Vehicular Intrusion Detection System for Controller Area Network: A Comprehensive Survey and Evaluation

Yangyang Liu, Lei Xue, Sishan Wang, Xiapu Luo, Kaifa Zhao, Pengfei Jing,
Xiaobo Ma, Yajuan Tang, Haiying Zhou

Abstract— **The progress of automotive technologies has made cybersecurity a crucial focus, leading to various cyber attacks. These attacks primarily target the Controller Area Network (CAN) and specialized Electronic Control Units (ECUs). In order to mitigate these attacks and bolster the security of vehicular systems, numerous defense solutions have been proposed. These solutions aim to detect diverse forms of vehicular attacks. However, the practical implementation of these solutions still presents certain limitations and challenges. In light of these circumstances, this paper undertakes a thorough examination of existing vehicular attacks and defense strategies employed against the CAN and ECUs. The objective is to provide valuable insights and inform the future design of Vehicular Intrusion Detection Systems (VIDS). The findings of our investigation reveal that the examined VIDS primarily concentrate on particular categories of attacks, neglecting the broader spectrum of potential threats. Moreover, we provide a comprehensive overview of the significant challenges encountered in implementing a robust and feasible VIDS. Additionally, we put forth several defense recommendations based on our study findings, aiming to inform and guide the future design of VIDS in the context of vehicular security.**

Index Terms—**In-vehicle network, Intrusion Detection System, CAN bus.**

I. INTRODUCTION

The Global Automotive Cybersecurity market size is projected to reach USD 3574.5 million by 2028, from USD 571 million in 2021, at a CAGR of 29.6% during 2022-2028 [1]. Modern vehicles consist of 70 to 100 ECUs that interface with the CAN. These units work together to execute various vehicle functions, encompassing powertrain, chassis, and body systems [2], [3]. Traditional designs do not fully consider security issues, such as fake messages, making the vehicle vulnerable to cyberspace [4], and many cyberattack surfaces are exposed [5], [6], [7], [8]. For example, CAN, the current de facto standard for in-vehicle network (IVN), is designed with multiple safety considerations but limited security considerations, such as the nature of the broadcast, the lack of network segmentation, the lack of authentication

Yangyang Liu, Xiapu Luo, Kaifa Zhao, and Pengfei Jing are with Department of Computing, The Hong Kong Polytechnic University;

Lei Xue is with School of Cyber Science and Technology, Sun Yat-Sen University;

Sishan Wang and Haiying Zhou are with Hubei University of Automotive Technology;

Xiaobo Ma is with Department of Computer Science and Technology, Xi'an Jiaotong University;

Yajuan Tang is with College of Engineering, Shantou University.

and data encryption, and the vulnerable arbitration mechanism, which lead to various security issues.

Recently, various attacks are launched against the real vehicles [9], [10] exploiting the vehicular vulnerabilities. In a notable case, researchers Don Bailey and Mathew Solnik from iSec gained unauthorized access to a vehicle and remotely started its engine. They exploited vulnerabilities in the protocols used for remote vehicle control, as documented in their research [11]. Similarly, researchers Miller and Valasek demonstrated their ability to remotely manipulate a Jeep Cherokee while it was traveling at a speed of 70 mph. Exploiting vulnerabilities in the vehicle's entertainment system, they gained control over critical functions such as steering and brake activation, as documented in their work [9]. Furthermore, researchers from Trend Micro showcased a potential attack vector in the realm of vehicular security. This demonstration involved the exploitation of inherent vulnerabilities in the error handling mechanisms of CAN protocols [12]. In addition, the Proof-of-Concept (PoC) attacks were conducted to assess the vulnerability of vehicles through the compromise of the Telematics Control Unit (TCU) [13]. In this comprehensive survey, our first focus entails an in-depth examination of the specific attacks that are targeted by IDSs as well as the CAN vulnerabilities that attackers exploit in their endeavors.

To address the vehicular security issues, especially the issues of CAN, various defense mechanisms are proposed to improve the vehicle security leveraging four major types of techniques, including message encryption [14], [15], ECU authentication [16], [17], safety-related component isolation [18], [19], and VIDS [20], [21]. Among these mechanisms, VIDSs detect potential attacks by monitoring the IVN traffic without modifying the existing IVN architecture or incurring additional IVN traffic, and so that they are more practical compared to other types of defense approaches [22], [23], [24]. Consequently, this survey focuses on the VIDSs for CAN.

More precisely, the VIDSs usually detect anomalies leveraging the features and patterns of the characteristics of the ECUs and in-vehicle traffic, such as the fingerprints of ECUs, the signal features, the clock skews, and message payloads [21], [25]. It is worth noting that, although these VIDS can improve the security of IVNs, they are mainly proposed with the consideration of special issues of the IVN and without comprehensive studies of the security limitations of the IVN. Hence, when they are applied in practice, various challenges will be encountered, such as efficiency, feasibility, and stability.

So we need to collect these papers and compare them in detail to illustrate the limitations of existing methods. Researchers can also find and effectively detect methods based on these limitations.

Although there are works that study the of-the-shelf VIDS [26], [27], [28], [29], [30], [31], to our best knowledge, they cannot provide a comprehensive and practical view of the VIDS to shed light for future VIDS design and implementation. First, many VIDSs have been proposed defending the attacks against IVNs, but the existing surveys just include a limited number of them, such as survey conducted by Tomlinson et al. [27], studying only 17 VIDSs and missing the state-of-art fingerprint-based VIDS. Second, these papers do not offer a detailed description and classification of the attacks targeted by VIDSs. Third, some surveys do not evaluate detection performance of these VIDSs, such as the survey conducted by Young et al. [28], where no evaluation is performed.

Consequently, To address these gaps, we offer a comprehensive survey of existing VIDS, summarizing all CAN-related attacks and detection methods, and providing a detailed comparison. Following the evaluation, we discuss the challenges faced by these methods and outline future development trends. We hope that our survey will generate increased interest in the field of vehicle intrusion detection. We aim for other researchers to gain a comprehensive understanding of existing attacks and detection methods targeting the CAN through our survey. By reading our work, we hope they will discern the differences and limitations among various methods, enabling them to identify potential research directions.

In general, this survey has the following four major contributions.

1) We analyzed 34 research studies related to vehicle attacks and systematically classified them into 18 distinct attack types.
2) We examined 53 different VIDS, carefully analyzing and comparing their threat models, defense scenarios, and defense mechanisms.
3) We reproduced VIDS that can be compared using the same dataset and evaluated these detection methods using real-world vehicle data.
4) In addition to the survey and evaluation results, we delve into a thorough examination of the constraints associated with the investigative defense approach. Subsequently, we explore forthcoming trends in vehicle advancements, elucidating their implications for the future of VIDS.

The remainder of the paper is organized as follows. Section II introduces and compares some other surveys on intrusion detection of IVNs. Section III gives a brief overview of the IVN composition and the vulnerabilities that make it vulnerable to attacks. Section IV analyses the attack models against the collected VIDSs, and Section V details the specific attack scenarios. Section VI details all the VIDS we find, which are evaluated from different perspectives in Section VII. We reproduce and evaluate some VIDSs, and show the test results and the challenges encountered in the implementation in Section VIII. Finally, Section IX discusses the current issues and trends with existing VIDSs. Simultaneously, for the sake of comprehensiveness, we introduce the intrusion detection of

heavy-duty vehicle CAN and the intrusion detection system for the Internet of Vehicles (IoV).

II. RELATED WORK

Although there are several survey papers on existing VIDS [37], [26], [27], [36], [35], [28], [29], [4], [34], [33], [33], [32], [30], [31], they do not provide a comprehensive evaluation of existing VIDSs. They have several limitations and we will describe them in detail. For better illustration, we provide an overview of recent surveys on VIDS and compare their contributions. The results of the comparison are shown in Table I.

First, it is necessary to include more state-of-the-art research works. There are more than 50 VIDSs and new VIDSs are constantly appearing, but some surveys only contain a small portion. For example, Liu et al. [37] merely describe 4 papers about VIDS and the latest paper among them was published in 2016. Avatefipour et al. [26] focus on introducing the CAN bus and its vulnerabilities, and they only analyze 5 research works related to intrusion detection of the IVN. Additionally, they do not give a further comparison and analysis of these papers. Tomlinson et al. [27] detail 17 research works which are published before 2018. Young et al. [28] introduce 15 VIDS based on the detection feature which are published before 2018. Rajapaksha et al. [31] primarily focused on introducing intrusion methods related to AI technology and did not comprehensively cover all IDS relevant to IVN.

Second, these papers do not offer a detailed description and classification of the attacks targeted by VIDSs. While some survey works mention attacks, they either refer to previous research or provide a brief overview of common attack scenarios. They do not enumerate the most recently proposed significant attacks and lack a detailed classification of all attacks. For instance, Aliwa et al. [32] only list six common attack scenarios: CAN bus sniffing, CAN bus fuzzing attack, CAN bus frame falsifying attack, CAN bus injection attack, CAN bus DoS attack, and ECU impersonation. They do not include the latest attack scenarios, such as voltage corruption attacks [38]. Additionally, Young et al. [28] only present three attack demonstrations to illustrate attacks on vehicles. Similarly, Rajapaksha et al. [31] only choose to address 5 common attack scenarios. Such a simple description is insufficient and detailed attack descriptions can help researchers understand the goals of defenses.

Third, appropriate experiments can help researchers understand the advantages of different approaches. All these surveys do not reproduce the VIDSs they introduce, and they also do not evaluate the detection performance of these VIDSs based on a large-scale dataset. The evaluation under the same dataset can help researchers intuitively compare the pros and cons of different methods.

Based on the above limitations of these surveys, we take the further study at existing intrusion detection systems for IVN. First, we search for various paper repositories and relevant conferences/journals to find comprehensive research works. We collect 53 specific VIDSs and analyze them carefully. Second, We analyze and summarise the threat models for

TABLE I: Summary of previous survey works on the field of VIDS

Survey	Year	No of Works	Attack Description	Performance Comparison	Experiment
Rajapaksha et al.[31]	2023	40	X	✓	X
Karopoulos et al.[30]	2022	40	X	✓	X
Aliwa et al.[32]	2021	30	✓	✓	X
Xie et al.[33]	2021	23	X	✓	X
Hafeez et a.[34]	2020	5	X	✓	X
Wu et al.[29]	2019	20	✓	✓	X
Young et al.[28]	2019	15	✓	✓	X
Al et al.[4]	2019	24	✓	✓	X
Lokman et al.[35]	2019	25	✓	✓	X
Dupont et al.[36]	2019	24	✓	✓	X
Tomlinson et al.[27]	2018	17	X	✓	X
Avatefipour et al.[26]	2018	5	X	X	X
Liu et al.[37]	2017	4	✓	✓	X

all these VIDSs, and we also provide a detailed description and classification of the attacks that these VIDSs target. Third, we classify and present these papers in detail based on the data features used by these VIDSs (e.g., ECU characteristics, semantic information, etc.). Finally, we compare the effectiveness of these VIDSs in various ways, including the features used, the detection technologies, the attacks included, the validation methods and the detection results. Furthermore, we also reproduce the VIDSs that can be implemented in real cars and test their detection effectiveness based on the same dataset.
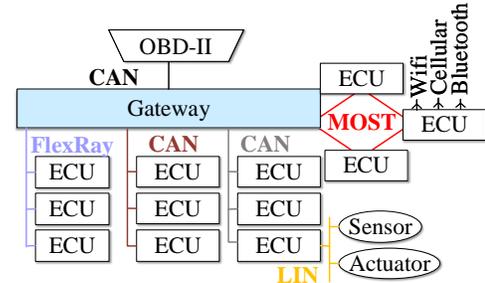
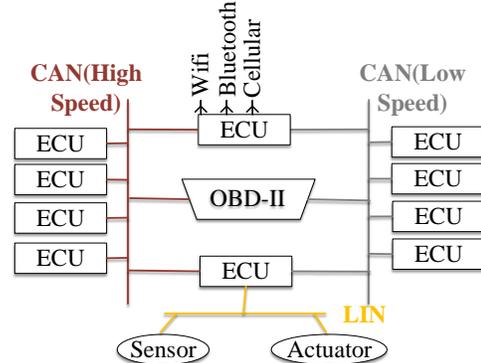## III. PRELIMINARIES

A. In-vehicle Network

Due to the increase of electronic control system complexity and the number of in-vehicle ECUs, the in-vehicle wiring harnesses also increases, which introduces various new challenges to guarantee the reliability and security of the in-vehicle communications. With the purpose of reducing IVN wiring zones and achieving efficient data sharing and exchange, the automotive electronic network system, namely IVN, was born mixed with a variety of network technologies [39]. In this section, we will present the preliminary knowledge of IVN from two major perspectives, including both the commonly used IVN technologies and the ECUs connected to IVN.

1) Electronic Control Unit: ECUs play an indispensable role in controlling the vehicle. Like an ordinary computer, an ECU consists of a microprocessor (MCU), memory (ROM, RAM), input/output interface (I/O), analog-to-digital converter (A/D), and large-scale integrated circuits. It adjusts and manipulates the running of vehicles with different sensors and controllers. In modern automobiles, ECUs are used in various modules, such as engine control module (ECM), Powertrain Control Module (PCM), Transmission Control Module (TCM), and so on. Also, the ECUs need to exchange information between each other during running. For example, the ECU that controls the dashboard display requires various vehicle states, such as vehicle speed. Consequently, the ECUs must possess a relatively stable and efficient network environment.

2) IVN Technologies: As shown in Figure 1, there are two common types of IVN architectures. In the first architecture (i.e., Figure 1(a)), the in-vehicle control domains of IVNs are connected to a central gateway, which provides an onboard diagnostic (OBD-II) port for diagnosing from outside of the

(a) The architecture of IVN with gateway [40].

(b) An IVN architecture without gateways [8].

Fig. 1: Two common IVN architectures.

TABLE II: Specifications of the widely used IVNs.

Network Technologies	Bitrate(Max)	Medium	Standard
LIN	19.2 Kbps	Single Wire	Serial
CAN	1 Mbps	Twisted Pair	CSMA/CR
CAN-FD	8 Mbps	Twisted Pair	CSMA/CR
FlexRay	10 Mbps	Twisted Pair or Optical Fibre	TDMA
MOST	150 Mbps	Optical Fibre	TDMA
Automotive Ethernet	10 Gbps	Twisted Pair	Switched Full Duplex

vehicle [40]. In Figure 1(b), the OBD-II port directly connects to the IVN without any gateway, and thus the external devices can easily monitor the in-vehicle communication data.

The in-vehicle ECUs have different requirements on the

speeds of the communication traffic. For example, the body-related states (such as lights and door locks) can be transmitted in a low speed, and whereas the safety-related states (such as steering wheel angle and brake pedal pressure) need to be transmitted in a high speed. Intuitively, the high communication speed require high cost and advanced techniques [41]. Therefore, in order to reduce costs and meanwhile meet the various in-vehicle communication requirements between different ECUs, then vendors design the IVNs with a mix of various network techniques. Such as shown Figure 1, the most commonly used network technologies are CAN [42], Local Interconnect Network (LIN) [43], FlexRay [44], and Media Oriented Systems Transport (MOST) [41]. Also, Table II illustrates specifications of these IVN techniques, including maximum transmission rate, transmission media, and the transmission standards. For example, LIN is a low-speed serial communication protocol with the maximum transmission rate of 19.2 Kbps, and it uses single wire as the medium in the physical layer.

Among them, CAN becomes a de facto IVN protocol and it is proposed by Robert Bosch GmbH to define the layer-1 and layer-2 functionalities of the Open Systems Interconnection (OSI) network model in 1986 [45]. CAN is typically used to provide an efficient, stable, reliable, and economical communication method between ECUs without a host computer, and it usually controls the core subsystem of vehicle, such as the engine power system, body control system, and electronic central electrical system.

LIN is a low-cost master-slave serial communication bus released in the late 1990s, and it is designed to serve as a cheap alternative to CAN in IVNs [46]. Nowadays, LIN is a complement to CAN and widely used in subsystems of IVNs, which do not have the high communication speed requirement.

FlexRay is a new communication bus, which is released in 2009, and it is developed to support faster and more stable communication than CAN. Compared with CAN, the main advantages of FlexRay are the higher maximum data rate (10 Mbps) and deterministic time-triggered standard (i.e. time division multiple access (TDMA)) [44].

MOST is developed mainly for the transmission of multimedia data, and its maximum data rate is 150 Mbps. Hence it is much more suitable to the multimedia data than CAN.

As a mature and reliable standard communication bus, CAN has been widely used in various vehicles for over 30 years. Usually, it controls the core part of the IVN. Whereas, LIN, FlexRay, and MOST are generally used as a supplement or auxiliary to CAN in the vehicle. However, CAN has various security limitations [47], [40], [48], and therefore most of the IVN intrusion detection systems are proposed for CAN.

In addition to traditional vehicle network technologies, we introduce two emerging technologies: CAN with Flexible Data-Rate (CAN-FD) and Automotive Ethernet (AE). Due to the increase in real-time data produced by control modules and sensors, CAN needs to meet stringent latency limits, thereby increasing its burden. Despite several alternatives being proposed, substantial efforts continue to focus on enhancing CAN, which has been upgraded to a CAN with Flexible Data-Rate (CAN-FD). This protocol was developed in 2011 and released by Bosch (in collaboration with industry experts) in 2012. Today, CAN-FD is used in modern high-performance vehicles [49]. CAN-FD, compatible with existing CAN networks, allows the new protocol to operate on the same network as traditional CAN. It can dynamically switch to different data rates and handle larger or smaller message sizes. The main differences between traditional CAN and CAN-FD are: 1) Increased length: Traditional CAN offers 8 data bytes, while CAN-FD provides flexible data rates ranging from 0-64 bytes per frame without needing to change the CAN physical layer, reducing protocol overhead and increasing efficiency. 2) Increased speed: Standard CAN networks are limited to 1 Mb/s. CAN-FD boosts the effective data rate to 8 Mb/s, which is eight times faster than traditional CAN. 3) CAN-FD can increase communication efficiency among multiple ECUs by up to 30 times, with faster speeds. 4) Higher reliability: One way to ensure reliability is through the use of Cyclic Redundancy Check (CRC). CAN-XL (CAN eXtended Length) is an advancement over CAN-FD, designed to further increase data transmission rates and flexibility. It supports larger data frames and higher transmission rates, providing enhanced scalability and performance potential for future automotive applications. On March 22, 2024, the ISO released the 11898-2:2024 standard, which elevates the maximum speed of the CAN bus from the industry-recognized 8 Mbps of CAN FD to up to 20 Mbps, with data payloads of up to 2048 bytes.

Automotive Ethernet is another protocol that could become mainstream in the future. In recent years, significant changes in the automotive industry, including the provision of various vehicle functions and the introduction of autonomous vehicles, have generated massive amounts of data. Automotive Ethernet has been proposed as the communication standard for IVNs because existing traditional protocol-based IVNs cannot cope with the increased bandwidth. Currently, various Ethernet protocols have been or are being used in Ethernet-based IVNs, such as BroadR-Reach, MOST150, IEEE 802.3bw (100BASE-T1), IEEE 802.3bq-2016, and IEEE 802.3ch-2020 [50]. In fact, with the increase in vehicle intelligence, many automakers, such as Tesla and BMW, have already started using Automotive Ethernet in commercial vehicles [51]. Moreover, automakers have unified their views on the use of Ethernet, and many diagnostic software applications are compatible with Automotive Ethernet [52]. As a new automotive network technology, the widespread adoption of Automotive Ethernet in vehicles will not be instantaneous. Automotive Ethernet will not replace existing vehicle network technologies in the short term. After entering the automotive field, Automotive Ethernet technology will initially integrate gradually from specific subsystems and ultimately advance the evolution of automotive network architecture. Automotive Ethernet holds significant potential. Given that CAN remains the mainstream transport protocol in current commercial vehicle networks, our study primarily focuses on traditional CAN.

IV. THREAT MODEL

In this section, our primary focus centers on an in-depth examination of the threat models associated with all VIDS

under consideration. In various variants of VIDS, the authors postulate diverse adversary profiles encompassing varying attack capabilities, thereby influencing the spectrum of detectable attack modalities by the system. Subsequently, a comprehensive consolidation of the aforementioned assumptions inherent to these systems is presented, establishing a profound linkage with the associated attack scenarios. Next, a thorough exposition of the threat models is articulated, encompassing three fundamental dimensions: attack surfaces, attack capabilities, and attack purposes. Furthermore, the interplay and synergy between these tripartite facets are visually depicted in Figure 2. First, adversaries access the IVNs through various attack surfaces. Second, adversaries can own various capabilities to invade the IVNs after they have access to the IVNs. Finally, adversaries can achieve different attack purposes when they have different capabilities to attack the IVNs.

A. Access Surfaces

Initially, the adversaries must establish connectivity with the IVNs through distinct access surfaces. In accordance with pertinent research conducted by Koscher et al. (2010) [48], it has been ascertained that adversaries possess the capability to gain access to the IVNs via two distinct categories of surfaces, namely physical surfaces and network surfaces. Physical surfaces commonly pertain to hardware components that establish a direct link with the vehicle, such as diagnostic ports. On the other hand, network surfaces encompass the network connections that bridge the vehicle to the cyberspace, encompassing technologies such as Wi-Fi and Bluetooth. Subsequently, an elaborate exposition elucidating the intricate particulars of these two attack surfaces shall ensue.

Physical surface: The adversaries that utilize physical surfaces have to get close to the target vehicle. They can take three methods to attack the vehicle. Firstly, adversaries can keep malicious devices on the OBD-II port (i.e., a physical diagnostic port which is usually above the accelerator pedal and connected to the IVN [22].) and attack the IVN directly. For example, researchers from the Argus Research Team find a way to hack into the Bosch Drivelog ODB-II dongle that is plugged into the OBD-II port, and inject different malicious messages into the CAN bus. They stop the engine of a moving vehicle by connecting to the dongle via Bluetooth [53]. Adversaries can also insert the device briefly and launch an attack by injecting malicious code into the ECU in the vehicle [54], [55]. Another method is that the adversaries change the firmware of ECUs or install an additional ECU while the vehicle is being repaired [8].

Network surface: There are already many studies conducted on the radio interfaces, which enable the vehicles to accept external inputs and may cause the relevant on-board ECU to be controlled [48], [56]. Among the attacks exploiting such attack surfaces, most of the attacks are only effective at short distances due the features of the target communication types [57], [58].

B. Attack Capabilities

The attack capacities of the adversaries are different, and we classify them into the following four major categories, including inserting an OBD device, partially compromising an ECU, fully compromising an ECU, and inserting an external ECU, according to the attack methods. Both of inserting an OBD device and inserting an external ECU add a new node to the IVN. The OBD device connects to the network directly via the OBD-II port while the external ECU connects to the IVN by changing the internal architecture of the vehicle. During partially or fully compromising an ECU, the attack target is an existing ECU of the IVNs. The partially compromised ECU cannot send CAN messages directly, and the fully compromised ECU is also able to inject forged messages into IVN.

1) The malicious OBD device: The OBD-II port is an important surface for communication between the IVN and external devices. Since the OBD-II port is exposed to the user, the adversary only needs to plug the attack device into the port without dismantling the vehicle. However, there are certain limitations when the adversary injects malicious messages through the OBD-II port. The layout of the IVN can affect the effectiveness of this attack. As the Figure 1(a) shows, the gateway in the vehicle can obstruct the broadcast of the normal in-vehicle messages and only allow the diagnostic messages to transmit in some particular vehicle models [59]. For example, Zhou et al. [59] find the IVNs of two vehicle models, 2019 Chevrolet Malibu and 2019 Chevrolet Cruze, are not directly connected to the OBD-II port. They can not get the in-vehicle traffic through the port. In contrast, the IVNs of another vehicle model, the 2012 Buick Regal, can be monitored directly through the OBD-II port.

2) The partially compromised ECU: Through a partially compromised ECU, it is assumed that the adversary suspends the ECU or puts the ECU in the listen-only mode. These adversaries who partially compromising an existing ECU can eavesdrop on in-vehicle communications and stop the ECU from sending normal messages to other ECUs, but they can not inject forged messages. The adversaries can suspend the ECU through the diagnostic commands or hardware vulnerability of the ECUs, and we introduce them in detail.

Nowdehi et al. [60] demonstrate the possibility of such an attack via diagnostic protocols. The state of ECU varies in different session modes. Nowdehi et al. show that when the session mode is changed to programming mode, the ECU can only listen to the bus but not send messages. In other words, the adversary can partially compromise an ECU by changing the session mode of this ECU through diagnostic command.

In [20], Cho et al. propose another method to partially compromise an existing ECU. They mention that an ECU with Microchip MCP2515 [61], which is one of the most common CAN controllers, can be changed into various operation modes like configuration, normal, and listen-only through Serial Peripheral Interface (SPI). Therefore, the adversaries can make the ECU enter different modes such as listen-only mode by utilizing the user-level features for configuring the CAN controller.

3) The fully compromised ECU: Unlike partially compromised ECU, with a fully compromised ECU, the adversary can control the ECU completely and have access to the memory data. Apart from listening to the bus and stopping ECU transmission, the adversary can also inject any fabricated messages into
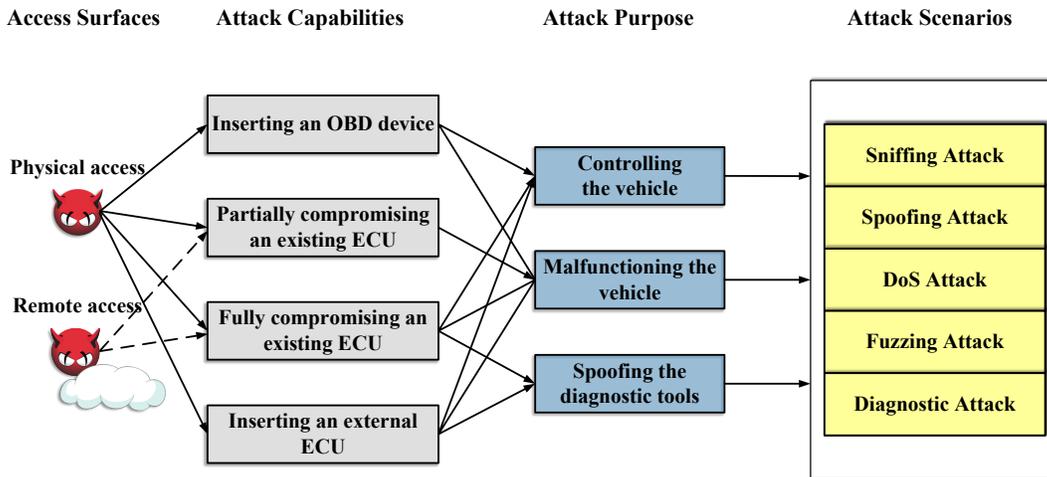
Fig. 2: The threat model of the attack.

the bus while fully controlling the ECU. Many researchers demonstrate the methods to fully compromise an ECU.

For example, Checkoway et al. [47] demonstrate vehicle vulnerabilities in some different external channels. In addition, they evaluate the potential for controlling the ECUs via the prototype implementations for TPMS (tire pressure monitoring system), Bluetooth, FM (Frequency modulation), RDS (Radio Data System), and Cellular channels based on the vulnerabilities. For example, they control the ECU in telematics unit to send CAN messages by predefined tire pressure sequences.

In [6], Hoppe et al. add a few lines of malicious code to the arbitrary ECU to control the vehicle. In the test, once a predefined condition is met, the code replays the CAN messages containing the flag for opening the driver window.

Koscher et al. [48] successfully control the vehicle operations and completely ignore driver input, such as disabling the brakes, stopping the engine, and so on. They propose an attack in which malicious code is embedded in the telematics unit, and the attack causes the vehicle to lose control. Furthermore, they completely erase any evidence of its presence after the attack.

4) The malicious additional ECU: By inserting an external ECU, the adversary can listen to the IVNs and inject self-defined messages into the IVN. The function of the external ECU is similar to that of the fully compromised ECU, and the adversary can also inject forged messages into the bus through the additional ECU. However, compared with fully compromising an ECU, inserting an external ECU has to manually install a piece of new hardware equipment into the vehicle. The implementation of the attack needs to dismantle the vehicle and requires the adversary to have detailed knowledge of the vehicle architecture. Additionally, when the adversary injects fabricated messages with different IDs that are supposed to be sent by other ECUs, the risk of detection by fingerprint-based VIDS [20] dramatically increases.

C. Attack Purposes

The adversaries launch attacks against the IVN with different purposes, which can be categorized into remote vehicle control, vehicle malfunctioning, and diagnostic data spoofing. The first

type of purposes indicate the adversaries aim to fully control the vehicle remotely. The adversaries with the seconde type of purpose aim to let the vehicle run out of control, causing driving accidents. The third type of adversaries target on spoofing the diagnostic devices and concealing the safety issues by injecting fake data into IVN. Next, we present more details about these attack purposes.

1) Controlling the vehicle: The adversaries try to make the vehicle run as they want and attack it at a specific moment. They can mislead the vehicle to react as they want by sending the forged in-vehicle messages to the ECUs, and they can also send well-designed diagnostic commands to control the vehicle's actions directly. For example, researchers from the Argus Research Team stop the engine of a moving vehicle through the diagnostic commands [53], while Miller et al. [8] manage to control the vehicle's turn signals by sending forged in-vehicle messages to the vehicle's ECU.

2) Malfunctioning the vehicle: Instead of taking full control of the vehicle, the adversary can also make the vehicle lose control. In this attack purpose, adversaries continuously send incorrect messages to the ECUs or prevent the ECUs from sending in-vehicle messages. For example, Koscher et al. [48] find that significant damage to the vehicle can be done by simple fuzzing of packets (i.e., iterative testing of random or partially random packets) because the range of valid CAN messages is rather small. Additionally, Cho et al. [62] propose a new type of Denial-of-Service (DoS) attack called bus-off attack. On two real vehicles, through iterative bus-off attacks, the victim ECU enter the bus-off mode and can not send any messages. As a result, the two vehicles get out of control.

3) Spoofing diagnostic tools: Another attack purpose is to spoof diagnostic tools and conceal security vulnerabilities in the vehicle. In this attack purpose, adversaries mask the loss of the safety functionalities which are removed or fail. This attack can endanger the vehicle's occupants due to the loss of a safety system. In order to conceal security vulnerabilities, the adversaries manage to emulate the behaviors of a safety system within a diagnostic session by any compromised device with access to the CAN bus. For example, Hoppe et al. [6] remove
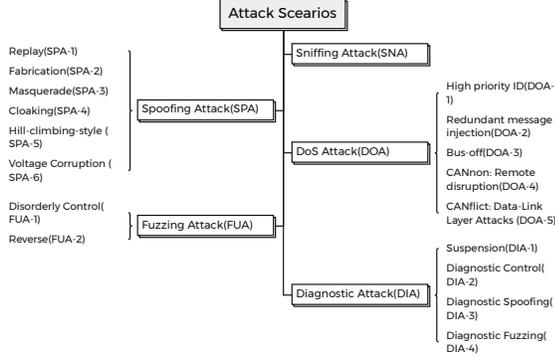
Fig. 3: Detailed taxonomy of attack scenarios.

the airbag control system and hide the absence of the system. They record the reactions to diagnostic queries in the presence of the airbag control module at first, and then they replay these replies when diagnostics software sends the diagnostic queries. As a result, the diagnostics software reports the airbag control module's presence (including its name, part no., etc.) without any error conditions.

V. TAXONOMY OF ATTACKS

The adversaries usually exploit the vulnerabilities of IVNs to attack the ECUs, and the attacks can prevent normal communication of ECUs on the IVNs or transmit malicious messages to specific ECUs [8], [48]. There are also attacks that are not related to the IVNs or are not targeted by the VIDS, and they are not the focus of our attention. For example, an attack against the remote keyless system may allow the adversary to freely open the door [63], [64]. If spoofing the remote keyless system is the ultimate purpose of the adversary, the IVNs are irrelevant, and we ignore the attacks.

To provide a taxonomy of IVN attacks, we collect and observe the attacks from the publications we studied. Afterward, we classify these attacks according to the injected malicious messages, the effects on the ECUs, the attack purpose, and the attack methods. Figure 3 shows the taxonomy.

Particularly, we classify the attacks according to the attack methods: Sniffing attack (SNA), Spoofing attack (SPA), DoS attack (DOA), Fuzzing Attack (FUA) and Diagnostic attack (DIA).

A. Sniffing Attack

Since ECUs broadcast all messages in CAN and there is no authentication and encryption in the communication process, any ECU that joins CAN network can listen to all messages [65]. The adversary can have access to CAN remotely or physically and listen to the CAN messages transmitted in CAN directly. Adversaries can directly speculate on the regularity of messages and the semantics of messages. They can detect specific private information in the vehicle or carry out further attacks based on message semantics. Existing IDSs are difficult to detect this kind of attack because the attack has little influence on the CAN.

B. Spoofing Attack

Spoofing attack against the vehicle is launched by forcing the target ECU to accept wrong messages and react in the wrong way. An adversary can disrupt the normal operation of the ECU or even take control of the ECU through a spoofing attack. Additionally, adversaries can take different methods to deceive the target ECU. Based on the methods to deceive the target ECU, these attacks can be divided into six categories.

1) Replay: The purpose of replay attack is to override the normal messages with the valid messages that have already been transmitted to the IVN. To mount a replay attack, the adversary needs to fully compromise an ECU or fix an extra ECU in the vehicle. Through the attack capability, the adversary can listen to the IVN and replay the target messages. What's more, the frequency of forged messages is higher than that of normal messages to occupy the control of the target ECU. For example, previous research [40], [66] mentioned that the adversary needs to inject messages 20-100 times faster than the original ECU to make the target ECU listen to the injected messages successfully.

2) Fabrication: The purpose of fabrication attack is to override any periodic messages sent by an uncompromised ECU so that the receiving ECUs are distracted and fail. Through an in-vehicle ECU fully compromised and an additional ECU added to the vehicle, the adversary can fabricate and inject messages with forged ID, data length, and payload to control the specific ECU. A fabrication attack is similar to the replay attack except for sending the messages that have been modified or forged. Additionally, the fabrication attack also needs a higher injection frequency, whose reason is the same as that of the replay attack. For example, in [67], the messages are inserted at 5 times of the transmission rate of normal messages to control the ECU.

3) Masquerade: Masquerade attacks aim to manipulate unauthorized or compromised ECUs to impersonate legitimate ECUs and affect vehicle operations, utilizing two main approaches. In the first approach, adversaries either connect an unauthorized device to the CAN bus or control an existing ECU, sending forged messages with IDs matching legitimate ECUs while the original legitimate ECUs remain active. The second approach requires compromising two ECUs: one fully compromised and one weakly compromised target ECU (or using an unauthorized device instead of the fully compromised ECU). The fully compromised ECU injects forged messages to replace the weakly compromised target ECU's transmissions [20], [21], [68]. This is achieved by triggering transmission errors in the weakly compromised target ECU to increase its Transmission Error Counter until reaching bus-off state, forcing it to cease transmission, while the fully compromised ECU simultaneously sends malicious messages that mimic the target ECU's normal traffic pattern, making detection challenging.

4) Cloaking: Clocking attack is a special attack against specific IDSs. Cho et al. [20] proposed a method to identify malicious ECUs by using clock offset as the fingerprint of the ECU. In previous detection systems, they assumed that clock skew could not be imitated. Sagong et. al. propose the cloaking attack, an intelligent masquerade attack in which an adversary

modifies the timing of transmitted messages to match the clock skew of a targeted ECU.

5) Hill-climbing-style: Hill-climbing-style attack is designed to deceive multi-frame based fingerprinting systems [69], such as Viden fingerprinting system [21] and Clock-based IDS (CIDS) [20]. In a multi-frame based fingerprinting system, a batch of multiple frames has to be collected in order to perform one update of the fingerprinting threshold. Such fingerprinting schemes are vulnerable to the Hill-climbing-style attack, where the adversary is able to control the quantity of attack frames among the batch of frames collected, so that the attacker ECU can both hide its identity and shift the fingerprinting decision threshold gradually.

6) Voltage Corruption: With the specific purpose of evading the existing voltage-based IDSs, the voltage corruption attack is launched through poisoning the training data of such IDSs using two compromised ECUs (i.e., an attacking ECU and an accomplice ECU) [38]. Intuitively, by exploiting the static ID, periodicity, and predictable payload-prefix characteristics of CAN frames from one ECU, the adversary can let the attacking ECU be in the error-passive state and perform simultaneous transmission with a legitimate ECU with the assistance of the accomplice ECU. Consequently, the mixed voltages are collected as the training data for fingerprinting and the voltage-based fingerprinting of the victim is corrupted. Even worse, since the attacking ECU and the victim transmit dominant bits at the same time, such attack cannot be detected by existing IDSs.

C. DoS Attack

During a DoS attack, the ECU is suspended or unable to receive normal messages. Considering the methods of attack against the ECU, we can classify DoS attacks into five major categories.

1) High priority message injection: The goal of the DoS attack with high priority ID messages is to occupy the CAN bus and block normal messages. To perform the attack, the adversary must have full control of a normal ECU or an additional ECU. Since a lower CAN ID means higher priority and can get CAN bus access according to the arbitration mechanism of CAN [62], the injected attack messages are usually set with low IDs, such as 0x000 that has topmost priority [70]. Additionally, the adversary must increase the number of messages to fill the bus. For example, in [66], 6000 topmost priority messages are injected into the bus per second to fill the bus. In the attack, the valid messages are be blocked, and all ECUs receive none message. As a result, these ECUs can not work normally, and the vehicle is out of control.

2) Redundant message injection: The purpose of redundant message injection attack is to interfere with normal ECUs receiving messages and make the ECUs fail. In order to mount the attack, the adversary has to fully compromise an ECU or add an extra ECU. In the attack, the adversary can forge and inject messages massively through the compromised ECU. The adversary can inject the traffic to surpass the CAN bus's maximum capacity, which is only 1 Mbps. Additionally, the maximum size of a CAN message is 128 bits (contains ID, CRC, bit stuffing and all other elements), and there are at least three consecutive recessive bits (i.e.,1) called *'interframe space'* between messages [71]. Therefore, the adversary can inject about 8000 messages per second to launch this attack [66].

3) Bus-off: The purpose of the bus-off attack is to disconnect or shut down an uncompromised ECU. Through a fully compromised ECU or an additional ECU, the adversary can monitor the transmission of in-vehicle messages and inject malicious messages at a specific moment. The bus-off attack utilizes the arbitration and the error handling mechanism in CAN [62]. To perform a bus-off attack, the adversary has to transmit forged messages that satisfy the following three conditions. First, the forged message should have the same ID as the message transmitted by the target ECU. Second, the forged message has to be transmitted at the same time as the message transmitted by the target ECU. Third, the forged message has at least one bit position in which its signal is dominant (i.e., 0), whereas victim's signal is recessive (i.e., 1),and all preceding bits of the two messages should be the same. When an adversary sends forged messages that meet the above conditions to the IVN, the can bus will detect a bit error and the error counter of the target ECU will increase. Then the adversary will send the forged messages constantly. After the error counter accumulates to a certain threshold, the target ECU will turn off itself because of the error handling mechanism. As a result, the target ECU can not send or receive CAN messages until it is reawakened.

4) CANnon: Remote disruption: Kulandaivel et al. introduce a new class of attacks that leverage the peripheral clock gating feature in modern automotive microcontroller units (MCUs) [10]. By using this capability, a remote adversary with purely software control can reliably "freeze" the output of a compromised ECU to insert arbitrary bits at any time instance. Utilizing on this insight, they develop the CANnon attack for remote shutdown.

5) CANFlict: Data-Link Layer Attacks: CANFlict is a stealthy attack that can shut down the ECU in a bit-level granular way [72]. De et al. exploit polyglot frames and pin conflicts to perform data-link layer attacks against CAN, making use of different peripherals already present on the microcontroller. CANflict enables an attacker to exploit known vulnerabilities of the CAN protocol to remotely implement read and write attacks without any assumption on the periodicity of the transmitted messages.

D. Fuzzing Attack

Fuzzy attack is a common attack that requires only a small amount of a priority knowledge about the IVN [66], [73], [74]. According to the validity of IDs, the fuzzy attack can be divided into two categories according to the CAN identifiers that the adversary uses, including

1) Disorderly Control: The fuzzy attack with random IDs aims to make all ECUs in the vehicles receive unpredictable messages and get messy. To mount an attack by injecting random messages with random IDs, the adversary needs to have a fully compromised ECU or additional ECU added to the vehicle. In this attack, the adversary does not need to have a

complete understanding of the IVNs or reverse-engineering [48]. In fact, because the range of valid CAN messages is rather small, significant damage can be done by simple fuzzing of messages completely (i.e., randomly spoofed identities with arbitrary data) [75], [73].

2) Reverse: The goal of this attack is to reverse engineer the specific meaning of CAN messages. During this attack, the attack capabilities that the adversary needs to master are the same as that of the other fuzzy attack. In this attack, the adversary has to inject carefully forged messages whose fields are constantly being modified [76]. Then, the adversary infers the meaning of each field in the CAN message based on the response of vehicles.

E. Diagnostic Attack

Diagnostic communication is usually used for vehicle mechanics and developers to test or diagnose the vehicle's state. The messages which are used in diagnostic communication (i.e., diagnostic messages), are different from the in-vehicle normal messages used for communication between ECUs, and they are usually injected into the vehicle from the OBD-II port. We conduct in-depth research on diagnostic communication and come up with some diagnostic attacks.

1) Suspension: Suspension attack in diagnostic communication aims to stop the transmissions of the target ECU and make it be listen-only mode. To mount a suspension attack in diagnostic communication, the adversary only needs to connect to the OBD-II interface. If the adversary can control or add an ECU, he can also carry out such an attack. The implementation of this attack exploits the diagnostic session in diagnostic communication. The diagnostic session enables a specific set of diagnostic services and functionality in the ECUs, and an ECU will be in various states for different sessions [77]. Nowdehi et al. [60] prove that the ECU can only monitor the bus when the session mode is changed to programming mode.

2) Diagnostic Control: The purpose of the control attack is to control the behaviors at a special moment and do harm to the vehicle and driver. Control attacks exploit services in diagnostic communications that can control the behaviour of the vehicle (such as stop the engine [53]), and the adversary can control the vehicle even when the vehicle is running. If an adversary sends a dangerous control command at an inopportune moment, this is a huge threat to the safety of drivers. The adversaries can control the motion state of the vehicle (such as turning off the engine, acceleration, braking and changing vehicle steering) through diagnostic messages directly. These control commands are most closely related to the security of the vehicle and difficult to reverse [8]. In addition, related dynamic parameters (such as speed, RPM, steering wheel angle) are also the focus of researchers and these attacks are easy to detect [78].

3) Diagnostic Spoofing: The spoofing attack in diagnostic communication aims to deceive the diagnostic devices and conceal the true condition of the vehicle. To mount this attack, the adversary needs a fully compromised ECU or an additional ECU to send diagnostic messages to the diagnostics devices used by vehicle mechanics. When the adversary fully compromises an ECU, he can record the reactions to diagnostic
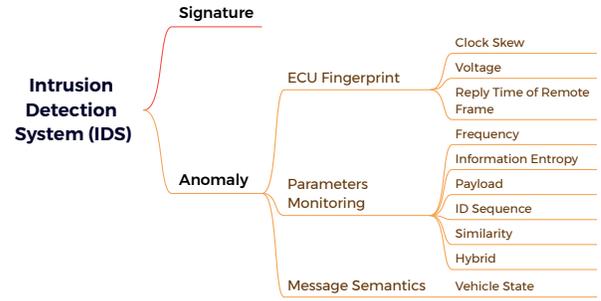

Fig. 4: Existing intrusion detection systems.

queries from diagnostic devices and replay the record messages to spoof the diagnostic devices. For example, in [6], Hoppe et al. spoof the diagnostics software and hide the absence of the airbag control module. Specifically, they record the reactions to diagnostic queries in the presence of the airbag control module at first. Then, these replies are successfully replayed in the absence of this module. As a result, the diagnostics software reports the airbag control module's presence (including its name, part no., etc.) without any error conditions.

4) Diagnostic Fuzzing: In IVN, the diagnostic messages are communicated following specific diagnostic protocols, thus the adversaries can first reverse-engineer the diagnostic protocols and then launch attacks by building the attacks messages following the diagnostic protocols [79]. Diagnostic fuzzing attack is the first step in reverse engineering, and adversaries can obtain the specific format of the diagnostic protocol through the feedback of the ECU. In addition, since all such attacks are launched leveraging the messages conforming to the protocols, it is hard to detect these attacks according to the underlying protocols.

VI. DESCRIPTION OF EXISTING INTRUSION DETECTION SYSTEMS

Cybersecurity becomes essential for vehicles, and various vehicular VIDSs have been proposed recently. We curated a collection of 53 seminal or impactful papers. It is important to highlight that our selection primarily focuses on papers investigating VIDS for the CAN. We intentionally omitted works related to other network protocols. In this section, we study the methodologies adopted by the existing VIDS in detail and Fig. 4 demonstrates our specific approach to classifying these IDSs. Tab. III shows the classification results of existing IDSs based on our approach.

A. Signature-based VIDS

The signature-based introduction detection approaches are manly applied to detecting the known attacks. Intuitively, the traffic features of the known attacks are summarized and set as signatures, and researchers monitor the current network traffic and detect intrusions according to these features. The messages whose features match these signatures are marked as violations.

The signature-based VIDS has various advantages. Since this method does not require ECU to possess powerful computing resources, signature-based VIDS is easy to deploy in

vehicle [80]. Furthermore, this type of detection method can detect known attacks with high accuracy and low error rate, and can determine which type of attack and how many times the ECU is confronting [81].

However, the signature-based VIDS also has its own limitations. First, it cannot detect the attack, of which the traffic features are not specified in the predefined knowledge base. Many researchers are devoted to proposing the different attack methods on IVN security continually (e.g., [7], [40], [8], [62]), and these new attacks suggest that it is impractical to consider all attack methods. It is critical and challenging to keep the signature databases up-to-date with frequent updates. Despite different problems and difficulties, the researchers also propose some signature-based VIDS. We will give details of them below.

In [82], Larson et al. propose a specification-based VIDS that can be implemented in the specific ECU. The ECU traffic can be analyzed based on the information derived from the ECU-behavior security specifications and CAN protocol stacks. They evaluate the applicability of the detection and show that most attacks can be detected. However, the paper is primarily based on rules developed by the *CANOpen* protocol [83], a typical application layer protocol used on CAN. In reality, the application layer protocols for IVNs are developed by individual OEMs themselves. The specifications they propose are not necessarily applicable to all vehicles.

In [68], Studnia et al. propose a language-based VIDS for vehicle embedded networks. They exploit the high predictability of the IVN and extract attack signatures from the behavior models of different ECUs in the vehicle. Using this approach, they can detect malicious sequences of messages transmitted on the IVN.

Brief Discussion: Signature-Based VIDS offers notable advantages, including high accuracy in detecting known attacks, low false positive rates, and low computational overhead, making it feasible for deployment on resource-constrained ECUs. However, its reliance on predefined attack signatures limits its ability to detect novel (zero-day) attacks, and maintaining an up-to-date signature database requires continuous updates and significant effort. Additionally, these methods often struggle with proprietary vehicle protocols, making them less adaptable across different automotive systems. Due to these limitations, researchers are increasingly focusing on anomaly-based detection methods, which can identify previously unknown threats by learning normal network behavior and detecting deviations, thereby offering greater adaptability and robustness against evolving cyber threats in CAN.

B. Anomaly-based VIDS

For anomaly-based intrusion VIDS, researchers build normal behavior profiles by training the normal model of the system activity at first. Then, they utilize the deviations between the profiles and the traffic under test to detect intrusions. Comparing with signature-based intrusion detection, the anomaly-based intrusion is not based on prior knowledge of the known attacks, and it can detect previously unknown attacks. However, it's challenging to determine reliable anomaly boundaries because some normal behaviors are not constant, and the adversary can imitate normal behaviors to spoof the detector [84].

Despite these disadvantages, many researchers pay attention to propose various detection methods to improve detection rates and avoid being evaded. In the following, we will introduce these methods detailedly. These methods can be divided into *ECU fingerprint-based VIDS*, *parameters monitoring-based VIDS*, and *message semantics-based VIDS*.

1) ECU Fingerprint-based VIDS: Resulting from the differences in physical properties of ECUs, different ECUs always have different hardware fingerprint. In the communication among ECUs within the IVN, each ECU possesses one or more unique IDs that only it can use for transmission. It is important to highlight that when developing current IDS, researchers often overlook special messages like diagnostic messages and remote frames. Therefore, the matching of ID and fingerprint can be exploited to detect the compromised ECUs that send malicious messages with forged ID. Researchers use various fingerprints of the ECUs to detect the intrusions. Based on the type of fingerprints, We distinguish between clock skew-based VIDSs, voltage-based VIDSs, and reply time of remote frame-based VIDSs.

a) Clock Skew-based VIDS: The sending time of a CAN message is affected by the clock frequency of the ECU. Due to hardware differences, the clock frequency of different ECUs is slightly different. In fact, researchers have proposed various schemes for fingerprinting network devices by estimating their clock skews through the timestamps carried in their control packet headers [85]. Therefore, researchers try to apply the technology to the IVN, and they propose many VIDSs that use the clock skew to mark off different ECUs and identify the mismatching of ECU and ID.

Cho et al. [20] propose a clock-based VIDS (CVIDS). They measure the intervals of periodic CAN messages at first. Then, they extract clock skews from these intervals for fingerprinting specific ECUs and model their clock behaviors using the recursive least squares (RLS) algorithm. Afterwards, based on the model, CVIDS detects intrusions via cumulative sum (CUSUM) analysis.

Ying et al. [86] also study the effect of clock skew and present a clock skew-based VIDS based on the widely used network time protocol (NTP). Compared with state-of-the-art (SOTA) VIDS [20], this method simplifies updating the average and accumulated skew caused by clock skew.

Furthermore, Ying et al. continue to study this feature. They propose the cloaking attack in [87] which is aimed to avoid the detection of clock skew-based VIDSs and provide formal analyses of the attack for two clocks skew-based VIDSs, i.e., the SOTA VIDS [20] and the NTP-based VIDS [86]. The experimental results find that the average prediction error is within 3.0% for the SOTA VIDS and 5.7% for the NTP-based VIDS.

Zhou et al. [59] directly measure the bit time of the CAN frames, which is determined by the CAN controller and transceiver. In contrast to previous VIDSs based on clock skew, the approach does not have to worry that an attacker will use software to simulate the clock skews of victim ECU. However, this method requires additional equipment to monitor the CAN's electrical signals and a separate detector for each CAN path.

b) Voltage-based VIDS: Instead of clock skew, researchers also focus on other fingerprints. In [88], Murvay et al. use the Mean Squared Error (MSE) of voltage measurements as fingerprints of ECUs, but they use the voltages measured on a low-speed (10Kbps) CAN bus, which is far from contemporary vehicles that usually operate on a 500Kbps CAN bus. Researchers attempt to apply this technology to IVNs, and they propose many voltage-based VIDS.

Cho et al. [21] propose a novel scheme that can identify the attacker ECU by measuring and utilizing the subtle difference voltages between the normal ECUs, called Viden. Via the first phase, Viden exploits the voltage measurements to construct and update the normal transmitter ECUs' voltage profiles as their fingerprints. According to the fingerprints, Viden can distinguish the normal ECUs from the attacker ECUs or compromised ECUs. However, Viden does not consider the complexity of the vehicle environment (such as variable temperature and power voltage) when the method is implemented. Furthermore, it uses two separate electrical signals, CAN high and CAN low [42], and the electrical signals used separately are less resistant to interference. These cases can both reduce its performance of anti-jamming.

Avatefipour et al. [89] also propose a physical-fingerprint model that identifies both channel and ECU. They extract 40 features based on both time and frequency domain signals, and then employ the features to train a neural network-based classifier. They evaluate the VIDS by using a dataset collected from 16 different channels and four identical ECUs transmitting same messages. Experimental results indicate that the proposed method achieves correct detection rates of 95.2% and 98.3% for channel and ECU classification, respectively.

Choi et al. [90] introduce a VIDS that can identify a message's origin using an additional fixed 18-bit value in the extended identifier field. Their approach increases the total number of bits transmitted per message, and the extended identifier can not be used for the other purpose. This method is difficult to apply to existing automobiles because it needs to modify the modern vehicles' existing CAN protocol. Subsequently, Choi et al. also present another VIDS [91] named VoltageVIDS that has improved the previous method in which the additional ID field is no longer needed. Furthermore, VoltageVIDS is evaluated in two vehicles and achieve identification rates ranging from 90.01% to 99.61%.

Kneib et al. [92] also propose a VIDS called Scission, which uses fingerprints extracted from CAN frames to identify the sending ECUs. Scission utilizes physical characteristics from analog values of CAN frames to determine whether a legitimate ECU sends it. Compared with the previous implementation of VIDS based on voltages [21], Scission uses the differential signal instead of high and low signals and is more reliable in terms of changing conditions such as battery charge or electromagnetic compatibility.

Foruhandeh et al. [69] demonstrate the vulnerability of the existing multi-frame-based automotive VIDSs to a hillclimbing-style attack, which allows a compromised ECU to impersonate another. Then, they show SIMPLE, a novel VIDS that uses physical layer features within a single frame to fingerprint the ECUs and is immune to hillclimbing-style attack. Additionally,

this method requires a relatively low sampling rate and adapts to various environments.

Kneib et al. [93] continue to study the VIDS based on the voltage characteristics of ECU. They believe that the previous research on ECU voltage requires an oscilloscope that needs a high sampling rate of up to 2.5 GS/s to generate the fingerprints, and the high sampling is a big obstacle to the implementation of these algorithms in real vehicles. Therefore, they reduce the resource requirements for sender identification using the characteristics of the rising edge. Furthermore, to cope with the complex environment on the vehicle, they also build an adjustable model to change signal characteristics during runtime.

Murvay et al. [94] introduce a novel VIDS called TIDAL-CAN. Differential delays of bus signals, which are affected by bus characteristics and sender location, are used by TIDAL-CAN. TIDAL-CAN identifies the specific location of the target ECU by comparing the difference in signal arrival time at the two bus ends, and it can successfully identify the attacks that are implemented by compromised ECUs. The results of their experimental evaluation show that the method provides high identification rates. Whereas TIDAL-CAN also needs the equipment whose sample rates reach 250MS/s, it is not easy to implement in modern vehicles.

c) Reply Time of Remote Frame-based VIDS: In addition to the physical properties of ECUs, researchers also used differences in ECU reaction times and relative positions as ECU fingerprints.

In [75], Lee et al. propose an intrusion detection method based on the remote frame by measuring the offset ratio and time interval between request and response messages. Each ECU will reply to the remote frame with the ID of the ECU [95]. Because of the different positions of the ECUs on the bus and different transmitting procedures of different IDs, the average intervals between the request and response messages can be used as the fingerprint of different IDs. Therefore, they can use the interval time to determine whether the original ECU sends a specific ID message.

Brief Discussion: Fingerprint-based VIDSs are one of the most popular methods for IVN intrusion detection. Several papers have been accepted at top conferences in the security field. These methods take advantage of the physical characteristics of the ECU and can effectively detect most compromised malicious ECUs and added ECUs. However, if a compromised ECU still sends the same ID and only changes the frequency or payload, it cannot be detected.

Additionally, these methods are difficult to implement on existing vehicles because they require complex equipment and operations. For example, voltage-based VIDSs require high-precision oscilloscopes to listen for changes in the voltage of CAN messages. Therefore, how to reduce additional operations is the next challenge to be considered for the fingerprint-based approach. Furthermore, the aging of the hardware and the impact of external environment (e.g., temperature) on the ECU's physical characteristics must also be considered.

2) Parameters Monitoring-based VIDS: Parameters monitoring-based VIDSs utilize the change of special in-vehicle parameters (such as frequency of CAN messages)

while detecting attacks. In these approaches, researchers do not consider the meaning or sender of the messages. They only need to monitor the traffic on the IVN and extract specific traffic parameters. Based on the used parameters, these VIDSs can be taken into the following six categories.

a) Frequency-based VIDS: In a normal vehicle, ECUs send their messages to the CAN bus periodically, and the transmission frequency is fixed [66]. When adversaries want to attack the IVNs by injecting special messages, the frequency of these messages will change. Additionally, since the ECUs will still send normal messages, adversaries need to inject forged messages to the bus at a faster frequency to override the normal messages [40]. As a result, the rate of messages on the bus increases significantly and is easily detected. For example, in [8], Miller and Valasek report that they need to inject at a rate of at least 20 times faster than normal for their attack to be successful. According to this phenomenon on the IVN, some researchers come up with some VIDSs based on the frequency of CAN messages.

Ling et al. [96] present a method for detecting CAN malicious messages based on the invariance of CAN IDs and the constant frequency of each ID. They aim to detect the injection attack and DoS attack. However, they can not deal with the attack where legitimate CAN ID messages are injected at a low speed. Additionally, their experiment is implemented in CANoe, a special bus simulation tool, and they do not apply the method to the real vehicle. The method can cause some misjudgments because of the complex situation of the real vehicle.

Taylor et al. [67] introduce a VIDS by measuring inter-packet timing over a sliding window and compare the timing to historical averages to yield an anomaly signal. In this method, the authors use a one-class support vector machine (OCSVM) to classify normal messages and malicious messages. Furthermore, they also show that a similar measure of messages' data contents is not effective for identifying anomalies.

Song et al. [66] propose a lightweight intrusion detection method for the IVN according to the time intervals of CAN messages. They capture CAN messages from a real car and perform three kinds of message injection attacks. They prove that time interval is a meaningful and effective feature to detect injection attacks in the CAN traffic.

Gmiden et al. [97] introduce a simple VIDS based on the analysis of CAN message time intervals. The advantage of the method is that it does not require a modification in the hardware layer and can be implemented in each ECU.

Moore et al. [98] also propose an anomaly detection system based on the regularity of normal signals. They find that for each CAN ID, the time of a message only depends on the previous message's time, and the wait time following a fixed distribution. Thus, they train models for each CAN ID based on the interval of two continuous messages. Each model will flag unusually short/long intervals as an anomaly while monitoring the traffic and the system produces an alert upon three consecutive anomalies.

Tomlinson et al. [99] use a time-defined window to detect message changes in CAN resulting from injection and reflash attacks. They analyze three methods (ARIMA, Z-score, and supervised method) that compare each interval for CAN messages within the window against the averages for all packets with the same ID within that window. This method reduces the calculation cost because it only needs to calculate the average at the end of the moving window. However, if attackers understand this detection mechanism, they can inject malicious messages at rates similar to the normal messages within a window to deceive the detection system.

Olufowobi et al. [73] present an VIDS based on change-point detection techniques using adaptive CUSUM algorithm to detect statistical changes and intrusions in CAN bus message stream. The method also judges the intrusion by detecting the abnormality of the message sending time. The attack can not be detected if the adversary does not change the frequency of the messages.

Young et al. [100] demonstrate that the basic assumption that all CAN messages have consistent timing intervals is not true. In normal vehicles, the timing intervals of some special ID can change due to normal driving operations, and the change can make VIDS based on constant timing intervals inaccurate. Furthermore, they propose and evaluate a frequency-based VIDS. They prove that this method could solve the problem raised by interval-based approaches.

In [101], Olufowobi et al. present an approach for detecting intrusions in IVNs using the pattern of message sending, called SAIDuCANT. They build a specification based on messages and worst-case response time analysis of the CAN bus at first and use the specification to detect the abnormal messages. SAIDuCANT considers the jitter and retransmission phenomenon in the CAN bus to more accurately define the transmit time of the message compared with other frequency-based VIDS. It achieves a better F1 score compared with interval-based and frequency-based approaches with less detection delay. However, this method can not solve attacks such as masquerade attacks that imitate the time of the victim ECU.

b) Information Entropy-based VIDS: The information entropy, often just entropy, is the average amount of information contained in any random variable, which can be interpreted as the intermediate level of "information," "surprise," or "uncertainty" inherent in the variable's possible outcomes [102]. In the context of network and Internet systems, the concept of entropy-based intrusion detection has been considered in various publications [103], [104], but entropy approach has a high rate of false positives because of the randomness of the standard computer networks [105]. Instead, the traffic in IVN is much more stable, and injected malicious messages will significantly change the entropy of traffic. The researchers can use the change of entropy to detect the injected malicious messages.

In [70], Michael Müter et al. introduce the VIDS based on information entropy for the first time. They suggest to measure the entropy of IVN and use it as the specification of the normal operation for the network. They use the entropy of a set of CAN IDs and special states to detect the intrusion. In this paper, they describe three attack scenarios to show the usefulness of their approach. Furthermore, they put forward different methods to detect these attacks. Firstly, they increase the message's frequency with a specific CAN ID while the engine is running (replay attack). To detect this attack, based on the concept of

relative entropy [106], they calculate the relative distance of the system's normal behavior and the behavior to be detected.

Secondly, they attack the availability of a bus system by performing a flooding attack on the CAN bus. The implementation is done by sending a mass of messages containing the most dominant identifier 0x000 (Dos attack). In this scenario, they measure entropy during the vehicle's regular operation and compare this value to that during the attack phase.

Thirdly, in this attack scenario, they think the adversary tries to disturb the system by injecting selective, spurious speed signals, e.g., to impact the ECUs that need the signals. To defend against the attack, they utilize the conditional self-information theory [107] to check the coherence to the speed signal's expected behavior and the previous value.

In [76], Marchetti et al. propose and evaluate an entropy-based method for detecting anomalies in CAN messages generated by a real vehicle. They find that if only one detector is used to detect anomalies, they can only detect attacks that inject many anomalous messages. On the other hand, to detect low-volume attacks, in which the attacker injects only 1 packet per second, they need to set up a detector for each ID.

In [108], Wu et al. present a novel VIDS based on information entropy, which uses a fixed number of messages as sliding windows. Compared with the above entropy-based VIDSs, the method uses a simulated annealing method [109] to get the best parameters (i.e., the best sliding window size, standard deviation, and corresponding sensitivity) at first. The experimental results demonstrate that the method can effectively improve the accuracy and effectiveness of intrusion detection for DoS and injection attacks on IVNs.

c) Payload-based VIDS: Many works utilize the data fields of CAN messages for anomaly detection. On the IVN, the payload syntax and semantics of the same ID are the same [110]. Furthermore, the changes in vehicle status such as speed are continuous and uniform. Reflected on the vehicle messages, the changes in data content are regular and stable. Therefore, the intrusion can be detected according to the dramatic changes in data fields of CAN messages.

Stabili et al. [25] propose a novel method that can identify malicious CAN messages injected by adversaries in the CAN bus. In particular, this detection method studies the payloads of all messages transmitted on the bus. It compares the Hamming distance between consecutive payloads of the same ID to build a valid range of the Hamming distance for each ID in the training phase. Furthermore, since the proposed method has very low computational complexity and small memory footprints, it can be implemented in the real vehicle.

Taylor et al. [111] consider the data interdependence between IDs and develop an anomaly detector by learning to predict the next data word originating from each sender on the bus on the base of long-short-term memory (LSTM) recurrent neural network for CAN bus anomaly detection. The message that that differs significantly from the predicted result isflagged as anomaly. After implementing this detector, they evaluate it by abnormal data created by modifying the CAN bus data.

Kang et al. [112] propose a novel VIDS by utilizing a deep neural network (DNN) to enhance the security of the IVN. In this paper, Kang et al. choose the data field that includes 64-bit positions (i.e., 8 bytes) in the CAN message and calculate the distribution of bit-symbols. They use the probabilities of bit-symbols as the features to distinguish normal or malicious messages.

Xiao et al. [113] propose a novel and robust VIDS by using spatiotemporal information enabled time series prediction. The proposed IDS analyzes the CAN traffic generated by the IVN in real time and identifies the abnormal state of the vehicle practically. In this method, the authors use the ConvLSTM model [114] to exploit the association between multiple CAN messages to find more effective features for intrusion detection. Experiment results show the performance of the model and the effectiveness against various attacks.

Kukkala et al. [115] present a novel VIDS called INDRA that utilizes a Gated Recurrent Unit (GRU) based recurrent autoencoder [116] to detect anomalies in CAN. They use the change of the payload to train the model and detect the anomalies. Additionally, they evaluate their proposed framework under different attack scenarios.

d) ID Sequence-based VIDS: The sequence of messages transmitted on the CAN bus can also be used for intrusion detection. The traffic on the CAN bus is constant and the messages are sent periodically for each ID. Hence, the sequence of message IDs observed in the CAN Bus is duplicated [120]. Researchers can use this feature to detect attacks.

Marchetti et al. [120] present an effective method based on the analysis of the sequence of normal CAN bus traffic. This method is implemented by limited memory and low computational complexity and can be applied to current vehicles.

Islam et at. [121] consider the VIDS in [120] vulnerable to intelligent attacks and they propose a four-stage intrusion detection system that uses the chi-squared method [136] and incorporates graph theory [137]. The proposed methodology exhibits up to 13.73% better accuracy compared to existing ID sequence-based methods [120].

e) Similarity-based VIDS: Due to the stability of the in-vehicle messages, the distribution of the IDs should be similar across different windows. Some researchers want to use this similarity to detect the malicious messages.

In [122], Ohira et al. propose a method based on the similarity of sliding windows that can detect every type of DoS attack by using the messages distribution of sliding windows. The method uses the Simpson coefficient [138] to calculate the similarity of message distribution in the train set and test set. The method can detect the DoS attack in 100% of the cases in their experiment, and the detection time is up to 93% (14 us) shorter than the conventional method. However, this method still can not solve the masquerade attack, which has little impact on the IVN.

In [139], Nguyen et al. propose a novel multi-class IDS using a transformer-based attention network (TAN) for an in-vehicle CAN bus. Their model builds on the self-attention mechanism, removing RNNs and classifying attacks into multiple categories. Furthermore, the proposed models can detect replay attacks by aggregating sequential CAN IDs.

f) Hybrid: As we have shown before, different features in the CAN network can be used to detect attacks in the vehicle

Signature			[82],[68]
Anomaly	ECU Fingerprint	Clock Skew	[20],[86],[59]
		Voltage	[21],[89],[92],[90],[69],[93],[94]
		Reply time	[75]
	Parameters Monitoring	Frequency	[96],[67],[66],[97],[98],[99],[73],[117],[100],[101],
		Information Entropy	[70],[76],[108]
		Payload	[111],[112],[110],[74],[25],[68],[118],[113],[60] ,[119],[115],
		ID Sequence	[120],[121]
		Similarity	[122]
		Hybrid	[123],[124],[125],[126],[127],[117],[128],[129]
	Message Semantics	Vehicle State	[78],[130],[131] ,[132],[133],[134],[135]

TABLE III: The classification of existing IDSs.

accurately. However, when these individual features are used to detect intrusions, they often bring some loopholes. For example, frequency-based VIDS usually cannot detect attacks in which the adversary imitates the victim ECU's frequency, and it can also produce false positives for event messages and messages with large periodic fluctuations. Furthermore, VIDS based on the payload cannot achieve a high detection rate when the attacker changes little to the data flow of CAN network . Therefore, many researchers try to propose some VIDSs that contain multiple features at the same time.

Theissler et al. [123] propose a VIDS that uses enhanced one-class Support Vector Machines (SVM) to detect intrusions [140]. This method directly uses normal multivariate time series from IVNs to learn the normal behavior of vehicles and detect intrusions based on deviations.

Tian et al. [124] introduce an VIDS that utilizes a regression Decision Tree with Gradient Boosting (GBDT) technique [141], [142] for CAN bus. Additionally, they propose a new feature based on entropy as the feature construction of the GBDT algorithm in which they consider the entropy of CAN ID and the payload of data. The experiment results show that the method achieves a high true positive (TP) (97.67%) and a low false positive (FP) (1.20%), which means the system has a good performance and can be used to protect the CAN bus.

Wang et al. [126] propose a distributed VIDS using hierarchical temporal memory (HTM) [143], [144], a machine learning algorithm aimed to capture the structure and algorithmic features of the new cerebral cortex. The method uses a standard HTM system and standard parameters to predict CAN data flow based on the bit sequences from a single ID data domain. The experiment results show that this method achieves good performance in AUC score, precision, and recall.

Tomlinson et al. [127] use a one-class compound classi-fier that combined euclidean distance and nearest neighbor algorithms [145], [146] to detect the IVN attacks. They only target a single type of attack test- *fuzzing test*, where the CAN messages are filled with random messages. However, the experiment results are relatively poor, and the best detection rate is the only 65%.

Weber et al. [125] introduce a hybrid anomaly detection system, which combines the advantages of an efficient rule-based system with the advanced detection measures provided by machine learning. Firstly, they perform a static check based on the format and transmission standard (e.g., transmission frequency and the payload range) [147]. Secondly, they use an unsupervised anomaly detection algorithm, called Lightweight

On-Line Detector of Anomalies (LODA) [148], to cooperate with the static check.

Koyama et al. [117] present a lightweight VIDS based on the quantized intervals for periodic CAN ID and the absolute difference of payloads. The results of their experiments show that the system achieves a high detection performance: a true positive rate of 97.55% and a false positive rate of 0.003%. However, the attack in which a small number of malicious messages are injected can not be detected.

Zhu et al. [128] propose a multi-task LSTM VIDS which utilizes mobile edge computing (MEC) [149] to assist in the identification of intrusions in the IVN. In this system, both the dimension of time and the dimension of data are combined to enhance detection accuracy. With the assistance of mobile edge computing (MEC), the detection can be finished with 0.61 milliseconds and achieve 90% of accuracy. However, the algorithm is still complicated for onboard ECUs, and it is difficult to apply to existing vehicles directly.

Hanselman et al. [129] present CANet, a novel VIDS based on a neural network architecture that is trained in an unsupervised manner. The method builds the first deep learning model in the literature that can naturally deal with the data structure of the high dimensional CAN bus. The basic idea is to introduce an independent LSTM input model for each ID that can capture the corresponding signals' temporal dynamics. Due to the comprehensive features, the true negative rate of CANet is fairly high, usually over 0.99.

Brief Discussion: Parameter-based monitoring VIDS is the most commonly used VIDS. The biggest advantage of these VIDSs is that they are easy to implement. Just by listening to the normal data inside the car, these VIDS do not need some additional equipment. However, these methods are typically targeted at specific attacks and may be less effective at detecting unconsidered security risks. Furthermore, due to the complexity of the IVN and the external environment, the monitored parameters will change, affecting the accuracy of detection.

3) Message Semantics-based VIDS: In addition to the fingerprint-based VIDS and parameters monitoring-based VIDS, the researchers also propose CAN message semantics-based VIDS. In these VIDSs, the researchers need to reverse the meaning of the CAN messages. Researchers mainly detect whether a vehicle is attacked based on abnormal changes in the vehicle states that are reversed from the CAN messages, and we call the methods 'vehicle state-based VIDS'.

a) Vehicle State-based VIDS: Normally, Some CAN messages on the IVN always contain different vehicle states,

such as vehicle speed, acceleration, RPM, the pedal position, and brake pedal position. When the vehicle runs normally, these states have a high correlation. For example, the rapid growth of vehicle speed means that the acceleration and the pedal position are greater than 0. If the relationship between these states changes, it means the vehicle is attacked.

Wasicek et al. [132] propose a context-aware VIDS (CAID) framework, which can recognize the control of the physical system through the IVN. CAID uses sensor information, which can be captured from the on-board diagnostics (OBD-II) interface and parsed according to the OBD protocol [150] to build models of the physical system by using an unsupervised Artificial Neural Network (ANN) [151]. Afterwards, CAID checks the correctness of current sensor data against the reference models. Thereby, it ensures the safety of the controller's operations.

Narayanan et al. [78] introduce OBD SecureAlert, a system that detects abnormal behavior in vehicles when they are being operated. They successfully extract data from various real automobiles by connecting to their OBD-II port. With the collected dataset, they generated a Hidden Markov Model [152] to predict anomalous states in vehicles. These techniques can be applied to identify anomalies and unsafe states in vehicles.

Casillo et al. [134] show an embedded VIDS for vhicle, which adopts a Bayesian Network [153] approach for the quick identification of malicious messages. It uses sensor data collected from the IVNs to detect commands sent by an attacker. Their experiments were carried out using an automotive simulator, CARLA, which can emulate a real vehicle and its interaction with the environment, along with some other matching equipment. They tested the effectiveness of the system against malicious commands on this device.

Brief Discussion: Message semantics-based VIDS is the most promising detection method. These methods typically reverse diagnostic messages or in-vehicle messages to obtain vehicle states and then detect intrusions through anomalies in vehicle states change. This method can detect harmful messages to the vehicle and is unaffected by the ECU's errors and external environment. However, the greatest challenge for the method is how to accurately reverse in-vehicle or diagnostic messages. While some of the protocols are publicly available (OBD protocols [150]), most of them are designed by the OEMs themselves. There is no research work available that provides a way to completely reverse these protocols. Therefore, obtaining accurate vehicle states is the focus of message semantics-based VIDS.

VII. EVALUATION OF EXISTING VIDS

Researchers propose VIDSs based on various detection principles and use different validation strategies to evaluate detection effectiveness of their methods. In this section, we complement the survey by introducing a taxonomy of the CAN VIDS in Table IV. Next, we compare these VIDSs from different perspectives: the used features, the detection technology, the attack covered, validation strategy, and detection result.

A. Feature

Feature used in the VIDS is a fundamental part of an intrusion detection system. Different features require different data to be collected. We count the features used in all the papers, which are the timing interval of the consecutive messages (can be classified as frequency), clock skew, voltage profiles, the data field, the entropy, the sequence of ID, the state of the vehicle, specification. Researchers use these features based on different principles. We give more details of these principles.

Researchers take advantage of the periodicity and stability of CAN message transmissions, and they use the stable time interval between CAN message transmissions, the information entropy of the data stream, and relatively fixed order of the CAN IDs to detect intrusions [66], [70], [120]. The VIDSs based on these features only need to collect the data stream from the IVNs. These systems calculate the pattern of normal data based on these data. During the actual testing, the VIDSs issue a warning if the test data violates this pattern.

Researchers also use the continuity of data fields in CAN messages to detect malicious messages. The data in a CAN message usually contains some practical meaning, such as sensors and counters [110]. Therefore, they use the difference between neighbouring data or the prediction of the next data to determine whether the message is malicious [111], [25]. The method also only requires the collection of data streams from the in-vehicle network.

Furthermore, researchers can utilise the semantic information in CAN messages to detect attacks on vehicles. They reverse the CAN messages to obtain the vehicle status and determine whether the vehicle is under attack based on the change of the vehicle status [132], [134]. While using semantic information to detect intrusions, the researcher not only needs to get messages from IVN but also needs to know how to reverse these messages.

Finally, researchers propose many VIDSs based on the fingerprint of ECUs [20], [21], [90]. They use the unique features of each ECU, such as clock skew and voltage, to determine whether a message source from the correct ECU. When using clock skew as the feature, researchers only need to collect data streams from the IVNs. However, researchers need sophisticated equipment such as oscilloscopes to capture the voltage values of CAN messages when voltage is used to detect intrusions. The complex data collection affects the deployment of this VIDS in real vehicles.

B. Detection Technology

Different intrusion systems take different technologies to model and build the system. Overall, these VIDSs take two technologies: rule-based technology and machine-learning technology.

Rule-Based Detection: Usually, they can be distinguished into two types. There are two popular types of rule-based detection technologies. For the first type, the researchers draw up some specifications according to the prior knowledge of attacks or standard protocols and detect malicious messages with these specifications [82]. For the other type, the researchers can build the outlines or thresholds of normal behaviors through features mentioned before by the mathematical formula or statistical experiment (e.g., [98]). The thresholds or outlines can determine whether the target messages are malicious. These VIDSs, which

TABLE IV: Evaluation

VIDS	Features	Detection technology	Attacks covered	Platform	Results
[82]	Priori knowledge of CAN protocols	Rule-based(specification)	DoS,Spoofing,Fuzzing	Simulation	Unobtainable
[70]	Entropy of ID	Rule-based(threshold)	DoS,Spoofing	Real car	Unobtainable
[96]	Frequency	Rule-based(threshold)	DoS,Spoofing	Simulation	Unobtainable
[123]	Multivariate time series messages	Machine-learning(SVDD)	Spoofing	Real car	Precision=32.3-100%
[67]	Frequency	Machine-learning(OCSVM)	DoS,Spoofing	Simulation	AUC $\geq$ 96.20%
[20]	Clock skew	Rule-based(threshold)	Spoofing,DoS	Real car,Prototype, Simulation	FP=0.055%,TP=100%
[111]	Payload	Machine-learning (RNN and LSTM)	Spoofing	Simulation	AUC=17.65%-100%
[112]	ID,Payload	Machine-learning(DNN)	Spoofing	Simulation	FP=1.6%,Accuracy=97.8%
[78]	State(OBD protocol)	Machine-learning(HMM)	Spoofing	Real car	Unobtainable
[76]	Entropy of ID	Rule-based(threshold)	Spoofing,Fuzzing	real car	TN=93.33%/88.89%
[66]	Interval	Rule-based(threshold)	DoS,Spoofing,Fuzzing	real car	Accuracy=100%
[97]	Frequency	Rule-based(threshold)	DoS,Spoofing	Simulation	Unobtainable
[75]	Interval(remote frame)	Rule-based(threshold)	DoS,Spoofing,Fuzzing	real car,Prototype	Unobtainable
[120]	ID sequence	Rule-based(outline)	Spoofing,Fuzzing	Real car,	Detection Rate:100%
[132]	State (OBD protocol)	Machine-learning (Bottleneck ANN)	Spoofing	Real car	Unobtainable
[98]	Interval	Rule-based(threshold)	Spoofing,DoS	Real car	FP=0.294%,TP=99.98%
[74]	Payload	Machine-learning (Fuzzy logic techniques)	DoS,Spoofing,Fuzzing	Simulation	FP=0-3.8%, Precision=96.3%-100%
[89]	Voltage profiles (high, low)	Machine-learning (ANN)	Spoofing	Prototype	Detection Rate:95.2%/98.3%
[110]	ID,Payload	Rule-based(specification)	Fuzzing	Real car,Simulation	FP=0
[25]	ID,Payload	Rule-based(threshold)	Spoofing,Fuzzing	Real car,Simulation	Detected Anomalies:100%
[21]	Voltage profiles (high, low)	Rule-based(threshold)	Spoofing	Real car,Prototype	FP=0.2%, Identification=99.8%
[130]	State (Sensor)	Machine-learning (Random Forest)	Spoofing	Real car,Simulation	Unobtainable
[131]	State (sensor)	Rule-based(threshold)	Spoofing	Simulation	Unobtainable
[124]	entropy of ID and Payload	Machine-learning (GBDT)	Spoofing	Simulation	TP:97.67%, FP:1.20%
[92]	Voltage profiles (differential)	Machine-learning (Logistic Regression)	Spoofing	Real car,Prototype	FP=0, Identification=99.85%
[99]	Frequency	Rule-based (threshold)	DoS,Spoofing	Simulation	Accuracy:99.19%-100%
[108]	Entropy of ID	Rule-based (threshold)	DoS,Spoofing	Simulation	Accuracy:92.3%/100%
[90]	Voltage profiles (differential)	Machine-learning (SVM,NN,BDT)	Spoofing	Prototype	FP=3.52 %,Identification=96.48%
[68]	ID,Payload	Rule-based(specification)	Spoofing	Simulation	Unobtainable
[118]	Payload	Machine-learning(GAN)	DoS,Spoofing,Fuzzing	real car	Accuracy:100%/98%
[86]	Clock skew	Rule-based(threshold)	Spoofing,DoS	Real car,Prototype	Prediction error<5.7%
[125]	ID sequence, Payload,Interval	Rule-based and Machine-learning(LODA)	Spoofing	Simulation	Unobtainable
[126]	ID,Payload, transmission time	Machine-learning (HTM)	Spoofing	Simulation	Precision>90%
[127]	Frequency and Payload	Machine-learning (Euclidean distance and nearest neighbor)	Fuzzing	Simulation	Detection Rate: 65%,/52%/45%
[73]	Frequency	Rule-based(threshold)	DoS,Spoofing,Fuzzing	Simulation	Unobtainable
[100]	Frequency	Rule-based(threshold)	Spoofing	Real car	FP=1.4%,Accuracy=100%
[119]	ID,Payload	Machine-learning (RNN and LSTM)	Spoofing	Real car	Unobtainable
[117]	Interval,Payload	Rule-based(State transition)	Spoofing	real car	FPR=0.003% TPR:97.57%
[60]	Payload	Rule-based(threshold)	Spoofing,DoS	Real car,Prototype, Simulation	Unobtainable
[128]	Interval,Payload	Machine-learning(LSTM)	DoS,Spoofing	Simulation	Accuracy:90%
[133]	State (reverse)	Machine-learning (HMM)	Spoofing	Real car	Unobtainable
[69]	Voltage profiles (differential)	Rule-based (Mahalanobis distance)	Spoofing	Real car,Prototype	EER:0/0.8985%
[101]	Frequency	Rule-based(specification)	Spoofing	Simulation	Accuracy>90%
[134]	State(reverse)	Machine-learning (Bayesian)	Spoofing	Simulation	Precision:85%
[59]	Bit time	Machine-learning (MLR)	Spoofing	Real car,Prototype	Detection Rate: 99.76%
[113]	ID,Payload, Timestamp	Machine-learning (ConvLSTM)	DoS,Spoofing,Fuzzing	Simulation	F1-score:96%
[93]	Voltage profiles (differential)	Machine-learning (LR,Naive Bayes,SVM)	Spoofing,	Real car,Prototype	Identification rate:99.94%
[94]	Differential Timing	Rule-based(threshold)	Spoofing,	Prototype	Identification rate:100%
[129]	ID,Payload, Frequency	Machine-learning (LSTM)	DoS,Spoofing,	Simulation	True negative $\geq$ 99%
[122]	Sliding Windows Similarity	Rule-based(threshold)	DoS,Spoofing,Fuzzing	Simulation	Accuracy:100%
[121]	ID sequence	Rule-based(graph)	DoS,Spoofing,	Simulation	Accuracy: 94.74%/100%/95.24%
[115]	Payload	Machine-learning(GRU)	DoS,Spoofing,Fuzzing	Simulation	False positive rate:2.5%
[154]	ID	Machine-learning(DCNN)	DoS,Spoofing,Fuzzing	Simulation	FNR:0.05-0.35%,ER:0.03%
[135]	State(reverse)	Rule-based(threshold)	DoS,Spoofing,Fuzzing	Real car,Simulation	Accuracy:100%

use rule-based techniques, require only comparison operation during detection, and so that they consume fewer resources and delays. However, as the threshold is fixed and the changes of the IVNs are complex, this method can cause false alarms when there are large changes in the condition of the vehicle. **Machine-Learning-Based Detection:** The machine-learning algorithms are already widely used in VIDSs, and they are quite suitable for solving the classification and modeling issues in VIDSs. Furthermore, three types of machine learning models are widely adopted by the VIDS, including traditional machine learning [74], recurrent neural network (RNN) [111], deep neural networks (DNN) [66]. Compared to rule-based algorithms, machine learning algorithms consume more time and computational resources [67]. Therefore, machine learning-based VIDSs require powerful computing power from the ECUs. However, the robustness of these systems is greatly enhanced because machine-learning algorithms can train large amounts of data containing a variety of scenarios [67].

C. Attack Covered

When the researchers designed an VIDS, they must consider the targeted attack scenarios before design. Since none of these algorithms explicitly mention sniffing attack and diagnostic attack, we only list attacks in in-vehicle communications. The attack scenarios are presented in Section V: *DoS attack*, *Spoofing attack*, *Fuzzing attack*. The various VIDSs target different attacks according to their own detection principles. For example, Kang et al. [112] propose a VIDS based on the continuity of data fields under the same ID. They target attacks that change the data field for a specific ID. However, they can not detect attacks that insert malicious messagse with undetected IDs (such as DoS attack and Fuzzing attack).

D. Test Platform

In this section, we assess the reliability of the evaluation method by comparing the utilization of test platforms in various works. Researchers evaluate the effectiveness of their VIDS in different ways. We can divide them into three categories based on the platforms used in the experiment: real vehicle, prototype, and simulation. When a vehicle is in operation, the changes of vehicle states are complex and varied. For the best validation, some researchers deploy their VIDSs directly on real cars [20], [70], [98]. However, this method requires a real vehicle that can be modified. Furthermore, the attack test can cause damage to the vehicle and even threaten the safety of the driver. Therefore, some researchers create a prototype with some microcontrollers and CAN modules to simulate the ECUs and CAN [90], [94]. This method also validates the detection effect of an VIDS in the CAN, but a microcontroller such as a Raspberry Pi cannot completely replace an ECU. The reliability of this method is poorer than that of real cars. Finally, some researchers only use a CAN bus simulator, such as CANoe, or use some online datasets [112], [73], [74]. Researchers modify the data to simulate the generation of attacks. This verification strategy is simple but not very reliable.

E. Detection Result

The results are an essential indicator for evaluating the effectiveness of an intrusion detection system. Since different papers describe their results from different perspectives (such as false positive or precision), we compared the relevant results for each paper with their own perspective during the assessment phase. Whereas some items do not perform detailed experiments or do not list the actual results, we use *'Unobtainable'* to represent them.

As the detection results of these systems are based on different data sets, it is not possible to directly compare the results. Specifically, The length of the data set, the proportion of positive and negative samples, and the vehicle states when the data is collected can affect the effectiveness of the detection. Furthermore, some VIDSs only use a single evaluation index to show the effectiveness of the test, but such results are unreliable. For example, Song et al. [66] only calculate the accuracy of the test. However, if the test data set is asymmetric, the accuracy rate can not represent the true detection effect.

VIII. EXPERIMENT

In this section, we select multiple typical VIDSs and laterally compare their detection performance by designing specific experiments and using a uniform testing dataset. First, we introduce the VIDSs and the dataset that we select. Second, we describe the challenges encountered in the process of running these VIDS. Third, we present the detection results of these VIDS with the same attack dataset. Finally, we discuss the potential attacks that can evade these VIDSs.

A. VIDS Selection And Implementation

To further explore the performance of VIDS, we choose the typical VIDSs from the papers listed in Table IV to imitate their algorithm and implement them following two criteria.

We select the methods that can be tested with a unified dataset. Parameters monitoring-based VIDSs usually only need to use a CAN module to collect all CAN frames, and these methods can directly use the same data set for horizontal comparison. However, ECU fingerprint-based VIDSs require special datasets for defense. For example, Kneib et al. [92] need an advanced oscilloscope to collect the voltage of CAN signals to construct a fingerprint of a normal ECU. These methods typically collect voltages at different fields in the CAN frame at different sampling rates, which are introduced in §VI. Data source limitations prevent us from evaluating them using a common dataset.

Taking the above reasons into account, we select these papers ([97], [66], [98], [100], [73], [20], [99], [70], [76], [108], [96], [120], [122], [67], [111], [112], [25]) from Table IV. It is particularly worth noting that some papers contain multiple methods. In [70], muter et al. proposed two different methods to detect intrusion. One uses the change in relative entropy (*[70](1)*), and the other uses the change in overall entropy (*[70](2)*). Tomlinson et al. [99] introduce two new unsupervised detection methods. One uses Z-score (*[99](1)*) and the other uses ARIMA (*[99](2)*).
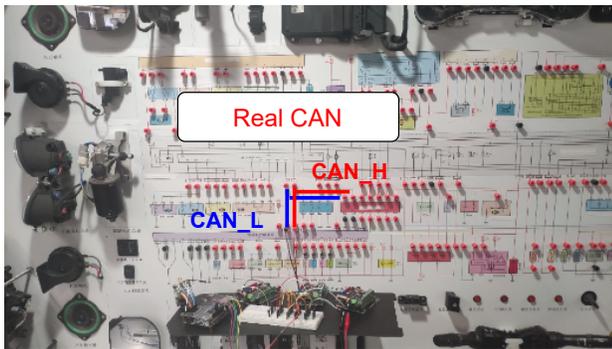
Fig. 5: The topology of the real CAN.

B. Dataset

We need to collect the CAN bus data in an attack-free state and under various attacks to implement these VIDS. We collect the data from a real CAN bus, which is shown in Fig. 5. The testbed consists of electronics from a 2014 Toyota Corolla. Both the hardware and the network are actually used by this car. We apply it to evaluation instead of actual vehicles due to security and safety considerations. During evaluation, we connect the CAN analyzer to the `CAN-H` and `CAN-L` of the CAN bus. Various attacks, such as DoS attack and Fuzzy attack, are launched on the real CAN. Also, we obtained the CAN information from its OEM (Original Equipment Manufacturer). This real CAN contains three internal ECUs. Meanwhile, 23 types of frames are transmitted (i.e., 23 various CAN IDs). We select the ID representing the speed as the target of the spoofing attack.

Then we describe the methods that we create the datasets. We do not test these defenses with all attacks. First, sniffing attack does not have any impact on the data of the IVN. Therefore we do not consider such attacks. Second, some attacks target specific defense methods and are not suitable as a unified test data set. For example, voltage corruption attack (SPA-6) is mainly aimed at voltage-based intrusion detection systems. The adversaries try to pollute the training set of the voltage fingerprint model, so it is outside the detection range of our chosen system. Based on this consideration, we selected suitable attacks for testing all selected methods.

Replay attack (*SPA-1*)): We randomly intercept a fixed-length data segment from the normal data at first. Then, we repeatedly insert this data segment into the real CAN. Each attack lasts 10 seconds and keeps the time interval of attack data unchanged.

Fabrication attack (*SPA-2*): In this attack, we choose a message which represents the speed of the vehicle. Then, we modify and insert the selected message into the CAN every 1ms for 10 seconds. We repeat this operation continuously afterward.

Masquerade attack (*SPA-3*): This attack requires us to pause the specific ECU for a long time, which is a very big challenge. So we make modifications in the existing normal dataset without attack. We select the messages with a specific ID and change their payload. Similarly, we also modify a piece of normal data every 10 seconds.

Disorderly Control attack (*SPA-2*): In this attack, we inject messages of totally random CAN ID and payload every 0.5 milliseconds. Each intrusion performed for 10 seconds.

Reverse attack (*FUA-2*): In this attack, we inject malicious messages that are composed of normal IDs and random payload. These messages are inserted into the CAN bus at 1-millisecond intervals and last for 10 seconds.

DoS attack with high priority ID (*DOA-1*): In this attack, we inject messages of '0x000' CAN ID every 0.3 milliseconds. 0x000 is the highest priority ID and most of the works inject messages of this ID to attack the vehicle.

Redundant message injection (*DOA-2*): The purpose of this attack is to fill the CAN bus with messages which have normal IDs. We inject malicious messages with normal IDs and random payloads into the CAN bus until the maximum load of the bus is reached.

Control attack in diagnostic communication (*DIA-2*): First, we get the threatening control commands from the diagnostic devices. In our experiment, we use the diagnostic equipment (i.e., Launch X431 [155]) to control the vehicle and reverse the messages exchanged by the equipment and vehicle. Afterwards, we inject a control command every 20 milliseconds into CAN bus as the malicious message.

Spoof attack in diagnostic communication (*DIA-3*): First, we use diagnostic equipment [155] to query the speed of the vehicle and record the response messages from the ECU. Then, we continuously inject these response messages into the CAN bus to constitute the spoof attack in diagnostic communication.

Fuzzy attack in diagnostic communication (*DIA-4*): We inject messages of totally random diagnostic CAN ID and payloads every 20 milliseconds to the real CAN bus.

Dataset with normal diagnostic messages (*DIA-Normal*): In order to determine that these VIDSs can distinguish between normal diagnostic messages and malicious diagnostic messages, we insert normal diagnostic messages in the data set for comparison. We choose the speed query command in the open diagnostic protocol to ensure that the injected messages can not harm the vehicle [150]. We inject the selected commands every 20 milliseconds to the CAN bus.

Through these operations, we obtain 11 datasets for testing. The number of normal data and malicious data in these datasets is displayed in Table V. Because the amount of malicious data in these attacks is less than normal data, we use various indicators to measure the algorithm's effectiveness, such as accuracy, precision, recall, and f1-score.

C. Challenges and Solutions in Reimplementation.

After choosing the appropriate dataset, we implement all the selected VIDSs based on the built dataset. When we implement these VIDSs, we find out various challenges, and we try to solve them using the following solutions.

1) Parameters Definition: Some VIDSs have uncertain or unmentioned parameters. When we try to reproduce the algorithm in the paper completely, we have to decide some parameters according to the dataset by ourselves. For example, in [76], the threshold of the entropy is decided by three

TABLE V: The composition of the attack dataset.

File Name	Normal Messages	Malicious Messages
SPA-1	549410	85320
SPA-2	532510	159752
SPA-3	456790	9331
DOA-1	487650	93074
DOA-2	523480	314083
FUA-1	513680	75486
FUA-2	497450	149236
DIA-2	524640	6826
DIA-3	532480	6929
DIA-4	473980	6166
DIA-Normal	507506	0

parameters: the average entropy value μ_e, standard deviation of entropy σ_e, and a model parameter k. Among them, μ_e and σ_e are calculated with the training dataset and k is a customized parameter which is used to adjust the threshold. To achieve the best effectiveness of these VIDSs, we adjust these uncertain parameters for each dataset separately.

2) Inconsitence Defeination of Attack Models: Each VIDS has its own attack model and attack scenario. For example, for VIDS proposed in [66], the target DoS attack is launched by transmitting abundant traffic to surpass the maximum capacity of CAN bus and has no requirement on the ID and data field. Whereas, in other papers, such as VIDS [74], DoS attack is performed by injecting messages whose ID are 0x000 at high speed. Additionally, based on the IV, we can see that many VIDSs only target part of the attacks scenarios contained in the selected dataset. For example, VIDS [100] mainly aims to the replay attack and does not mention DoS attack and fuzzy attack. To compare the differences between the methods, we select the same dataset. And for a more comprehensive evaluation of the methods, we have expanded the attack dataset to include the attacks mentioned above.

D. Reproduction

After implementing the above selected VIDSs and also choosing the appropriate dataset, we conduct the following experiments to check the effectiveness of these methods. Particularly, we first apply the data collected during normal vehicle running to obtaining the desired threshold or model for each algorithm, and then we evaluate the accuracy of these methods with various attack datasets. Afterwards, we present the used evaluation metrics as well as the evaluation results.

1) Evaluation Metrics: We experimentally compare the VIDS based on the following metrics.

Accuracy is the most straightforward performance indicator and is simply the ratio of correctly predicted observations to the total number of observations. Accuracy is a good measure, only if we have symmetrical datasets where the values of false positives and false negatives are almost identical. Therefore, we must look at other parameters to evaluate the performance of the model.

Precision is the ratio of correctly predicted positive observations to the total number of predicted positive observations. Precision demonstrates the system's ability to distinguish between normal messages.

Recall is the ratio of correctly predicted positive observations to all observations in the actual class. Recall reflects the system's ability to recognize malicious messages.

F1 score is a weighted average of "accuracy" and "recall rate". Therefore, the score takes into account both false negatives and false positives. Intuitively, it is not as easy to understand as accuracy, but the F1 score is usually more useful than accuracy, especially if the class distribution is uneven.

2) Detection Result: Fig. 6 shows the detection results of these VIDSs for different attacks. We analyze detection results of the VIDSs and find out the advantages and disadvantages of these methods.

Let us consider the work by Gmidene et al. [97] as an illustrative example. The method showcased a relatively high accuracy in countering diverse attacks, owing to the notable true negative (TN) outcomes and the predominance of normal messages over abnormal ones. However, the detection rates exhibited a relatively low efficacy against the *FUA-2* and *SPA-1* attacks. This outcome indicates that the method's ability to detect multiple ID attacks is suboptimal. The underlying reason lies in the fact that malicious messages are identified by frequency changes within a single ID, while the *FUA-2* and *SPA-1* attacks do not significantly alter the frequency of a single ID, thus making them challenging for the method to detect. Consequently, the frequency-based VIDS struggle to effectively identify these malicious messages.

Furthermore, the precision, recall, and f1-score of the method against the *SPA-3* attack were observed to be zero. This finding indicates the algorithm's incapacity to detect the *SPA-3* attack, where malicious messages replace normal ones while maintaining an unaltered time interval from the preceding message. The frequency-based VIDSs are unable to detect such attacks due to their reliance on changes in message frequency.

Additionally, the precision, recall, and f1-score of the method against the *DIA-1*, *DIA-2*, *DIA-3*, and *DIA-4* attacks were all found to be zero, with an accuracy of 1. This outcome indicates that the method struggles to differentiate between normal diagnostic messages and malicious ones. This challenge arises from the method's utilization of the stability of in-vehicle messages, while diagnostic messages lack a stable transmission pattern, rendering them indistinguishable.

Another illustrative example can be found in the work by Muter et al. [70]. The study presents two detection methods [70]. The first method leverages the concept of relative entropy among different IDs to identify intrusion instances. However, it is observed that this method fails to detect the *SPA-3* and *SPA-1* attacks. In the *SPA-3* attack, the IDs remain unchanged within the attack dataset, resulting in an unaltered entropy value for the attack data. On the other hand, the *SPA-1* attack introduces new malicious messages with a distribution similar to that of normal messages, resulting in a relatively minor change in the entropy of the attack data. Consequently, the anomalies in entropy go undetected by this method. Moreover, due to the unstable transmission patterns of diagnostic messages within the IVN and the method's inability to obtain a stable relative entropy for these messages, the malicious diagnostic messages remain undetected by the employed VIDS.

Fig. 6: The results of the algorithm evaluation.

The second method examines the overall entropy changes within the data. However, similar to the first algorithm, it fails to detect the *FUA-2*, *SPA-3*, and *SPA-1* attacks. The inability to detect the *SPA-3* and *SPA-1* attacks is attributed to the same reasons as the first method. In the *FUA-2* attack, the adversary inserts malicious messages with random yet valid IDs. Although these malicious messages increase the entropy within a fixed time window, the overall change in entropy for the entire window is not distinct. Notably, for individual IDs within the window, the change in entropy remains notable. Consequently, while the first algorithm can detect the *FUA-2* attack, the second method fails to do so. Moreover, the detection rates for the *DIA-1*, *DIA-4*, *DIA-2*, and *DIA-3* attacks are poor. Our analysis reveals that the frequency of diagnostic messages is low, thereby limiting their impact on the overall data entropy. Additionally, the method employs a lenient threshold, resulting in the failure to detect malicious diagnostic messages.

Through a comprehensive analysis of various VIDSs, we have reached a comprehensive and conclusive summary finding. **Brief Discussion:** Primarily, it is imperative to emphasize that the direct evaluation of the merits and demerits of these methods based solely on experimental results is not viable, owing to the inherent divergence in their respective threat models. The primary objective of our experiments is to rigorously assess the detection capabilities of these methods in combating prevalent attacks, thereby elucidating their inherent limitations. Conclusions can be drawn from the empirical findings as follows.

The frequency-based, information entropy-based, ID sequence-based, and similarity-based methods are inherently reliant on the periodicity exhibited by CAN messages, specifically the stability of the ID attribute. In scenarios where adversaries transmit supplementary messages to manipulate vehicle control, these methods exhibit a notably high detection rate for identifying malicious messages. However, it is important to note that in instances where adversaries intentionally simulate a normal message cycle, such as in masquerade attacks, these methods may not be able to adequately detect these malicious messages as expected.

The payload-based method, which hinges upon detecting malicious messages through the change in the normal payload, provides a defense mechanism against masquerade attacks. However, owing to the intricate nature of the IVN, establishing a robust and consistent model for the payload of normal CAN messages proves to be challenging. Consequently, discerning the distinction between malicious and normal data becomes arduous, thereby leading to a relatively low detection rate for this method.

IX. DISCUSSION

Through an extensive review of various VIDS, we identified significant limitations that hinder their practical application. Additionally, we examine the future development of VIDS in the context of emerging automotive technologies.

While our primary focus is on CAN-based VIDS, it is important to consider broader vehicular cybersecurity solutions. This section also explores VIDS in intelligent transportation systems, which utilize large-scale data from connected vehicles and infrastructure, VIDS on J1939 heavy-duty vehicle CAN buses, which face unique challenges due to their distinct network structures, and VIDS for the Internet of Vehicles (IoV), where intrusion detection must adapt to highly connected and dynamic environments using cloud computing, edge processing, and V2X communication. These discussions provide a comprehensive view of vehicular intrusion detection and potential directions for future research.

A. Current Issues

Initially, an exhaustive compilation of the limitations inherent to all defense methods is presented.

1) Practicality: In the majority of prevailing vehicle models, conventional ECUs continue to be utilized, employing communication via the CAN bus. In order to safeguard this type of automobile, we think that a plug-and-play incremental protection approach or lightweight protection approach aligns more aptly with the requirements of contemporary OEMs. To commence, it should be noted that the ECUs found in the majority of vehicle models exhibit constrained computational capabilities and the transmission capacity of the CAN is also subject to limitations. The incorporation of intricate encryption or authentication algorithms within the existing IVN poses a substantial burden, given the aforementioned constraints.

Secondly, the implementation of extensive security updates for legacy automobile models poses considerable challenges for automakers. Integrating over-the-air (OTA) capabilities to existing vehicle models is a rare occurrence, thereby presenting a formidable obstacle in terms of incorporating modified communication protocols and intricate defense mechanisms into the original ECUs.

Another paramount consideration revolves around cost implications. Heightened computing power and accelerated communication technologies entail elevated expenses. For OEMs, undertaking hardware and software updates incurs substantial financial investment. Additionally, accommodating the requirements of previous vehicle models necessitates additional expenditures.

2) Targeted attack: According to our survey, it is commonly observed that when selecting target attacks, the prevailing tendency of VIDS is to opt for conventional attack types, such as Spoofing attacks, Fuzzing attacks, and Denial-of-Service (DoS) attacks. It is noteworthy that these attack categories were originally proposed in works dating back a decade [48]. Despite the significant detrimental impact caused by these aforementioned attacks, we contend that VIDS should be geared towards addressing more pragmatic or sophisticated attack scenarios.

Primarily, it is observed that numerous papers make references to real-world instances of car attacks. However, a distinct shortcoming within the existing research is the dearth of focused investigations pertaining to defenses specifically tailored to counter these real-world attacks. A noteworthy instance is the research conducted by Miller and Valasek, wherein they successfully employed the vehicle's diagnostic protocol to exert remote control over the car. Regrettably, this particular form of attack has received limited attention from researchers thus far.

Secondly, a considerable number of contemporary studies put forth more sophisticated attack methodologies [10], [38]. Within these attacks, adversaries possess the capability to obfuscate the attack traces, thereby evading detection by both users and defense systems. Moreover, these attacks also present a substantial threat to the overall safety of the automobile and they warrant significant attention and scrutiny from the research community.

3) Detection method based on machine learning: The utilization of machine learning techniques in VIDS holds great promise. Nonetheless, the prevailing detection defenses employed within VIDS continue to exhibit a relative simplicity in harnessing the potential of machine learning technology.

Primarily, these methods typically rely on direct utilization of machine learning algorithms for scrutinizing the abnormality in CAN message frequency or payload. In essence, this approach capitalizes on the inherent periodicity and predictability of CAN messages. However, noteworthy advancements beyond prior rule-based methods have not been significantly achieved.

It is noteworthy that this methodology remains susceptible to manipulation through carefully crafted falsified messages, thereby impeding its robustness and reliability. Furthermore, in comparison to the rule-based approach, the machine learning-based methodology generally necessitates enhanced computational power and entails greater time consumption for the ECU.

4) Abruptness of CAN messages: The accuracy of detection can be affected by the abruptness of CAN messages transmission. Many research works design their systems according to the stability and sustainability of the IVN. However, some research works show that these systems falsely detect benign event messages because the event messages deviate from the periodicity [117]. Besides, some special situations (e.g., retransmission after competing, bit errors) can also destroy the periodicity of in-vehicle messages. Therefore, how to distinguish malicious attacks and event messages or special situations is a great challenge. The anomaly-based VIDSs, which use the periodicity of in-vehicle messages, are difficult to solve the problems resulting from the abruptness of CAN messages transmission.

5) Hardware Limitations: The practical application of certain VIDS is severely impeded by the hardware limitations of ECUs. Conventional low-end ECUs typically comprise microcontrollers with modest computational cores [25], operating at frequencies in the range of several hundred megahertz and equipped with a few hundred kilobytes of RAM. However, certain approaches (e.g., [112], [74]) demand substantial computing resources, rendering their deployment in present-day automobiles challenging. As a consequence, VIDS implementations need to be tailored to accommodate the memory and computational constraints of current ECUs.

Furthermore, a few papers even propose VIDS solutions that necessitate the addition of supplementary equipment, such as oscilloscopes, for monitoring the IVN [21], [92]. While these methods offer exceptional detection efficacy, their associated costs are deemed unacceptable. Given the reluctance of Original Equipment Manufacturers (OEMs) to modify the existing IVN architecture of contemporary automobiles, the feasibility of implementing such approaches remains unlikely. Exploring alternative avenues that enable researchers to attain comparable detection capabilities in a more convenient and cost-effective manner, such as employing method EASI [93], represents a highly promising trajectory worth considering.

6) Private Communication Protocols: The adoption of proprietary protocols by various OEMs presents a significant obstacle to the development of semantic information-based VIDS. While certain papers propose VIDS solutions based on the collection of vehicle status data from normal CAN messages or diagnostic messages, the existing ECU systems and transport protocols for CAN messages are provided independently and secretly by different OEMs. Consequently, the parsing of diverse transport protocols on the bus and the acquisition of vehicle status pose substantial challenges.

Although the OBD diagnostic protocol allows for the retrieval of limited vehicle status information, additional diagnostic messages must be injected into the vehicle, thereby impeding normal ECU communication. This limitation necessitates careful consideration as it impacts the practicality of the approach and its potential effects on vehicle safety.

B. Trends

Despite the existing vulnerabilities and loopholes within the current vehicle network, it is important to recognize the rapid advancements taking place in automotive-related technologies. Ongoing efforts are being made to address hardware limitations and software vulnerabilities within modern vehicles, indicating a gradual resolution of these issues. Consequently, there is a strong possibility of significant breakthroughs in VIDS. Subsequently, we will outline several proposals for VIDS tailored specifically for current vehicle models. Additionally, we will present a forward-looking perspective on future defense methodologies that integrate seamlessly with intelligent automotive systems.

1) Integrating multiple methods: By integrating multiple methods, the effectiveness of intrusion detection can be enhanced. Each detection method possesses its own limitations, but through their combination, a broader range of attack scenarios and types can be accurately identified. For instance, frequency-based VIDS demonstrates advantages such as resource efficiency, high detection rates, and ease of implementation. However, it may be susceptible to evasion by adversaries employing carefully crafted messages, thus exhibiting a certain degree of unreliability. In such cases, VIDS based on voltage signatures can effectively identify these crafted messages. Consequently, when aiming to detect covert attacks [38], the utilization of voltage-based VIDS in conjunction with frequency-based VIDS can provide valuable support and enhance overall detection capabilities. The integration of methods in VIDS presents a promising and straightforward avenue for development, offering both simplicity and effectiveness.

2) Advancing Machine Learning in VIDS: Opportunities and Limitations: Machine learning has shown great potential in enhancing VIDSby leveraging anomaly detection techniques based on CAN message frequency and payload analysis. However, despite these advancements, ML-based VIDSstill face several limitations that hinder their practical deployment.

One major challenge is the computational overhead associated with deep learning models, which often require significant processing power and memory, making them difficult to deploy on resource-constrained ECUs. To address this, lightweight ML techniques such as model quantization, pruning, and knowledge distillation can be explored. These techniques reduce the size and complexity of ML models while maintaining detection accuracy. Additionally, TinyML—a framework designed for running ML models on low-power embedded devices—can be investigated to enhance the feasibility of ML-driven VIDS in real-world automotive environments.

Another limitation of ML-based VIDS is their static nature, as most models are trained on a fixed dataset and lack adaptability to new attack patterns. Future research should focus on incremental learning and online learning techniques, enabling models to continuously update and adapt to emerging threats without requiring complete retraining. Furthermore, federated learning (FL) can be employed to allow multiple vehicles to collaboratively improve their intrusion detection capabilities while preserving data privacy. This decentralized approach reduces the need for centralized data storage and minimizes communication overhead.

3) Addressing the Impact of Bursty CAN Message Transmission on Detection Accuracy: Traditional VIDS designs often assume a stable and periodic CAN message transmission pattern, relying on deviations from expected message intervals as indicators of potential attacks. However, real-world CAN traffic exhibits bursty transmission behavior, where event-triggered messages deviate from periodic patterns, leading to increased false positives in anomaly-based detection systems.

To mitigate this issue, advanced time-series analysis techniques, such as Long Short-Term Memory (LSTM) networks, Transformer models, and Hidden Markov Models (HMMs), can be leveraged to improve anomaly detection in bursty CAN environments. These models can learn temporal dependencies and distinguish between legitimate event-driven message bursts and malicious anomalies.

Additionally, multi-modal data fusion can be explored by integrating CAN message analysis with other vehicle sensor data (e.g., wheel speed, braking pressure, and GPS data) to provide additional context for anomaly detection. By correlating information across multiple data sources, VIDS can reduce false alarms caused by benign event-driven deviations.

Another promising approach is the use of adaptive anomaly detection mechanisms, where detection thresholds dynamically adjust based on contextual information. For instance, reinforcement learning algorithms can be employed to continuously refine the decision boundaries of an ML-based VIDS, ensuring that benign variations in CAN traffic do not trigger unnecessary alerts while still detecting genuine intrusions.

4) Overcoming ECU Hardware Limitations for Efficient VIDS Deployment: The computational constraints of traditional ECUs pose a significant challenge for the deployment of sophisticated VIDS, particularly those utilizing deep learning or complex statistical models.

To address these limitations, hardware acceleration techniques such as Field-Programmable Gate Arrays (FPGAs) and Application-Specific Integrated Circuits (ASICs) can be explored to offload computationally expensive tasks from the ECU. FPGA-based implementations of intrusion detection algorithms can significantly improve processing speed while maintaining energy efficiency.

Another viable solution is the adoption of edge computing for VIDS, where computationally intensive tasks are offloaded to dedicated edge nodes within the vehicle (e.g., a central gateway ECU or an onboard automotive AI processor). This architecture enables real-time analysis while reducing the computational burden on individual ECUs.

Finally, lightweight cryptographic techniques such as elliptic curve cryptography (ECC) and hash-based authentication mechanisms should be investigated to enhance security without overburdening ECU processing capabilities. By integrating these efficient cryptographic methods, VIDS can maintain robust security features while remaining feasible for deployment in modern vehicles.

5) Addressing Challenges Posed by Proprietary Communication Protocols: One of the major barriers to the development and adoption of semantic-based VIDS is the lack of standardization in CAN message semantics. Automotive OEMs often implement proprietary communication protocols, making it difficult for intrusion detection systems to interpret and analyze vehicle-specific CAN messages. .

To overcome this challenge, reverse engineering techniques can be explored to infer the meaning of proprietary CAN messages. Recent advancements in unsupervised learning and natural language processing (NLP) techniques may provide new ways to automatically extract semantic information from CAN traffic without requiring access to OEM-proprietary documentation.

Another promising approach is the use of blockchain technology to create a decentralized and immutable repository of CAN message definitions shared across multiple stakeholders in the automotive industry. By leveraging blockchain for secure and transparent data sharing, researchers and industry practitioners can collaborate to build more standardized and interpretable VIDS solutions.

Furthermore, the adoption of standardized automotive communication protocols, such as AUTOSAR Adaptive Platform and Vehicle-to-Everything (V2X) security frameworks, can help mitigate the challenges posed by proprietary protocols. Encouraging industry-wide adoption of open standards can facilitate the development of more effective and interoperable VIDS solutions.

6) Protection Mechanisms for Smart Driving Cars: The advancement of vehicle intelligence has brought about a transformation in the defense mechanisms employed in automobiles. As previously discussed, conventional vehicles still rely on low-computing ECUs and CAN for vehicle control. However, with the progress of intelligent and autonomous driving technologies,OEMs are increasingly adopting high-performance ECUs capable of supporting intelligent driver-assistance systems or automated driving systems. Furthermore, the realization of intelligent driving necessitates the integration of data from high-precision sensors like cameras and lidars, thereby demanding the utilization of higher-speed networks. Consequently, a number of automotive manufacturers have

initiated the adoption of advanced network technologies as substitutes for CAN in their vehicles. Examples of these technologies include CAN-FD (CAN with Flexible Data-Rate) and vehicle Ethernet, among others.

Through the utilization of enhanced hardware and higher-speed communication buses, a broader range of methods can be employed to safeguard the IVN. One such approach involves car manufacturers implementing authentication techniques to ensure the secure transmission of messages. OEMs can implement sophisticated authentication techniques that verify the integrity and authenticity of transmitted data, effectively mitigating the risk of unauthorized access or tampering. Additionally, the use of encrypted data can effectively safeguard the confidentiality of sensitive information within the vehicle. Employing encryption methods can effectively safeguard the confidentiality of private information, ensuring that critical data remains inaccessible to unauthorized entities. By leveraging encryption protocols, car manufacturers can bolster privacy protection and instill confidence in users regarding the security of their personal information. These methods hold promise in surpassing the efficacy of traditional intrusion detection systems, thereby fortifying the security of the IVN.

In reality, despite the presence of intelligent assisted driving system or automated driving system, the IVN of the smart car continues to be predominantly based on the CAN bus at present. As a result, researchers have shifted their focus away from the IVN of smart cars and towards new attack surfaces, including but not limited to the perception modules of vehicles [156], [157], autonomous driving algorithms [158], and the Vehicle-to-Everything(V2X) [159], [160]. In forthcoming endeavors, we shall embark upon an exhaustive investigation of all scholarly undertakings pertaining to the safety of intelligent automobiles.

C. Vehicular Intrusion Detection Systems in Intelligent Transportation Systems

In the current intelligent transportation system, the IVN, a crucial component of the internal network, primarily facilitates communication among ECUs within the vehicle using protocols like CAN (or other low-speed protocols). As technology advances, newer communication protocols are likely to replace existing ones. In existing research, intrusion detection for IVN and defenses for other networks often progress independently. These methods are typically based on different communication protocols and system models, with limited integration of various intrusion detection approaches. The following are key challenges and considerations when devising an intrusion detection system within the Intelligent Transportation System (ITS) framework.

Data Alignment and Accuracy. One significant challenge in developing a comprehensive intrusion detection system is addressing the delays in information transmission between various networks. When designing such a system, decision-making often relies on data collected from different networks, encompassing information like vehicle speed, steering angle, and radar data in the CAN. The challenge arises from the disparate data transmission rates across these networks, resulting in a complex and potentially messy dataset. Effectively aligning and maintaining the accuracy of this diverse data pose challenges that must be carefully considered in the design process.

Impact Analysis between Networks and Modules. When devising anomaly detection algorithms, it is crucial to take into account the interactions between different networks and intelligent modules. For instance, in cases where an intelligent assisted driving system bases acceleration and deceleration decisions on sensors like cameras, the instructions are transmitted to the IVN. In this context, the rationality of these instructions can be assessed by considering the status of the IVN. This assessment helps determine whether the intelligent assisted driving system is under attack [161]. Moreover, in traditional intrusion detection designs, there was a prevailing assumption that messages within the in-car network followed a periodic and stable pattern. However, with the introduction of various intelligent driving modules transmitting diverse data and instructions, these messages may disrupt the continuity and periodicity of the original messages. Consequently, when developing detection algorithms, it becomes essential to comprehensively consider the impact of different networks.

Utilization of Advanced Technologies. There is an opportunity to leverage more machine learning algorithms and artificial intelligence technologies. In prior research, a significant challenge restricting the design of intrusion detection algorithms stemmed from the limited performance of the ECU itself. However, with contemporary car manufacturers incorporating higher-performance ECUs for intelligent driving, there is room to employ newer technologies for anomaly detection, such as deep learning and large language models.

Verification and Encryption. It is essential to contemplate the verification and encryption of data. In the past, due to constraints related to the transmission speed of in-car networks and the performance of the ECU, data within the car was typically not encrypted by manufacturers. Researchers could design intrusion detection systems by directly analyzing changes in in-vehicle data. However, as ECUs evolve and higher-speed networks are employed, there is a likelihood that car manufacturers will implement data encryption. Consequently, researchers must develop more advanced detection algorithms aligned with the communication protocols utilized for data transmission.

Scalability and Flexibility. Algorithm design should prioritize scalability and flexibility. The swift evolution of intelligent transportation systems translates to frequent changes in the quantity and types of automotive sensors and network architecture. Intrusion detection systems for intelligent transportation are often deployed across diverse vehicles. Therefore, researchers must account for variations in hardware and software among different vehicle types when crafting intrusion detection algorithms. Simultaneously, the designed system should remain unaffected by upgrades to the car's internal software or hardware.

In summary, addressing these challenges and considerations is essential for designing effective and robust intrusion detection systems in the dynamic and interconnected environment of intelligent transportation systems.

D. Vehicular Intrusion Detection Systems on J1939 Heavy-Duty Vehicle CAN Buses

In contrast to regular commercial vehicles, heavy-duty vehicles also employ the CAN protocol for transmitting in-vehicle messages. However, heavy-duty vehicles diverge from the traditional CAN approach by utilizing a specialized CAN protocol based on the SAE J1939 standard. This standard incorporates extended frames and a dedicated transport protocol for multi-packet transmission. Only a limited number of recent studies have delved into addressing safety concerns specifically for heavy-duty vehicles utilizing the SAE J1939 standard [162]. Due to the disparate protocols in focus, direct comparisons with the intrusion detection systems discussed for typical commercial vehicles pose challenges. Consequently, we only presented these intrusion detection systems for CAN based on the SAE J1939 standard.

H. Shirazi et al. transform the original transmission message into specific parameters representing the vehicle's status. Subsequently, they employ machine learning algorithms to construct a model of the normal vehicle. This model is then utilized to identify DoS and fuzz attacks [163]. Mukherjee et al. introduced a priority graph-based method for detecting message injection attacks [164]. In a recent development, Jichici et al. proposed a two-stage intrusion detection mechanism for J1939 [165]. The initial phase verifies the legitimacy of the encrypted addresses (source and destination) in the CAN ID. The subsequent phase focuses on detecting single-bit alterations in the data field through appropriate range checks. Given the encryption of CAN frame data fields, the avalanche effect of block ciphers aids in identifying adversarial manipulation. Rogers et al. presented an alternative approach relying on timing and data analysis to identify spoofing and masquerading attacks in J1939 and NMEA2000 networks [166]. This mechanism can detect manipulation attacks by scrutinizing unusual changes in electrical potential during the transition from the dominant to the passive state, i.e., a single bit flip. Popa et al. investigated whether ECU voltage characteristics can serve as fingerprints for detecting spoofing attacks in J1939 [167].

E. Vehicular Intrusion Detection Systems for Internet of Vehicles

In this section, we provide a brief overview of research related to IoV intrusion detection. It is important to note that the CAN bus is a subset of IoV, and intrusion detection for IoV is not fully covered in our survey. However, considering it as a significant direction in the latest advancements in vehicle technology, we briefly mention related advanced works.

In essence, the Internet of Vehicles represents the integration of Vehicular Ad Hoc Networks (VANETs) and the Internet of Things (IoT) [168]. Modern connected vehicles utilize IoT to connect to networks, accessing real-time traffic data, navigation, and other driving conveniences. IoV employs various network technologies to enable communication within vehicles and between different entities on the road, fostering intelligent knowledge sharing. However, the extensive connectivity in the Internet of Vehicles, which involves numerous IoT sensors and processors, poses inherent risks. The continuous communication between road entities and the network makes IoV susceptible to intruders [169]. Security in the Internet of Vehicles is a critical concern, as incorrect information interfering with vehicle decision-making could have severe consequences, even leading to fatalities. Potential attackers might exploit vulnerabilities in network communications to take control of a vehicle, disseminate misleading information, or conduct other malicious activities that compromise the confidentiality, integrity, availability, and authenticity of vehicle systems. An illustrative example is a group of hackers successfully tricking Tesla's Autopilot software into veering into oncoming traffic [170]. Moreover, the wealth of data generated by autonomous driving raises privacy concerns, as this data can be utilized for artificial intelligence (AI) applications and data mining, exposing users' sensitive information to potential risks.

To bolster the security of the Internet of Vehicles, researchers recognize the need for an IDS capable of efficiently detecting anomalous behaviors in the network and promptly alerting authorities or users to potential threats [118]. Deep learning proves effective in discerning the inherent patterns within sample data. It accommodates higher-dimensional learning and prediction needs by establishing a nonlinear network structure with multiple hidden layers. Certain researchers [171], [172], [173] employ deep learning methods and edge computing technologies to analyze the traffic and speed of vehicles in the Internet of Vehicles. This analysis furnishes personalized safety information to drivers, thereby laying the groundwork for intrusion detection in the Internet of Vehicles. The studies [174], [175], [176] consistently highlight that the application of deep learning methods significantly enhances intrusion detection performance, making it a widely adopted approach in the field of Internet of Vehicles intrusion detection. Yang et al. [177] introduced an intrusion detection method tailored for IVN. Their approach leverages federated deep learning, capitalizing on the periodicity of network messages. The ConvLSTM model is employed to identify network intrusions, and the intrusion detection model is trained using federated deep learning techniques. Li et al. [178] presented an intrusion detection scheme for the IoV that relies on transfer learning. The proposed method incorporates two modes: cloud-assisted update and local update. Shone et al. [179] introduced an unsupervised deep learning intrusion detection technology utilizing an asymmetric deep autoencoder to construct a classification model. However, this method faces challenges in achieving better classification performance in unbalanced samples. Xu et al. [180] devised a Log-Cosh variational autoencoder method, incorporating a logarithmic hyperbolic chordal function to design a loss term for generating diverse intrusion data, thereby enhancing detection accuracy. Despite these advancements, deep learning-based solutions still encounter a high false-positive rate, primarily attributed to inadequate extraction of relevant features in the IoV. Intrusion data within the IoV encompasses numerous spatio-temporal features that can reflect certain attacker characteristics. Consequently, researchers have explored the utilization of deep learning methods, such as CNN or LSTM, to extract and process these spatio-temporal features

Hu et al. [[181] developed an intrusion detection technique employing CNN with a split convolution module. This approach

aims to enhance the diversity of spatial characteristics and reduce the impact of information redundancy across channels on the model. Park et al. [182] transformed network traffic into a grayscale image, established a Siamese CNN based on the small sample learning method, and determined the attack type based on the similarity score of the attack samples. To capture time-dependent dynamic features in network traffic, Zhou et al. [183] proposed an incremental LSTM network intrusion detection method. This method introduces state changes into LSTM, processing network data by acquiring the hidden layer state of LSTM dynamic information. Ashraf et al. [184] employed a combination of LSTM and autoencoder to extract timing features from Internet of Vehicles network traffic, enhancing the accuracy of intrusion detection in the Internet of Vehicles. While previous solutions often use only CNN or LSTM to process spatiotemporal features, this approach might suffer from insufficient feature extraction. Consequently, some researchers advocate for hybrid models integrating both CNN and LSTM to address this limitation. Wang et al. [185] introduced a hierarchical intrusion detection system based on spatiotemporal features. Initially, CNN is utilized to learn spatial features in network traffic packets, followed by LSTM to learn temporal features between multiple network traffic packets. This sequential approach results in a more accurate spatiotemporal feature vector. However, these solutions overlook the challenge of variable time intervals between packets in the data stream. To tackle this issue, Han et al. [186] proposed a space- and time-aware intrusion detection model. They developed a time and length-sensitive LSTM method to capture broader temporal features from intermittent flows. Shams et al. [187] devised an IDS model capable of collaboratively collecting network data from both vehicles and Roadside Units (RSUs). They implemented a multi-class IDS utilizing a Convolutional Neural Network (CNN) with a novel feature extraction method named Context-Aware Feature Extraction-Based CNN (CAFECNN). Leveraging the collected network flow data, the CAFECNN model effectively identifies both passive and active types of attacks. Results indicate that the proposed model demonstrates superior identification capabilities for hard-to-detect passive attacks in comparison to traditional machine learning methods.

The intrusion detection methods leveraging deep learning have proven effective in detecting network attacks in the Internet of Vehicles. However, these AI-based approaches also introduce risks and challenges, including vulnerabilities to adversarial sample attacks and concerns about the security of the intrusion detection system itself. Researchers are increasingly exploring the use of formal methods [188], [189] to enhance the reliability of artificial intelligence solutions. By employing mathematical logic, models, and proofs, these methods aim to verify whether the Internet of Vehicles intrusion detection system aligns with design specifications and identify potential errors, ultimately improving the security and dependability of intrusion detection. In the current landscape, intrusion detection methods relying on spatiotemporal features often utilize deep learning techniques like CNN and LSTM to establish sequential intrusion detection models. However, these methods can be susceptible to the influence of previous models, and there is a

tendency to overlook comprehensive spatiotemporal characteristics. There is a need for more comprehensive extraction of spatiotemporal features to enhance the overall performance of these methods.

X. SUMMARY

The advancement of the automotive industry has prominently elevated the significance of ensuring cyberspace security within vehicular systems. A proliferation of attacks has been observed, predominantly focusing on the CAN utilized IVN. In response to these threats, numerous defense strategies have been devised to mitigate attacks and fortify the security of vehicular systems. Nevertheless, the practical implementation of these solutions encounters certain constraints and hurdles that warrant further attention and exploration.

This paper offers a comprehensive investigation into the current landscape of vehicle attack and defense strategies, with a specific focus on the CAN. The objective of this study is to critically evaluate the limitations of existing approaches and provide valuable insights for the future design of VIDS. We provide a comprehensive synthesis of existing VIDS from multiple perspectives and conduct evaluations on a unified dataset to assess the effectiveness of selected methodologies. Our analysis reveals a predominant emphasis on specific attack categories within the examined VIDS, thereby disregarding the more sophisticated and realistic attack scenarios. To address these shortcomings, we put forth a set of defense recommendations based on our research findings. Furthermore, considering the advancement of automotive intelligence, we propose additional cybersecurity recommendations tailored to the domain of smart car technology.

ACKNOWLEDGMENTS

REFERENCES

[1] "Automotive cybersecurity market research report 2023 — growth rate and forecast till 2031," https://www.linkedin.com/pulse/automotive-cybersecurity-market-research-report-tadqf, 2023.
[2] D. K. Nilsson, P. H. Phung, and U. E. Larson, "Vehicle ecu classification based on safety-security characteristics," 2008.
[3] S. Tuohy, M. Glavin, C. Hughes, E. Jones, M. Trivedi, and L. Kilmartin, "Intra-vehicle networks: A review," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 534–545, 2014.
[4] O. Y. Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby, and A. Mouzakitis, "Intrusion detection systems for intra-vehicle networks: A review," *IEEE Access*, vol. 7, pp. 21 266–21 289, 2019.
[5] E. Biham, O. Dunkelman, S. Indesteege, N. Keller, and B. Preneel, "How to steal cars a practical attack on keeloq," in *EUROCRYPT*, 2008, pp. 1–18.
[6] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive can networks—practical examples and selected short-term countermeasures," *Reliability Engineering & System Safety*, vol. 96, no. 1, pp. 11–25, 2011.
[7] C. Miller and C. Valasek, "Adventures in automotive networks and control units," *Def Con*, 2013.
[8] ——, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, p. 91, 2015.

[9] A. Greenberg, "Hackers remotely kill a jeep on the highway—with me in it," *Wired*, vol. 7, p. 21, 2015.

[10] S. Kulandaivel, S. Jain, J. Guajardo, and V. Sekar, "Cannon: Reliable and stealthy remote shutdown attacks via unaltered automotive micro-controllers," in *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 195–210.

[11] T. Lee, "Hackers discover a way to hack into your car's remote control app," https://www.ubergizmo.com/2011/07/hackers-discover-a-way-to-hack-into-your-cars-remote-control-app/, 2011.

[12] Trend Micro, "Connected car vulnerabilities affect the can standard," https://www.trendmicro.com/en_us/research/17/h/connected-car-hack.html, 2017.

[13] I. Foster, A. Prudhomme, K. Koscher, and S. Savage, "Fast and vulnerable: A story of telematic failures," in *9th {USENIX} Workshop on Offensive Technologies ({WOOT} 15)*, 2015.

[14] W. A. Farag, "Cantrack: Enhancing automotive can bus security using intuitive encryption algorithms," in *2017 7th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO)*. IEEE, 2017, pp. 1–5.

[15] L. Dariz, M. Selvatici, M. Ruggeri, G. Costantino, and F. Martinelli, "Trade-off analysis of safety and security in can bus communication," in *2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*. IEEE, 2017, pp. 226–231.

[16] G. Carel, R. Isshiki, T. Kusaka, Y. Nogami, and S. Araki, "Design of a message authentication protocol for can fd based on chaskey lightweight mac," in *2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW)*. IEEE, 2018, pp. 267–271.

[17] B. Palaniswamy, S. Camtepe, E. Foo, and J. Pieprzyk, "An efficient authentication scheme for intra-vehicular controller area network," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3107–3122, 2020.

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

[19] S. Hu, Q. A. Chen, J. Joung, C. Carlak, Y. Feng, Z. M. Mao, and H. X. Liu, "Cvshield: Guarding sensor data in connected vehicle with trusted execution environment," in *Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security*, 2020, pp. 1–4.

[20] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in *Proc. USENIX Security*, 2016.

[21] ——, "Viden: Attacker identification on in-vehicle networks," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017, pp. 1109–1123.

[22] H. Wen, Q. A. Chen, and Z. Lin, "Plug-n-pwned: Comprehensive vulnerability analysis of obd-ii dongles as a new over-the-air attack surface in automotive iot," 2020.

[23] K. Jeong, S. B. Choi, and H. Choi, "Sensor fault detection and isolation using a support vector machine for vehicle suspension systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 3852–3863, 2020.

[24] K. Joo, W. Choi, and D. H. Lee, "Hold the door! fingerprinting your car key to prevent keyless entry car theft," *arXiv preprint arXiv:2003.13251*, 2020.

[25] D. Stabili, M. Marchetti, and M. Colajanni, "Detecting attacks to internal vehicle networks through hamming distance," in *2017 AEIT International Annual Conference*. IEEE, 2017, pp. 1–6.

[26] O. Avatefipour and H. Malik, "State-of-the-art survey on in-vehicle network communication (can-bus) security and vulnerabilities," *arXiv preprint arXiv:1802.01725*, 2018.

[27] A. Tomlinson, J. Bryans, and S. A. Shaikh, "Towards viable intrusion detection methods for the automotive controller area network," in *2nd ACM Computer Science in Cars Symposium. ACM, Munich, Germany*, 2018, pp. 1–9.

[28] C. Young, J. Zambreno, H. Olufowobi, and G. Bloom, "Survey of automotive controller area network intrusion detection systems," *IEEE Design & Test*, vol. 36, no. 6, pp. 48–55, 2019.

[29] W. Wu, R. Li, G. Xie, J. An, J. Bai, J. Zhou, and K. Li, "A survey of intrusion detection for in-vehicle networks," *IEEE Transactions on Intelligent Transportation Systems*, 2019.

[30] G. Karopoulos, G. Kambourakis, E. Chatzoglou, J. L. Hernández-Ramos, and V. Kouliaridis, "Demystifying in-vehicle intrusion detection systems: A survey of surveys and a meta-taxonomy," *Electronics*, vol. 11, no. 7, p. 1072, 2022.

[31] S. Rajapaksha, H. Kalutarage, M. O. Al-Kadri, A. Petrovski, G. Madzudzo, and M. Cheah, "Ai-based intrusion detection systems for in-vehicle networks: A survey," *ACM Computing Surveys*, vol. 55, no. 11, pp. 1–40, 2023.

[32] E. Aliwa, O. Rana, C. Perera, and P. Burnap, "Cyberattacks and countermeasures for in-vehicle networks," *ACM Computing Surveys (CSUR)*, vol. 54, no. 1, pp. 1–37, 2021.

[33] Y. Xie, Y. Zhou, J. Xu, J. Zhou, X. Chen, and F. Xiao, "Cybersecurity protection on in-vehicle networks for distributed automotive cyber-physical systems: State-of-the-art and future challenges," *Software: Practice and Experience*, vol. 51, no. 11, pp. 2108–2127, 2021.

[34] A. Hafeez, K. Rehman, and H. Malik, "State of the art survey on comparison of physical fingerprinting-based intrusion detection techniques for in-vehicle security," SAE Technical Paper, Tech. Rep., 2020.

[35] S.-F. Lokman, A. T. Othman, and M.-H. Abu-Bakar, "Intrusion detection system for automotive controller area network (can) bus system: a review," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–17, 2019.

[36] G. Dupont, J. den Hartog, S. Etalle, and A. Lekidis, "A survey of network intrusion detection systems for controller area network," in *2019 IEEE International Conference on Vehicular Electronics and Safety (ICVES)*. IEEE, 2019, pp. 1–6.

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

[38] R. Bhatia, V. Kumar, K. Serag, Z. B. Celik, M. Payer, and D. Xu, "Evading voltage-based intrusion detection on automotive can." in *NDSS*, 2021.

[39] B. Ramesh and S. Murthy, "In vehicle networking," in *Proceedings of the third International Conference on Automotive and Fuel Technology*. Allied Publishers, 2004, p. 194.

[40] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," *black hat USA*, 2014.

[41] M. Cooperation, "Most specification," *Rev. 3.0, URL: www. mostcoop-eration. com, Jun*, 2008.

[42] C. Specification, "Robert bosch gmbh," *Stuttgart, Germany*, 1991.

[43] L. S. Package, "Revision 2.0," *LIN consortium*, 2003.

[44] R. Makowitz and C. Temple, "Flexray-a communication network for automotive control systems," in *2006 IEEE International Workshop on Factory Communication Systems*. IEEE, 2006, pp. 207–212.

[45] R. Bosch *et al.*, "Can specification version 2.0," *Rober Bousch GmbH, Postfach*, vol. 300240, p. 72, 1991.

[46] M. Ruff, "Evolution of local interconnect network (lin) solutions," in *2003 IEEE 58th Vehicular Technology Conference. VTC 2003-Fall (IEEE Cat. No. 03CH37484)*, vol. 5. IEEE, 2003, pp. 3382–3389.

[47] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno *et al.*, "Comprehensive experimental analyses of automotive attack surfaces." in *USENIX Security Symposium*, vol. 4. San Francisco, 2011, pp. 447–462.

[48] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham *et al.*, "Experimental security analysis of a modern automobile," in *Proc. IEEE SP*, 2010.

[49] A. B. C. Douss, R. Abassi, and D. Sauveron, "State-of-the-art survey of in-vehicle protocols and automotive ethernet security and vulnerabilities," *Mathematical Biosciences and Engineering*, vol. 20, no. 9, pp. 17 057–17 095, 2023.

[50] H. Kim, W. Yoo, S. Ha, and J.-M. Chung, "In-vehicle network average response time analysis for can-fd and automotive ethernet," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 6, pp. 6916–6932, 2023.

[51] Brandon Lewis, "Automotive ethernet: A crossroads for the connected car," https://embeddedcomputing.com/application/automotive/vehicle-networking/automotive-ethernet-a-crossroads-for-the-connected-car, 2018.

[52] Vector, "Solutions for automotive ethernet," https://www.vector.com/int/en/products/solutions/networks/automotive-ethernet/#, 2024.

[53] "A Remote Attack on the Bosch Drivelog Connector Dongle," https://argus-sec.com/remote-attack-bosch-drivelog-connector-dongle/.

[54] L. Christensen and D. Dannberg, "Ethical hacking of iot devices: Obd-ii dongles," 2019.

[55] H. Wen, Q. Zhao, Q. A. Chen, and Z. Lin, "Automated cross-platform reverse engineering of can bus commands from mobile apps," in *Proceedings 2020 Network and Distributed System Security Symposium (NDSS'20)*, 2020.

[56] G. Costantino, A. La Marra, F. Martinelli, and I. Matteucci, "Candy: A social engineering attack to leak information from infotainment system,"

in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*. IEEE, 2018, pp. 1–5.

[57] T. P. Oman and K. J. Hawes, "Relay attack prevention for passive entry passive start (peps) vehicle security systems," Jan. 6 2015, uS Patent 8,930,045.

[58] P. Kapoor, A. Vora, and K.-D. Kang, "Detecting and mitigating spoofing attack against an automotive radar," in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*. IEEE, 2018, pp. 1–6.

[59] J. Zhou, P. Joshi, H. Zeng, and R. Li, "Btmonitor: Bit-time-based intrusion detection and attacker identification in controller area network," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 18, no. 6, pp. 1–23, 2019.

[60] N. Nowdehi, W. Aoudi, M. Almgren, and T. Olovsson, "Casad: Can-aware stealthy-attack detection for in-vehicle networks," *arXiv preprint arXiv:1909.08407*, 2019.

[61] "Microchip MCP2515 Datasheet," www.microchip.com/MCP2515.

[62] K.-T. Cho and K. G. Shin, "Error handling of in-vehicle networks makes them vulnerable," in *Proc. ACM CCS*, 2016.

[63] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. Eidgenössische Technische Hochschule Zürich, Department of Computer Science, 2011.

[64] F. D. Garcia, D. Oswald, T. Kasper, and P. Pavlidès, "Lock it and still lose it—on the (in) security of automotive remote keyless entry systems," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*, 2016.

[65] R. E. Haas and D. P. Möller, "Automotive connectivity, cyber attack scenarios and automotive cyber security," in *2017 IEEE International Conference on Electro Information Technology (EIT)*. IEEE, 2017, pp. 635–639.

[66] 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 *2016 international conference on information networking (ICOIN)*. IEEE, 2016, pp. 63–68.

[67] A. Taylor, N. Japkowicz, and S. Leblanc, "Frequency-based anomaly detection for the automotive can bus," in *2015 World Congress on Industrial Control Systems Security (WCICSS)*. IEEE, 2015, pp. 45–49.

[68] I. Studnia, E. Alata, V. Nicomette, M. Kaâniche, and Y. Laarouchi, "A language-based intrusion detection approach for automotive embedded networks," 2018.

[69] M. Foruhandeh, Y. Man, R. Gerdes, M. Li, and T. Chantem, "Simple: Single-frame based physical layer identification for intrusion detection and prevention on in-vehicle networks," in *Proceedings of the 35th Annual Computer Security Applications Conference*, 2019, pp. 229–244.

[70] M. Müter and N. Asaj, "Entropy-based anomaly detection for in-vehicle networks," in *2011 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2011, pp. 1110–1115.

[71] "Controller Area Network (CAN) Overview," https://www.ni.com/en-us/innovations/white-papers/06/controller-area-network--can--overview.html, 2019.

[72] A. de Faveri Tron, S. Longari, M. Carminati, M. Polino, and S. Zanero, "Canflict: Exploiting peripheral conflicts for data-link layer attacks on automotive networks," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 711–723.

[73] H. Olufowobi, U. Ezeobi, E. Muhati, G. Robinson, C. Young, J. Zambreno, and G. Bloom, "Anomaly detection approach using adaptive cumulative sum algorithm for controller area network," in *Proceedings of the ACM Workshop on Automotive Cybersecurity*. ACM, 2019, pp. 25–30.

[74] F. Martinelli, F. Mercaldo, V. Nardone, and A. Santone, "Car hacking identification through fuzzy logic algorithms," in *2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*. IEEE, 2017, pp. 1–7.

[75] H. Lee, S. H. Jeong, and H. K. Kim, "Otids: A novel intrusion detection system for in-vehicle network by using remote frame," in *2017 15th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2017, pp. 57–5709.

[76] M. Marchetti, D. Stabili, A. Guido, and M. Colajanni, "Evaluation of anomaly detection for in-vehicle networks through information-theoretic algorithms," in *2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI)*. IEEE, 2016, pp. 1–6.

[77] "Road vehicles–unified diagnostic services (uds)–part 1: Specification and requirements," 2013.

[78] S. N. Narayanan, S. Mittal, and A. Joshi, "Obd_securealert: An anomaly detection system for vehicles," in *IEEE SMARTCOMP*, 2016.

[79] D. S. Fowler, "A fuzz testing methodology for cyber-security assurance of the automotive can bus," Ph.D. dissertation, Coventry University, 2019.

[80] J. Singh and M. J. Nene, "A survey on machine learning techniques for intrusion detection systems," 2013.

[81] V. Jyothsna, V. R. Prasad, and K. M. Prasad, "A review of anomaly based intrusion detection systems," *International Journal of Computer Applications*, vol. 28, no. 7, pp. 26–35, 2011.

[82] U. E. Larson, D. K. Nilsson, and E. Jonsson, "An approach to specification-based attack detection for in-vehicle networks," in *2008 IEEE Intelligent Vehicles Symposium*. IEEE, 2008, pp. 220–225.

[83] M. Farsi, K. Ratcliff, and M. Barbosa, "An introduction to canopen," *Computing & Control Engineering Journal*, vol. 10, no. 4, pp. 161–168, 1999.

[84] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *computers & security*, vol. 28, no. 1-2, pp. 18–28, 2009.

[85] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," *IEEE Transactions on Mobile Computing*, vol. 9, no. 3, pp. 449–462, 2009.

[86] S. U. Sagong, X. Ying, A. Clark, L. Bushnell, and R. Poovendran, "Cloaking the clock: emulating clock skew in controller area networks," in *2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 2018, pp. 32–42.

[87] X. Ying, S. U. Sagong, A. Clark, L. Bushnell, and R. Poovendran, "Shape of the cloak: Formal analysis of clock skew-based intrusion detection system in controller area networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 9, pp. 2300–2314, 2019.

[88] P.-S. Murvay and B. Groza, "Source identification using signal characteristics in controller area networks," *IEEE Signal Processing Letters*, vol. 21, no. 4, pp. 395–399, 2014.

[89] O. Avatefipour, "Physical-fingerprinting of electronic control unit (ecu) based on machine learning algorithm for in-vehicle network communication protocol "can-bus"," Ph.D. dissertation, 2017.

[90] W. Choi, H. J. Jo, S. Woo, J. Y. Chun, J. Park, and D. H. Lee, "Identifying ecus using inimitable characteristics of signals in controller area networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 4757–4770, 2018.

[91] W. Choi, K. Joo, H. J. Jo, M. C. Park, and D. H. Lee, "Voltageids: Low-level communication characteristics for automotive intrusion detection system," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, 2018.

[92] M. Kneib and C. Huth, "Scission: Signal characteristic-based sender identification and intrusion detection in automotive networks," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2018, pp. 787–800.

[93] M. Kneib, O. Schell, and C. Huth, "Easi: Edge-based sender identification on resource-constrained platforms for automotive networks," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2020, pp. 1–16.

[94] P.-S. Murvay and B. Groza, "Tidal-can: Differential timing based intrusion detection and localization for controller area network," *IEEE Access*, vol. 8, pp. 68 895–68 912, 2020.

[95] D. Paret, *Multiplexed networks for embedded systems: CAN, LIN, Flexray, Safe-by-Wire...* John Wiley & Sons, 2007.

[96] C. Ling and D. Feng, "An algorithm for detection of malicious messages on can buses," in *2012 National Conference on Information Technology and Computer Science*. Atlantis Press, 2012.

[97] M. Gmiden, M. H. Gmiden, and H. Trabelsi, "An intrusion detection method for securing in-vehicle can bus," in *2016 17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*. IEEE, 2016, pp. 176–180.

[98] M. R. Moore, R. A. Bridges, F. L. Combs, M. S. Starr, and S. J. Prowell, "Modeling inter-signal arrival times for accurate detection of can bus signal injection attacks: a data-driven approach to in-vehicle intrusion detection," in *Proceedings of the 12th Annual Conference on Cyber and Information Security Research*, 2017, pp. 1–4.

[99] A. Tomlinson, J. Bryans, S. A. Shaikh, and H. K. Kalutarage, "Detection of automotive can cyber-attacks by identifying packet timing anomalies in time windows," in *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. IEEE, 2018, pp. 231–238.

[100] C. Young, H. Olufowobi, G. Bloom, and J. Zambreno, "Automotive intrusion detection based on constant can message frequencies across
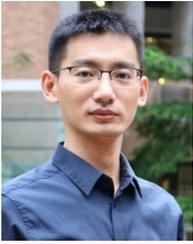
vehicle driving modes," in *Proceedings of the ACM Workshop on Automotive Cybersecurity*. ACM, 2019, pp. 9–14.

[101] H. Olufowobi, C. Young, J. Zambreno, and G. Bloom, "Saiducant: Specification-based automotive intrusion detection using controller area network (can) timing," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 2, pp. 1484–1494, 2019.

[102] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE mobile computing and communications review*, vol. 5, no. 1, pp. 3–55, 2001.

[103] Y. Gu, A. McCallum, and D. Towsley, "Detecting anomalies in network traffic using maximum entropy estimation," in *Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement*, 2005, pp. 32–32.

[104] W. Lee and D. Xiang, "Information-theoretic measures for anomaly detection," in *Proceedings 2001 IEEE Symposium on Security and Privacy. S&P 2001*. IEEE, 2000, pp. 130–143.

[105] R. A. Kemmerer and G. Vigna, "Intrusion detection: a brief history and overview," *Computer*, vol. 35, no. 4, pp. supl27–supl30, 2002.

[106] T. M. Cover and J. A. Thomas, "Entropy, relative entropy and mutual information," *Elements of information theory*, vol. 2, pp. 1–55, 1991.

[107] ——, "Information theory and statistics," *Elements of Information Theory*, vol. 1, no. 1, pp. 279–335, 1991.

[108] W. Wu, Y. Huang, R. Kurachi, G. Zeng, G. Xie, R. Li, and K. Li, "Sliding window optimized information entropy analysis method for intrusion detection on in-vehicle networks," *IEEE Access*, vol. 6, pp. 45 233–45 245, 2018.

[109] D. Bertsimas, J. Tsitsiklis *et al.*, "Simulated annealing," *Statistical science*, vol. 8, no. 1, pp. 10–15, 1993.

[110] M. Markovitz and A. Wool, "Field classification, modeling and anomaly detection in unknown can bus networks," *Vehicular Communications*, vol. 9, pp. 43–52, 2017.

[111] A. Taylor, S. Leblanc, and N. Japkowicz, "Anomaly detection in automobile control network data with long short-term memory networks," in *2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA)*. IEEE, 2016, pp. 130–139.

[112] 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, p. e0155781, 2016.

[113] J. Xiao, H. Wu, and X. Li, "Robust and self-evolving ids for in-vehicle network by enabling spatiotemporal information," in *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. IEEE, 2019, pp. 1390–1397.

[114] X. Shi, Z. Chen, H. Wang, D.-Y. Yeung, W.-K. Wong, and W.-c. Woo, "Convolutional lstm network: A machine learning approach for precipitation nowcasting," *Advances in neural information processing systems*, vol. 28, pp. 802–810, 2015.

[115] V. K. Kukkala, S. V. Thiruloga, and S. Pasricha, "Indra: Intrusion detection using recurrent autoencoders in automotive embedded systems," *arXiv preprint arXiv:2007.08795*, 2020.

[116] J. Chung, C. Gulcehre, K. Cho, and Y. Bengio, "Empirical evaluation of gated recurrent neural networks on sequence modeling," *arXiv preprint arXiv:1412.3555*, 2014.

[117] T. Koyama, T. Shibahara, K. Hasegawa, Y. Okano, M. Tanaka, and Y. Oshima, "Anomaly detection for mixed transmission can messages using quantized intervals and absolute difference of payloads," in *Proceedings of the ACM Workshop on Automotive Cybersecurity*. ACM, 2019, pp. 19–24.

[118] E. Seo, H. M. Song, and H. K. Kim, "Gids: Gan based intrusion detection system for in-vehicle network," in *2018 16th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2018, pp. 1–6.

[119] K. Pawelec, R. A. Bridges, and F. L. Combs, "Towards a can ids based on a neural network data field predictor," in *Proceedings of the ACM Workshop on Automotive Cybersecurity*. ACM, 2019, pp. 31–34.

[120] M. Marchetti and D. Stabili, "Anomaly detection of can bus messages through analysis of id sequences," in *2017 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2017, pp. 1577–1583.

[121] R. Islam, R. U. D. Refat, S. M. Yerram, and H. Malik, "Graph-based intrusion detection system for controller area networks," *IEEE Transactions on Intelligent Transportation Systems*, 2020.

[122] S. Ohira, A. K. Desta, I. Arai, H. Inoue, and K. Fujikawa, "Normal and malicious sliding windows similarity analysis method for fast and accurate ids against dos attacks on in-vehicle networks," *IEEE Access*, vol. 8, pp. 42 422–42 435, 2020.

[123] A. Theissler, "Anomaly detection in recordings from in-vehicle networks," *Big data and applications*, vol. 23, 2014.

[124] D. Tian, Y. Li, Y. Wang, X. Duan, C. Wang, W. Wang, R. Hui, and P. Guo, "An intrusion detection system based on machine learning for can-bus," in *International Conference on Industrial Networks and Intelligent Systems*. Springer, 2017, pp. 285–294.

[125] M. Weber, S. Klug, E. Sax, and B. Zimmer, "Embedded hybrid anomaly detection for automotive can communication," 2018.

[126] 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.

[127] A. Tomlinson, J. Bryans, and S. A. Shaikh, "Using a one-class compound classifier to detect in-vehicle network attacks," in *Proceedings of the Genetic and Evolutionary Computation Conference Companion*, 2018, pp. 1926–1929.

[128] K. Zhu, Z. Chen, Y. Peng, and L. Zhang, "Mobile edge assisted literal multi-dimensional anomaly detection of in-vehicle network using lstm," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 4275–4284, 2019.

[129] M. Hanselmann, T. Strauss, K. Dormann, and H. Ulmer, "Canet: An unsupervised intrusion detection system for high dimensional can bus data," *IEEE Access*, vol. 8, pp. 58 194–58 205, 2020.

[130] H. Li, L. Zhao, M. Juliato, S. Ahmed, M. R. Sastry, and L. L. Yang, "Poster: Intrusion detection system for in-vehicle networks using sensor correlation and integration," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 2531–2533.

[131] A. Ganesan, J. Rao, and K. Shin, "Exploiting consistency among heterogeneous sensors for vehicle anomaly detection," SAE Technical Paper, Tech. Rep., 2017.

[132] A. Wasicek, M. D. Pese, A. Weimerskirch, Y. Burakova, and K. Singh, "Context-aware intrusion detection in automotive control systems," in *ESCAR USA Conference*, 2017.

[133] L. ben Othmane, L. Dhulipala, M. Abdelkhalek, M. Govindarasu, and N. Multari, "Detection of injection attacks in in-vehicle networks," 2019.

[134] M. Casillo, S. Coppola, M. De Santo, F. Pascale, and E. Santonicola, "Embedded intrusion detection system for detecting attacks over can-bus," in *2019 4th International Conference on System Reliability and Safety (ICSRS)*. IEEE, 2019, pp. 136–141.

[135] L. Xue, Y. Liu, T. Li, K. Zhao, J. Li, X. L. Le Yu, Y. Zhou, and G. Gu, "SAID: State-aware defense against injection attacks on in-vehicle network," in *USENIX Security Symposium (USENIX Security)*, 2022.

[136] A. Ugoni and B. F. Walker, "The chi square test: an introduction," *COMSIG review*, vol. 4, no. 3, p. 61, 1995.

[137] B. Bollobás, *Modern graph theory*. Springer Science & Business Media, 2013, vol. 184.

[138] J. J. Flynn, "Faunal provinces and the simpson coefficient," *Rocky Mountain Geology*, vol. 24, no. special_paper_3, pp. 317–338, 1986.

[139] T. P. Nguyen, H. Nam, and D. Kim, "Transformer-based attention network for in-vehicle intrusion detection," *IEEE Access*, 2023.

[140] M. Amer, M. Goldstein, and S. Abdennadher, "Enhancing one-class support vector machines for unsupervised anomaly detection," in *Proceedings of the ACM SIGKDD workshop on outlier detection and description*, 2013, pp. 8–15.

[141] M. Xu, P. Watanachaturaporn, P. K. Varshney, and M. K. Arora, "Decision tree regression for soft classification of remote sensing data," *Remote Sensing of Environment*, vol. 97, no. 3, pp. 322–336, 2005.

[142] J. H. Friedman, "Greedy function approximation: a gradient boosting machine," *Annals of statistics*, pp. 1189–1232, 2001.

[143] D. George and J. Hawkins, "A hierarchical bayesian model of invariant pattern recognition in the visual cortex," in *Proceedings. 2005 IEEE International Joint Conference on Neural Networks, 2005.*, vol. 3. IEEE, 2005, pp. 1812–1817.

[144] D. E. Padilla, R. Brinkworth, and M. D. McDonnell, "Performance of a hierarchical temporal memory network in noisy sequence learning," in *2013 IEEE International Conference on Computational Intelligence and Cybernetics (CYBERNETICSCOM)*. IEEE, 2013, pp. 45–51.

[145] B. G. Batchelor, "Classification and data analysis in vector spaces," in *Pattern Recognition*. Springer, 1978, pp. 65–116.

[146] ——, *Machine Vision Handbook*. Springer, 2012.

[147] M. Müter, A. Groll, and F. C. Freiling, "A structured approach to anomaly detection for in-vehicle networks," in *IEEE IAS*, 2010.

[148] T. Pevnỳ, "Loda: Lightweight on-line detector of anomalies," *Machine Learning*, vol. 102, no. 2, pp. 275–304, 2016.

[149] X. Chen, W. Li, S. Lu, Z. Zhou, and X. Fu, "Efficient resource allocation for on-demand mobile-edge cloud computing," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8769–8780, 2018.

[150] I. O. for Standardization, "Road vehicles—diagnostics on controller area networks (can)—requirements for emissions-related systems," *ISO Standard 15765-4:2005(E)*.

[151] M. H. Hassoun *et al.*, *Fundamentals of artificial neural networks*. MIT press, 1995.

[152] Z. Bar-Joseph, "Analyzing time series gene expression data," *Bioinformatics*, vol. 20, no. 16, pp. 2493–2503, 2004.

[153] N. Friedman, D. Geiger, and M. Goldszmidt, "Bayesian network classifiers," *Machine learning*, vol. 29, no. 2-3, pp. 131–163, 1997.

[154] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," *Vehicular Communications*, vol. 21, p. 100198, 2020.

[155] LAUNCH, "X-431 pad," http://en.cnlaunch.com/prod_view.aspx?TypeId=12&Id=317&FId=t3:12:3, 2019.

[156] Y. Cao, S. H. Bhupathiraju, P. Naghavi, T. Sugawara, Z. M. Mao, and S. Rampazzi, "You can't see me: physical removal attacks on lidar-based autonomous vehicles driving frameworks," *arXiv eprint archive*, 2022.

[157] Z. Jin, J. Xiaoyu, Y. Cheng, B. Yang, C. Yan, and W. Xu, "Pla-lidar: Physical laser attacks against lidar-based 3d object detection in autonomous vehicle," in *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 2022, pp. 710–727.

[158] A. Wachi, "Failure-scenario maker for rule-based agent using multi-agent adversarial reinforcement learning and its application to autonomous driving," *arXiv preprint arXiv:1903.10654*, 2019.

[159] M. Zhou, L. Han, H. Lu, and C. Fu, "Distributed collaborative intrusion detection system for vehicular ad hoc networks based on invariant," *Computer Networks*, vol. 172, p. 107174, 2020.

[160] A. R. Nair, N. K. Jadav, R. Gupta, and S. Tanwar, "Ai-empowered secure data communication in v2x environment with 6g network," in *IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2022, pp. 1–6.

[161] L. Xue, Y. Liu, T. Li, K. Zhao, J. Li, L. Yu, X. Luo, Y. Zhou, and G. Gu, "{SAID}: State-aware defense against injection attacks on in-vehicle network," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 1921–1938.

[162] C. Jichici, A. Berdich, A. Musuroi, and B. Groza, "Control system level intrusion detection on j1939 heavy-duty vehicle buses," *IEEE Transactions on Industrial Informatics*, 2023.

[163] H. Shirazi, I. Ray, and C. Anderson, "Using machine learning to detect anomalies in embedded networks in heavy vehicles," in *Foundations and Practice of Security: 12th International Symposium, FPS 2019, Toulouse, France, November 5–7, 2019, Revised Selected Papers 12*. Springer, 2020, pp. 39–55.

[164] S. Mukherjee, J. Walkery, I. Rayz, and J. Daily, "A precedence graph-based approach to detect message injection attacks in j1939 based networks," in *2017 15th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2017, pp. 67–6709.

[165] C. Jichici, B. Groza, R. Ragobete, P.-S. Murvay, and T. Andreica, "Effective intrusion detection and prevention for the commercial vehicle sae j1939 can bus," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 17 425–17 439, 2022.

[166] M. Rogers, P. Weigand, J. Happa, and K. Rasmussen, "Detecting can attacks on j1939 and nmea 2000 networks," *IEEE Transactions on Dependable and Secure Computing*, 2022.

[167] L. Popa, B. Groza, C. Jichici, and P.-S. Murvay, "Ecuprint—physical fingerprinting electronic control units on can buses inside cars and sae j1939 compliant vehicles," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1185–1200, 2022.

[168] A. Dureja and S. Sangwan, "A review: Efficient transportation—future aspects of iov," *Evolving Technologies for Computing, Communication and Smart World: Proceedings of ETCCS 2020*, pp. 97–108, 2020.

[169] A. Garg, A. Chauhan, and P. G. Shambharkar, "Security threats & attacks in iov environment: Open research issues and challenges," in *2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT)*. IEEE, 2022, pp. 803–810.

[170] Y. Wadhawan, C. Neuman, and A. AlMajali, "Ignore: A policy server to prevent cyber-attacks from propagating to the physical domain," *Applied Sciences*, vol. 10, no. 18, p. 6236, 2020.

[171] C. Spandonidis, F. Giannopoulos, E. Sedikos, D. Reppas, and P. Theodoropoulos, "Development of a mems-based iov system for augmenting road traffic survey," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–8, 2022.

[172] F. Busacca, C. Grasso, S. Palazzo, and G. Schembra, "A smart road side unit in a microeolic box to provide edge computing for vehicular applications," *IEEE Transactions on Green Communications and Networking*, vol. 7, no. 1, pp. 194–210, 2022.

[173] S. Wan, S. Ding, and C. Chen, "Edge computing enabled video segmentation for real-time traffic monitoring in internet of vehicles," *Pattern Recognition*, vol. 121, p. 108146, 2022.

[174] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, "Cloud-based cyber-physical intrusion detection for vehicles using deep learning," *IEEE Access*, vol. 6, pp. 3491–3508, 2017.

[175] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6g: Opening new horizons for integration of comfort, security, and intelligence," *IEEE Wireless Communications*, vol. 27, no. 5, pp. 126–132, 2020.

[176] T. Alladi, A. Agrawal, B. Gera, V. Chamola, B. Sikdar, and M. Guizani, "Deep neural networks for securing iot enabled vehicular ad-hoc networks," in *ICC 2021-IEEE International Conference on Communications*. IEEE, 2021, pp. 1–6.

[177] J. Yang, J. Hu, and T. Yu, "Federated ai-enabled in-vehicle network intrusion detection for internet of vehicles," *Electronics*, vol. 11, no. 22, p. 3658, 2022.

[178] X. Li, Z. Hu, M. Xu, Y. Wang, and J. Ma, "Transfer learning based intrusion detection scheme for internet of vehicles," *Information Sciences*, vol. 547, pp. 119–135, 2021.

[179] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE transactions on emerging topics in computational intelligence*, vol. 2, no. 1, pp. 41–50, 2018.

[180] X. Xu, J. Li, Y. Yang, and F. Shen, "Toward effective intrusion detection using log-cosh conditional variational autoencoder," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6187–6196, 2020.

[181] Z. Hu, L. Wang, L. Qi, Y. Li, and W. Yang, "A novel wireless network intrusion detection method based on adaptive synthetic sampling and an improved convolutional neural network," *IEEE Access*, vol. 8, pp. 195 741–195 751, 2020.

[182] D. Park, S. Kim, H. Kwon, D. Shin, and D. Shin, "Host-based intrusion detection model using siamese network," *IEEE Access*, vol. 9, pp. 76 614–76 623, 2021.

[183] H. Zhou, L. Kang, H. Pan, G. Wei, and Y. Feng, "An intrusion detection approach based on incremental long short-term memory," *International Journal of Information Security*, vol. 22, no. 2, pp. 433–446, 2023.

[184] J. Ashraf, A. D. Bakhshi, N. Moustafa, H. Khurshid, A. Javed, and A. Beheshti, "Novel deep learning-enabled lstm autoencoder architecture for discovering anomalous events from intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4507–4518, 2020.

[185] W. Wang, Y. Sheng, J. Wang, X. Zeng, X. Ye, Y. Huang, and M. Zhu, "Hast-ids: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection," *IEEE access*, vol. 6, pp. 1792–1806, 2017.

[186] X. Han, R. Yin, Z. Lu, B. Jiang, Y. Liu, S. Liu, C. Wang, and N. Li, "Stidm: A spatial and temporal aware intrusion detection model," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2020, pp. 370–377.

[187] E. A. Shams, A. Rizaner, and A. H. Ulusoy, "Flow-based intrusion detection system in vehicular ad hoc network using context-aware feature extraction," *Vehicular Communications*, vol. 41, p. 100585, 2023.

[188] S. A. Seshia, D. Sadigh, and S. S. Sastry, "Toward verified artificial intelligence," *Communications of the ACM*, vol. 65, no. 7, pp. 46–55, 2022.

[189] M. Krichen, A. Mihoub, M. Y. Alzahrani, W. Y. H. Adoni, and T. Nahhal, "Are formal methods applicable to machine learning and artificial intelligence?" in *2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH)*. IEEE, 2022, pp. 48–53.

XI. BIOGRAPHY SECTION

Yangyang Liu received the bachelor degree in Hunan university, Hunan, China, in 2017. He is currently pursuing the Ph.D. degree at the Hong Kong Polytechnic University since 2021. His research focuses on network measurement and the security of in-vehicle networks with papers published in top-tier venues, such as S&P, USENIX Security, NDSS, and JSAC.

Lei Xue (Member, IEEE) received the Ph.D. degree in computer science from The Hong Kong Polytechnic University. He is an Associated Professor with the School of Cyber Science and Technology, Sun Yat-sen University. He is also a member with Guangdong Provincial Key Laboratory of Information Security Technology. He is a Yat-sen Scholar. His current research topics mainly focus on mobile and IoT system security, program analysis, and automotive security.

Haiying Zhou received his B.E., M.E. and Ph.D. degrees in Electronic Engineering from Wuhan University in 1997, 1999 and 2005. He is a Full Professor at Hubei University of Automotive Technology (HUAT, China). His research interests are in the area of new technologies and smart applicants of Internet of Things (IoT), Electric Vehicle and Intelligent Drive.

Sishan Wang received his Master degree in Wuhan University, China, in 2010. He received his Bachelor degree in Hubei University of Automotive Technology, China, in 2005. He is currently a Lecture at Institute of Automotive Engineers in Hubei University of Automotive Technology. His research interests are Intra-Vehicle Networking, Automotive Ethernet, and Autonomous Vehicle Control.

Xiapu Luo (Senior Member, IEEE) is a Professor with the Department of Computing, The Hong Kong Polytechnic University. His research focuses on mobile/IoT security and privacy, blockchain/smart contracts, network/web security and privacy, software engineering, and internet measurement. He has published papers in top security/software engineering/networking conferences and journals. His research has led to more than ten best/distinguished paper awards and several awards from industry.

Kaifa Zhao is a Ph.D. candidate in the Department of Computing at The Hong Kong Polytechnic University, Hong Kong, China. His research interests span LLM4Code, AI4Security, Security4AI, and mobile security and privacy.

Pengfei Jing received his Ph.D. degree from the Department of Computing at The Hong Kong Polytechnic University (PolyU) in 2025, under the supervision of Prof. Luo Xiapu. His research interests mainly include the safety and security of modern vehicles, and cutting-edge autonomous driving systems, including end-to-end systems and vision-language-action (VLA) systems.

Xiaobo Ma (Member, IEEE) received the Ph.D. degree in control science and engineering from Xi'an Jiaotong University, Xi'an, China, in 2014. He is a Professor with the MOE Key Laboratory for Intelligent Networks and Network Security, Faculty of Electronic and Information Engineering, Xi'an Jiaotong University. He was a Post-Doctoral Research Fellow with The Hong Kong Polytechnic University in 2015. He is a Tang Scholar. His research interests include internet measurement and cyber security

Yajuan Tang received the Ph.D. degree in radio physics from Wuhan University in 2006. She is currently an Associate Professor with the Department of Electronic and Information Engineering, Shantou University. Her current research focuses on network security, network privacy, and malicious traffic analysis in networks using advanced signal processing techniques.