A Survey of Intrusion Detection for In-Vehicle Networks

Wufei Wu, *Student Member, IEEE*, Renfa Li, *Senior Member, IEEE*, Guoqi Xie, *Member, IEEE*, Jiyao An, *Member, IEEE*, Yang Bai, Jia Zhou, and Keqin Li, *Fellow, IEEE*

***Abstract*— The development of the complexity and connectivity of modern automobiles has caused a massive rise in the security risks of in-vehicle networks (IVNs). Nevertheless, existing IVN designs (e.g., controller area network) lack cybersecurity consideration. Intrusion detection, an effective method for defending against cyberattacks on IVNs while providing functional safety and real-time communication guarantees, aims to address this issue. Therefore, the necessity of its research has risen. In this paper, an IVN environment is introduced, and the constraints and characteristics of an intrusion detection system (IDS) design for IVNs are presented. A survey of the proposed IDS designs for the IVNs is conducted, and the corresponding drawbacks are highlighted. Various optimization objectives are considered and comprehensively compared. Lastly, the trend, open issues, and emerging research directions are described.**

***Index Terms*— Controller area network (CAN), cybersecurity, in-vehicle network (IVN), intrusion detection system (IDS), information entropy, machine learning.**

I. Introduction

INCREASING numbers of electronic control units (ECUs) and external communication interfaces have been assembled inside automobiles to provide intelligent services and safety to users [1]. For example, more than 100 ECUs have been installed in luxury vehicles [2]. By 2020, 75% of vehicles will have the capability to connect to the Internet [3]. However, the security risks of automobiles have become prominent along with the increasing complexity and connectivity of modern vehicles.

Manuscript received April 4, 2018; revised November 28, 2018 and March 1, 2019; accepted March 11, 2019. Date of publication April 11, 2019; date of current version February 28, 2020. This work was supported in part by the National Key Research and Development Plan of China under Grant 2016YFB0200405, in part by the National Natural Science Foundation of China under Grant 61702172, Grant 61672217, Grant 61502405, Grant 61370097, and Grant 61502162, in part by the Natural Science Foundation of Hunan Province, China, under Grant 2018JJ3076 and Grant 2018JJ2063, in part by the China Postdoctoral Science Foundation under Grant 2016M592422, in part by the CCF-NSFOCUS Open Research Fund under Grant CCF-NSFOCUS2018009, and in part by the Fundamental Research Funds for the Central Universities. The Associate Editor for this paper was S. A. Birrell. *(Corresponding authors: Renfa Li; Keqin Li.)*

W. Wu, R. Li, G. Xie, J. An, Y. Bai, and J. Zhou are with the Key Laboratory for Embedded and Network Computing of Hunan Province, College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China (e-mail: wufeiwu@hnu.edu.cn; lirenfa@hnu.edu.cn; xgqman@hnu.edu.cn; jt_anbob@hnu.edu.cn; baiyang@hnu.edu.cn; knight_zhoujia@163.com).

K. Li is with the College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China, and also with the Department of Computer Science, State University of New York, New Paltz, NY 12561 USA (e-mail: lik@newpaltz.edu).

Digital Object Identifier 10.1109/TITS.2019.2908074

The cybersecurity problem is emerging as a major concern for IVN systems given the increasing number of security researchers demonstrating their ability to implement attacks to actual automobiles [4]–[8]. Millions of automobiles face various security risks [9]–[11]. Miller et al. for instance, used a Wi-Fi open port to intrude an in-vehicle network (IVN) system of Jeep Cherokee and reprogram the firmware of ECUs [11]. They successfully controlled a wide range of automotive functions (e.g., disabling brakes and stopping engines), triggering a recall of 1.4 million vehicles. These examples of automotive attacks have greatly stimulated researchers' enthusiasm for IVN's cybersecurity research. Moreover, IVN's intrusion detection capabilities should be improved to prevent serious damage caused by hacking.

The following categorizes have been proposed as countermeasures that provide IVN protection against various types of malicious attacks [12]–[14]: (1) ensuring the confidentiality and integrity of IVN message frames through encryption and authentication technologies [15]–[17], (2) separating potential attacking interfaces from IVNs (firewall policy) [18]–[20], and (3) developing intrusion detection systems (IDSs) for IVNs (IVN IDSs).

Different IVN security enhancement methods bear some advantages and disadvantages. Encryption and authentication methods are effective ways of guaranteeing consumer network security. IVN environments require of real-time reliability and is constrained by cost, computing capacity, bandwidth, and storage resources [21], [22]. Consequently, these methods are often inapplicable to IVN environments. For example, providing message authentication for a controller area network (CAN) bus is difficult because of the limited space available (8 bytes for CAN and 64 bytes for CAN with flexible data-rate [CAN-FD]) for appending a message authentication code [23]. Moreover, completely isolating threats and various attack sources through firewalls is impractical, given the long life cycle of automotive and multiple attack entrances to IVNs. Designing and implementing an entirely secure IVN system is difficult. Moreover, the conversion and upgrade of existing automotive electronic systems for security enhancement require a long period of time.

IVN IDSs aspire to provide (1) the capability to identify abnormal intrusions with a time guarantee, (2) accurate reference information for intrusion prevention systems (IPSs) [24], and (3) the capability to prevent further damage to IVN attacks (Early alert can reduce the risks from malicious adversaries.).

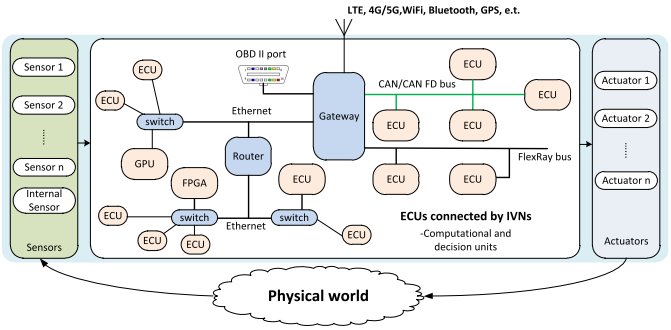


Fig. 1. Overview of automotive CPS (ACPS).

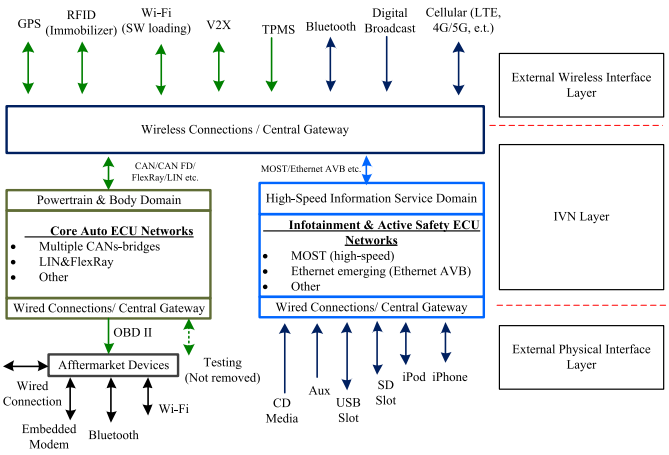


Fig. 2. Three-layer structure of the IVN structure from the perspective of external interface.

IVN IDS is an effective and backward-compatible method for protecting IVNs from attacks and can be applied to computing and bandwidth resource-constrained IVN environments in consideration of the deficiencies of the aforementioned methods. Therefore, a literature review based on recent IVN IDS studies is necessary and timely.

Some state-of-the-art surveys about IVN cybersecurity and cyber-physical systems (CPSs) are available [25]–[27]. Nevertheless, to the best of our knowledge, this study is the first to investigate the use of intrusion detection technology for IVNs.

The remaining parts of this study are structured as follows. In Section II, we provide an overview of the environment, common attack scenarios, and constraints and challenges of intrusion detection for IVNs. In Section III, we introduce the current research status of intrusion detection for IVNs. In Section IV, we discuss the evaluation methods of intrusion detection for in-vehicle networks and comparatively analyze existing technologies. Section V summarizes the current trend and describes the future outlook of intrusion detection for IVNs. In Section VI, we present our conclusion.

II. Preliminaries

A. Background on IVNs

According to Figure 1, an automotive electronic system is a heterogeneous distributed real-time system that consists of multiple ECUs interconnected with an IVN (e.g., CAN [34], local interconnect network (LIN) [35], FlexRay [36], and media-oriented system transport [37]). These networks communicate through a central gateway. The IVN holds heterogeneous, real-time, and cost-sensitive features described as follows.

- **Heterogeneous distributed real-time system environment:** An automotive electronics system is a typical CPS system (ACPS). The heterogeneity of the ACPS system is reflected not only in that of the ECU node processor (FPGA, DSP, and MCU, etc.) but also in that of the internal network. An automobile's internal network environment often consists of multiple protocols used to achieve cost and performance balance. Data among the different networks interact through the gateway. Means of balancing cost and performance is also one of the key issues in the design of IVN IDSs.
- **Multiple external interfaces:** Vehicles rapidly integrate with the external network to provide intelligent and convenient services. Consequently, the external communication interface of vehicles and security threats to the IVN system are increased. These external interfaces are integrated with the IVN, including wireless and wired interfaces. Figure 2 shows the summary of IVNs three-layer structure from the perspective of the external interface to elucidate the external interfaces of the IVN. The main part of the automotive electronic system is the IVN layer, which includes power, body and high-speed information services, and other functional domains. The computing power of the ECU is varied because of cost, and most of their external communication needs to pass through the automotive gateway, including physical and wireless interfaces.
- **Multi-function safety critical level system:** ACPS is a highly functional safety-critical system that needs to comply with corresponding functional safety standards (e.g., ISO26262 [38]). In an automotive environment, different functional domains have corresponding safety and security requirements [39]. For example, an entertainment system has high bandwidth demand, and a powertrain-domain is a safety-critical system. ISO26262 standard divides automotive electronic systems into four automotive safety integrity levels, namely, A, B, C, and D. Initially guaranteeing the functional safety of automobile electronic systems and complying with relevant safety standards are necessary for the problem of IVN security. Notably, automobile electronic systems are safety-critical systems. Therefore, the security problem of IVNs is not only an information security or privacy issue but also a functional safety-related concern. Cybersecurity threat can directly affect the safety of drivers and surrounding individuals.
- **Lack of cybersecurity design:** The previous vehicle in the Figure 1 is a relatively independent individual and does not consider changes in the access network environment (e.g., the existing network protocols lack basic security mechanisms). Moreover, IVNs do not have authentication and encryption mechanisms and thus

TABLE I
EXPERIMENTAL ATTACKS TO AUTOMOBILES

Example	Categories	Attacker surface	Security threats	Contributions
Rouf et al. (2010) [28]	Physical layer	Tire-pressure Monitoring Systems (TPMS)	TPMS spoofing TPMS tracking	The attack mode-based on sensor data is implemented.
Petit et al. (2015) [29]	Physical layer	Perception systems: camera and LiDAR	Blinding attack Jamming attack Replay attack Spoofing attack	The countermeasures are given.
Checkoway et al. (2011) [9]	Data-link layer	OBD port Bluetooth Cellular	System failure	Multiple attack entrances to the vehicle were analyzed.
Cho et al. (2016) [30]	Data-link layer	CAN physical layer	Denial-of-service (DoS) attack	Bus off attack is proposed.
Hoppe et al. (2008) [31]	Application layer	CAN bus interface OBD port	Frame sniffing Replay attack	Control the window lift, warning lights, and ABS; stop these functions.
Koscher et al. (2010) [4]	Application layer	OBD port	Frame sniffing Replay attack DoS attack Frame injection Frame falsifying	Control body, control module, radio, and engine.
Woo et al. (2015) [32]	Application layer	Bluetooth Wi-Fi OBD port (OBD scan tool)	Frame sniffing Replay attack DoS attack Frame injection Frame falsifying	Implement wireless attack. Control dash board, engine, and handle control. Security enhancement protocol is proposed.
Keen Security Lab (2017) [33]	Application layer	Wi-Fi	Remote wireless access Intrusion into the control system	Fully controlled vehicle.

urgently need a responsive security authentication mechanism and intrusion detection design for security, given the increasing number of external communication interfaces for automobiles.

As a de-facto standard in-vehicle communication network, CAN (ISO 11898) has been widely used in automobiles and other industry environment over 30 years, often for safety-critical system connections. Nevertheless, studies in [9] and [6] mentioned that the CAN protocol does not provide security mechanisms, such as message authentication or data encryption, during the design phase. Particularly, in [16], the CAN was reported to lack security guarantee and that it is vulnerable to attack. Therefore, the CAN bus is the main research object of IVN intrusion detection for IVN security researchers. The present work focuses on the intrusion detection technologies suitable for the CAN.

B. Attacks to IVNs

Malicious adversaries can implement attacks to IVNs easily due to the intrinsic vulnerabilities of such networks and the increasingly rich interfaces that provide connectivity between in-vehicle and outside networks. Attacks to IVNs can be generally divided into three steps. First, malicious adversaries need to access the target IVN through a physical or wireless interface. Second, the firmware of the compromised ECU is replaced, and the network is sniffed and parsed. Third, different levels of attacks against the vehicle are conducted, which includes specific functional (e.g., controlling the start and stop of the vehicle) and network failures (e.g., DoS).

To describe the attacks of the IVN system clearly, this study divides the influence of attacks on different network layers into three categories, namely, physical, data-link, and application layers. Experimental attacks to automobiles are described in Table I. The characteristics of attacks on the three layers of IVNs are as follows.

1) Attacks From Sensing Layer (Physical Layer): On the basis of the prediction in [40], an array of sensors (e.g., LiDAR, RaDAR, cameras, and GPS) will be equipped to collect information in a future automobile. They will provide an autonomous vehicle the capability to sense the environment and make driving decisions without human intervention. This type of attack scenario mainly occurs in the maintenance of the vehicle. Malicious adversaries can launch sniffer and bus failure attacks after loading the malicious node to the bus. Consequently, the attack on the automobile through the physical layer will become a new threat to the automobile's security. Rouf et al. realized the reorganization of the message by the TPMS [28]. Petit *et al.* presented remote cyberattacks on a camera-based system and LiDAR using commodity hardware [29]. They also proposed software and hardware countermeasures to improve sensor resilience against these attacks.

2) Illegal Access (Data-Link Layer): Current vehicle attacks can be classified in different ways. In [9], Checkoway *et al.* suggested a classification method for vehicle attacks based on attack distance, which can be classified into direct physical, short-range wireless, and long-distance wireless. They discovered that malicious attacks are feasible via a broad range of attack surfaces. In addition, a series of experiments

was conducted for a comprehensively analysis of the security threats faced by various external attack surfaces of a modern automobile. Malicious adversaries can perform attacks easily once they gain access to network devices, given the lack of security and authentication mechanisms of IVNs. For example, in [30], the network availability of an IVN was threatened by DoS attack. The attack portal mainly has OBD II at the physical layer. Once the data link layer access attack is implemented, the attack behaviors including frame injection, frame falsifying, frame sniffing, fabrication, suspension, and DoS attack. The characteristics of the attack behavior on the network mainly include bus voltage fluctuation and equivalent resistance change. These parameter characteristics are used as the input parameters of the IVN IDS.

3) Attacks From Interfaces (Application Layer): Cyberattacks against vulnerabilities or protocol weaknesses of external networks and equipment have been covered by [4]. The available intrusion interfaces include but are not limited to: Bluetooth, OBD_II, and Wi-Fi. Malicious adversaries can perform several targeted attacks (e.g., remote control or vehicle braking [32]). Hoppe *et al.* proposed a type of attacks against automotive CAN, which can control the window lift, warning lights, and ABS [31]. Short-term countermeasures are also selected to respond such an attack. Woo *et al.* used an actual vehicle and a malicious smartphone app in a connected-vehicle environment to demonstrate a long-range wireless attack [32]. A secure protocol mechanism for handling such attack was also proposed. Nevertheless, detecting attacks from the application layer is difficult due to the lack of illegal access nodes and evident message frame anomalies. In [33], researchers from Keen Security Lab achieved remote wireless access to, and gained complete control over, Tesla electric cars, thereby prompting Tesla to issue an emergency system update via OTA.

C. Constraints, Challenges, and Characteristics of IVN IDS

The concept of IVN IDS was introduced in [31], in which the characteristics of IVN IDS were first presented. The design and implementation of IDS for IVNs have some characteristics that can be used to optimize IDS design while facing various challenges and constraints from the IVN environment in consideration of the investigation of IVNs and the technical review of IVN IDSs. This section tackles the potential challenges and constraints during the implementation of an IVN IDS and introduces two of its characteristics.

1) Constraints of Intrusion Detection for IVNs: Designing and implementing IVN IDS will face various challenges and limitations. This section discusses the potential challenges and constraints during the implementation of an IVN IDS.

- **Hardware constraints.** Presently, ECUs in automotive are mainly powered by a 32-bit embedded processor (e.g., NXP_Freescale, Infine, and Renesas processors), and computational performance and memory resources are tight. Therefore, intrusion detection for IVN design is also constrained by computing power, memory size, and communication capability.

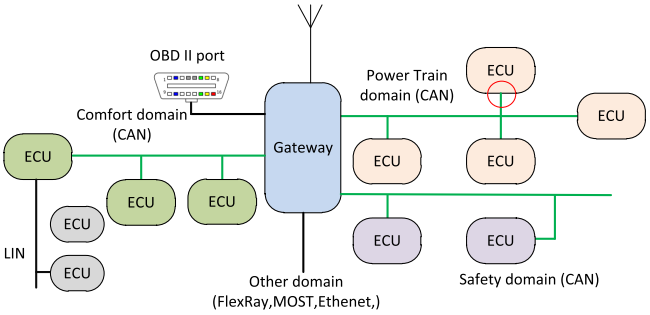


Fig. 3. Example of domain-aware intrusion detection for IVNs.

- **Cost constraints.** An automotive electronic system is a type of industrial embedded system. Reducing hardware costs can provide companies with additional profits given that automobiles are mass-produced. The cost of automotive manufacturing will increase once the IVN IDS design methodology requires hardware modifications to all ECUs. Therefore, IVN IDS design is subject to cost constraints.
- **Detection accuracy and response time.** An automotive network system is a safety-critical system where IVN is responsible for communication; thus, automotive network attacks can cause serious safety problems. Therefore, intrusion detection for IVNs should fulfill the real-time and high-precision requirements of vehicles [41]. The detection accuracy must be analyzed from four aspects, namely, true-positive, false-positive, true-negative, and false-negative.
- **Standardized construction.** IVN IDS aims to provide automotive electronic systems with security defense capabilities. IVN IDS is part of an automotive electronic system, which needs to provide functional security guarantee and follow the ISO26262 standard [38]. The SAE J3061 guidebook [42] for cyber-physical vehicle systems focuses on designing security-aware systems in close relation to the automotive safety standard ISO 26262. SAE J3061 describes a set of high-level guiding principles for automobile security and defines a process framework of security for the lifecycle of cyber-physical vehicle systems. Software specifications in the AUTOSAR (secure onboard communication module) [43] have also been developed to create resource-efficient and practicable authentication mechanisms for critical data transport among ECUs, and such mechanisms have been used by vehicle manufacturers [44].

2) Characteristics of Intrusion Detection for IVNs: This section mainly to introduce the characteristics of IVNs that can be used to improve the performance of IVN IDS design.

- **Domain-aware.** As shown in Figure 3, the automotive electronic system is divided into several parts according to different functional domains, such as power-train domain, entertainment domain, and body domain. Different domains are independent and interconnected through an in-vehicle gateway. The characteristics of traffic messages in different domains also vary. Some of them are

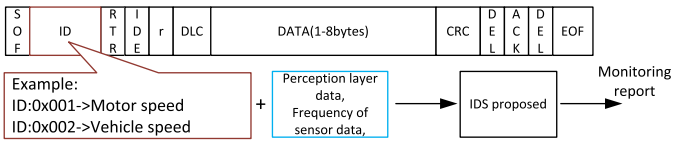


Fig. 4. Example of context-aware intrusion detection for IVNs.

information intensive, and some others are safety-critical. Therefore, different security monitoring schemes can be designed on the basis of the characteristics of different domains to improve detection accuracy. For instance, a domain-aware anomaly detection system for CAN bus network traffic is described in [45] by Markovitz and Wool. Through inspection of real CAN bus communication, they discovered the presence of semantically meaningful constant fields, multi-Value fields and counter or sensor fields.

- **Context-aware.** Context-aware computing has been extensively investigated [46]. A renewed interest in this area has emerged because of ubiquitous technologies that expand the idea of context to the physical world [47]. Meanwhile, with the development of intelligent technology, intelligent vehicle systems will have numerous intelligent sensors, a combination of the data and mode of the perception layer, and an integration of this layer with a security monitoring system can effectively reduce the probability of miscalculation. For instance, as shown in Figure 4, by using the vehicle speed sensor, we can obtain the current state and behavior of the vehicle through a machine learning algorithm, and simulate the normal driving state of the vehicle to determine the attack state.

As shown in Figure 5, in order to more clearly describe the characteristics of IVN IDS design, we creatively draw an IVN IDS design summary map based on the correlation between attack access sources, vulnerabilities of IVNs, attack threats, extractable feature parameters and IDS countermeasures from the perspective of IDS design.

III. State-of-the-Art Intrusion Detection Technology for IVNs

Recent years have noted increased number of automotive malicious attacks. Therefore, the issue of IVN security has received increasing attention [48]. Intrusion detection technology, as a network security enhancement method, is low cost and offers convenient deployment. A large number of studies have been conducted in recent years about intrusion detection technologies for IVN [45], [49], [50]. In this section, these different methods will be explained in greater detail. From the perspective of IVN IDS design, IVN IDSs can be divided into the following categories.

A. Fingerprints-Based Methods (Bus Level)

Due to the physical properties of ECUs, different ECU on the in-vehicle networks usually have unique hardware fingerprint information, IVN security researchers attempt to extract fingerprint information of ECUs in various ways (e.g., clock-based intrusion detection design [51] and voltage measurements-based [52]). According to the uniqueness electrical characteristics of ECUs (i.e., the dominant, positive-slope and negative-slope parts), fingerprint information can be established for legal and illegal access to ECUs. Cho and Shin, for instance, presented a method named Viden which fingerprinted ECUs based on voltage measurements [52]. Via the ACK learning phase, Viden obtained correct measurements of voltages only from the message transmitters, and exploited them for constructing and updating correct voltage profiles or fingerprints. This method can detect the illegal access nodes quickly and accurately. However, this method is not effective for detecting network attacks at the application layer, because this method is only applicable to the physical layer.

In [53], Choi *et al.* proposed a novel IVN IDS (VoltageIDS), which is based on the inimitable characteristics of electrical CAN signals. Evaluation experiments on moving and idling vehicles show this method's ability to detect bus-off attack [30].

Brief Discussion: The next step for the IVN IDS after obtaining the network fingerprint characteristics will be a classification problem. Therefore, fingerprint-based IVN IDS is a comprehensive strategy, and the technology used will also combine machine learning methods. For example, many machine learning methods have their own unique advantages for the stage of feature extraction and classification.

B. Parameters Monitoring-Based Methods (Message Level)

Some attacks can be discovered on the basis of the observation and comparison of network parameters. These parameter monitoring-based intrusion detection methods include the following.

1) Frequency-Based Techniques: As shown in Figure 6, message frames transmitted over an IVN usually have a fixed period. For example, transmission intervals of CAN messages can be detected and compared against the established baseline, which is similar to a statistics-based anomaly detection method [54]. IVN security researchers have shown that the frequencies will increase when malicious adversaries perform a spoofing or DoS attack by injecting legitimate messages [11], [55]. Such detection methods are possible with good accuracy and low false-positive rate, but only works for periodic traffic. Adrian et al. evaluated the effectiveness of frequency-based anomaly detection for packet injection attacks [56]. When the period exceeds the threshold, the system will issue an abnormal status alarm and store the log.

2) Remote Frame: As shown in Figure 7, when a node on CAN bus receives a remote frame, it needs to respond with a message to the sender. The offset ratio of the response frame can reflect the suspicious activity. Furthermore, Lee et al. proposed an intrusion detection method on the basis of the remote frame of CAN messages by measuring the response performance of the existing nodes which based on the offset ratio and time interval between request message and response message [57].

Figure 8 shows how time/frequency features can be processed independently of IVN data sequences. From the

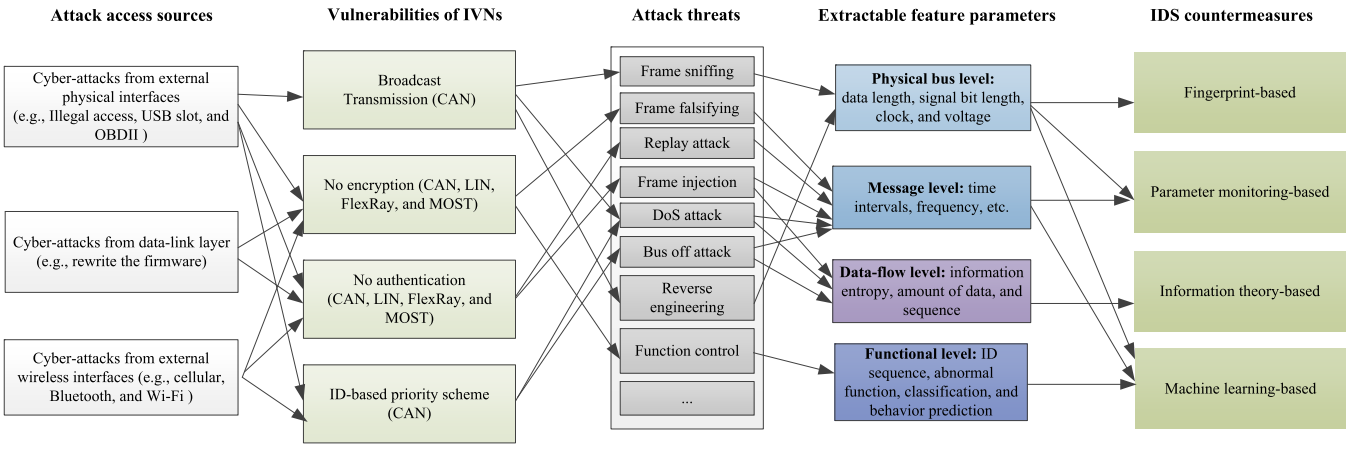


Fig. 5. A summary view of the IDS design for IVN.

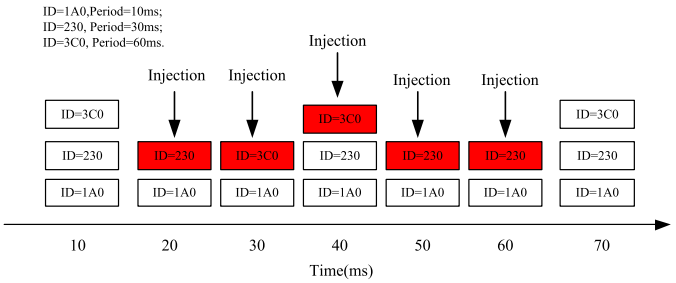


Fig. 6. Frequency-based IDS. *When an attack occurs, the fixed period of the message will be changed, and this feature is used for intrusion detection.*

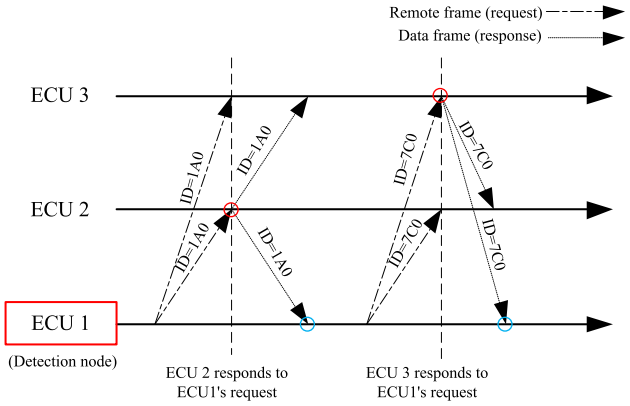


Fig. 7. Remote frame-based IDS. *In a CAN bus, when the target node receives a remote frame, a data frame is returned to the sending node, and the measurement of the return time can be used to determine whether the network is in an attack state.*

figure, IVN IDS technologies can be divided into the observation of data flow [58] and sequences [59]. In response to attacks from the data flow level of IVN; the intrusion detection methods based on parameter detection have good detection accuracy and low performance overhead.

Brief Discussion: Parameter monitoring-based methods may be ineffective for unknown security threats, and parameters might vary in different vehicle networks. Attacks against automobiles will show increasing uncertainty and complexity as IVNs continue to integrate into external networks. IVN security researchers have proposed many IVN IDS designs based on information theory and machine learning to address these issues, which will be introduced in the following chapters.

C. Information-Theoretic-Based IVN IDSs (Data-Flow Level)

Using information-theoretical-based measures is another approach for unsupervised anomaly detection design in the IVN environment. Specifically, the internal communication of each ECU is often in order; thus, systematic information entropy should be relatively stable. Numerous malicious messages injected into the normal communication will affect the network stability, and the information entropy can reflect the anomaly. Wang et al. collected 6.673 million CAN messages from various automobiles and conducted entropy and pattern analysis of the messages. CAN messages are identified to have low entropy, with an average of 11.436 bits [15].

Establishing a model of information entropy analysis based on the characteristics of CAN network is necessary for detecting the information entropy of automobile networks. We calculate message ID's entropy using Shannon entropy definition. Assume system X's limited set of possible states is $\{x_1, x_2, \ldots, x_N\}$. Then the information entropy of system X is

$$H(X) = -\sum_{i=0}^{N} p(x_i) \log p(x_i), \tag{1}$$

where $p(x_i)$ is the probability of system X in state x_i.

Entropy Analysis Model of CAN IDs: For the evaluation of the information entropy of CAN IDs, a CAN system model can be represented by $\Phi = (I, C, T)$, where $I = \{\imath_1, \imath_2, \imath_3, \ldots, \imath_n\}$ is a set of different IDs appearing within time T, and $C = \{c_1, c_2, c_3, \ldots, c_n\}$ is the set of periods or the minimum intervals of n different IDs that appear within time T. Subsequently, the entropy function of CAN IDs in period T can be expressed as

$$H(I) = -\sum_{\imath \in I} p_\imath \log p_\imath. \tag{2}$$

Assuming that the system is schedulable, all CAN messages can meet their deadlines [60], and the total number of

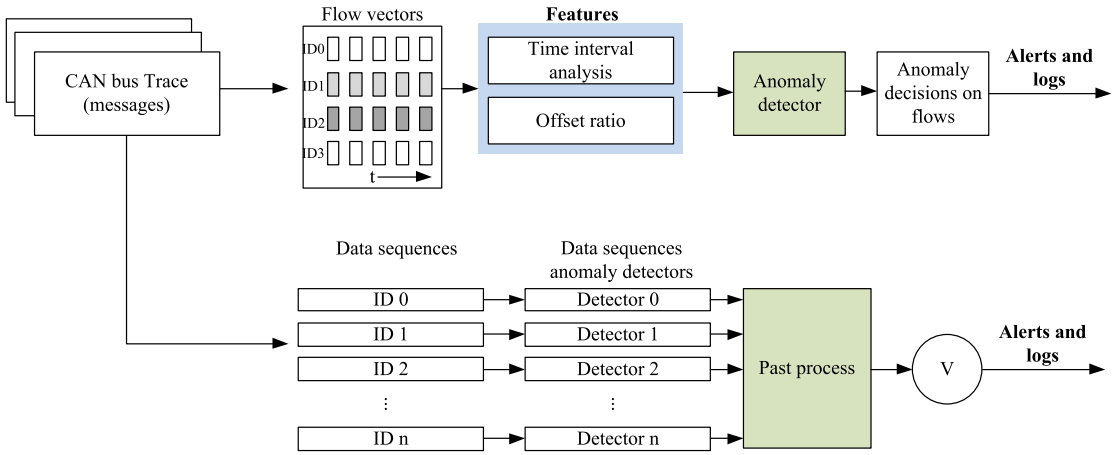


Fig. 8. Time/frequency features are processed independently from data sequences.

messages N_{total} in time T can be obtained by the period of messages appearing within time T and the length of T, as shown as follows:

$$N_{total} = \left(\frac{T}{c_1} + \frac{T}{c_2} + \cdots + \frac{T}{c_n}\right) = T\sum_{i=1}^{n}\frac{1}{c_i}. \tag{3}$$

The number of ι_i in T is $n_i = T/c_i$. Then the probability of ι_i appearing in T can be presented as $P(\iota_i)$, as shown as follows:

$$P(\iota_i) = \frac{n_i}{N_{total}} = \frac{T}{c_i} \times \frac{1}{T\sum_{i=1}^{n}\frac{1}{c_i}} = \frac{1}{c_i\sum_{i=1}^{n}\frac{1}{c_i}}. \tag{4}$$

Evidently, $\sum_{i=1}^{n} P(\iota_i) = 1$, $P(\iota_i) > 0$ $(i = 1, 2, \ldots, n)$. The self-information of i is:

$$U_i = \log\frac{1}{P(\iota_i)} = \log c_i \sum_{i=1}^{n}\frac{1}{c_i}. \tag{5}$$

Then, in the sampling period T, the entropy of IDs in CAN bus is:

$$H_i = P(\iota_i)U(\iota_i) = \frac{\log c_i \sum_{i=1}^{n}\frac{1}{c_i}}{c_i\sum_{i=1}^{n}\frac{1}{c_i}}. \tag{6}$$

The average entropy of IDs in sampling period T is:

$$H(I) = E[U(\iota_i)] = \sum_{i=1}^{n} H_i. \tag{7}$$

Some entropy-based methods have been established and tested in practice to detect attacks. Muter et al. first introduced the concept of entropy-based attack detection for in-vehicle networks, which is efcient for detecting DoS attacks; however, a small number of malicious messages injected by malicious adversaries are difficult to recognize [61]. Similarly, in [62], Marchetti *et al.* proved through experiments that the intrusion detection method based on information entropy requires attack intensity (high volume attacks).

In [63], we proposed a novel sliding window strategy based on a fixed message number for information entropy, which effectively solves the problem of IDS performance based on information entropy for aperiodic CAN messages. Dario et al. proposed a Hamming distance measurement method for monitoring the status of IVNs and obtained good results for detecting attacks to the CAN [64]. The main feature of this method is the small computational overhead, and the disadvantage is that the attack model is limited (not for replay attacks).

Brief Discussion: Notably, the intrusion detection method based on information entropy is ineffective in attacks that modify the content of the CAN data field. To improve the accuracy of the information entropy-based intrusion detection mechanism, the two characteristics of IVN (i.e., context and domain awareness) mentioned in Section II-C.2 could be used to optimize IVN IDS design.

D. Machine Learning-Based IVN IDSs (Functional Level)

Machine learning algorithms have been used extensively as a powerful mathematical tool in computer and artificial intelligence and have a good effect on classification, regression, and clustering; thus, they can develop security solutions on different levels of IVNs. They are especially suitable for defense against future unknown attacks. In this section, we will review machine learning-based IVN IDSs. Further details will be introduced from the following three aspects.

1) Classification-Based Techniques: Classification algorithms have been used extensively as a powerful method for security solutions. Intrusion detection for IVNs can be designed along with a classification algorithm to learn the normal behavior of network traffic, and any deviation from that will be identified as an abnormal behavior of CAN bus. As shown in Figure 9, the scheme mainly includes two phases, namely, offline training and online detection. In the training phase, selecting and labeling the training data set are important. In the automotive environment, Theissler et al. proposed a one-class SVM with the radial basis function kernel to learn the baseline normal behavior and classify deviations

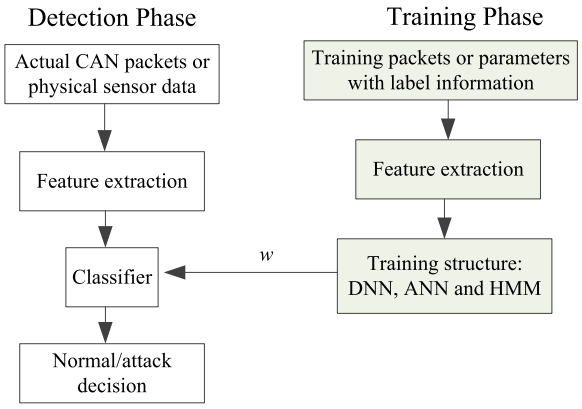


Fig. 9. Machine learning approach for IVN IDS.

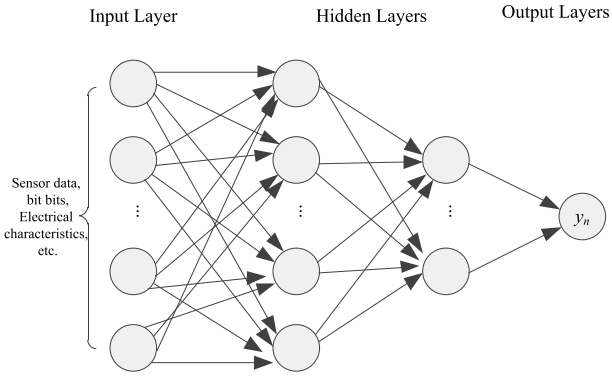


Fig. 10. Architecture of deep neural network (DNN) for intrusion detection for IVNs.

as anomalies [65]. The resulting classifier is applicable to sequences of events but does not detect point anomalies.

2) Deep Learning Techniques: For developing anomaly-based IVN IDS, deep learning and neural networks are adopted and deployed for IVNs. Kang and Kang proposed an intrusion detection technique using a DNN [50]. In the proposed technique, IVN packets exchanged between ECUs are trained to extract low-dimensional features and used for discriminating normal and hacking packets. According to [50], the proposed technique can provide a real-time response to the attack with a considerably high detection ratio (99.8%). Taylor *et al.* suggested an anomaly detector based on a long short-term memory (LSTM) recurrent neural network (RNN) to detect attacks with low false alarm rates [66]. The prediction of the next packet data based on neural network is used for intrusion detection; thus knowledge of the specific protocol is not required.

Figure 10 shows the three layers of the neural network applied to intrusion detection for IVNs. Among them, the difference between the normal neural network models is mainly the input and output layers, where the input features can be bits of CAN data field or signal features extracted from the physical layer of the CAN bus. The output layer outputs normal and abnormal results. The DNN model of intrusion detection for IVNs environment can be described as follows.

DNN Model of Intrusion Detection for IVNs: The training set can be represented as $(b^{(1)}, y^{(1)}, \ldots, b^{(k)}, y^{(k)})$ of k samples, where $b = \{b_0, b_1, \ldots, b_B\} = R^B$ is the set of feature including B parameters, and y is the binary result of intrusion detection. Therefore, the cost function C can be defined as,

$$C(W; b, y) = \frac{1}{2}||h_W(b) - y||^2, \tag{8}$$

where two nodes in the DNN are connected by W (adaptation weight), and $h_W(b)$ is an assumption that provides an estimated output. For the convenience of batch training, the overall cost function can be defined as

$$C(W) = \frac{1}{K}\sum_{k=1}^{K} C(W, b^k, y^k) + \frac{\gamma}{2}\sum_{n=1}^{N}\sum_{i=1}^{M_l}\sum_{j=1}^{M_l+1}(w_{ji}^n)^2, \tag{9}$$

where N is the depth of the neural network, M_l is the number of nodes in the l_{th} layer, and $w_{ji}^n = W$ is the weight of the connection between a node i in the $(n-1)_{th}$ layer and a node j in the n_{th} layer. In each node of a layer, the output is computed with the sigmoid function of the linear combination of input values and the weights.

The aim is to minimize the cost function in Function 9 to obtain the weighting parameters. A stochastic gradient method can be used to train the network given the efficiency of back propagation algorithm with predefined parameters in this problem. Specifically, the partial derivative of the cost function $C_k(W)$ can be used for the adaptation in each iteration, as shown as follows:

$$w_{ji}^n = w_{ji}^{n-1} + \eta\frac{\vartheta}{\vartheta w_{ji}^{(n-1)}}C(W), \tag{10}$$

where η is an adaptation parameter.

3) Sequential Techniques: The order of message transmitted from an ECU can be used for anomaly detection. CAN message from the ECU should seen as a specific order. They will be transmitted one after the other based on the priorities of messages, and any deviation from this order can be flagged. Narayanan et al. developed a hidden Markov model (HMM) to detect anomalous states from actual data collected from vehicles [67]. Marchetti and Stabili proposed an algorithm of building a model of the normal behavior of a CAN bus based on particular features and recurring patterns within the sequence of message IDs observed in the CAN bus, which is the first algorithm based on the analysis of the sequences of messages on the CAN bus [68].

Features should be selected and acquired at the design stage following the implementation of machine learning-based intrusion detection for IVNs. Choi *et al.* proposed a new method, which can extract suitable statistical features from the sampled signal $S(k)$ [69] based on the method proposed by Dey *et al.* [70]. This method can quickly identify certified ECUs by using inimitable characteristics of signals in CAN. Fourty scalar features in time and frequency domains are extracted using LibXtract [71] for the sampled signal $S(k)$, which is a well-known feature extraction library. Anomaly detection methods based on verifying the message contents have also been proposed in addition to using message ID bits

as input features [50]. Muter *et al.* for instance, used in-vehicle sensors to verify message range and correlation [72].

Brief Discussion: IVN IDSs require more reliability and certainty than do IDSs of consumer networks. Therefore, IVN IDS prefers supervised machine learning methods. Attacks by malicious adversaries will generate anomalous features at different layers of the IVN, and most of them can be used for machine learning-based IDS.

E. Other Methods

Notably, IVN IDS technologies can be classified from several other perspectives, such as IDS deployment (i.e., host- and network-based), and attack type (i.e., anomaly- and signification-based). In this study, we classify IVN IDS technology from the perspective of technical implementation and introduce several detailed major directions. Other notable research methods are as follows.

Domain-Aware IVN IDS: Markovitz and Wool [45], described a domain-aware anomaly detection system for CAN bus network traffic. The CAN bus message format is proprietary and nonpublicly documented. However, the authors developed a classifier that automatically identifies the boundaries and types of these fields. The anomaly detection system built a model for normal messages on the basis of field classification. In [59], Markovitz and Wool described a novel domain-aware anomaly detection system for in-vehicle CAN bus traffic. A greedy algorithm was developed to split the messages into fields and classify the fields into the types they observed. In addition, a semantically aware anomaly detection system was designed for CAN bus traffic. Experiments on actual CAN bus traffic showed that the IDS achieved a median false-positive rate of 0% with an average of 252 ternary content-addressable memory.

Context-Aware IVN IDS: Wasicek *et al.* [73], described a context-aware intrusion detection system (CAID) and framework to detect manipulations in automotive control systems. In this study, CAID uses sensor information to establish reference models of the physical system and then checks the correctness of the current sensor data against the reference models. Muter *et al.* [72] developed a sensor-based detection method that could recognize a malicious intrusion by using several sensors designed for cyber attack scenarios. In [74], Cho *et al.* used CarSim to obtain realistic sensor readings for the slip ratio and the normalized traction force. CarSim is a high-fidelity commercial software that predicts vehicle performance in response to control from the driver. Abnormal measurements in brake-related sensors can be detected using the tire friction model.

Brief Discussion: Many design studies have shown that IVN IDSs need to be combined with the characteristics of an automotive electronic system. Designing an IVN IDS from a system perspective (with domain and context awareness) can effectively improve not only the effect of IDS (detection accuracy and response time) but also its market compatibility.

F. IDS Design for Other IVNs

High-bandwidth IVNs (e.g., CAN-FD [75], FlexRay, and automotive Ethernet [76]) have been rapidly developed and valued by automotive electronics researchers because of the increasing demand for IVN bandwidth in the new generation of automotive electronic systems. Similar to CAN protocol, such IVNs lack cybersecurity mechanisms at the beginning of the design process. The most common intrusion detection methods for IVN design are for the CAN. Therefore, IDS design for the current research status has also become a research hotspot.

The difference between CAN-FD and CAN mainly lies in two aspects. First, the maximum data field length of CAN-FD can be 64 bytes. Second, the transmission rate of CAN-FD can be variable. Therefore, the existing CAN-based IDS design is basically applicable to CAN-FD.

Specific cyberattacks against FlexRay networks exist [4], [77]. Therefore, research on FlexRay network security is becoming increasingly important. Some studies on FlexRay network security enhancements are available. In [78], Han *et al.* proposed a novel architecture and communication middleware design for FlexRay static segment scheduling to address the new challenge on security that is synthesized to satisfy security requirements, on top of extensibility, costs, and end-to-end latencies. In [79], Gu *et al.* suggested a security-aware mapping and scheduling mechanism with hardware co-processors for FlexRay-based distributed embedded systems. Nevertheless, no research has been published on FlexRay IDS design.

The LIN network communicates in master slave mode mainly in the body control domain (e.g., glass and wiper control) in an IVN environment. Meanwhile, the LIN master node is often a node of CAN. The LIN intrusion detection technology problem is generally classified into CAN IDS, in consideration of the small size of the LIN network and the small number of external communication interfaces.

Automotive Ethernet is currently used primarily in body imaging and active safety. The large-scale application of automotive Ethernet in IVN systems remains to have problems that warrant solution (e.g., time determination) [80]–[82]. Similarly, no research on the automotive Ethernet IDS design is available. Great advantages of on-board Ethernet in bandwidth and cost make it a potential candidate to become the backbone network of IVNs in the future [83]. Therefore, the security mechanism should be considered in combination with IVN background in the design and theoretical analysis stage of automotive Ethernet.

IV. Evaluation and Comparison of Intrusion Detection for IVNs

The evaluation of IVN IDS technology is a challenging issue, given the different malicious adversary scenarios and attack and threat models. Here, an attempt to make a general assessment was conducted by combining IVN design constraints from the perspective of security objectives. This section introduces the tools and data sets used in the IVN IDS evaluation and presents a comprehensive comparison and analysis of the IVN IDSs mentioned in Section III.

A. Data Sets and Tools Used in Previous Works

Obtaining the data set is very important in evaluating the performance of an IVN IDS design. Presently, the data set commonly used in CAN message's functional safety verification and analysis simulation experiments is the SAE benchmark message set [87]. However, a standard data set for IVN IDS design evaluation is currently unavailable. In state-of-the-art studies, many researchers have provided methods for generating data sets for IVN IDS design evaluation. Marchetti *et al.* [62] obtained CAN traffic data from the main CAN bus of a 2011 Ford Fiesta and designed and instrumented a custom CAN bus logger, which was realized with a Genuino UNO prototyping board that writes CAN messages to an SD memory card. Furthermore, Levi *et al.* [88] built a small simulation for connected vehicles on the basis of the well-known traffic simulator Simulation of Urban Mobility [89]. In [50], Kang and Kang used a CAN packet generator to generate a test data set named Open Car Test bed and Network Experiments OCTANE [90].

Lee *et al.* [57] released the data set collected during their experiment through the URL (http://ocslab.hksecurity.net/Dataset/CAN-intrusion-dataset), which includes DoS, fuzzy, and impersonation attack and attack-free states. Moreover, some effective IVN simulation software tools can be used for IVN IDS verification experiments. Noras et al. used CANoe to provide a complete set of development, simulation, and testing frameworks for IVN [49].

Experimental data sets can generally be divided into two parts: data under normal operation condition and data with attack signals under various attack modes. The more data are monitored and evaluated, the better the overall understanding of the system state.

B. Comparison of Intrusion Detection for IVNs

As regards the evaluation of intrusion detection methods for IVNs, false-negative cases are considered an important metric because these methods cannot detect an actual intrusion on a network, thereby causing poor user experiences.

The confidentiality, integrity, and availability (CIA) triad [91] have established frameworks, which are used in security domain to explain the most important goals of providing in-vehicle cybersecurity. Detection rate and effectiveness of IVN IDS mainly include the occurrence probability of true-positive, false-positive, true-negative and false-negative results. IVN IDS design problem can be transformed into multi-objective constraint optimization problem after classification function is completed. As we mentioned in our previous work [63], during the design of an IVN IDS, the R_A (detection accuracy rate) should be as high as possible, whereas the R_N (false-positive rate) should be as low as possible. The problem can be described as minimizing the following energy function when evaluating IVN IDS:

$$E() = C_1 \times R_A(\%) - C_2 \times R_N(\%) - C_3 \times R_t, \quad (11)$$

where $E()$ is the energy function representing the detection accuracy and efficiency of the proposed model. And, three weighted parameters C_1, C_2, and C_3 are used to assess the characteristics of the proposed IDS; these parameters are obtained in the training phase. Additional parameters (e.g., expected cost, intrusion detection capability, and detection latency) are necessary for analyzing intrusion detection for IVNs [92]. For example, an IDS that consumes excessive time to detect intruders may give malicious adversaries sufficient time to damage the vehicle. Thus, detection latency should be a key intrusion detection metric.

Table II presents that some representative IVN IDSs for comprehensive comparison are selected to more clearly show the current status of IVN IDS researches. Figure 11 presents the four categories of IVN IDS designs from the perspective of implementation technology. A comprehensive comparison of the IVN IDSs mentioned in Section III was presented, and the following observations are drawn.

Observations: The following observations are known by comparing the different schemes in Table II:

(1) Different IVN IDSs can be used against diverse cyber-attacks from various IVN layers (e.g., external physical or wireless interface layer). Meanwhile, the IVN features that can be used for IDS are mainly from the following four levels: physical bus, message, data-flow, and functional interpretation. For eaxmple, machine learning methods are in good standing in defending against attacks from the application layer, and fingerprint based methods can be effect tools against attacks from the physical layer. The latter methods are more efficient and have shorter response time than the former. However, the defending system which can against all types and various sources attack is not yet be developed.

(2) The machine learning-based intrusion detection methods have a good effect against unknown IVN attacks, but they require considerable for computing and storage resources and are thus not suitable for the automotive network environment. Levi *et al.* [88], proposed a cloud-based method to address this issue.

(3) Table II shows that most of the current security researchers' methods have lower false-positive rate (except for some papers that failed to provide relevant information). Most of the methods have high detection accuracy. However, dealing with all existing attacks by one method is difficult because some cyberattacks come from the physical layer, while others come from the application layer. Nevertheless, existing methods only monitor on a single layer of the IVN. Therefore, features that are distributed across different IVN layers can be used to enhance future IVN IDSs design, rather than being limited to one IVN layer's features.

C. Intrusion Prevention System (IPS)

It is worth noting that IDS plays a limited role in security protection. As the first line of security defense, IDS is often apart of the IPS. For instance, an IPS for the automotive CAN was proposed in [24], and Abbott-McCune and Shay proposed an algorithm to detect replay attacks of valid and invalid arbitration identifiers through the monitoring timing of events. Thereafter, they extended the IDS into an IPS by designing an additional CAN transceiver based on the FPGA.

TABLE II
SELECTED COMPARISONS OF INTRUSION DETECTING METHODS FOR IVNS

Research Work	Categories	Main technology	Contribution	False-positive rate	Drawback
Shin et al. (2017) [51]	Fingerprint	Clock-based	Attacker detection.	0.055%	Only for periodic messages.
Wonsuk et al. (2018) [53]	Fingerprint	VoltageIDS-based	The moving and idling vehicles are assessed	Unobtainable	Only for masquerade attack and bus off attack
Kyong et al. (2017) [52]	Fingerprint	Viden, voltage profiles based identify	The attack ECU node can be pinpointed.	0.2%	Additional hardware is required.
NORAS et al. (2017) [49]	Parameter monitoring	Rule-Based White-list based	Software-based Light-weight Real-time	0%	Prototype phase High cost
Adrian et al. (2015) [56]	Parameter monitoring	Frequency-based	Only overt and subtle attacks are determined.	0%	Not include non-periodic packet types
Han et al. (2015) [54]	Parameter monitoring	Statistical-based	Low computational complexity and available for low-end ECUs.	0%	It treats each ID's data sequence as independent.
Lee et al. (2017) [57]	Parameter monitoring	Remote Frame based observational	Message injection and impersonation node attack, Locate the attack message type and node.	Unobtainable	Requires additional node arrangement.
Hyun et al. (2016) [55]	Parameter monitoring	Time intervals based observational	The corresponding in millisecond, Light-weight.	0%	Just for injection attack.
Dario et al. (2017) [64]	Information-theoretic	Hamming distance measurement	Low computational complexity and available for low-end ECUs.	0%	Not for replay attacks.
Mirio et al. (2016) [62]	Information-theoretic	Entropy analysis-based	Complete independence with respect to the content of CAN messages.	Unobtainable	Only possible for high volume CAN messages attacks.
Wu et al. (2018) [63]	Information-theoretic	Entropy analysis-based	Counting-based sliding window strategy	0%	Only for injection and DoS attacks
Taylor et al. (2016) [66]	Machine learning	LSTM and RNN	Low false alarm rates. No domain knowledge of the system is required	0%	It treats each ID's data sequence as independent
Moti et al. (2015) [45]	Machine learning	TCMAs	Automatically identifies the boundaries and types of CAN traffic data.	0%	High computational cost.
Jain et al. (2012) [85]	Machine learning	Decision tree-based	Inaccessible.	Unobtainable	No actual verification
Narayanan et al. (2015) [67]	Machine learning	HMM	Backwards compatible as a plug-n-play device	Unobtainable	Not well-suited to online problems.
Kang et al. (2016) [50]	Machine learning	DNN	Features directly extracted from a bit stream in the network before decoding.	0.02%	High computational cost.
Armin et al. (2017) [73]	Machine learning	CIAD, bottleneck ANN.	A Bottleneck ANNs was capable to detect deviations in the behavior of the control system.	Unobtainable	No actual verification
Miro et al. (2017) [68]	Machine learning	ID sequences analysis based method.	Cost small memory and computational footprints.	0%	Only for message injected attack.
Wang et al. (2018) [86]	Machine learning	Hierarchical temporal memory (HTM) based	Can detect unknown attacks	0.02%	Long time model training is required
Rieke et al. (2017) [87]	Machine learning	Petri net model Behavior analysis based	Design and implementation of a model-based method to compare the measured behavior of a vehicle with the expected behavior.	0.07%	The attack on payload changes is invalid.

IVN IDSs have no mechanisms in place to prevent transmissions from the malicious node despite being able to flag malicious cyberattacks. Giannopoulos *et al.* [93], described a novel IPS countermeasure for the CAN bus to address this issue. They first proposed a basic IDS design, which relies on blacklisted arbitration IDs, and implemented it in the FPGA. This mechanism only requires a single custom controller, which has the characteristics of low cost and strong compatibility. The way to use the characteristics of IVN to better combine IDS and IPS will be an ideal research direction

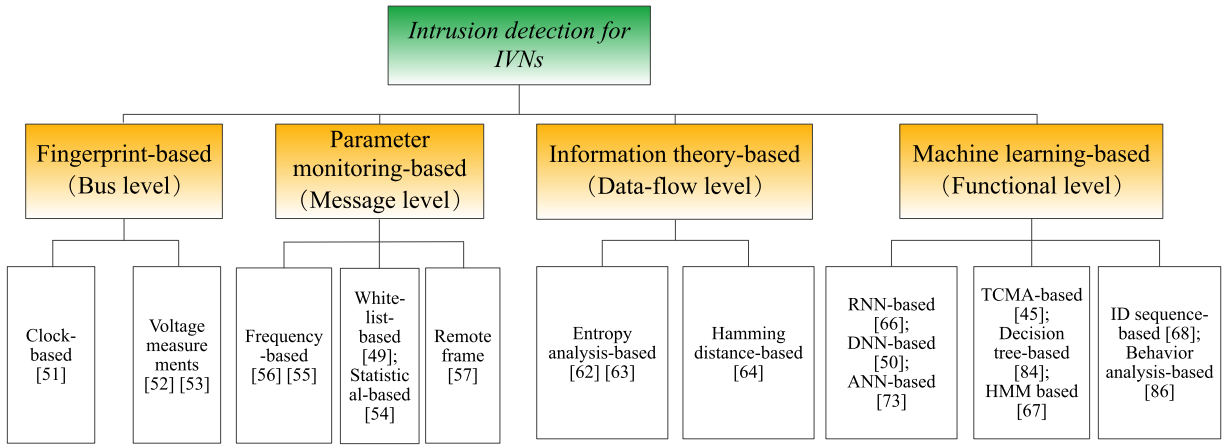


Fig. 11. Taxonomy of IVN IDS. *From the perspective of technology implementation.*

for our future research to improve the actual ability of IVN to resist cyberattacks.

V. Trends and Prospects

Vehicles are revolutionized through the integration of modern computing and communication technologies to improve user experience and driving safety. With the increasing number of attacks to actual vehicles, enhanced security precautions and extended protection mechanisms must be provided for new automobiles. This section presents trends and upcoming issues regarding IVN IDS technology for the development of future automotive electronic systems.

A. Trends

The deployment of sensors and high-precision map technology brings about the birth of numerous applications and services for autonomous vehicles. The following predictions are set for the future development of IDS technology:

(1) Existing IVN protocols for autonomous vehicles encounter difficulties in meeting bandwidth and design performance requirements. Therefore, the development of autonomous vehicles will inevitably accelerate the development of IVNs. The security mechanism should be considered at the beginning of the development of new IVN standards in order to provide security guarantee for the future IVN environment. Moreover, the IDS function should be considered at the same time when determining the next-generation IVN protocol standard.

(2) In terms of the network security of IVN system, the development of edge computing technology will address the bottleneck problem of limited computing and storage resources of IDS technology in the implementation process.

(3) Automobile manufacturers have a complete set of design, test, and verification development processes for the functional security of automotive electronic systems. With the increasing concern about security problems, the information security of IVN systems in the future needs the support of the test and verification platform.

B. Open Issues

Many open issues are identified in the area of IVN IDSs. Five important research directions are listed as follows.

(1) One of the most urgent issues of IVN IDS design is to enhance the accuracy and response time of IVN IDSs. How to distinguish malicious attacks and abnormal situations (e.g., emergency breaking, crashes, updates) on IVN environment will be a challenging study. For IDS methods of the signal layer (e.g., frequency-based IDS), anomalous and malicious messages cannot be distinguished. Possibly, the IDS of the functional layer can compensate for this concern. A future IDS design with integrated features may be an efficient method to address this issue, given that existing IDS solutions can target only specific attack scenarios and types.

(2) ACPS is a highly safety-critical system. Thus, an important issue in the automotive domain is to adapt established functional safety process and methods to security engineering. Functional safety of vehicles and security of IVNs are different domains, and a gap exists between them. To ensure the functional safety of vehicles, Many automotive electronics researchers focus on this domain and have obtained promising research results [94]–[96]. Further details about the relationship between security and functional safety of IVN system can be found in [42] and [97] .

(3) Current automotive electronic components are provided separately by the different parts of the supply chain, with different vendors developing different distributed subsystems. This situation poses a challenge to system security deployment. All security vulnerabilities appear at the boundaries of the code provided by different developers. Uniform standards should be established to effectively coordinate supply chains.

(4) Different steps will inevitably affect different network layers and then produce some characteristics that can be used for IDS observation in the process of intruding the IVN. Nevertheless, how to utilize these network characteristics across IVN layers comprehensively and use them to improve the performance of IVN IDS will be an important direction to study in the future, particularly in the heterogeneous network environment where multiple networks coexist.

(5) Machine learning algorithms have unique advantages in realizing anonymous intrusion detection. Unfortunately, they experience two challenges, One is how to deploy machine learning algorithms in an IVN system with limited computing resources, and the other is how to obtain data sets that can be effectively trained.

VI. Conclusion

The design of security enhancement for vehicles needs to meet multiple design metrics, such as reliability, safety, performance, and cost, which are sometimes conflicting given the cost sensitivity and safety critical of the automobile. IVN IDS is an effective method of defending against attacks to automobiles. Thus, the research on it is growing rapidly. In this study, the external interface for vehicle attacks on three layers was creatively analyzed, and the vulnerabilities of each layer were discussed. Furthermore, the characteristic parameters available for IVN IDS design in the four levels of the IVN (i.e., bus, message, data-flow, and functional levels) were analyzed. State-of-the-art intrusion detection methods for IVNs were categorized into four types on the basis of implementation techniques. Furthermore, advanced intrusion detection solutions for IVNs were analyzed and comprehensively compared. Open challenges regarding IVN intrusion detection methods from future works were presented with regard to our investigation.

Acknowledgment

The authors would like to express their gratitude to the associate editor and anonymous reviewers for their constructive comments, which have helped improve the quality of this paper.

References

[1] S. Tuohy, M. Glavin, C. Hughes, E. Jones, M. Trivedi, and L. Kilmartin, "Intra-vehicle networks: A review," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 534–545, Apr. 2015.

[2] N. E. Team. (Nov. 20, 2015). *Future Advances in Body Electronics* [Online]. Available: https://www.nxp.com/docs/en/white-paper/BODYDELECTRWP.pdf

[3] J. Greenough. (May 2015). *Connecting Cars to the Internet has Created a Massive New Business Opportunity*.[Online]. Available: http://www.businessinsider.com/connected-car-marketforecast-report-2015-5

[4] K. Koscher *et al.*, "Experimental security analysis of a modern automobile," in *Proc. IEEE Symp. Secur. Privacy*, May 2010, pp. 447–462.

[5] J. Liu, S. Zhang, W. Sun, and Y. Shi, "In-vehicle network attacks and countermeasures: Challenges and future directions," *IEEE Netw.*, vol. 31, no. 5, pp. 50–58, Sep./Oct. 2017.

[6] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," Black Hat USA, Las Vegas, NV, USA, Tech. Rep. 8, 2014.

[7] M. Marchetti and D. Stabili, "Read: Reverse engineering of automotive data frames," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 4, pp. 1083–1097, 2019.

[8] S. Fröschle and A. Stühring, "Analyzing the capabilities of the can attacker," in *Proc. Eur. Symp. Res. Comput. Secur.* Oslo, Norway: Springer, 2017, pp. 464–482.

[9] S. Checkoway *et al.*, "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. 20th USENIX Conf. Secur.*, Aug. 2011, p. 6.

[10] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2015.

[11] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," Black Hat USA, Las Vegas, NV, USA, Tech. Rep. 23, 2015.

[12] W. Wu *et al.*, "IDH-CAN: A hardware-based ID hopping CAN mechanism with enhanced security for automotive real-time applications," *IEEE Access*, vol. 6, pp. 54607–54623, 2018.

[13] C. Lin and A. Sangiovanni-Vincentelli, "Cyber-security for the controller area network (CAN) communication protocol," in *Proc. Int. Conf. Cyber Secur.*, Dec. 2012, pp. 1–7.

[14] D. K. Nilsson, U. E. Larson, and E. Jonsson, "Efficient in-vehicle delayed data authentication based on compound message authentication codes," in *Proc. IEEE 68th Veh. Technol. Conf.*, Sep. 2008, pp. 1–5.

[15] W. Eric, X. William, S. Suhas, L. Songsong, and Z. Kai, "Hardware module-based message authentication in intra-vehicle networks," in *Proc. ACM/IEEE 8th Int. Conf. Cyber-Phys. Syst. (ICCPS)*, Apr. 2017, pp. 207–216.

[16] J. Van Bulck, J. T. Mühlberg, and F. Piessens, "VulCAN: Efficient component authentication and software isolation for automotive control networks," in *Proc. 33rd Annu. Comput. Secur. Appl. Conf.*, Dec. 2017, pp. 225–237.

[17] A. Hazem and H. Fahmy, "Lcap-a lightweight can authentication protocol for securing in-vehicle networks," in *Proc. 10th Escar Embedded Secur. Cars Conf.*, Berlin, Germany, vol. 6, pp. 283–300, Nov. 2012.

[18] G. Macher, H. Sporer, E. Brenner, and C. Kreiner, "An automotive signal-layer security and trust-boundary identification approach," *Procedia Comput. Sci.*, vol. 109, pp. 490–497, May 2017.

[19] G. Macher, H. Sporer, E. Brenner, and C. KREINER, "Signal-layer security and trust-boundary identification based on hardware-software interface definition," *J. Ubiquitous Syst. Pervasive Netw.*, vol. 10, no. 1, pp. 1–9, 2018.

[20] G. Macher, H. Sporer, E. Brenner, and C. Kreiner, "Supporting cyber-security based on hardware-software interface definition," in *Proc. Eur. Conf. Softw. Process Improvement*. Graz, Austria: Springer, Sep. 2016, pp. 148–159.

[21] S. Chakraborty, M. A. A. Faruque, W. Chang, D. Goswami, M. Wolf, and Q. Zhu, "Automotive cyber–physical systems: A tutorial introduction," *IEEE Design Test*, vol. 33, no. 4, pp. 92–108, Aug. 2016.

[22] A. Wasicek, P. Derler, and E. A. Lee, "Aspect-oriented modeling of attacks in automotive cyber-physical systems," in *Proc. 51st ACM/EDAC/IEEE Des. Automat. Conf. (DAC)*, Jun. 2014, pp. 1–6.

[23] M. J. Dworkin, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, document NIST SP-800-38B, 2016.

[24] S. Abbott-McCune and L. A. Shay, "Intrusion prevention system of automotive network can bus," in *Proc. IEEE Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2016, pp. 1–8.

[25] T. Huang, J. Zhou, Y. Wang, and A. Cheng, "On the security of in-vehicle hybrid network: Status and challenges," in *Information Security Practice and Experience*, J. K. Liu and P. Samarati, Eds. Cham, Switzerland: Springer, 2017, pp. 621–637.

[26] O. Avatefipour and H. Malik. (2018). "State-of-the-art survey on in-vehicle network communication (can-bus) security and vulnerabilities." [Online]. Available: https://arxiv.org/abs/1802.01725

[27] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Comput. Surv.*, vol. 46, no. 4, Apr. 2014, Art. no. 55.

[28] I. Rouf *et al.*, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *Proc. 19th USENIX Conf. Secur.*, Washington, DC, USA, Aug. 2010, p. 21.

[29] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and lidar," in *Proc. Black Hat Eur.*, Amsterdam, The Netherlands, Nov. 2015.

[30] K.-T. Cho and K. G. Shin, "Error handling of in-vehicle networks makes them vulnerable," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 1044–1055.

[31] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks—Practical examples and selected short-term countermeasures," *Rel. Eng. Syst. Saf.*, vol. 96, no. 1, pp. 11–25, Jan. 2011.

[32] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 993–1006, Apr. 2015.

[33] K. Security lab. Jun. 12, 2017. *Car Hacking Research: Remote Attack Tesla Motors*. [Online]. Available: https://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free- Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus.pdf

[34] Bosch. (1991). *Can Specifications*. [Online]. Available: https://www.kvaser.com/software/7330130980914/V1/can2spec.pdf

[35] AUTOSAR. (Dec. 2017). *Specification of Lin Interface*. [Online]. Available: https://www.autosar.org/fileadmin/LINInterface.pdf

[36] F. Sagstetter, M. Lukasiewycz, and S. Chakraborty, "Generalized asynchronous time-triggered scheduling for flexray," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 36, no. 2, pp. 214–226, Feb. 2017.

[37] MOST. (Oct. 2006). *Most Specification*. [Online]. Available: https://www.mostcooperation.com/publications//mostspecificationpdf/

[38] *Road Vehicles—Functional Safety—Part 1: Vocabulary*, Standard ISO 26262-1, International Organization for Standardization, 2011.

[39] S. K. Baruah, A. Burns, and R. I. Davis, "Response-time analysis for mixed criticality systems," in *Proc. 32nd Real-Time Syst. Symp.*, Dec. 2012, pp. 34–43.

[40] U. Ozguner, T. Acarman, and K. Redmill, *Autonomous ground vehicles*. Norwood, MA, USA: Artech House, 2011.

[41] A. Tomlinson, J. Bryans, and S. A. Shaikh, "Using a one-class compound classifier to detect in-vehicle network attacks," in *Proc. Genetic Evol. Comput. Conf. Companion*, Jul. 2018, pp. 1926–1929.

[42] C. Schmittner, Z. Ma, C. Reyes, O. Dillinger, and P. Puschner, "Using SAE J3061 for automotive security requirement engineering," in *Proc. Int. Conf. Comput. Saf., Rel., Secur.* Trondheim, Norway: Springer, 2016, pp. 157–170.

[43] G. Del Vigna, "Security modeling and automatic code generation in AUTOSAR," Ph.D. dissertation, Pisa Univ., Tech. Rep., 2016. [Online]. Available: https://core.ac.uk/download/pdf/79621273.pdf

[44] M. Akiyama, M. Iwamura, Y. Kawakoya, K. Aoki, and M. Itoh, "Design and implementation of high interaction client honeypot for drive-by-download attacks," *IEICE Trans. Commun.*, vol. 93, no. 5, pp. 1131–1139, May 2010.

[45] M. Markovitz and A. Wool, "Field classification, modeling and anomaly detection in unknown CAN bus networks," *Veh. Commun.*, vol. 9, Jul. 2017, pp. 43–52.

[46] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the Internet of Things: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 414–454, 1st Quart., 2014.

[47] K. Habib and W. Leister, "Context-aware authentication for the Internet of Things," in *Proc. 11th Int. Conf. Autonomic Auton. Syst.*, May 2015, pp. 134–139.

[48] C. Lin, B. Zheng, Q. Zhu, and A. Sangiovanni-Vincentelli, "Security-aware design methodology and optimization for automotive systems," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 21, no. 1, Nov. 2015, Art. no. 18.

[49] M. B. NORAS SALMAN, "Design and implementation of an intrusion detection system (IDS) for in-vehicle networks," Dept. Comput. Sci. Eng., Chalmers Univ. Technol., Gothenburg, Sweden, Tech. Rep. 1, 2017.

[50] M.-J. Kang and J.-W. Kang, "A novel intrusion detection method using deep neural network for in-vehicle network security," in *Proc. IEEE 83rd Veh. Technol. Conf. (VTC Spring)*, May 2016, pp. 1–5.

[51] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in *Proc. 25th USENIX Conf. Secur. Symp.*, Austin, TX, USA, Aug. 2016, pp. 911–927.

[52] K. G. Shin and K.-T. Cho, "Viden: Attacker identification on in-vehicle networks," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Dallas, TX, USA, Oct./Nov. 2017, pp. 1109–1123. doi: 10.1145/3133956.3134001.

[53] W. Choi, K. Joo, H. J. Jo, M. C. Park, and D. H. Dong, "VoltageIDS: Low-level communication characteristics for automotive intrusion detection system," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 2114–2129, Aug. 2018.

[54] M. L. Han, L. Jin, A. R. Kang, S. Kang, J. K. Park, and H. K. Kim, *A Statistical-Based Anomaly Detection Method for Connected Cars Internet Things Environment*. Cham, Switzerland: Springer, 2015.

[55] 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. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2016, pp. 63–68.

[56] A. Taylor, N. Japkowicz, and S. Leblanc, " Frequency-based anomaly detection for the automotive CAN bus," in *Proc. World Congr. Ind. Control Syst. Secur. (WCICSS)*, Dec. 2015, pp. 45–49.

[57] H. Lee, S. H. Jeong, and H. K. Kim, "OTIDS: A novel intrusion detection system for in-vehicle network by using remote frame," in *Proc. 15th Annu. Conf. Privacy, Secur. Trust (PST)*, Aug. 2017, pp. 5709–5757.

[58] A. Taylor, "Anomaly-based detection of malicious activity in in-vehicle networks," Ph.D. dissertation, Ottawa-Carleton Institue Elect. Comput. Eng., Univ. Ottawa, Ottawa, ON, Canada, 2017.

[59] M. Markovitz and A. Wool, "Field classification, modeling and anomaly detection in unknown CAN bus networkss," *Veh. Commun.*, vol. 9, pp. 43–52, Jul. 2017.

[60] R. I. Davis, A. Burns, R. J. Bril, and J. J. Lukkien, "Controller Area Network (CAN) schedulability analysis: Refuted, revisited and revised," *Real-Time Syst.*, vol. 35, no. 3, pp. 239–272, Apr. 2007.

[61] M. Müter and N. Asaj, "Entropy-based anomaly detection for in-vehicle networks," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2011, pp. 1110–1115.

[62] M. Marchetti, D. Stabili, A. Guido, and M. Colajanni, "Evaluation of anomaly detection for in-vehicle networks through information-theoretic algorithms," in *Proc. IEEE 2nd Int. Forum Res. Technol. Soc. Ind. Leveraging Better Tomorrow (RTSI)*, Sep. 2016, pp. 1–6.

[63] W. Wu *et al.*, "Sliding window optimized information entropy analysis method for intrusion detection on in-vehicle networks," *IEEE Access*, vol. 6, pp. 45233–45245, 2018.

[64] D. Stabili, M. Marchetti, and M. Colajanni, "Detecting attacks to internal vehicle networks through hamming distance," in *Proc. AEIT Int. Annu. Conf.*, Aug. 2017, pp. 1–6.

[65] A. Theissler, "Anomaly detection in recordings from in-vehicle networks," in *Proc. Big Data Appl. Princ. (BIGDAP)*, vol. 23, Sep. 2014, pp. 1–12.

[66] A. Taylor, S. Leblanc, and N. Japkowicz, "Anomaly detection in automobile control network data with long short-term memory networks," in *Proc. IEEE Int. Conf. Data Sci. Advanced Anal. (DSAA)*,Oct. 2016, pp. 130–139.

[67] S. N. Narayanan, S. Mittal, and A. Joshi. (2015). "Using data analytics to detect anomalous states in vehicles." [Online]. Available: https://arxiv.org/abs/1512.08048

[68] M. Marchetti and D. Stabili, "Anomaly detection of CAN bus messages through analysis of ID sequencess," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2017, pp. 1577–1583.

[69] W. Choi, H. J. Jo, S. Woo, Y. C. Ji, J. Park, and D. H. Lee, "Identifying ECUs using inimitable characteristics of signals in controller area networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 4757–4770, Jun. 2016.

[70] S. Dey, N. Roy, W. Xu, R. R. Choudhury, and S. Nelakuditi, "AccelPrint: Imperfections accelerometers make smartphones trackable," in *Proc. NDSS Symp.*, Feb. 2014, pp. 1–16.

[71] Libxtract. (Apr. 24, 2015). *Libxtract: Feature Extraction Library Documentation*. [Online]. Available: http://libxtract.sourceforge.net

[72] M. Müter, A. Groll, and F. C. Freiling, "A structured approach to anomaly detection for in-vehicle networks," in *Proc. 6th Int. Conf. Inf. Assurance Secur.*, Aug. 2010, pp. 92–98.

[73] A. R. Wasicek, M. D. Pesé, A. Weimerskirch, Y. Burakova, and K. Singh, "Context-aware intrusion detection in automotive control systems," in *Proc. 5th ESCAR USA Conf.*, Jun. 2017, pp. 21–22.

[74] K.-T. Cho, K. G. Shin, and T. Park, "CPS approach to checking norm operation of a brake-by-wire system," in *Proc. ACM/IEEE 6th Int. Conf. Cyber-Phys. Syst.*, Apr. 2015, pp. 41–50.

[75] R. Bosch, "Can with flexible data-rate specification," Robert Bosch Gmbh, stuttgart, Tech. Rep., 2012. [Online]. Available: https://can-newsletter.org/assets/files/ttmedia/raw/e5740b7b5781b8960f55efcc-2b93edf8.pdf

[76] P. Hank, S. Müller, O. Vermesan, and J. Van Den Keybus, "Automotive ethernet: in-vehicle networking and smart mobility," in *Proc. Des., Automat. Test Eur. Conf. Exhib. (DATE)*, Mar. 2013, pp. 1735–1739.

[77] D. K. Nilsson, U. E. Larson, F. Picasso, and E. Jonsson, *A First Simulation of Attacks in the Automotive Network Communications Protocol FlexRay*. Berlin, Germany: Springer, 2009.

[78] G. Han, H. Zeng, Y. Li, and W. Dou, "SAFE: Security-aware flexray scheduling engine," in *Proc. Des., Automat. Test Eur. Conf. Exhib. (DATE)*, Mar. 2014, pp. 1–4.

[79] Z. Gu, G. Han, H. Zeng, and Q. Zhao, "Security-aware mapping and scheduling with hardware co-processors for FlexRay-based distributed embedded systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 10, pp. 3044–3057, Oct. 2016.

[80] R. Queck, "Analysis of Ethernet AVB for automotive networks using network calculus," in *Proc. IEEE Int. Conf. Veh. Electron. Saf. (ICVES)*, Jul. 2012, pp. 61–67.

[81] D. Thiele and R. Ernst, "Formal worst-case performance analysis of time-sensitive ethernet with frame preemption," in *Proc. IEEE 21st Int. Conf. Emerg. Technol. Factory Automat. (ETFA)*, Sep. 2016, pp. 1–9.

[82] M. H. Farzaneh, S. Shafaei, and A. Knoll, "Formally verifiable modeling of in-vehicle time-sensitive networks (TSN) based on logic programming," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2016, pp. 1–4.

[83] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The future of industrial communication: Automation networks in the era of the Internet of Things and industry 4.0," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 17–27, Mar. 2017.
[84] N. Jain and S. Sharma, "The role of decision tree technique for automating intrusion detection system," *Int. J. Comput. Eng. Res.*, vol. 2, no. 4, 2012.
[85] C. Wang, Z. Zhao, L. Gong, L. Zhu, Z. Liu, and X. Cheng, "A distributed anomaly detection system for in-vehicle network using HTM," *IEEE Access*, vol. 6, pp. 9091–9098, 2018.
[86] R. Rieke, M. Seidemann, E. K. Talla, D. Zelle, and B. Seeger, "Behavior analysis for safety and security in automotive systems," in *Proc. 25th Euromicro Int. Conf. Parallel, Distrib. Netw.-Based Process. (PDP)*, Mar. 2017, pp. 381–385.
[87] K. Tindell and A. Burns, "Guaranteeing message latencies on control area network (CAN)," in *Proc. 1st Int. CAN Conf.*, 1994, pp. 1–11.
[88] M. Levi, Y. Allouche, and A. Kontorovich. (2017). "Advanced analytics for connected cars cyber security" [Online]. Available: https://arxiv.org/abs/1711.01939
[89] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, "Recent development and applications of sumo-simulation of urban mobility," *Int. J. Adv. Syst. Meas.*, vol. 5, nos. 3–4, pp. 128–138, Dec. 2012.
[90] P. Borazjani, C. Everett, and D. McCoy, "Octane: An extensible open source car security testbed," in *Proc. Embedded Secur. Cars Conf.*, Jun. 2014, p. 60.
[91] D. Coss, "The cia strikes back: Redefining confidentiality, integrity and availability in security," *J. Inf. Syst. Secur.*, vol. 10, no. 3, pp. 21–45, Jul. 2014.
[92] C. Corbett, T. Basic, T. Lukaseder, and F. Kargl, "A testing framework architecture for automotive intrusion detection systems," in *Automotive-Safety Security 2017-Sicherheit und Zuverlässigkeit für automobile Informationstechnik*. 2017.
[93] H. Giannopoulos, A. M. Wyglinski, and J. Chapman, "Securing vehicular controller area networks: An approach to active bus-level countermeasures," *IEEE Veh. Technol. Mag.*, vol. 12, no. 4, pp. 60–68, Dec. 2017.
[94] D. Tămaç-selicean and P. Pop, "Design optimization of mixed-criticality real-time embedded systems," *ACM Trans. Embedded Comput. Syst.*, vol. 14, no. 3, New York, NY, USA: ACM, May 2015, Art. no. 50.
[95] G. Xie, G. Zeng, Y. Liu, J. Zhou, R. Li, and K. Li, "Fast functional safety verification for distributed automotive applications during early design phase," *IEEE Trans. Ind. Electron.*, vol. 65, no. 5, pp. 4378–4391, May 2017.
[96] G. Xie, G. Zeng, L. Liu, R. Li, and K. Li, "High performance real-time scheduling of multiple mixed-criticality functions in heterogeneous distributed embedded systems," *J. Syst. Archit.*, vol. 70, pp. 3–14, Oct. 2016.
[97] M. Wolf, A. Weimerskirch, and T. Wollinger, "State of the art: Embedding security in vehicles," *Eurasip J. Embedded Syst.*, vol. 2007, no. 1, 2007, Art. no. 074706.

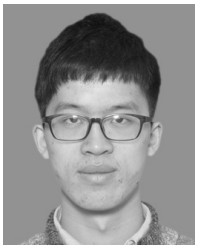
Wufei Wu (S'17) is currently pursuing the Ph.D. degree with the College of Computer Science and Electronic Engineering, Hunan University, China. His research interests include distributed system, embedded computing systems, and cyber-physical systems. He is a Student Member of CCF.

Renfa Li (M'05–SM'10) is currently a Professor of computer science and electronic engineering and also the Dean of the College of Computer Science and Electronic Engineering, Hunan University, China. He is also the Director of the Key Laboratory for Embedded and Network Computing, Hunan, China. He is also an Expert Committee Member of the National Supercomputing Center, Changsha, China. His major interests include computer architectures, embedded computing systems, cyber-physical systems, and the Internet of Things. He is a member of the council of CCF and a Senior Member of ACM.

Guoqi Xie (M'15) received the Ph.D. degree in computer science and engineering from Hunan University, China, in 2014. He was a Post-Doctoral Researcher with Nagoya University, Japan, from 2014 to 2015, and also with Hunan University from 2015 to 2017. He is currently an Associate Professor of computer science and engineering with Hunan University. His major interests include embedded and cyber-physical systems, parallel and distributed systems, and industrial and systems engineering. He is a member of ACM and CCF. He received the Best Paper Award from ISPA 2016.

Jiyao An (M'11) received the M.Sc. degree in mathematics from Xiangtan University, China, in 1998, and the Ph.D. degree in mechanical engineering from Hunan University, China, in 2012. He was a Visiting Scholar with the Department of Applied Mathematics, University of Waterloo, ON, Canada, from 2013 to 2014. Since 2000, he has been with the College of Computer Science and Electronic Engineering, Hunan University, Changsha, China, where he is currently a Full Professor. He has published more than 60 papers in international and domestic journals and refereed conference papers. His research interests include automotive cyber-physical systems (ACPS), fuzzy systems, intelligent systems, computational intelligence, and big data analysis. He is a member of ACM and a Senior Member of CCF. He is an active reviewer of international journals.

Yang Bai received the B.S. and M.S. degrees from Hunan University, Hunan, in 2013 and 2016, respectively, where she is currently pursuing the Ph.D. degree. Her research interests include embedded and cyber-physical systems, and automotive cyber-physical systems.



Jia Zhou is currently pursuing the Ph.D. degree with Hunan University, Changsha, China. His research interests include distributed embedded systems and safety-critical cyber-physical systems.

Keqin Li (M'90–SM'96–F'15) is currently a SUNY Distinguished Professor of computer science with the State University of New York. He is also a Distinguished Professor with Hunan University, China. He has published more than 640 journal articles, book chapters, and refereed conference papers. His current research interests include cloud computing, fog computing and mobile edge computing, energy-efficient computing and communication, embedded systems and cyber-physical systems, heterogeneous computing systems, big data computing, high-performance computing, CPU-GPU hybrid and cooperative computing, computer architectures and systems, computer networking, machine learning, and intelligent and soft computing. He has received several best paper awards. He currently serves or has served on the Editorial Boards of the IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, the IEEE TRANSACTIONS ON COMPUTERS, the IEEE TRANSACTIONS ON CLOUD COMPUTING, the IEEE TRANSACTIONS ON SERVICES COMPUTING, and the IEEE TRANSACTIONS ON SUSTAINABLE COMPUTING.