusion related data [10]–[14]. We examine approaches and implementations of traditional IDS and how these principles can be applied to automotive security.

A. Host-based

A Host-based Intrusion Detection System (HIDS) resides in and monitors the host system. In automobiles, a host-based IDS would reside in individual ECUs, where it monitors the traffic packets entering and leaving, and check to ensure packets are not malicious. A HIDS would also monitor the ECU itself to detect behavior indicative of an intrusion. A practical challenge with any automotive HIDS is that unlike traditional hosts, many ECUs lack sufficient processing power. Implementing an automotive HIDS would consequently require significant ECU redesign by manufacturers.

B. Network-based

A Network-based Intrusion Detection System (NIDS) is part of the communication system and monitors all traffic traversing the network. Information monitored include header and content of each message or packet. An automotive NIDS monitors all traffic on the network with the NIDS acting as an ECU, so that it can receive and monitor all messages broadcast.

C. Intrusion Detection Methods

Intrusion detection methods can be classified under two main categories: signature and anomaly-based.

1) Signature-Based: Signature-based approaches detect attacks using a pre-defined knowledge base of attack signatures that is captured and created, and current network traffic is monitored for these signatures. This detection mechanism is effective in detecting known attacks with high accuracy and low error rates. However, signature-based IDSs cannot detect any attack not defined in the database, and therefore are unable to detect new attacks, nor any deviation from known attacks. It is critical to maintain the knowledge base and update it frequently for accurate detection.

2) Anomaly-Based: Anomaly-based intrusion detection typically starts with a training or normal model of the system's activity. To obtain best accuracy in detection, the normal model must be thorough. The IDS then compares current system's activity to past captured normal model to detect variations in behavior and label those deviations as anomalies. Any deviation not captured in the normal profile could be correctly or mistakenly identified as an intrusion. It is important to have the most complete normal profile, so the system does not suffer from high rates of false positives. The main advantage of anomaly detection is its ability to identify new and previously unknown attacks.

IV. Intrusion Detection Systems for Automotive Security

We investigate how researchers are applying traditional intrusion detection approaches to securing automotive networks. We summarize some of the cutting edge work on automotive intrusion detection in Table I and discuss their advantages and drawbacks.

A. Message Timing

In normal vehicle operation, each message ID generated by an ECU has a regular frequency. When attackers inject messages to execute a command to an ECU, this frequency will unexpectedly change. Even when an attacker is injecting messages, the ECUs still send their messages periodically. Eventually, rate of messages on the network will be increased by a factor of more than 2 to 100 times, depending on the attacker's injection speed. Miller and Valasek reported that they needed to inject at a rate of at least 20 times faster than normal for their attack to be successful [9]. Because the original ECU is still transmitting its message, an attacker needs to send in messages at a fast enough rate to overwrite the normal message with the same ID.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/MDAT.2019.2899062, IEEE Design and Test

Detection is based on the following principles.

1) When a new message is transmitted on the CAN bus, the IDS will check the ID and compute the time interval from the arrival time of the latest message.
2) If the time interval of the new message is shorter than the normal model, the IDS indicates message as an anomalous message due to this message is arriving sooner than expected.

A conceptual diagram on the effects of message injection attacks on normal traffic is given in Figure 2.

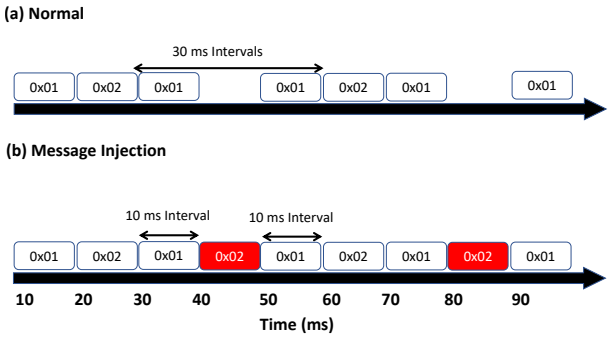

Fig. 2. Transmitted messages on CAN bus (a) under normal status and (b) under message injection attack. The time interval of message CAN ID 0x02 is shortened by the injection of attack messages. Based on Song et at. [15]

Miller and Valasek [16] introduced a concept of analyzing the rate of messages for in-vehicle network intrusion detection. The number of messages on the CAN bus is the sum of the number of normal messages and attack messages. By analyzing the distribution rate of messages, it should be possible to detect anomalous messages.

Researchers have explored utilizing message timing features for intrusion detection. These works have shown good results in using message intervals for detecting a significant threat to automotive security, message injection. Gmiden et al. [17] proposed a simple intrusion detection method for CAN bus. Their proposed algorithm does not require any modification to the CAN bus, which would mitigate changes to the native system and computational overhead, and is based on the analysis of time intervals of CAN messages. Their future work involves implementing and evaluating their proposed detection method.

Moore et al. [19] proposed an anomaly detector based on the regularity of CAN message frequency. Similar to the detection method proposed by Gmiden [17], Moore's detector relies on the time intervals of CAN messages. They observed regularity in the signal frequencies, and hypothesize that a simple anomaly detection system monitoring the inter-signal wait times of CAN bus traffic will provide accurate detection of a regular-frequency signal injection attacks. To test their detector, they defined and executed three signal injection attacks. They conclude that their approach is a promising avenue for accurate detection of an important class of CAN bus attacks.

Song et al. [15] also proposed a lightweight intrusion detection algorithm that examines the time interval of CAN messages. They evaluated how three different types of message injection attacks affect the unique time interval of each CAN ID. They combined 100 one-second samples of normal and attack data logs and then applied their IDS to determine which logs were of attacks. They determined that the time interval is a feature capable in detecting message injection attacks in CAN bus traffic by showing there was a clear difference between time intervals of messages in normal status and attack status. The strength of their proposed detection algorithm is that it is simple and efficient to use.

Utilizing the CAN message timing intervals show good detection capabilities with minimal change to the vehicle's native network. This approach using CAN message timing features has shown the most success in detecting known attacks. However, the simplicity of these methods currently limit them to detecting attacks that inject numerous messages onto the CAN bus. While the majority of demonstrated attacks have been message injection, it is conceivable that other methods of attacks exist. We examine alternative detection methods in the following sections.

B. Signature-Based

Larson et al. [20] proposed a specification-based attack detection approach that has a detector placed in each ECU. The incoming and outgoing network traffic can be analyzed based on information from the protocol stack and object directory of the CAN-protocol at the expected ECU. They show that potential attacks can be detected from the trace of extracted information through theoretical simulation. The authors inferred that a likely target for attackers is the gateway ECU because a variety of attacks can be accomplished when it is compromised. Further development in this area is likely needed.

C. Anomaly-Based

As previously mentioned, a limiting factor of implementing complex intrusion detection systems is the computing power of ECUs. ECUs come in varying complexity and sophistication from a simple seat control unit that adjusts seat height and angle to complex engine control units that control a variety of engine functions. Some of the following techniques are computationally heavy and implementing them onto automotive networks may require major redesign of the underlying components.

1) Cyber-Physical: Several researchers have proposed using innate characteristics of individual ECUs to build an alternative to timing-based IDS. Cho and Shin [21] introduced a clock-based IDS that uses clock skew (timing error) to authenticate ECUs. The IDS records communications on the CAN bus and creates fingerprints of every ECU on the network. Each ECU is assigned a fingerprint based on their specific clock skew and this is used to distinguish them. The authors proposed that by analyzing the CPU clocks behaviors, spoofing attacks can be detected in the network. A similar approach is considered by Ji et al. [22]. They investigate a detection method based on clock drift.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/MDAT.2019.2899062, IEEE Design and Test

TABLE I
COMPARISON OF PROPOSED IDSS FOR IN-VEHICLE NETWORKS

Detection Feature	Proposed System	Intrusions Detected	Evaluation
Message Frequency	Miller and Valasek (2016) [16]	Message Injection	Live Road Tests
	Hoppe (2008) [18]	Message Injection and Deletion	Testbench Simulation
Message Interval	Gmiden (2016) [17]	N/A	No Evaluation
	Song (2016) [15]	Message Injection	Live Road Tests
	Moore (2017) [19]	Message Injection	Real Vehicle Simulation
Signatures	Larson (2008) [20]	Known Attacks with Defined Signatures	Theoretical Simulation
Cyber-Physical	Cho and Shin (2016) [21]	Spoofing	Real Vehicle Simulation
	Ji (2018) [22]	Injection and Suspension Attack	Testbench Simulation
	Choi (2018) [23]	Bus-Off Attack	Real Vehicle Simulation
Entropy	Marchetti (2016) [24]	Message Injection	Real Vehicle Simulation
	Müter (2011) [25]	Various Attacks	Real Vehicle Simulation
CAN Fields	Matsumoto (2012) [26]	Message Spoofing	No Evaluation
	Markovitz (2017) [27]	N/A	Real and Simulated CAN Traffic
Sensor Data	Müter (2010) [28]	Message Injection	No Evaluation
Deep Neural Network	Kang and Kang (2016) [29]	Attacks based off Statistical Features	SW Simulation with OCTANE

Choi et al. [23] proposed VoltageIDS, a system that leverages the electrical CAN signal characteristics as a fingerprint of the ECUs. This approach does not require any modification of the vehicular system and can distinguish between errors and bus-off attacks. They evaluated their IDS on moving as well as idling vehicles. The method is shown to be capable of detecting the recently introduced bus-off attack.

2) Entropy: Entropy-based intrusion detection has been applied to traditional network-based systems, but typically has a high rate of false positives [25] due to typical traffic variance. As automotive network traffic tends to be more periodic, entropy-based detection has been shown to detect anomalies with a low rate of false-positives. Müter et al. [25], using data recorded from the in-vehicle network communication during normal operation, calculated the Shannon entropy value. Deviations from that entropy are identified as potential intrusions. Marchetti et al. [24] proposed an entropy-based algorithm for detecting anomalies in CAN messages in an unmodified vehicle. They conducted extensive evaluations based on several hours of CAN traffic captured during driving sessions on public motorways. Their experimental evaluations show that entropy-based anomaly detectors are a viable approach for identifying CAN bus anomalies caused by attackers injecting messages.

3) Message Rate: Hoppe et al. [18] proposed an anomaly-based IDS that is placed on the CAN bus so that it can listen to network traffic. Their IDS examines the rate of transmission of specific messages and compares it to what is normal to detect additional or missing messages. This approach differs from other timing-based approaches as it counts rate of transmission of packets as opposed to the timing intervals of the packets. Deviations from the expected normal number of messages transmitted are identified as anomalies. Their future work involves implementing and evaluating their proposed detection method.

4) CAN-Fields: Several works utilize the makeup and data fields of CAN messages for anomaly detection. Matsumoto et al. [26] proposed a method of preventing unauthorized data transmission in CAN. Each ECU monitors all the data on the bus, and broadcasts an error message if it recognizes spoofed messages with its own ID, before the unauthorized message is completely transmitted. Markovitz et al. [27] proposed a novel domain-aware anomaly detection system for CAN bus traffic. They discovered semantically meaningful fields through the inspection of real CAN traffic. They developed a greedy algorithm to split CAN messages into fields and classify these fields into specific types they observed. Their anomaly detection system uses classifiers to characterize the fields and build a model for the messages, based on their field types in the learning phase. In the enforcement phase, the system detects deviations from the model. They evaluated their system on simulated and real CAN traffic and achieved near zero false positives. These methods require a deeper understanding of CAN messages and reverse engineering of the messages and their data fields.

5) Other Works: Müter et al. [28] introduced an approach for anomaly detection using sensors to recognize attacks on in-vehicle networks during normal vehicle operation. The authors discussed the design and the application criteria for attack detection in the network, especially the CAN bus, without causing false positives. This detection scheme consists of eight sensors for detecting an attack. The sensors serve as a criteria for recognizing a threat to the automobile by monitoring different aspects of the network. In their proposed approach, the applicability of these sensors is based on different criteria such as the type and number of messages, the number of buses they need to access, and if the payload of the message needs inspection. The authors showed sensor data results can be evaluated and how to integrate the approach into an holistic IDS concept.

Kang and Kang [29] proposed a machine learning based IDS approach using a deep neural network structure to monitor CAN packets to extract feature bits. The IDS consists of two modules. A monitoring module that decides a type of

CAN packet based on trained features of known attacks. Once the monitoring module identifies a new attack, a profiling module records the attack model and updates the system for an upcoming packet. They reported a 99 percent detection ratio while keeping false positives under 1 to 2 percent through software simulation. However, the authors did not discuss the overhead to implement their machine learning approach on modern vehicles.

There are multiple CAN and vehicle ECU characteristics that can be leveraged for intrusion detection in vehicles. Some works [21]–[23] capture specific characteristics without requiring changes to the native vehiclular system to detect attacks. There are methods [26], [27] that require reverse engineering of the CAN system and its messages to implement an intrusion detection system. While it is difficult to determine whether which approach is better, as some have not been evaluated, the best approach to detect the most comprehensive range of attacks may be a combination of some of these works.

V. Conclusion

In this paper, we examined methods for applying IDSs to securing automotive systems with an overview of the techniques and a discussion of their advantages and disadvantages. We attempted to clarify and unify the concept of anomalies and intrusion detection regarding automotive security. This begins with identifying threat models for automotive security and identifying threats that effect all vehicles and not just one specific model. From a technical perspective, IDSs can work well for detecting intrusions on the CAN bus. Different implementations of anomaly detection methods can detect different types of anomalies. Current approaches have a focus on message injection attack detection because it is the main attack vector for hackers trying to manipulate a vehicle to misbehave. The link to the next step after detection is to enable prevention; an effective IDS for cyber-physical systems should have an active response to cyberattacks. We have identified ways for detecting attacks, but more research is needed on mitigating those attacks after detection.

The complexity of in-vehicle networks continues to increase with the introduction of other communication protocols including FlexRay, LIN, and Ethernet [30]. These new protocols introduce new vulnerabilities to vehicles. Future work should involve investigating whether the reviewed IDS approaches for CAN could be applied to these new protocols. Speculatively, some of the reviewed IDS approaches could be applied to these new networks. As research in this field continues to progress, so will the attackers and their attacks. This progression requires continual updates to threat models to identify new vulnerabilities and attacks, and subsequent adjustments to IDS to counter them. The fundamental issue remains that CAN, while inherently insecure is a modern day vehicle standard, exemplifying the need for security to be addressed throughout the design process.

About the Authors

Clinton Young (cwyoung@iastate.edu) is a graduate student pursuing a Ph.D. in Computer Engineering at Iowa State University. He is a research assistant working on automotive security.

Habeeb Olufowobi (habeeb.olufowobi@bison.howard.edu) is currently a Ph.D. candidate and a research assistant at the Embedded Systems Security Laboratory at Howard University.

Gedare Bloom (gedare@scs.howard.edu) received his Ph.D. in computer science from George Washington University. He joined the Dept. of Computer Science at Howard University as Assistant Professor and founding director of the Embedded Systems Security Lab in 2015.

Joseph Zambreno (zambreno@iastate.edu) is a Professor in the Dept. of Electrical and Computer Engineering at Iowa State University. He received the Ph.D degree in electrical and computer engineering from Northwestern University in 2006.

Acknowledgment

This material is supported by the National Science Foundation under Grant No. CNS 1646317 and CNS 1645987.

References

[1] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces." in *Proc. of USENIX Security Symposium*, 2011.

[2] F. Koushanfar, A. R. Sadeghi, and H. Seudie, "EDA for secure and dependable cybercars: Challenges and opportunities," in *Proc. of 49th ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2012.

[3] T. Zhang, H. Antunes, and S. Aggarwal, "Defending Connected Vehicles Against Malware: Challenges and a Solution Framework," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 10–21, Feb 2014.

[4] S. Corrigan, "Introduction to the Controller Area Network (CAN)," *Texas Instruments Application Report*, 2016.

[5] B. Carnevale, F. Falaschi, L. Crocetti, H. Hunjan, S. Bisase, and L. Fanucci, "An implementation of the 802.1AE MAC Security Standard for in-car networks," in *Proc. of 2nd World Forum on Internet of Things (WF-IoT)*, Dec. 2015.

[6] P. Mundhenk, S. Steinhorst, M. Lukasiewycz, S. A. Fahmy, and S. Chakraborty, "Lightweight authentication for secure automotive networks," in *Proc. of the 2015 Design, Automation & Test in Europe Conference & Exhibition*, 2015.

[7] C.-W. Lin and A. Sangiovanni-Vincentelli, "Cyber-security for the controller area network (CAN) communication protocol," in *Proc. of International Conference on Cyber Security (CyberSecurity)*, 2012.

[8] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, and H. Shacham, "Experimental security analysis of a modern automobile," in *Proc. of IEEE Symposium on Security and Privacy (SP)*, 2010.

[9] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle." BlackHat USA, 2015.

[10] D. Puthal, S. Mohanty, P. Nanda, and U. Choppali, "Building security perimeters to protect network systems against cyber threats," *IEEE Consumer Electronics Magazine*, vol. 6, no. 4, Oct. 2017.

[11] F. M. Tabrizi and K. Pattabiraman, "Flexible intrusion detection systems for memory-constrained embedded systems," in *Proc. of Dependable Computing Conference (EDCC)*. IEEE, 2015, pp. 1–12.

[12] M.-K. Yoon, S. Mohan, J. Choi, J.-E. Kim, and L. Sha, "Securecore: A multicore-based intrusion detection architecture for real-time embedded systems," in *Proc. of Real-Time and Embedded Technology and Applications Symposium (RTAS)*. IEEE, 2013, pp. 21–32.

[13] C. Zimmer, B. Bhat, F. Mueller, and S. Mohan, "Time-based Intrusion Detection in Cyber-physical Systems," in *Proc. of the 1st ACM/IEEE International Conference on Cyber-Physical Systems*, 2010.

[14] L. Portnoy, E. Eskin, and S. Stolfo, "Intrusion detection with unlabeled data using clustering," in *Proc. of the ACM Workshop on Data Mining Applied to Security*, 2001.
[15] H. M. Song, H. R. Kim, and H. K. Kim, "Intrusion detection system based on the analysis of time intervals of can messages for in-vehicle network," in *Proc. of International Conference on Information Networking (ICOIN)*, 2016.
[16] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," 2014.
[17] M. Gmiden, H. Mohamed, and H. Trabelsi, "An intrusion detection method for securing in-vehicle CAN bus," in *Proc. of Sciences and Techniques of Automatic Control and Computer Engineering*, 2016.
[18] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive can networks - practical examples and selected short-term countermeasures." *SAFECOMP*, 2008.
[19] M. Moore, R. Bridges, F. Combs, M. Starr, and S. Prowell, "Modeling inter-signal arrival times for accurate detection of CAN bus signal injection attacks," *Proc. of 12th Annual Conference on Cyber and Information Security Research*, 2017.
[20] U. E. Larson, D. K. Nilsson, and E. Jonsson, "An approach to specification-based attack detection for in-vehicle networks," in *Proc. of Intelligent Vehicles Symposium*. IEEE, 2008, pp. 220–225.
[21] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection." in *Proc. of USENIX Security Symposium*, 2016.
[22] H. Ji, Y. Wang, H. Qin, X. Wu, and G. Yu, "Investigating the effects of attack detection for in-vehicle networks based on clock drift of ecus," in *Proc. of IEEE Access*. IEEE, 2018.
[23] W. Choi, H. J. Jo, M. C. Park, and D. H. Lee, "Voltageids: Low-level communication characteristics for automotive intrusion detection system," in *Proc. of IEEE Transactions on Information Forensics and Security*, 2018.
[24] M. Marchetti, D. Stabili, A. Guido, and M. Colajanni, "Evaluation of anomaly detection for in-vehicle networks through information-theoretic algorithms," in *Proc. of International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI)*. IEEE, 2016.
[25] M. Müter and N. Asaj, "Entropy-based anomaly detection for in-vehicle networks," in *2011 IEEE Intelligent Vehicles Symposium (IV)*, Jun 2011, pp. 1110–1115.
[26] T. Matsumoto, M. Hata, M. Tanabe, K. Yoshioka, and K. Oishi, "A method of preventing unauthorized data transmission in controller area network," in *Proc. of Vehicular Technology Conference (VTC Spring)*. IEEE, 2012, pp. 1–5.
[27] M. Markovitz and A. Wool, "Field classification, modeling and anomaly detection in unknown can bus networks," in *Proc. of Vehicular Communications)*, 2017.
[28] M. Müter, A. Groll, and F. C. Freiling, "A structured approach to anomaly detection for in-vehicle networks," in *Proc. of Information Assurance and Security (IAS)*, 2010.
[29] M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PloS one*, vol. 11, no. 6, 2016.
[30] S. Otsuka, T. Ishigooka, Y. Oishi, and K. Sasazawa, "CAN Security: Cost-Effective Intrusion Detection for Real-Time Control Systems," SAE Technical Paper, Tech. Rep., 2014.