Survey of Automotive Controller Area Network Intrusion-Detection Systems

Clinton Young and Joseph Zambreno
Iowa State University

Habeeb Olufowobi and Gedare Bloom
Howard University

Editor's note:
Control Area Network (CAN) is one of the most popular targets for malicious attacks and exploitations in modern automotive systems. The goal of intrusion detection systems (IDS) is to identify and mitigate security attacks; consequently, they are of paramount importance to automotive security. This article surveys the state of the art in IDS, with special emphasis on techniques for detecting attacks on CAN modules.
—Sandip Ray, University of Florida

The continued integration of Internet-of-Things technologies and demonstrated cyberattacks on automotive in-vehicle networks [1]–[3] motivate the need for automotive cybersecurity. Network-based attacks are relatively new in automobiles due to the introduction of interconnectivity in modern vehicles. As depicted in Figure 1, modern vehicles contain multiple interfaces, i.e., the on-board diagnostic (OBD)-II port, that expose the vehicle to cyberattacks. With the future emergence of a fully autonomous vehicle, the need for securing automobiles will greatly increase. These vehicles must behave securely, predictably, and reliably. Automotive cyberattacks can result in catastrophic consequences, including the loss of human life.

One option to enhance the security of in-vehicle networks is to adopt intrusion detection and prevention techniques. Intrusion-detection systems (IDSs) 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 necessity.

In this article, we explore the methods and approaches that researchers have taken to identify the threats against vehicles and analyze 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.

Digital Object Identifier 10.1109/MDAT.2019.2899062
Date of publication: 12 February 2019; date of current version: 31 October 2019.

Vulnerabilities and threats

Vulnerabilities of CAN

A Controller Area Network (CAN) is an asynchronous, serial, multimaster communication network protocol that connects electronic control units (ECUs) [4]. Vehicles, airplanes, and industrial machinery utilize CAN to reduce the network complexity and wiring costs. CAN architecture was envisioned to be lightweight and robust and was designed to be unsegmented, unencrypted, and lacking authentication so that CAN messages can flow freely to and from each ECU. However, these properties directly lead to CAN's security vulnerabilities.

Copublished by the IEEE CEDA, IEEE CASS, IEEE SSCS, and TTTC

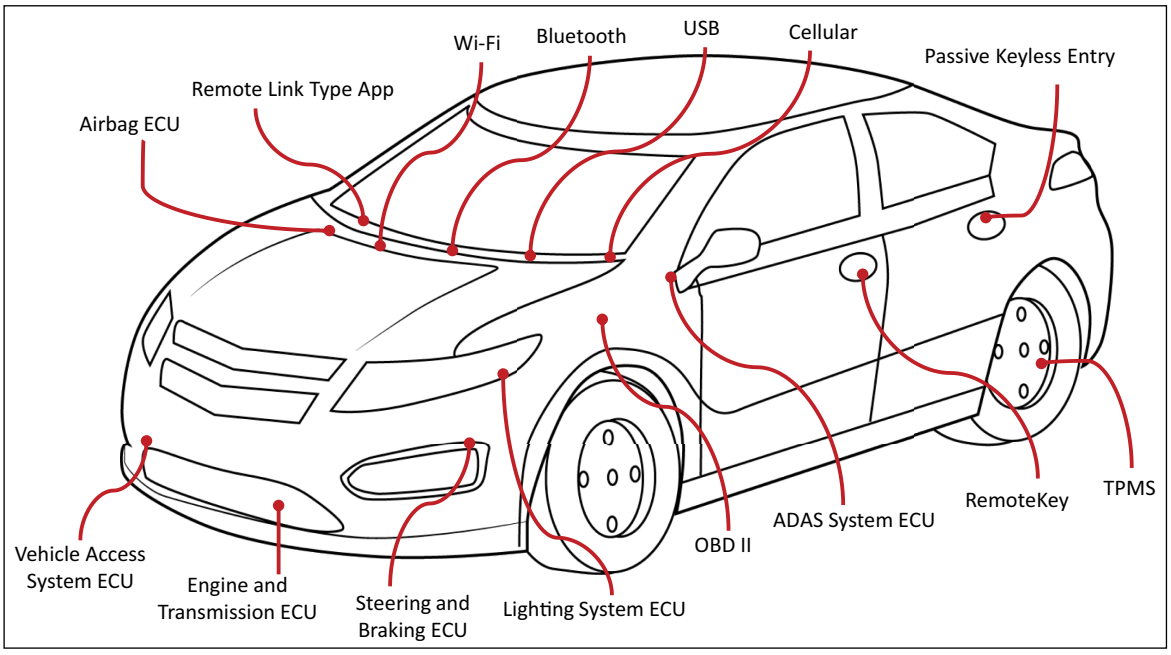

Figure 1. Automotive attack surfaces.

1) Lack of message authentication: Each ECU broadcasts and receives all data on the CAN bus then decides whether the 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 need for point-to-point connections between automotive systems. However, this reduction means a system component dealing with infotainment can communicate to safety-critical vehicle systems. Although some manufacturers utilize different networks for safety-critical systems, there is still cross-communication between safety-critical and noncritical systems.

3) Unencrypted messages: CAN was designed to be lightweight and robust back in the 1980s when car hacking was not a reality. Addition of encryption would only slow down the CAN messages and clog the network. However, as 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].

Threats and attacks

Recent research 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 the 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.

Miller and Valasek [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.

Background on intrusion-detection systems

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

Host-based

A host-based IDS (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 checks to ensure the packets are not malicious. HIDS also monitors the ECU itself to detect behavior indicative of an intrusion. The issue with host-based IDS is that some ECUs lack the processing power required to support an HIDS. Implementing an HIDS in automobiles would require rework on the part of manufacturers on their ECUs.

Network-based

A network-based IDS (NIDS) is part of the communication system, which monitors all traffic traversing the network. Information monitored includes 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.

Intrusion-detection methods

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

1) Signature-based: Signature-based approaches detect attacks using a predefined knowledge base of attack signatures that are 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 the 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 the best accuracy in detection, the normal model must be thorough. The IDS then compares the current system's activity to the previously 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

Table 1. Comparison of the 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) [17]	Message Injection and Deletion	Testbench Simulation
Message Interval	Gmiden (2016) [18]	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) [25]	Message Injection	Real Vehicle Simulation
	Müter (2011) [24]	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

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-based detection is its ability to identify new and previously unknown attacks.

Intrusion-detection systems for automotive security

We investigate how researchers are applying traditional intrusion-detection approaches to secure automotive networks. We summarize some of the cutting-edge work on automotive intrusion detection in Table 1 and discuss their advantages and drawbacks.

Message timing

In a 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, the 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 [9] reported that they needed to inject at a rate of at least 20 times faster than normal for their attack to be successful. As 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.

Detection is based on the following principles:

- 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.
- If the time interval of the new message is shorter than the normal model, the IDS indicates that it is an anomalous message due to the message arriving sooner than expected.

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

Miller and Valasek [16] introduced a concept of analyzing the rate of messages for in-vehicle network intrusion detection. The number of messages on 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.

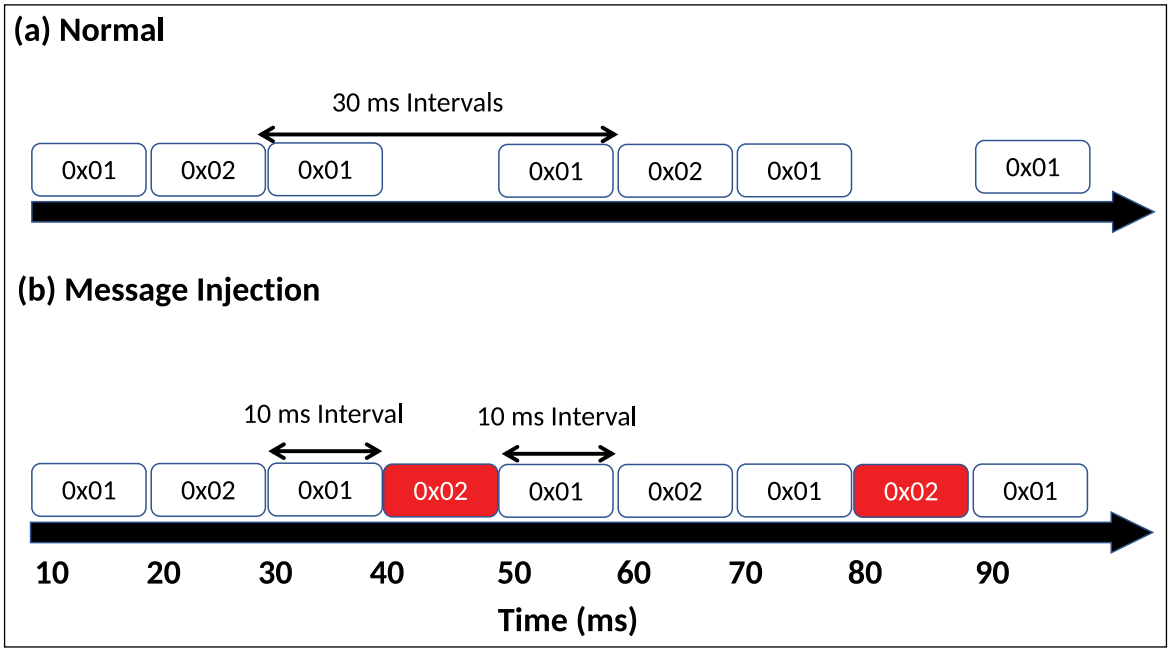

Figure 2. Transmitted messages on a CAN bus on (a) normal status and (b) under message injection attack. The time interval of message CAN ID 0x02 is shortened by the injection of attack messages. Based on Song et al. [15].

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. [18] 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 et al. [18], 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 intersignal wait times of CAN bus traffic will provide accurate detection of 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 of detecting the message injection attacks in CAN bus traffic by showing a clear difference between the 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 shows 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 the known attacks. However, the methods are very simple and are currently limited 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 attack exist. We examine alternative detection methods in the following sections.

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 the 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. This type of detection is not as developed as anomaly-based detection, which we delve into in the following section.

Anomaly-based

Researchers also explored other avenues applying intrusion detection to automotive networks beyond the simple examination of message-timing features. However, a limiting factor in implementing complex IDSs 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 rework of the automotive system:

1) Cyberphysical: The following works define different ECU characteristics to authenticate individual vehicle ECUs. Each IDS proposes using a specific characteristic that is unique to every ECU on the vehicle. Similar to message-timing anomaly detection, when these properties vary from the captured normal, an anomaly is detected. The works here describe alternative features to message timing that can be captured and examined to detect certain attacks.

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.

Ji et al. [22] investigate a detection method based on clock drift. Their approach considers that every ECU has a fixed clock skew and it is possible to establish a normal model of ECU's clock behaviors to detect abnormal measurements. They evaluate the effectiveness of the method against injection and suspension attacks. The analysis results demonstrated that the proposed detection method can detect a small-scale change of packets transmitted in CAN networks.

Choi et al. [23] proposed a novel automotive IDS, VoltageIDS. This system leverages the electrical CAN signal characteristics as a fingerprint of the ECUs. The VoltageIDS 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 [24] 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 and Asaj [24], using the 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. [25] 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 the entropy-based anomaly detectors are a viable approach for identifying CAN bus anomalies caused by attackers injecting messages.

3) Message rate: Very similar to the message-timing detection, Hoppe et al. [17] proposed an anomaly-based IDS that is placed on the CAN bus so that it can listen to the 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 the previously examined works as it counts the 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 and Wool [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.

Other works proposed modifications to the vehicle network with the addition of sensors. Mtiter 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 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 a holistic IDS concept.

Kang and Kang [29] proposed a machine-learning-based IDS approach using a deep neural network structure to monitor the CAN packets. Their IDS consists of two modules. A monitoring module decides the type

of CAN packet based on the 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. These two modules would be embedded in each ECU to analyze CAN packets. They used an unsupervised deep-belief network to capture the underlying statistical features of CAN data and used them to classify the messages as benign or anomalous. They reported a 99% detection ratio while keeping false positives under 1%–2% through the use of software simulation. However, the authors did not discuss the overhead to implement their machine learning approach on modern vehicles.

These works show that 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 vehicular system to detect attacks. There are works [26], [27] that require reverse engineering of the CAN system and its messages to implement an IDS. Although it is difficult to determine 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.

In this article, we examined the 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 affect 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 cyberphysical systems should have an active response to cyberattacks. We have identified the 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, local interconnect network (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 in order 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. ■

Acknowledgments

This article is supported by the National Science Foundation under Grant CNS 1646317 and under Grant CNS 1645987.

■ References

[1] S. Checkoway et al., "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. USENIX Security Symp.*, 2011.

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

[3] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," *IEEE Internet Things J.*, 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 et al., "An implementation of the 802.1AE MAC Security Standard for in-car networks," in *IEEE Proc. 2nd World Forum Internet Things*, Dec. 2015.

[6] P. Mundhenk et al., "Lightweight authentication for secure automotive networks," in *IEEE Proc. 2015 Design Autom. Test Euro. Conf. Exhibition*, 2015.

[7] C.-W. Lin and A. Sangiovanni-Vincentelli, "Cybersecurity for the controller area network (CAN) communication protocol," in *IEEE Proc. Int. Conf. Cyber Security*, 2012.

[8] K. Koscher et al., "Experimental security analysis of a modern automobile," in *IEEE Proc. Symp. Security Privacy*, 2010.

[9] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *BlackHat USA,* 2015.
[10] D. Puthal et al., "Building security perimeters to protect network systems against cyber threats," *IEEE Consum. Electron. Mag.*, vol. 6, no. 4, Oct. 2017.
[11] F. M. Tabrizi and K. Pattabiraman, "Flexible intrusion detection systems for memory-constrained embedded systems," in *IEEE Proc. Depend. Comput. Conf.*, 2015, pp. 1–12.
[12] M.-K. Yoon et al., "Securecore: A multicore-based intrusion detection architecture for real-time embedded systems," in *IEEE Proc. Real-Time Embedded Technol. Appl. Symp.*, 2013, pp. 21–32.
[13] C. Zimmer et al., "Time-based intrusion detection in cyber-physical systems," in *IEEE Proc. 1st ACM/IEEE Int. Conf. Cyber Phy. Syst.*, 2010.
[14] L. Portnoy, E. Eskin, and S. Stolfo, "Intrusion detection with unlabeled data using clustering," in *IEEE Proc. ACM Workshop Data Mining Appl. Secur.*, 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 *IEEE Proc. Int. Conf. Inf. Netw.*, 2016.
[16] C. Miller and C. Valasek, *A Survey of Remote Automotive Attack Surfaces*, 2014.
[17] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive can networks—Practical examples and selected short-term countermeasures," *SAFECOMP*, 2008.
[18] M. Gmiden, H. Mohamed, and H. Trabelsi, "An intrusion detection method for securing in-vehicle CAN bus," in *Proc. Sci. Tech. Autom. Cont. Comput. Eng.*, 2016.
[19] M. Moore et al., "Modeling inter-signal arrival times for accurate detection of CAN bus signal injection attacks," in *IEEE Proc. 12th Ann. Conf. Cyber Inf. Security Res.*, 2017.
[20] U. E. Larson, D. K. Nilsson, and E. Jonsson, "An approach to specification-based attack detection for in-vehicle networks," in *IEEE Proc. Intell. Veh. Symp.*, 2008, pp. 220–225.
[21] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in *IEEE Proc. USENIX Security Symp.*, 2016.
[22] H. Ji et al., "Investigating the effects of attack detection for in-vehicle networks based on clock drift of ecus," in *Proc. IEEE Access*, 2018.
[23] W. Choi et al., "Voltageids: Low-level communication characteristics for automotive intrusion detection system," in *Proc. IEEE Trans. Inf. Forensics Security*, 2018.
[24] M. Müter and N. Asaj, "Entropy-based anomaly detection for in-vehicle networks," in *2011 IEEE Intell. Veh. Symp.*, Jun. 2011, pp. 1110–1115.
[25] M. Marchetti et al., "Evaluation of anomaly detection for in-vehicle networks through information- theoretic algorithms," in *IEEE Proc. Int. Forum Res. Technol. Soc. Ind. Leveraging a Better Tomorrow*, 2016.
[26] T. Matsumoto et al., "A method of preventing unauthorized data transmission in controller area network," in *IEEE Proc. Veh. Techn. Conf.*, 2012, pp. 1–5.
[27] M. Markovitz and A. Wool, "Field classification, modeling and anomaly detection in unknown can bus networks," in *IEEE Proc. Veh. Commun.*, 2017.
[28] M. Müter, A. Groll, and F. C. Freiling, "A structured approach to anomaly detection for in-vehicle networks," in *IEEE Proc. Inf. Assurance Security*, 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 et al., *CAN Security: Cost-Effective Intrusion Detection for Real-Time Control Systems*, Tech. Rep., 2014.

Clinton Young is a Research Assistant working on automotive security. Young is currently pursuing a PhD in computer engineering with Iowa State University, Ames, IA.

Joseph Zambreno is a Professor with the Department of Electrical and Computer Engineering, Iowa State University, Ames, IA. Zambreno received a PhD in electrical and computer engineering from Northwestern University, Evanston, IL, in 2006.

Habeeb Olufowobi is a Research Assistant with the Embedded Systems Security Laboratory, Howard University, Washington, DC. Olufowobi is currently pursuing a PhD with the Embedded Systems Security Laboratory, Howard University.

Gedare Bloom is an Assistant Professor with the Department of Computer Science, Howard University, Washington, DC. Bloom has a PhD in computer science from George Washington University, Washington, DC.

■ Direct questions and comments about this article to Joseph Zambreno, ECpE Department, Iowa State University, Ames, IA 50011 USA; zambreno@iastate.edu.