Received 23 May 2024; accepted 25 June 2024. Date of publication 2 July 2024;
date of current version 19 July 2024. The review of this article was coordinated by Editor Wen Liu.

Digital Object Identifier 10.1109/OJVT.2024.3422253

Deep Learning in the Fast Lane: A Survey on Advanced Intrusion Detection Systems for Intelligent Vehicle Networks

MOHAMMED ALMEHDHAR [1] **(Graduate Student Member, IEEE), ABDULLATIF ALBASEER** [1] **(Member, IEEE), MUHAMMAD ASIF KHAN** [2] **(Senior Member, IEEE), MOHAMED ABDALLAH** [1] **(Senior Member, IEEE), HAMID MENOUAR**[2] **(Senior Member, IEEE), SAIF AL-KUWARI** [1] **(Senior Member, IEEE), AND ALA AL-FUQAHA** [1] **(Senior Member, IEEE)**

[1]Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University, Doha 34110, Qatar
[2]Qatar Mobility Innovations Center, Qatar University, Doha 2713, Qatar

CORRESPONDING AUTHOR: MOHAMMED ALMEHDHAR (e-mail: moal44567@hbku.edu.qa).

This work was supported by Qatar National Research Fund (a member of Qatar Foundation) through TUBITAK-QNRF joint funding Program (Tubitak-QNRF 4th Cycle) under Grant AICC04-0812-210017.

ABSTRACT The rapid evolution of modern automobiles into intelligent and interconnected entities presents new challenges in cybersecurity, particularly in Intrusion Detection Systems (IDS) for In-Vehicle Networks (IVNs). This survey paper offers an in-depth examination of advanced machine learning (ML) and deep learning (DL) approaches employed in developing sophisticated IDS for safeguarding IVNs against potential cyber-attacks. Specifically, we focus on the Controller Area Network (CAN) protocol, which is prevalent in in-vehicle communication systems, yet exhibits inherent security vulnerabilities. We propose a novel taxonomy categorizing IDS techniques into conventional ML, DL, and hybrid models, highlighting their applicability in detecting and mitigating various cyber threats, including spoofing, eavesdropping, and denial-of-service attacks. We highlight the transition from traditional signature-based to anomaly-based detection methods, emphasizing the significant advantages of AI-driven approaches in identifying novel and sophisticated intrusions. Our systematic review covers a range of AI algorithms, including traditional ML, and advanced neural network models, such as Transformers, illustrating their effectiveness in IDS applications within IVNs. Additionally, we explore emerging technologies, such as Federated Learning (FL) and Transfer Learning, to enhance the robustness and adaptability of IDS solutions. Based on our thorough analysis, we identify key limitations in current methodologies and propose potential paths for future research, focusing on integrating real-time data analysis, cross-layer security measures, and collaborative IDS frameworks.

INDEX TERMS In-vehicle network (IVN), intrusion detection system (IDS), machine learning (ML), deep learning (DL), cybersecurity, controller area network (CAN).

I. INTRODUCTION

In recent years, modern automobiles have undergone a dramatic transformation, transitioning from simple transport mechanisms to sophisticated, intelligent, and interconnected entities known as the Internet of Vehicles (IoV). This shift has not only enhanced their features and capabilities, making them more secure, but also facilitated their integration into the larger ecosystem of the Internet of Things (IoT) [1]. Vehicles have seen marked incorporation of intricate software and numerous hardware electronic components to support this vast array of functions and components. Among these, the advent of autonomous vehicles has prompted a significant integration of Electronic Control Units (ECUs). The ECUs present in electric vehicles function through an interconnected network, employing a diverse range of communication protocols to ensure efficient operation. The aforementioned

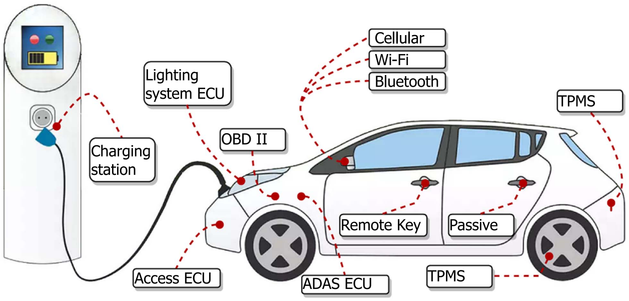


FIGURE 1. An electric vehicle.

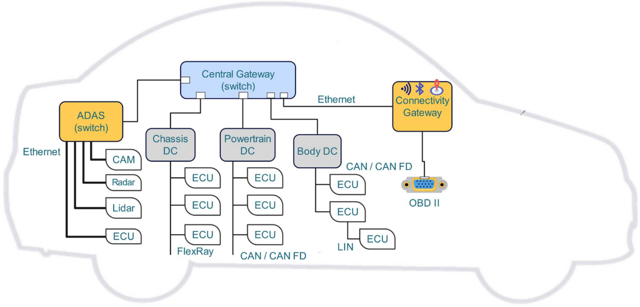


FIGURE 2. An electrical vehicle ECU's connected by IVNs.

protocols, such as CAN, Local Interconnect Network (LIN) [2], and FlexRay [3], serve the purpose of facilitating various vehicle functions by establishing effective communication channels between the various components and systems present in the vehicle. As crucial elements, these ECUs facilitate seamless data processing and internal communication within the vehicle's network and the wider Vehicle Ad-hoc Network (VANET) [1]. As vehicles transform into interconnected IoT entities, the integration of extensive connectivity features has raised the specter of increased security risks, particularly with regard to vehicle electronic controllers. Although the automotive industry has traditionally prioritized safety, the potential repercussions of compromised ECUs or manipulated communication messages - which can lead to critical failures akin to mechanical faults - have necessitated a greater focus on security. Consequently, the industry is paying increasingly more attention to security measures in parallel with safety concerns.

In addition to the various network protocols used within vehicles, including FlexRay, LIN, and MOST [4], the CAN protocol is currently the prevailing standard due to its cost-effectiveness and robustness in handling faults [5]. Moreover, implementing a general-purpose sensor/actuator bus system holds significant utility in facilitating distributed real-time control across various domains, including industrial automation and microcomputer/microcontroller-based systems. The CAN network system operates on two wires and is designed for high-speed short-message applications. The CAN architecture between the various ECUs is shown in Fig. 1. The CAN is a half-duplex system with several advantages, including its reliable performance, resilience, and widespread adoption by the semiconductor sector. In contemporary times, the emergence of car networking services, namely vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I), necessitates the deployment of computing devices to facilitate intra-vehicle communication [6], and inter-vehicle communication [7] The above-mentioned components are organized into subnets, which establish communication via gateways utilizing various protocols, constituting a densely interconnected network within the vehicle. Including a growing quantity of electronic components in modern vehicles, with 70 to 100 ECUs connected to the vehicle network (IVN), is crucial for advancing autonomous vehicles. However, this progression also presents a significantly expanded attack surface, which could compromise passenger safety. Practical traffic systems can use car communications in various ways [8], [9]. As depicted in Fig. 2, modern automobiles feature numerous interfaces that render them susceptible to cyber threats. The imminent emergence of fully autonomous vehicles will lead to a notable increase in the need to ensure the security of automobiles. The automobiles in question are required to function in a secure, reliable, and consistent manner. The occurrence of cyber-attacks on automobiles has the potential to result in catastrophic consequences, such as the unfortunate loss of human life.

The challenge of protecting vehicles from cyberattacks is considerable due to their initial design, which did not adequately account for security measures. The underlying premise of this design was based on the notion that vehicles would function autonomously, without any communication capabilities. The high level of connectivity, time sensitivity, limited resources, and complexity of IVNs make traditional proactive security measures, such as encryption methods and access control, inappropriate [10]. In addition, the inherent characteristics of messages transmitted in CAN enable potential attackers to exploit vulnerabilities within the system for malicious purposes. Additionally, the CAN lacks inherent authentication and encryption mechanisms, leaving the system vulnerable to potential security breaches. Consequently, IVNs are susceptible to numerous security risks due to the potential exposure to remote attackers [11].

Analysis of vehicle security threats can be understood by utilizing the three-layer Autonomous Vehicular Sensing Communication Control (AutoVSCC) framework [12] illustrated in Fig. 3. The sensing layer is the first layer of the hierarchical structure, constituted by vehicular sensors. This layer is vulnerable to spoofing and eavesdropping attacks on vehicle sensors, including inertial or radar sensors. Furthermore, the sensing layer encompasses potential disruptions such as jamming the Global Positioning System (GPS), intercepting communications within Tire Pressure Monitoring Systems (TPMSs), and manipulating ultrasonic sensors to detect non-existent objects. Notably, threats to the sensing layer can propagate upward to the communication layer. This transmission occurs through the physical datalink interface, converting analog data from the sensors into digital

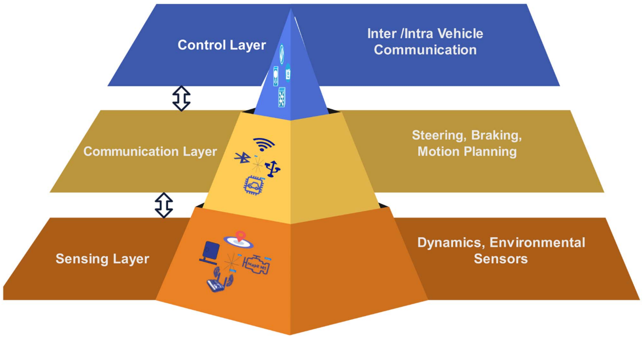

Control Layer
Inter /Intra Vehicle Communication
Communication Layer
Steering, Braking, Motion Planning
Sensing Layer
Dynamics, Environmental Sensors

FIGURE 3. Three-layer connected and automated vehicle architecture (AutoVSCC Framework).

information, subsequently employed for inter-vehicle and intra-vehicular communications. Beyond the sensing layer lies the communication layer, which includes both inter-vehicular and intra-vehicular data exchanges and is susceptible to eavesdropping, message manipulation between vehicles and roadside infrastructure, and unauthorized access to vehicle functions via infotainment and telematics systems. Possible threats at the sensing and communication layers can impact the control layer's ability to transfer and convert important digital data into real-time automotive applications like automated steering, lane change maneuvers, and brake usage through the transport-application interface.

In the literature, researchers have been working to propose different IDS approaches for IVNs. However, these approaches are evolving, primarily due to the revolution of artificial intelligence (AI) to improve the performance of IDS. Hence, conducting a literature review grounded on the latest research studies on IVN IDS is imperative and opportune. IVN IDSs aim to offer three key functionalities: (1) timely identification of abnormal intrusions; (2) provision of precise reference information for intrusion prevention systems (IPSs) [13], and (3) the ability to prevent further damage resulting from IVN attacks. Implementing an early alert system can potentially mitigate threats from malicious adversaries. IDS categorizes based on its detection strategy, including signature-based and anomaly-based detection. The limitations of signature-based IDS, such as their inability to detect new and unknown attacks and the need for regular updates to the known-attack database, have led previous researchers to focus on anomaly-based detection approaches. These approaches have gained attention due to their ability to detect novel attacks [14]. The present group of literature has categorized IDS into various subcategories, including fingerprint-based, parameter monitoring-based, information theory-based, and DL-based. Among these categories, Deep Learning (DL)-based approaches, as popular methodologies for IDS, have demonstrated promising performance. Furthermore, it is worth noting that a significant proportion of DL-based IDSs are specifically engineered to identify irregularities within the CAN bus as the most dominant communication protocol utilized in IVNs. Thus, our main focus in this paper is to summarize the DL-based IDS used to enhance CAN bus security. Table I lists the acronyms used in this survey.

TABLE 1. List of Acronyms

Acronym	Description
ADM	Anomaly Detection Model
BERT	Bidirectional Encoder Representations from Transformers
CAN	Controller Area Network
CNN	Convolution Neural Network
CRC	Cyclic Redundancy Check
CAID	Context-Aware IDS
DBN	Deep Belief Network
DIDS	Distributed IDS
DL	Deep Learning
DLS	Data Length Code
DoS	Denial of Service
DDQN	Double Deep Q-Networks
DRL	Deep Reinforcement Learning
ECU	Electronic Control Unit
EoF	End of Frame
FGSM	Fast-Gradient-Sign Method
GBDT	Gradient Boosting Decision Tree
GNB	Gaussian naive Bayes
GGNB	Gated Graph Neural Network
GPT	Generative Pre-trained Transformer
GRU	Gated Recurrent Unit
HIDS	Host-based IDS
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ITS	Intelligent Transportation System
IVN	In-Vehicle Network
KNN	k-Nearest Neighbor
LDS	Linear Discriminant Analysis
LIN	Local Interconnect Network
LSTM	Long Short Term Memory
ML	Machine Learning
MGA	Modified Genetic Algorithm
MLP	Multilayer Perceptron
MOST	Media Oriented Systems Transport
NIDS	Network based IDS
OBS	On-Board Diagnostics
RSU	Road-Side Unit
RNN	Recurrent Neural Network
RTR	Remote Transmission Request
SMOTE	Synthetic Minority Over-sampling Technique
SVM	Support Vector Machine
SoF	Start of Frame
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UDS	Unified Diagnostic Service
VANET	Vehicle Ad- hoc Network
VENTOS	Vehicular Network Open Simulator
VPN	Virtual Private Network
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
V2X	Vehicle-to-Everything
XGBoost	Extreme gradient boosting

A. RELATED WORK

This survey paper aims to provide a thorough and up-to-date examination of existing research and development efforts focused on building IDS based on ML and DL in IVN.

Our primary focus covers a range of advanced ML/DL approaches tailored to enhance cyber defense mechanisms in IVNs. These include, but are not limited to, deep

TABLE 2. Comparison of the Existing Surveys on IDSs for In-Vehicle Networks

Study	AI-Based Taxonomy	Non-ML	Traditional ML	DL	Datasets	Tools
Al-Jarrah et al [5]	✗	✗	✗	✓	✗	✓
Tomlinson et al. [15]	✗	✗	✗	✗	✓	✓
Young et al [16]	✗	✗	✗	✗	✓	✓
Dupont et al [17]	✓	✗	✗	✓	✗	✓
Siti-Farhana et al. [18]	✗	✗	✗	✗	✗	✗
Wu et al [19]	✓	✗	✗	✗	✗	✓
Aliwa at al [11]	✗	✗	✗	✗	✓	✓
karopoulos et al [20]	✓	✗	✗	✓	✗	✗
Rajapaksha et al [21]	✓	✗	✓	✓	✗	✓
Arshad et al [22]	✗	✓	✗	✗	✗	✓
Jay et al. [23]	✗	✗	✓	✓	✓	✓
This Survey	✓	✓	✓	✓	✓	✓

reinforcement learning (DRL), transfer learning, transformers, FL, generative adversarial networks (GANs), and meta-learning. In-depth illustrations for each of these techniques are provided in Sections V.

There are several surveys of IDSs for car networks in the literature. To analyze ML/DL detection methods of IoVs, Al-Jarrah et al. [5] primarily focused on in-vehicle IDSs. IDSs are divided into three types in this work: flow-based, payload-based, and hybrid. Finally, they spoke about some research roadblocks and IVN-IDS deficiencies. A thorough taxonomy focused on several vehicle kinds (aircraft, land vehicles, and watercraft) was presented by Loukas et al. Under the audit approach, statistical, ML, and rule-based IDSs were addressed. Only 13 ML-based IDSs for the CAN bus released between 2011 and 2017 were examined in this work. Authors [22] spoke about possible attacks and the CAN network's weaknesses. IDSs identified in the literature were studied regarding detection methods, deployment plans, attack strategies, and technical difficulties. A few current CAN IDSs were characterized using [17]. The study of Aliwa et al. [16] reviewed and contrasted current CAN bus IDS techniques. The authors divided in-vehicle IDSs into signature-based and anomaly-based categories, much as [19]. Anomaly detection-based IDSs were further divided into statistical, DL, rule-based, and physical fingerprinting techniques. 14 ML-based IDSs that were released between 2014 and 2020 were briefly examined in this article. However, the majority of these works (12 out of 14 ML-based IDSs) are from 2018 or before, and the most recent pieces were not included. A standardized taxonomy for IVN IDS was supplied by Karopoulos et al. [20]. They discovered 33 ML-based IVN-specific IDSs. There were no individual article summaries in this survey. Table II presents a detailed comparison.

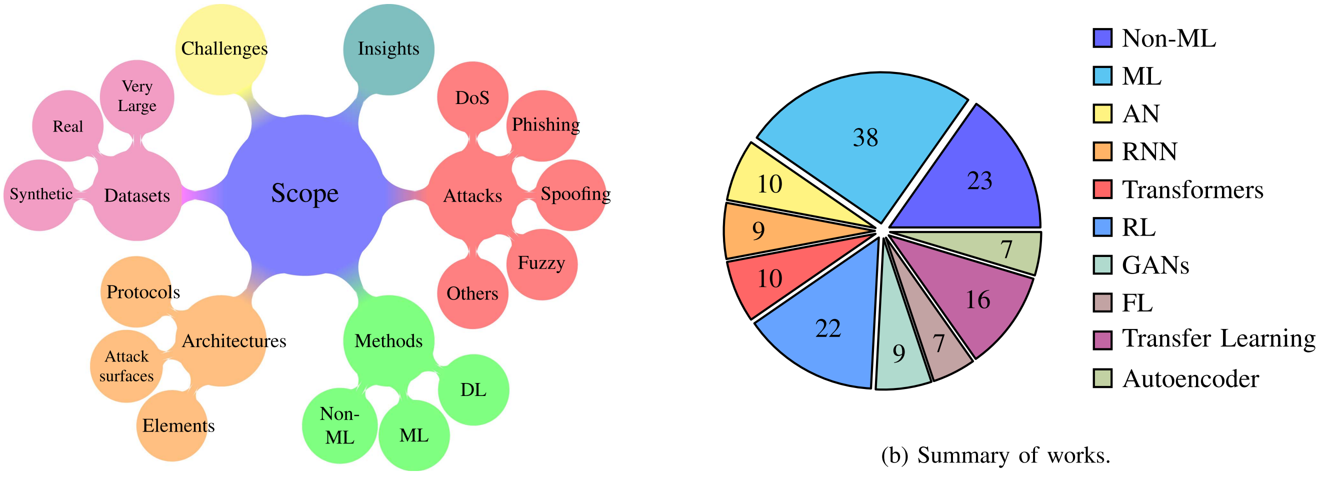
B. CONTRIBUTION

Despite the existence of several related surveys, none have adequately addressed the DRL, transfer learning, and transformers, which this survey covers. This serves as the primary driving force behind the undertaking of this investigation. The systematic literature review conducted in this survey diverges significantly from the approaches discussed in the preceding section I. This survey article provides an overview of the most recent advancements in the field, surveying and analyzing works published from 2016 to April 2024. The primary focus of this review is on the various methods employed for detection, the evaluation and benchmark datasets utilized, the different types of attacks considered, and the methods used for performance evaluation. The survey's contributions can be briefly summarized as follows:

- This survey presents a systematic literature review encompassing scholarly articles published between 2017 and 2024 and includes a novel taxonomy for IDS for IVNs. The survey emphasizes traditional ML and DL schemes, including DRL, transfer learning, and transformers. The proposed taxonomy covers multiple attack types on IVNs and CAN bus, and AI algorithms used, including detection methods, popular features, benchmark datasets, and simulation tools currently accessible for training and evaluating CAN bus systems.
- Based on a comprehensive analysis of existing literature, this survey aims to identify and critically examine the limitations inherent in current ML-based methodologies employed to ensure the security of IVNs, explicitly focusing on the CAN bus protocol.
- The paper presents a range of potential avenues for future research in IVN security.

C. ORGANIZATION

This survey paper is organized as follows: Section II presents a detailed description of IVN architectures and explains the various components of an IVN system, communication among various components, the IVN standard protocols, and security aspects such as security requirements, potential attacks, and security measures specific to IVN systems. Section III provides foundations of the current IDS for IVNs covering aspects such as data collection and analysis techniques and different types of IDSs. Section IV provides our proposed taxonomy of existing literature on IDSs for IVNs,



(a) Scope of the survey.

(b) Summary of works.

FIGURE 4. Scope of the survey paper and summary of scholarly articles on IVN-IDS covered in this survey.

emphasizing ML-based IDS schemes. The subsequent sections provide the most significant contribution of this survey paper. Section V-A surveys the recent literature on using traditional MLl schemes (e.g., support vector machines, decision trees, gradient-based methods, probabilistic models, etc.) to implement IDS in IVNs. Section V-B covers the most significant contributions to the use of DL methods (e.g., neural networks, convolution neural networks, recurrent neural networks, autoencoders, transformers, RL, generative adversarial networks, FL, transfer-learning based approaches). The paper then provides an overview of publicly available datasets used in these works and also covers simulation tools and testbeds to implement and evaluate IDS systems. Based on the literature covered in these sections, the paper then presents open issues and insights for prospective researchers in IVN security for future work. Lastly, the conclusions are drawn to summarize the survey paper. Fig. 5 shows the organization of our paper.

II. IN-VEHICLE NETWORK (IVN) ARCHITECTURE

An IVN is an interconnected system that uses communication technologies, sensors, and computational resources to create a smart and cooperative environment for vehicles on the road. Communication in an IVN happens at different levels. For example, various components within a vehicle depend on seamless collaboration with other devices and sensors to perform their designated functions. Such collaboration mandates either unidirectional or bidirectional communication channels among these entities. This inter-component communication within the vehicle is termed *internal vehicular communication* [9].

Additionally, an IVN may also connect to external entities for other purposes, e.g., diagnostics to firmware updates. As a contemporary development, there's an increasing preference for features that keep passengers connected to the internet.

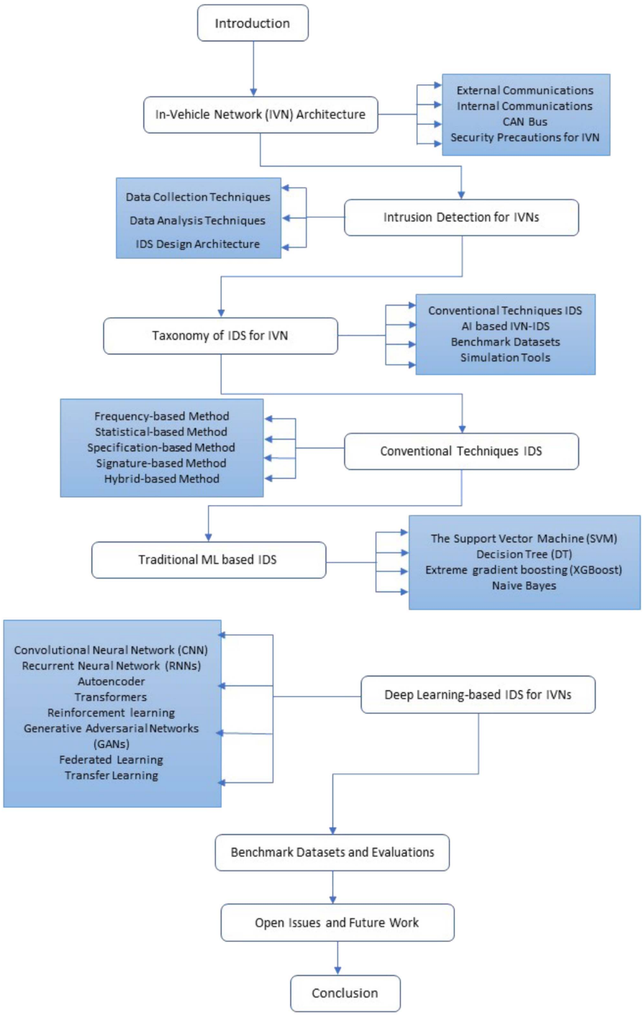

Introduction
In-Vehicle Network (IVN) Architecture
External Communications
Internal Communications
CAN Bus
Security Precautions for IVN
Data Collection Techniques
Data Analysis Techniques
IDS Design Architecture
Intrusion Detection for IVNs
Taxonomy of IDS for IVN
Conventional Techniques IDS
AI based IVN-IDS
Benchmark Datasets
Simulation Tools
Frequency-based Method
Statistical-based Method
Specification-based Method
Signature-based Method
Hybrid-based Method
Conventional Techniques IDS
Traditional ML based IDS
The Support Vector Machine (SVM)
Decision Tree (DT)
Extreme gradient boosting (XGBoost)
Naive Bayes
Convolutional Neural Network (CNN)
Recurrent Neural Network (RNNs)
Autoencoder
Transformers
Reinforcement learning
Generative Adversarial Networks (GANs)
Federated Learning
Transfer Learning
Deep Learning-based IDS for IVNs
Benchmark Datasets and Evaluations
Open Issues and Future Work
Conclusion

FIGURE 5. Paper organization structure.

This communication category, which involves external entities, is termed *external vehicular communication* [8].

In the subsequent sections, we will dive deeper into both types and discuss their intricacies and nuances.

A. EXTERNAL COMMUNICATIONS

Intelligent vehicles communicate with other vehicles on the road and infrastructure, such as traffic signals, roadside units (RSUs), etc., to improve road safety, traffic efficiency, and overall transportation effectiveness. These vehicles communicate via V2V, V2I, V2P, V2N, and V2C in V2X. According to 3GPP standards, V2X includes cellular (LTE Uu) and direct communication (LTE PC5) methods [24]. The discussion in the following expands on [25] extra-vehicle communication assault areas. (1) Cooperative connected and autonomous vehicles (CAVs) with vehicle-to-infrastructure (V2I) communication capabilities, such as smart parking systems, roadside communication units, and smart traffic signals, make infrastructure vulnerable to cyber attacks, putting these cars at risk. (2) CAVs: Hackers can also use other CAVs to send false signals to the targeted autonomous vehicle. (3) Remote Areas: Hackers can target CAVs from any conventional network connected to the vehicular network via the Internet. High-level threats include map database manipulation and deception. For example, inaccurate information from other connected CAVs or intelligent infrastructure may cause a vehicle to engage its braking system, abruptly endangering passengers. Wireless connectivity allows malicious actors to access sensitive data, such as a vehicle's location, execute fraudulent software or firmware updates on its embedded systems, and onboard sensors from a remote location. Many of these vulnerabilities are remote access vulnerabilities [26].

Manufacturers may request periodic reports to provide remote support for vehicles. Typically, these forms of communication are facilitated via Virtual Private Networks (VPNs) supplied by the manufacturer or third-party entities. Furthermore, it is imperative from the manufacturer's perspective to have diagnostic messages in place to facilitate the deployment of remote firmware updates over the air (FOTA) [27], thereby ensuring optimal post-purchase customer satisfaction. The implementation of vehicle communication technologies, namely Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructures (V2I) and VANETs [28] are promising development that guarantees a more secure driving experience. The concepts above prove the significant influence of technology on the design and driving encounters of modern automobiles. The breakdown of communication methods that affect the car is illustrated in Fig. 6.

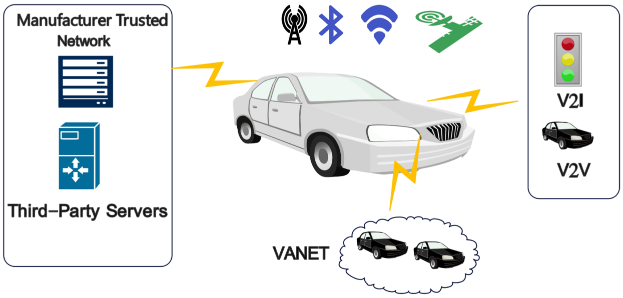


FIGURE 6. External vehicle communications.

B. INTERNAL VEHICULAR COMMUNICATIONS

Most functions in modern automobiles are operated by one or more ECUs. An ECU is a small-scale embedded computing system characterized by its ability to perform real-time computing, operate within specified time constraints, and consume low power levels. The principal duty of the ECU is to collaborate in the dissemination of sensor data via message exchange. The classification of ECUs can be categorized into five discrete groups [29]:

1) Power-train,
2) Comfort-train,
3) Safety,
4) Infotainment, and
5) Telematics.

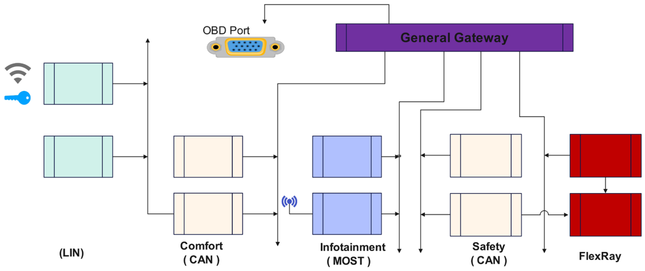


FIGURE 7. Internal vehicular communications.

The power train manages car control and navigation functions, such as brakes, gearshifts, and engine acceleration. The safety group encompasses the control of passenger safety features, for example, airbags, tire pressure, and collision avoidance. The comfort train covers thermal control, window control, and parking assistance. Infotainment includes multimedia, audio and video streaming, traffic, and weather information. Finally, telematics covers external network applications and mobile communication such as WiFi, internet, and mobile application-controlled services.

The IVN is comprised of numerous buses and ECUs that establish a network. Vehicle ECUs are interconnected through various communication technologies, including but not limited to CAN, Local LIN, FlexRay, MOST, and Ethernet. The messages are transferred and read across multiple local area network (LAN) domains within the vehicle to ensure synchronization and collaboration in managing diverse operations. Gateways, which are particular types of ECUs, facilitate the transmission of messages between different domains in cases where the sender and receiver are not connected to the same LAN [18].

The construction of an IVN is illustrated in Fig. 7. CAN is the dominant bus technology utilized in modern automobiles, providing reliable, efficient, and cost-effective means of connecting ECUs. The system enables the interconnected ECUs to engage in bidirectional communication over the bus, utilizing a single channel. Below, we introduce the main bus protocols and ports for the IVN.

1) *The local interconnect network (LIN):* [2] is a supplementary communication technology for a serial bus that functions comparable to CAN in terms of latency. This is particularly evident in scenarios where time sensitivity and high fault tolerance are critical factors [30]. The LIN protocol is classified as a linear communication protocol with a maximum data rate of 20 Kbps. However, it is important to note that this bit rate is much lower than the CAN bus and Flex Ray protocols. On the contrary, it exhibits the most economical pricing compared to other treatments. Several instances of LIN utilization may be seen, such as the application of LIN in lights, door locks, electric chairs, and other components that do not need high network performance standards in terms of latency, reliability, and bandwidth consumption [31].
2) *FlexRay:* is a communication protocol that is considered to be more sophisticated than CAN. It can provide fast data transmission, particularly useful for time-critical operations such as backbone systems, drive-by-wire, and brake-by-wire. The technology was designed to offer faster and more reliable communication than CAN. In contrast to CAN, FlexRay provides a dual-channel communication system and supports various topologies such as star and ring. It should be noted that the implementation of FlexRay incurs higher expenses [3]
3) *The On-Board Diagnostics (OBD):*OBD provides a standardized interface for accessing diagnostic data from the various ECUs within the IVN. By connecting a diagnostic tool to the OBD port, mechanics can communicate with the ECUs to retrieve live sensor data and other information related to the vehicle's operation. The initial version of OBD focused primarily on identifying electrical malfunctions. This version lacked standardized Diagnostic Trouble Codes (DTC), communication formats, and connector locations. The subsequent version, OBD-II, became a federal mandate for U.S. vehicles in 1996. In contrast to its predecessor, OBD-II continued monitoring electrical issues and extended its scope to include emission-related systems. Moreover, it introduced standardization measures across various manufacturers. OBD systems with OBD-II ports are typically located beneath a vehicle's steering column. The Unified Diagnostic Service (UDS) standard, which has replaced its predecessor, offers expanded functionalities and a wider reach to the CAN network. These include updating ECU firmware, accessing and altering ECU memory locations, and bypassing ECU input/output (I/O) operations. However, attaining such access typically requires an authentication-based process, such as challenge-response [4].

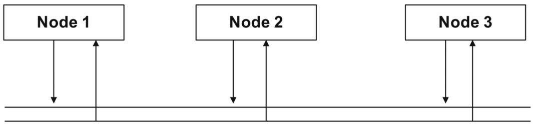


FIGURE 8. CAN bus and ECUs.

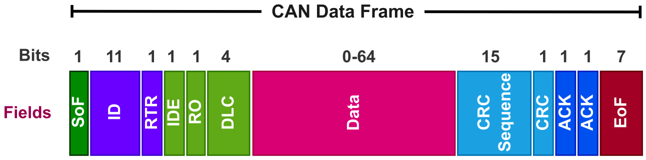


FIGURE 9. CAN data frame.

C. CAN BUS

The CAN Bus is a communication protocol used in the automotive industry to transmit data between ECUs in vehicles [32]. CAN is the most widely used serial bus system for connecting automobile devices. The connected devices are frequently called electronic control units (ECUs). Fig. 8 shows how ECU nodes are connected to a CAN bus. An electronic control unit manages an electrical subsystem in a vehicle. Most newer vehicles have an average of 100-200 ECUs. ECUs are utilized in transmission management, engine regulation, speed control, airbag activation, powertrain supervision, and many other vehicle subsystems [33]. As discussed in section II-B, the CAN bus protocol is predominant within the automotive sector due to its attributes that contribute to its popularity [7]. Hence, this section provides an in-depth understanding of CAN. The focus will remain on aspects relevant to this paper, particularly the data frames, as they are the most utilized in CAN bus communication. A CAN data frame consists of:

- The Start of Frame (SoF): A signaling bit marking the beginning of a data frame on the CAN bus.
- Arbitration field: Comprises 11 bits for identification and one Remote Transmission Request (RTR) bit.
- Identifier bits: These provide a unique ID to each message, and the RTR bit activates for a remote frame.
- Control field: Contains a 4-bit Data Length Code (DLC), which denotes the amount of data in the data field, and two reserved bits.
- Data field: Houses the message's content, accommodating between 0 to 8 bytes.
- Cyclic Redundancy Check (CRC) field: Houses the CRC for error detection during transmission.
- Ack field: Includes an Acknowledgment bit, signifying the successful receipt of a message by receivers.
- End of Frame (EoF): A sequence of 7 bits marking the end of a message.

The CAN protocol also includes extended data frames, which utilize a 29-bit identifier, unlike the standard 11-bit. As shown in Fig 9 , CAN messages lack sender or receiver fields,

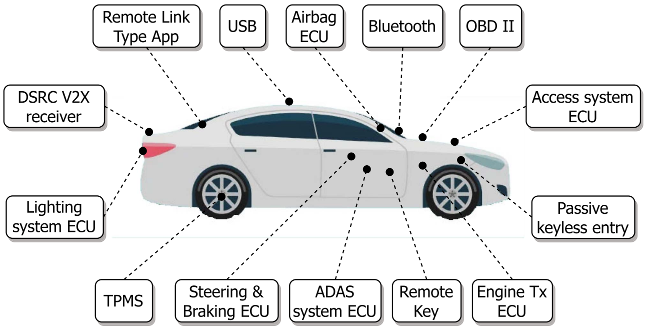


FIGURE 10. **Possible sources and surfaces of vehicular attacks.**

commonly seen in protocols such as ICMP and UDP, etc. Messages have a unique identifier (ID) representing the data type. The originator sends the message to all other ECUs in the CAN, with each ECU then deciding to process or discard the message based on its ID [33].

ID also plays a vital role in message arbitration for the CAN protocol. In scenarios where multiple ECUs transmit messages simultaneously, leading to conflicts, the arbitration rule determines which message gets bus access. A message with a lower ID has a higher priority; thus, in a simultaneous transmission scenario, the message with the smallest ID continues [34].

1) CAN SECURITY ISSUES

Upon analyzing the CAN specification by BOSCH, it is notable that there were no provisions for network security [35]. To furnish a fundamental synopsis of the complications that ensue from the nonexistence of security mechanisms, we enumerate a few conceivable attack vectors directed towards the CAN bus, highlighting the security vulnerabilities using the Confidentiality, Integrity, and Availability (CIA) triad:

1) *Confidentiality:* With all nodes broadcasting messages on the bus and receivers selecting based on message IDs, eavesdropping becomes feasible.
2) *Authenticity and Non-repudiation:* The absence of sender details can lead to message integrity threats. An attacker can send messages of their choice to any network node.
3) *Integrity:* If attackers gain control of a relay gateway, they can alter message data. Though CAN messages have CRCs for error detection, malicious nodes can still tamper with messages while adding valid checksums.
4) *Availability:* An attacker's ability to send arbitrary data can disrupt the functionality of nodes. Furthermore, control over a gateway node allows an attacker to selectively block messages.

2) ATTACKS ON THE CAN BUS

The CAN bus has been susceptible to many attacks, making the previously mentioned DoS attack more destructive in Fig 10. Basic fuzzing, where arbitrary or semi-random CAN messages are generated, can also disrupt the network, helping to map the bus and deducing potential attack vectors [36].

- Replay attacks, in which attackers read and retransmit data, are particularly difficult to detect due to their repetitive nature. An attacker can, based on previously captured messages, craft malicious CAN messages [37]. Technicians utilize diagnostic packets for tests, which can endanger road safety if exploited by an attacker. Although the automotive industry has implemented authentication safeguards against diagnostic tampering, Miller and Valasek argue these are insufficient, noting the potential of replay attacks and trivial authentication responses in some ECUs [38].
- Spoofing attacks involve attackers masquerading as genuine nodes on the CAN bus. With sufficient knowledge of ECU behavior, an attacker can impersonate authentic nodes and launch subsequent attacks, potentially jeopardizing driver safety [39], [40]. Additionally, an attacker can overwrite an ECU's firmware in Bootrom mode, rendering it inoperative or, worse, control it via malicious firmware [14].
- Data falsifying attacks manipulate the content of CAN packets. By exploiting the knowledge of arbitration IDs, attackers can deceive vehicle services, compromising driver control over critical systems like braking [10], [11], [41]. Fuzzing attacks exploit the CAN bus's lack of authentication, sending arbitrary CAN frames to ECUs, inducing unintended network responses [11], [18].
- DoS attacks disrupt ECU message transmissions, potentially leading to system unavailability and safety hazards [42]
- Fabrication attacks replace genuine ECU messages to divert or halt the operation of receiving ECUs. In a Masquerade Attack, one ECU is compromised by a high-strength attacker, and another by a low-strength attacker. [43]
- In masquerade attacks, initially, the attacker halts a particular message and sends counterfeit packets with identical transmission intervals, message formats, and payload value ranges [44]. Typically, masquerade attacks do not alter the volume of traffic within a specific time frame, making them more difficult to detect than injection attacks.
- A fuzzing attack is a method used to rapidly assess the effects of various packets on ECUs by sending messages with arbitrarily protocol headers and payload into the system. This attack differs from DoS attacks because injected packets may resemble legitimate traffic, causing the receiving node to use the information in these malicious packets in unexpected ways [45], [46].
- A suspension attack is designed to disrupt the delivery of messages from the target ECUs, affecting the operation of other ECUs that depend on this regularly updated information [47]. For example, the opponent may disrupt the may frame by utilizing a specific ID to create an error frame, such as a staff error. This action goes against

the specifications of the CAN protocol and results in the target node entering an error condition. In addition, this attack against SOME/IP enables the interception and subsequent disposal of information using a man-in-the-middle technique [48].

D. SECURITY PRECAUTIONS FOR IVN

The lack of inherent security in the CAN bus has spurred extensive research to bolster its resilience against malicious threats. These threats range from intercepting communication for unauthorized access to introducing directives that compromise vehicle safety. Scholars and professionals have proposed numerous solutions to mitigate these concerns. We delineate several key strategies adopted by researchers to fortify CAN bus security, including authentication protocols, encryption algorithms, IDS, and time-sensitive networking principles. These approaches not only affirm the legitimacy of communicating nodes and protect data confidentiality, but also thwart unauthorized interventions and ensure prompt command delivery, thus collectively fostering a more secure vehicular communication landscape [42].

1) MESSAGE ENCRYPTION AND SIGNING

To address confidentiality lapses in message transmission, end-to-end encryption is pivotal. Given the constrained processing capabilities of nodes, there is a need for lightweight cryptographic solutions to prevent latency that could obstruct bus communication. Their integrity is protected by integrating cryptographic signatures in messages. Furthermore, encryption improves security by preserving communication confidentiality [49]. Wolf et al. emphasized the importance of ensuring authentication, integrity, and privacy. This can be realized using public-private key cryptography for authentication, complemented by symmetric key cryptography and firewalls for integrity and confidentiality. Concurrently, comprehensive security modules have been designed to defend both hardware and software using cryptography [28].

2) NODE AUTHENTICATION

A node's authenticity can be ascertained using certificates and public key encryption, as mentioned in [35]. However, this is not the only method. Authenticity can also be discerned by monitoring any deviations in the transmitting ECU's message frequency. Integrating node authentication, encryption, and signing can substantially reduce security breach odds on the bus. In particular, [50] found that if an attacker breaches an ECU fortified with security protocols, they can access all its memory data, including encryption keys. The work in [51] further revealed that perpetrators can disable these safeguards by initiating a firmware flash. Nilsson et.al proposed replacing the CRC fields in CAN messages with a Message Authentication Code (MAC), ensuring solutions comply with vehicular system resource constraints [52]. It is essential to remember that conventional cryptographic methods often require large allocations of resources.

3) FIREWALLS AND POLICY ENFORCEMENT

Messages encapsulate details about content, identity, and timing. Network security can be reinforced by incorporating hardware elements, such as firewalls, or by embedding these functions into the software. This is facilitated by initiating policies that specify the allowed message types and their transmission times [18]

4) HONEYPOT

Honeypots, prevalent in standard computing ecosystems, emulate genuine system behaviors [53]. They offer a safe platform for analyzing attacker patterns by segregating actual system resources. The inception of honeypots in IVNs is a burgeoning research area, as shown in [54].

Reactive models, as discussed, pinpoint and counteract real-time attacks. Their core goal is discerning typical from malicious behaviors. As in [54], this goal becomes achievable by crafting rules that define the expected behavior of the system, while deviations from these rules are flagged as malicious.

III. INTRUSION DETECTION FOR IVNS

IDS has attracted attention due to its efficiency in monitoring network or host activities and detecting unexpected occurrences or intrusions [55]. These intrusions, internal or external, aim to gain unauthorized access. While internal intrusions are initiated by individuals with valid access privileges, external intrusions seek unauthorized access from outside the network. Depending on its configuration, an IDS can be passive, merely detecting an attack, or active, taking preventative measures. A typical IDS comprises sensors, a detection engine, and a reporting module [56].

A. DATA COLLECTION TECHNIQUES

IDS classification depends on the nature of the collected data. There are two primary IDS types: Network-based (NIDS) and Host-based (HIDS). NIDS monitors network traffic, typically on traffic routing devices, while HIDS operates on a host machine, examining the behavior of the host system [56]. Other subcategories include [57]:

1) *Stack-based:* Monitoring data transfer across protocol stack layers.
2) *Protocol-based:* Observing protocols used by the host system.
3) *Graph-based:* Analyzing relationships among nodes or hosts.

With advances in technology, especially the rise of IoT, IDSs have increasingly incorporated ML and DL techniques, as explained in depth in Sections V.

B. DATA ANALYSIS TECHNIQUES

There are three primary techniques for data analysis for intrusion detection; (i) anomaly-based, (ii) signature-based, and

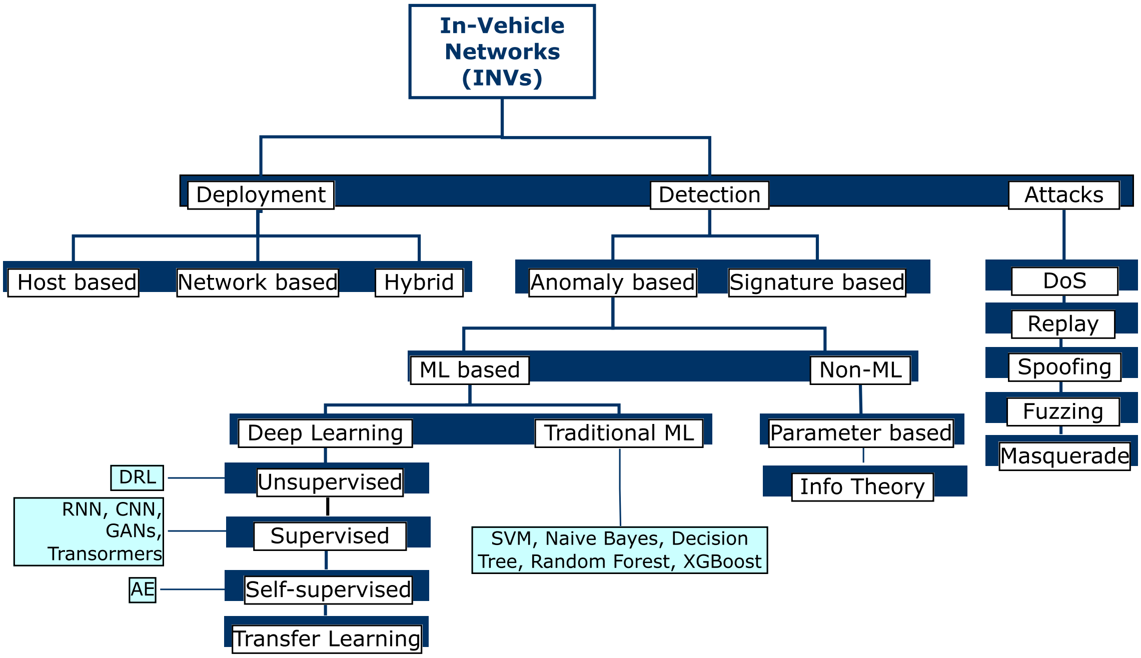


FIGURE 11. Intrusion detection system classification (TBA).

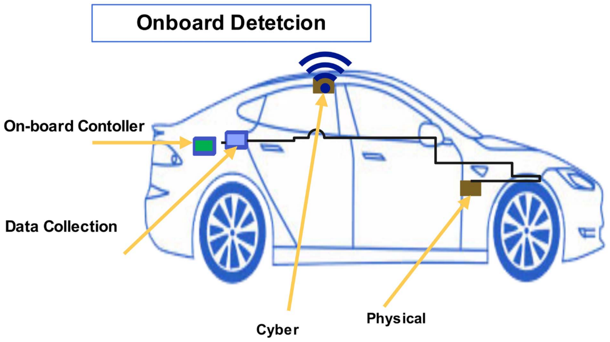


FIGURE 12. Insight into the Intrusion Detection System (IDS) Architectural Components for Autonomous Connected Vehicles.

(iii) specification-based. Anomaly detection focuses on identifying deviations using statistical techniques [58]. Signature-based detection examines messages for known patterns. Messages are filtered using allow and block lists, presenting challenges for open systems with diverse content [59]. Specification-based detection relies on properties derived from protocol design to detect anomalies [58].

C. IDS DESIGN ARCHITECTURE

While there's no universally accepted IDS structure, we provide an overview of the prevalent and effective architectures.

1) *Onboard Self-detection* A vehicle self-detects threats using its onboard data collection, aggregation, and reasoning capabilities, as illustrated in Fig. 12 [60]. With onboard detection, the vehicle is bound by its computational power and sensor range, possibly affecting performance and energy consumption [60].
2) textitCollaborative Detection This involves vehicles operating in tandem, such as in truck platoons or UAV swarms. Here, vehicles can act as network nodes, performing detection tasks collectively or for neighboring nodes, as depicted in Fig. 13 [61], [62], [63]. However, the trustworthiness of network nodes is a challenge [64].
3) *Remote Detection* This approach offloads detection to a remote service, suitable when onboard detection isn't mandatory, and collaboration isn't feasible [65].

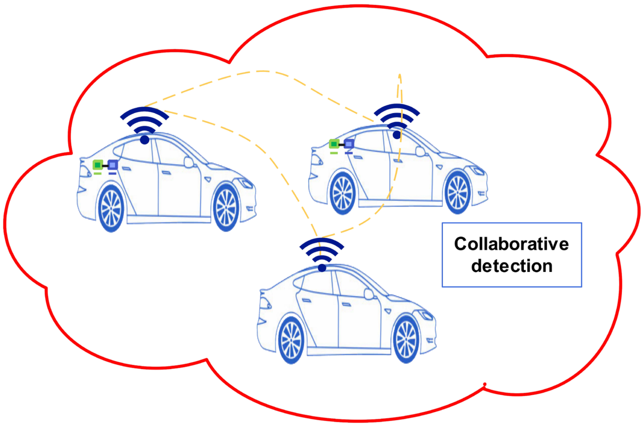


FIGURE 13. The conceptual framework for collaborative detection is a crucial aspect of the field.

D. SUMMARY AND DISCUSSION

The integration of IoVs and their associated communication technologies introduces security concerns in the realm of vehicle safety. Therefore, much research has focused on building smart car IDS. Many of these approaches identify IVN IDS, abnormalities, and attacks. Since CAN is a frequent IVN, researchers presented many detection techniques. However, several detection approaches target external vehicle network IDS, anomalies, and attacks. Of course, hybrid vehicle identification systems consider IVN and external networks. The IVN detection approaches in this research utilized AI-based IDS.

IV. TAXONOMY OF IDS FOR IVN

Automobile systems, due to their diverse nature, exhibit different susceptibilities to various attacks. This requires different methodologies, classifications, and attributes to pinpoint and counteract these threats. Fig. 11 presents the taxonomy of legacy and modern IDS techniques. A key differentiator of vehicular IDS is its placement: onboard or external to the vehicle. When a vehicle's computing system cannot accommodate an efficient onboard IDS or lacks cooperative vehicular systems, the IDS can be run externally. This could involve a human operator's computer system managing the car from a distance, or offloading the IDS operation to a remote cloud infrastructure [65].

A. CONVENTIONAL NON-ML TECHNIQUES

The effectiveness of automotive IDS largely depends on its detection mechanism. The detection methods can be classified into anomaly-based, signature-based, specification-based, and hybrid-based, detailed as follows:

1) *Frequency-based Method* Relies on the predictability of the CAN packet identifiers' frequency. However, its effectiveness is limited in noisy environments or with periodic CAN packets [66], [67].
2) *Statistical-based Method* Involves comparing a current statistical observation to a previous one, examining the CAN ID fields, and considering the high interdependence of automotive parameters [68].
3) *Specification-based Method* Uses manually defined rules and thresholds to identify threats when network behavior deviates from established standards [69].
4) *Signature-based Method* Relies on a database of known attack patterns. It's easy to construct but needs constant updates. Its effectiveness is limited by the comprehensiveness of its database [70].
5) *Hybrid-based Method* Also known as distributed IDS (DIDS), it combines various intrusion detection methods, enabling better detection coverage [71], [72].

Conventional methods for IDS use hard-coded features and are typically robust to detect previously known attacks but underperform on detecting new attacks with varying attack patterns. In recent years, there has been a significant surge in the development of IDS software using artificial intelligence algorithms techniques. In the following, we discuss the research efforts in applying AI methods for intrusion detection in IVNs.

V. ARTIFICIAL INTELLIGENCE BASED IVN-IDS

Several studies [73], [74], [75], [76] show the increasing use of AI algorithms in intrusion detection reporting remarkable proficiency in detecting and identifying intrusions. This section introduces a taxonomy of several ML/DL solutions. Traditional machine learning (ML) methods are the most fundamental approach adopted in many preliminary and recent studies. These methods often employ supervised learning models such as support vector machines (SVMs), tree-based models, gradient boosting, and probabilistic classifiers such as Naive Bayes.

A. TRADITIONAL ML BASED IDS

IDS empowered by traditional ML techniques promise superior classification between typical traffic patterns and malicious activities. Such systems use predictive modeling for efficient detection and mitigation of potential attacks. The significance of having an effective method for extracting and preprocessing raw CAN data cannot be adequately emphasized, especially considering the reluctance of vehicle manufacturers to share exhaustive specifications or offer instructions for decoding raw data attributes. Despite their resilience, supervised ML algorithms introduce temporal limitations due to the requirement to annotate unprocessed CAN data, detect attacks based on CAN, and subsequently categorize and annotate the data. In contrast, unsupervised ML paradigms eliminate the need for labeled datasets, enabling algorithms to independently identify and analyze recurring patterns within the data. Subsequently, these patterns can be used for traffic classification and the detection of abnormal behavior, thus enhancing the efficiency of the overall IDS procedure [16]. The concepts of ML are shown for better comprehension, as seen in Fig. 14. In the following, we elucidate and summarize the primary traditional ML techniques employed for IDS within IVN in Table III.

1) THE SUPPORT VECTOR MACHINE (SVM)

The SVM method forms decision boundaries using kernels to handle high-dimensional data effectively, making it popular for IDS applications [77]. It excels in generalization and finds a global minimum-risk solution. SVM's independence from empirical risk measures enables it to choose optimal parameters, offering computational efficiency crucial for real-time intrusion detection [78]. SVMs can dynamically update the training of IDS patterns when encountering a new pattern during the classification process [79], [80].

Al-Saud et al. [81] proposed an OCSVM-based ADM that utilized ID frequencies as features. The researchers employed the social spider optimization algorithm to determine the optimal parameters for support vector regression. The proposed model was evaluated using a genuine vehicle dataset subjected to a DoS attack. The Anomaly Detection Model (ADM) proposed by Avatefipour et al. [82] is based on an improved statistics analysis and a One-Class SVM (OCSVM) to detect anomalies. The authors used the modified bat algorithm as the algorithm for parameter optimization. To evaluate the model, the researchers utilized CANbus data obtained from an unaltered vehicle and two additional publicly available CAN bus datasets [83]. In a separate study [81], an OCSVM-based

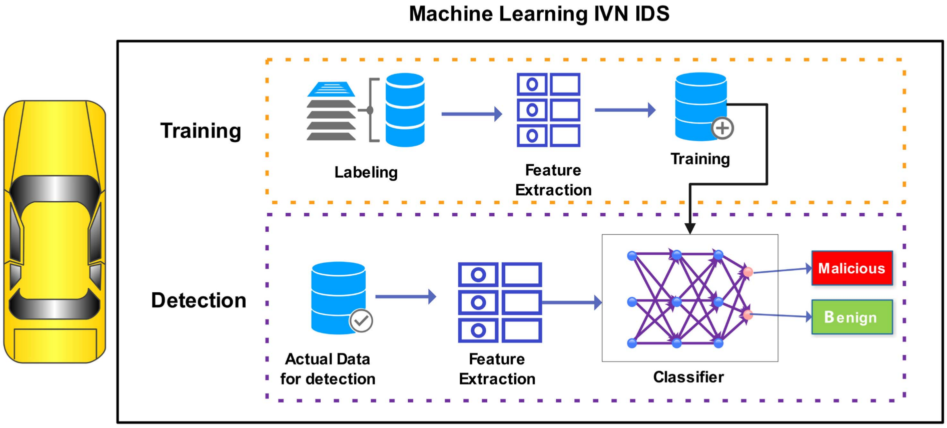


FIGURE 14. Machine learning method in IVN IDS.

TABLE 3. Outline of INV-IDS Using Traditional ML Algorithms

Technique	Key Features	Datasets Used	Performance	Pros	Cons	References
LR	Statistical model, Outputs probability	CAN intrusion dataset, National Research Council Canada, CAR-Hacking	High accuracy	Good for imbalanced data, Fast	Requires feature engineering	[101], [103], [111]
SVM	High-dimensional data handling, Decision boundaries	Genuine vehicle dataset, Real datasets from an EV	Promising results	Computational efficiency, Handles high-dimensional data	Limited real-world testing	[79], [80], [81], [82], [98], [107], [112]
DT	Hierarchical classification, Minimal computational requirements	Alsvin CHANA, CAN-hacking, HCRL-car hacking, UNSW-NB15, CIC-IDS2017	High yield, Over 90% accuracy	Easy to interpret, Low computational cost	May overfit	[57], [84], [85], [86], [87], [88], [92], [104]
XGBoost	Classification and Regression, High computational efficiency	'Car Hacking: Attack and Defence Challenge', CAN bus datasets	Accuracy exceeding 99%	High accuracy, Resistant to overfitting	Computationally intensive	[86], [89], [90], [91], [92], [105]
Naïve Bayes	Probability-based classifier, Effective for various attack types	OTIDS, Huge CAN dataset by Kalkan and Sahingoz	Near 100% accuracy	Fast, Good with imbalanced datasets	Assumes feature independence	[80], [93], [94], [95], [96], [97], [100], [106], [107], [108], [110], [113]

ADM utilized ID frequencies as features. The social spider optimization method identified optimal settings for support vector regression. This model was assessed using data from a car exposed to a DoS attack. A shared limitation between both models was their lack of testing against varied real-world attack scenarios, despite their promising results. The presented model is evaluated using the real datasets collected from an EV.

2) DECISION TREE (DT)

The Decision Tree is a hierarchical model employed to classify inputs utilizing a sequence of decision-making procedures that rely on the input data [84]. The DT is a composite structure consisting of two primary components: the decision points and the terminal points, called the leaves. One of the primary advantages associated with the utilization of DT in IDS is their ability to perform classification tasks with minimal computational requirements. Additionally, DT possesses the capability to identify and classify significant network attributes that can effectively discern malicious activities. Consequently, decision trees have been employed as IDS in the context of the IoV [85], [86].

The work in [57] introduced an IDS using DT and Multilayer Perceptron (MLP) techniques to differentiate between DoS and Fuzzy attacks. The effectiveness of the system was evaluated using real-time data from a Hyundai YF Sonata. The authors in [87] showed that the tree-based and ensemble learning models exhibit superior detection performance compared to other models. The Can-hacking dataset was used to train and evaluate the Random Forest, Bagging, and AdaBoosting techniques. The DT-based model demonstrates high performance. In their study, the authors [88] devised an

IDS that utilizes a Gradient Boosting Decision Tree (GBDT) for the CAN-Bus. They also introduced a feature creation method for GBDT, using entropy as the basis for feature generation. To assess the effectiveness of their model, they used a dataset obtained from a genuine domestic automobile, namely the Alsvin CHANA.

3) EXTREME GRADIENT BOOSTING (XGBOOST)

XGBoost is an ML algorithm that has recently gained significant popularity. XGBoost is a highly efficient implementation of the gradient boosting ML algorithm, which utilizes stochastic gradient or tree boosting techniques to create a robust ML approach that demonstrates strong performance across various complex problem domains [89].

XGBoost, a robust and highly efficient model, has demonstrated significant efficacy in the domain of IDS. One of the notable advantages of XGBoost is its ability to effectively handle both classification and regression tasks, making it well suited for detecting various intrusions using diverse data types. XGBoost employs the concept of gradient boosting, a technique that aggregates numerous weak prediction models, often in the form of DTs, to construct a robust predictive model. The strong robustness that XGBoost exhibits reduces the risk of overfitting, improving the model's ability to generalize well to new and unexplored data. Additionally, XGBoost is widely acclaimed for its high computational efficiency [90]. Therefore, the aforementioned characteristics establish XGBoost as a highly efficient model for IDSs [91].

This study [92] investigates the application of the extreme gradient boosting machine (XGBoost) for IDS on the CAN bus. Given the vulnerability of the CAN bus to remote attacks, monitoring mechanisms are crucial. Authors employ XGBoost to classify unexpected events within the CAN data payload, using ten-fold cross-validation to improve predictions. Overfitting is addressed through early-stopping and grid search techniques. The evaluation, based on authentic CAN bus datasets from various vehicles covering different attack scenarios, reveals an accuracy rate exceeding 99%. The primary dataset is the car-hacking dataset, while the secondary is the survival analysis dataset.

4) NAIVE BAYES

The Naïve Bayes method is a probability-based classifier, as discussed in [93]. The core principle of the Naive Bayes algorithm is to compute the posterior probability from the prior, and then categorize the data point based on this probability. It has been applied in various fields such as pattern recognition [94], spam classification [95], and IDS [96]. The utilization of an NN model for density ratio estimation was implemented by Tanaka et al. Authors in [96] proposed an algorithm for IDS, known as the graph-based Gaussian naive Bayes (GGNB) algorithm, which utilizes graph properties and incorporates PageRank-related features. The application of the Gated Graph Neural Network (GGNB) on the real raw CAN dataset. Nair et al. [97] integrated ML and blockchain technology to create an IDS for CAN. This system uses blockchain to store CAN and RSU data securely and immutably in a decentralized manner, offloading data storage from vehicles and RSUs. The system's IDS uses the Gaussian naive Bayes algorithm to analyze CAN traffic properties, classifying communication windows as normal or abnormal. The system was evaluated against three attack types: (1) DoS, (2) fuzzing, and (3) impersonation. The authors have employed a CAN dataset (OTIDS) to train and test the model.

Current ML research on IDS shows a clear trend toward hybrid methods. Many studies combine techniques to increase IDS robustness and efficiency. By blending strategies, researchers aim to improve anomaly detection accuracy and lower false positives, highlighting the evolving nature of cyber threats and the need for adaptable defenses.

The authors [98] introduce ML-based IDS that employs the SVM, DT, and KNN algorithms to identify and categorize cyber-attacks on vehicle communication networks. Tested on numerous real-world vehicular datasets. The paper underscores the surge in cybersecurity incidents within contemporary vehicles, emphasizing the pressing need for fortified communication protocols and sophisticated intrusion detection systems. Authors in [99] thoroughly compare several ML algorithms applied to IDS in CAN bus. It uses a variety of ML models, including GaussianNB, k-KNN, DT, RF, LSTM, and CNN, to evaluate their efficacy against different types of cyberattacks on vehicles. The study utilizes the real ORNL Automotive Dynamometer (ROAD) dataset, which includes various types of attacks such as Fuzzing, Targeted ID, and Masquerade attacks. In their recent study, Heng Sun et al. [100] introduced the CCID-CAN, an IDS for CAN bus in autonomous vehicles. This model combines a rule-based Valid Bit index (VBIN) with ML techniques like a Kalman filter and a Naïve Bayes classifier to enhance detection speed and accuracy. Additionally, it incorporates a cross-chain mechanism for secure log sharing among non-trusting vehicles, improving system robustness. Tested on XPeng vehicle data, CCID-CAN outperformed existing models in detection efficiency and accuracy.

The study [101], introduces an IDS using ML techniques and ensemble classifiers for heightened effectiveness. The research employed eight ML algorithms, including Logistic Regression (LR), RF, DT, and XGBOSST, to detect both typical and abnormal behaviors in CAN traffic datasets. Results suggest that ensemble classifiers, such as voting, stacking, and bagging, outperform individual models, achieving higher accuracy rates in assault detection. The dataset used for this study is the Car Hacking: Attack and Defense Challenge 2020 dataset [102]. The paper [103] introduces an IDS utilizing AI algorithms for detecting known attacks on IVN. The authors explored various IDS techniques, including LR, feed-forward neural networks, RF, SVC, and LSTM. An evaluation was conducted using a merged dataset, combining normal messages from the National Research Council Canada and attack messages from the CAR-Hacking dataset. The IDS inspects the CAN's messages, timestamps, and data packets to pinpoint potential cyberattacks. The study emphasizes the importance of time series features in improving attack detection.

In recent study [92], the authors introduced an advanced methodology for IDS in IVN, emphasizing vulnerabilities in the widely adopted CAN bus due to limited security features. The framework utilizes a modified genetic algorithm (MGA) to select feature subsets from the dataset optimally. They then employ five classifiers, including DT, SVM, LR, k-nearest neighbors (KN), and linear discriminant analysis (LDA), to design a robust IDS. This analysis utilized HCRL-car hacking, UNSW-NB15, and CIC-IDS2017 datasets.

In [104], the authors fused a two-stage IDS rule-based system with ML techniques such as DT, RF, and XGBoost. The IDS aims to identify and counteract malicious attacks quickly and accuratly. The efficacy of the hybrid model is showcased through its performance on the CAN intrusion dataset. The study further delves into various attack types on the CAN bus, underscoring the imperative for a robust IDS to combat them. This approach holds promise for bolstering automotive system security, utilizing the "Car-Hacking Dataset" for evaluation.

The study [105] investigates IDS in Intelligent Transport Systems (ITS), highlighting the vulnerability of autonomous cars, especially through the CAN bus. Current IDS algorithms for CAN are computationally intensive and may not fit low-end ECUs in vehicles. This research introduces a detection model using ML methods like XGBoost, RF, LightGBM, Naive Bayes, and DT. Using the publicly available "Car Hacking: Attack and Defence Challenge" dataset, more details about the dataset are provided in VI-A-9. The authors Han et al. [86] have presented a method for detecting anomalies and identifying attacks in IVNs. Statistical features were computed for event-triggered intervals corresponding to each CAN identifier. The ML models, namely XGBoost, DT, and RF were trained using computed feature values to detect attacks. The datasets used were extracted from driving data from real vehicles. The experimental outcomes, which employed two authentic datasets featuring practical attacks, demonstrated a notable capacity for detecting anomalies and attacks.

In another study, the attack detection performance of six alternative ML models—RF, bagging, ADA boosting, NB, LR, and NN—was compared using Kalkan and Sahingoz's [106] huge CAN dataset. The authors used simple ML algorithms (LR, ANN, Naive Bayes, Adaptive Boosting, Bagging Tree, RF) with default settings to get a decent detection rate. However, they did not discuss how the dataset was produced or what attributes were used to train the algorithms. Similarly, Alfardus and Rawat [107] also employed ML algorithms to identify threats to the CAN bus, including KNN, RF, SVM, and Multilayer Perceptron (MLP). Moulahi et al. [80] compared detection capabilities using RF, DT, SVM, and MLP. Time, ID, DLC, and payload features were used. The HCRL OTIDS dataset performance study revealed inferior detection capacity for fuzzy assaults. In the HCRL CH dataset, Amato et al. [108] used models based on NN and MLP to identify attacks. In their study, Authors [109] developed an IDS for IVN. This system integrates CNN and Bidirectional Bi-LSTM with a multi-attention mechanism, enhancing anomaly detection. CNN layers extract spatial features from network traffic, while BiLSTM layers analyze temporal sequences, improving the system's accuracy in identifying malicious activities. The effectiveness of this model was validated using the Car-Hacking dataset, demonstrating superior performance in detecting various attack scenarios compared to traditional methods.

The paper [110] introduces an IDS to identify anomalies and attacks on CAVs using LSTM and Naïve Bayes. Using the LSTM model for the CAN bus, a protocol with limited inherent security, IDS monitors CAN activities to spot unusual behaviors from potential attacks. The LSTM is trained on attack-free data to predict upcoming CAN messages. Prediction errors are then analyzed using a Gaussian Naïve Bayes classifier to determine message categories: normal or attack. The IDS outperforms existing classifiers, achieving near 100% accuracy and F-score in detecting attacks, as validated in the Car Hacking and Survival Analysis Datasets.

The aforementioned traditional ML methods offer protection against new attack types and do not rely on hard-coded signatures or other attack patterns. Instead, they rely on certain features in the historical data to learn and identify new attacks. A known limitation of the traditional ML techniques is the use of hand-crafted features, derived from the actual raw data of the network traffic. Such manual feature engineering limits the information that is fed to the model. Additionally, the traditional ML models have also limitations in learning complex representations from high-dimensional data. Most recent studies focus on the use of DL techniques. DL methods can alleviate the laborious task of feature selection and the need to obtain sensitive information, as they can automatically extract and select features from raw data. From a resource perspective, training the DL-based methods may require substantial computational investment. However, recent advancements in the field of DL have enabled the development of DL classifiers to be relatively compact and computationally efficient.

B. DEEP LEARNING-BASED IDS FOR IVNS

DL has garnered considerable attention and has been extensively employed in various domains to enhance the efficacy of previous methodologies [114]. DL-based methods have the potential to achieve superior performance using only raw traffic input and minimal resource requirements, making them an optimal choice for IoV implementation [115].The concepts of DL are shown for better comprehension, as seen in Fig. 15. Fig. 16 depicts the operational structure of the DL process in the IDS. The process begins by supplying training data to the DL model of the IDS. The data may be subjected to various preparation procedures, such as standardization and sanitization, to guarantee its appropriateness for training purposes.

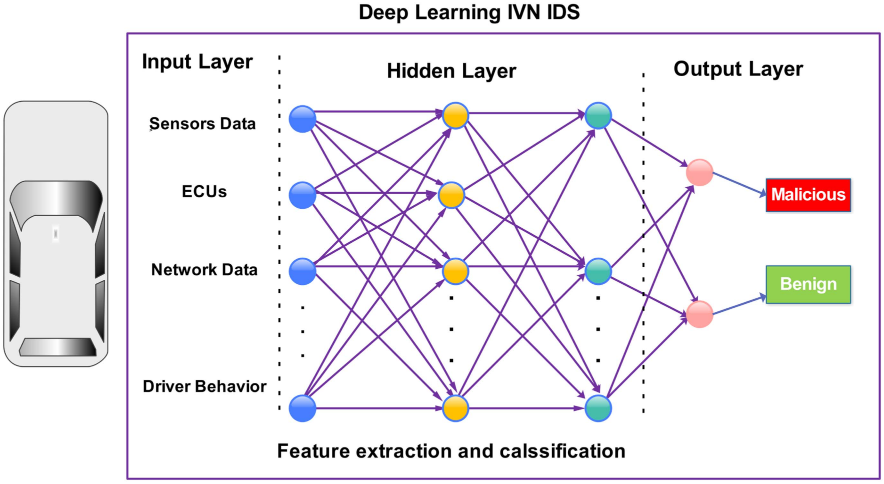


FIGURE 15. Deep learning method in IVN IDS .

After completing this preparation, the model undergoes training using the revised data. After the training phase, the model undergoes testing to assess its performance. If the model satisfies the preset performance requirements, the IDS switches to running mode; otherwise, it undergoes retraining. While monitoring, the IDS actively evaluates incoming automotive network data using its anomaly detection algorithm. An alarm is triggered when traffic is recognized as anomalous, but the IDS continues to monitor non-anomalous traffic in Table IV.

1) CONVOLUTIONAL NEURAL NETWORKS (CNNS)

CNNs have gained significant attention in computer vision due to their ability to capture spatial correlation among features [116]. This phenomenon can be attributed to using filters, which are shared weights among neurons. The CNN model possesses advantageous characteristics such as sparse connectivity, standard weights, and pooling layers, making them well-suited for extracting location-invariant features. Consequently, it has been extensively employed within computer vision for image classification. The most prevalent features of network traffic are those that remain consistent across different locations, but change over time. As mentioned above, the functionality can effectively categorize network traffic by converting traffic into visual representations through traffic images and sequences of traffic flows. Hence, CNN models open potential avenues for advancing a precise IDS. Several researchers have employed this methodology, showcasing its significant potential to improve IDS outcomes. Tan et al. [117] employed a time series analysis approach to detect DoS attacks. The detection method involved using a dissimilarity metric known as earth-movers distance. The authors proposed utilizing temporal characteristics derived from network traffic to represent its intrusive nature. Similarly, Ariu et al. [118] have devised a proficient IDS that utilizes a hidden Markov model to account for the temporal association among network traffic payloads. In their study, Wang et al. [119] used CNN to extract distinct network traffic features from the Malviya traffic data set. The study focuses on the design and implementation of IDS to protect the system [120], [121].

Song et al. [120] introduced an IDS that utilizes the Inception-ResNet CNN architecture. The IDS extracts the CAN ID characteristics from each CAN message, converting them into a 29-bit binary representation. These binary representations are then arranged in a 29x29 grid format and used as input for the CNN model. The authors train and test the model using datasets including four distinct attack types and all conceivable combinations of these assaults. In addition, an autoencoder is used to effectively minimize the dimensionality of the data, hence mitigating the complexity of the model.

Baldini [122] employed a bag-of-words methodology to identify intrusions in IVNs. The sequential pattern of CAN data can be utilized to identify atypical behavior. Song et al. [123] introduced a Deep CNN (DCNN) based IDS that utilizes a specific property to safeguard the CAN bus against cyber threats. During the period of injection attack, a sequential pattern of ID alterations occurs due to frequent frame injection. The aforementioned authors leveraged this alteration to identify instances of message injection attacks. The DCNN model utilized for the study was Inception-ResNet, with an input size of 29 × 29 × 1 and a binary output. The proposed solution was evaluated using the HCRL CH dataset. The results indicate that the DCNN model exhibited better performance than the baseline models in all types of attacks. Desta et al. [124] employed a CNN-based IDS trained on recurrence plots. The deployment results on NVIDIA's Jetson TX2 indicate a detection latency of 117 ms, which is relatively high.

2) RECURRENT NEURAL NETWORK (RNNS)

RNNs are developed to process sequential data effectively. In contrast to conventional feed-forward NNs, RNNs exhibit a distinctive memory mechanism that enables them to retain state information throughout different time steps. This characteristic makes them highly suitable for tasks that involve time series data or sequences. The process of memory formation is supported by establishing interconnected cycles within

TABLE 4. **Deep Learning Approaches for IDS in IVNs**

Category	**Ref**	**Method**	**Attack Types**					**Attack Source [* is dataset]**	**Platform**	**Metrics**	**Best Accuracy Results**
			DoS	Fuzzy	Spoof	Replay	Other				
AFFNN/MLP	[133]	DBN	✗	✗	✓	✗	✗	Synthetic	Simulation	Acc	0.98
	[134]	GDM	✗	✗	✓	✗	✗	Simulated	Real vehicle	Veracity rate	0.98
	[135]	IL	✗	✗	✗	✗	✗	Simulated	car-hacking	**Acc**,Pr,Re,F1	0.99
	[137]	GA	✗	✗	✓	✗	✗	Simulated	Renault Zoe EV	Acc,PPV,TPR	Varies (0.9-1.0)
Autoencoders	[159]	AE	✗	✗	✗	✗	✗	OTIDS dataset	KIA Soul vehicle	AUC,AUPR	0.91,0.86
	[160]	LSTM-AE	✗	✗	✓	✗	✓	DCASE dataset	-	Acc	0.87
CNNs	[120]	CNN	✓	✓	✓	✗	✗	Simulated	Real vehicle	Acc,Rec,Prec	0.98-0.99
	[124]	ResNet	✓	✓	✓	✗	✗	Car-hacking*	Jeep Cherokee	Acc	0.99
	[242]	ResNet	✓	✓	✓	✗	✓	Car-hacking*	Simulation	FNR	-
RNN/LSTM/GRU	[141]	LSTM	✗	✗	✓	✗	✗	Simulated	Ford Transit	Acc	0.97
	[142]	Bi-LSTM	✓	✓	✓	✗	✗	UNSWNB*,car-hacking*	Simulation	Acc	0.99
	[143]	LSTM	✗	✓	✗	✓	✓	Synthetic	Real-vehicle	Acc	0.90
	[156]	LSTM	✓	✓	✗	✓	✓	Synthetic	Giulia Veloce	Pr,Rec,F1	>0.94
	[161]	GRU	✗	✗	✗	✓	✓	-	-	**Acc**,FPR	>0.8
	[150]	GRU+MLP	✗	✗	✗	✓	✓	KDD19*,NSL-KDD*	Simulation	Pr,FPR	0.99,.05
	[243]	LSTM-FCN	✓	✗	✗	✗	✓	KDD99*,NSL-KDD*	Simulation	**Acc**	1.0
	[244]	BiGRU	✗	✗	✗	✓	✓	UNSW-NB15*,NSL-KDD*,CIC-IDS2017*	Simulation	**Acc**,Pr,Re,F1	>0.99
	[151]	Bi-LSTM	✗	✗	✗	✓	✓	Car-hacking*, Defense Challenge-2020	Simulation	**Acc**,Pr,Re,F1	>0.99
Transformers	[171]	GPT	✗	✗	✓	✓	✓	Simulated	Hyundai Avante	TPR	0.98
	[174]	BERT	✓	✓	✓	✗	✓	Simulated	-	Acc	1.0
	[175]	BERT	✗	✓	✗	✗	✓	IVN-IDS*	multiple cars	F1	0.99
	[172]	TAN	✓	✓	✓	✗	✗	car-hacking*, IVN-IDS*,survival*	-	Pr,Rec,**F1**	>0.99
	[173]	LSTM	✓	✓	✓	✗	✗	Car-hacking	Real vehicle	**Pr**,Rec	>0.99
	[177]	MPMHit	✓	✓	✓	✗	✗	Car-hacking	Real vehicle	**Pr**,Rec,Acc,F1	>0.99
	[178]	DNN	✓	✓	✓	✗	✗	survival analysis data	Real vehicle	**Pr**,Rec,Acc,F1	>0.99
RL/DRL	[200]	Q-learning	✗	✗	✗	✗	✗	NSL-KDD*	Simulation	Acc	0.98
	[192]	AE-RL	✗	✗	✗	✗	✗	NSL-KDD*,AWID*	Simulated	Acc,F1	0.8, 0.79
	[199]	DDQN	✗	✗	✗	✗	✗	NSL-KDD*,AWID*	Simulated	**Acc**,Pr,Rec,F1	0.95
	[194]	SARSA-DRL	✗	✗	✗	✗	✗	NSL-KDD*,UNSW-NB15*	Simulated	Acc,Pr,Rec,F1	-
	[201]	AE-DQN	✓	✗	✗	✗	✓	NSL-KDD*	Simulated	Acc,F1	0.8,0.7
	[202]	DQN	✓	✗	✗	✗	✓	NSL-KDD*, CICIDS2017*	Simulated	Acc,Pr,Re,F1	-
	[203]	DQL	✓	✗	✗	✗	✓	NSL-KDD*	Simulated	**Acc**,Pr,Re,F1	0.94
	[204]	DRL	✓	✗	✗	✗	✗	Synthetic	Simulation	Acc	0.91
	[205]	RL	✓	✗	✗	✗	✗	Synthetic	Simulation	Acc	-
	[207]	RL	✓	✗	✗	✗	✗	Simulated	FastNetMon	Acc	0.98
	[208]	RL	✓	✗	✗	✗	✓	Simulation	Matlab	Pr,Re,F1	-
	[210]	DRL	✗	✗	✗	✗	✓	Simulated	SUMO	-	-
	[211]	DQN	✗	✗	✗	✗	✗	Simulated	NS2+SUMO	Re	0.99
	[212]	NDRL	✗	✗	✗	✗	✗	Simulation	Matlab	Acc	-
	[214]	DQN	✗	✗	✗	✗	✗	NSL-KDD	Simulation	**Acc**,Pr,Re,F1	0.80
	[215]	DDQN	✗	✗	✗	✗	✗	CIC-DDoS2019*	Simulation	Acc	0.98
	[216]	CN+POMDP	✗	✗	✗	✗	✗	Simulation	Simulation	Acc,Pr,Re,F1	-
GAN	[244]	GAN	✓	✓	✓	✗	✓	Car-hacking*	Sonata	Precision, **Acc**	0.98
	[224]	ACGAN	✓	✓	✓	✗	✗	Synthethic	-	**Acc**,Pr,Re,F1	>0.99
	[225]	ACGAN	✓	✓	✓	✗	✗	Car-hacking*	Simulation	**Acc**,Pr,Re,F1	>0.99
	[228]	CAAE	✓	✓	✓	✗	✓	Simulated	Real car	Pr,Re,**F1**	>0.99
	[226]	DNN-GAN	✗	✗	✗	✗	✓	Car-hacking*	Simulation	Acc	0.99
	[230]	GAN	✓	✓	✓	✓	✓	CSynthetic	Simulation	**Acc**,Pr,Re,F1	0.999
FL	[236]	ConvLSTM	✓	✗	✓	✓	✓	OTIDS*	Simulation	**Acc**,Pr,Re,F1	0.91
	[237]	GRU	✓	✗	✓	✓	✓	Car-hacking Attack&Defense*	-	**Acc**,Pr,Re,F1	> 0.99
	[238]	CNN,XGBoost,MLP,AE	✓	✓	✓	✗	✓	NAIST CAN attack*	Real vehicles	Acc	> 0.99
	[240]	-	✗	✓	✗	✓	✗	Dataset*	Real vehicles	Pr,Re,**F1**,ER,FAR	> 0.90
	[241]	RF	✓	✓	✗	✗	✓	OTIDS*	Simulation	**Acc**,Pr,Re,F1	0.98

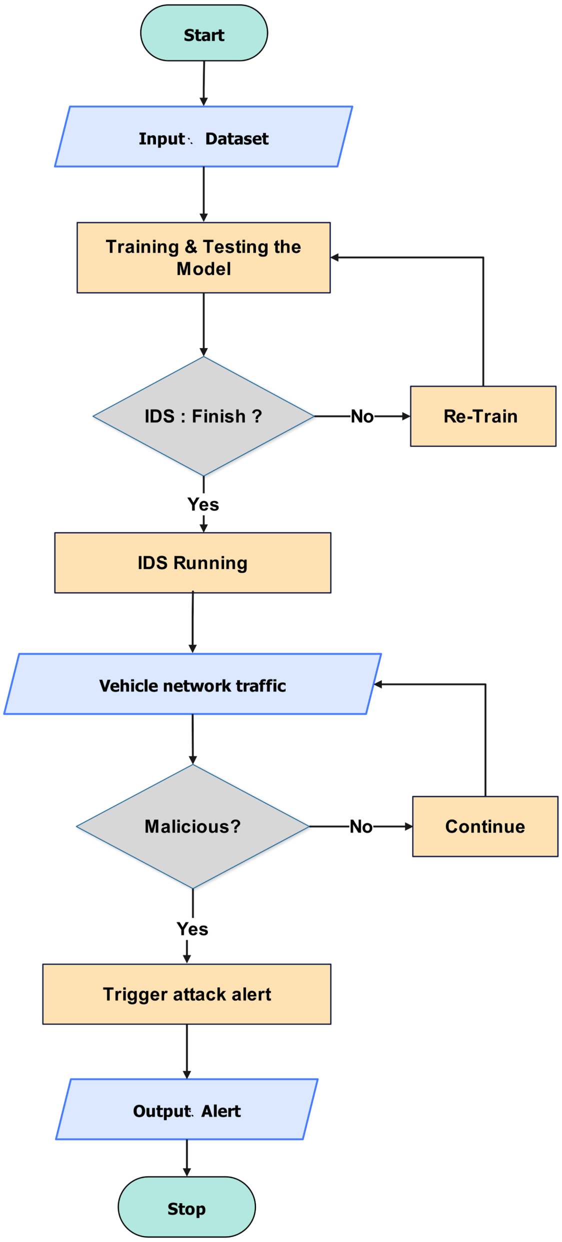


FIGURE 16. Operational flowchart for deep learning in intrusion detection systems.

the network, allowing the transmission of information in a manner that resembles the temporal dynamics of sequential patterns [125], [126].

RNNs comprise a range of models, including, but not limited to, Simple RNNs, Long Short-Term Memory networks (LSTMs), and Gated Recurrent Units (GRUs). Each variant possesses distinct architectural characteristics intended to improve the network's capacity to learn from and predict sequential data. In particular, LSTMs and GRUs incorporate advanced mechanisms to capture long-term dependencies within data [127].

Using RNNs within IDS is a powerful and effective approach in vehicular networks. Using RNNs is advantageous in vehicular systems due to the inherent sequential nature of network traffic data. By training RNNs, it becomes possible to discern regular patterns of network behavior and subsequently detect anomalies that deviate from these patterns. Such anomalies may serve as indicators of potential intrusions or attacks. The intrinsic temporal characteristics of vehicular network traffic render RNNs suitable for IDS. This selection allows these models to offer resilient and immediate detection capabilities, thus improving the overall security of vehicular networks [107].

a) Long short-term memory (LSTM): The LSTM model uses an internal memory with input and output and forget gates to manage data flow. The cell state stores past data, while the gates control what new information enters or leaves. The forget gate selectively removes old information based on input and previous hidden state. The input gate decides what new information to include, and the output gate determines what part of the updated cell state should be outputted. However, RNNs cannot effectively capture long-term dependencies between consecutive tasks, which can be attributed to the issue of vanishing gradient descent. The LSTM model is expected to capture and model long-term dependencies effectively. The main objective of LSTM is to address the issue of vanishing gradient descent, an optimization algorithm used to determine the weights of artificial neural networks, to mitigate long-term dependency problems, making LSTM an excellent candidate for IDS [128], [129].

b) Gated recurrent unit (GRU): The GRU is a simplified version of the LSTM with fewer gates, combining the forget and input gates functions into one "update gate." It also merges the hidden and cell states for a leaner architecture. Multilayer GRUs feature GRU cells in each hidden layer of an RNN, making them more computationally efficient and suitable for resource-constrained environments such as automotive ECUs. Despite being newer and less studied, GRUs show considerable promise compared to traditional RNNs and LSTMs [130], [131].

GRU recurrent RNNs use fewer parameters than LSTM networks, making them computationally efficient. GRU trains the dataset faster, executes faster, and uses less memory than LSTM. GRU is more efficient than LSTM in IDS for these reasons [132]. Kang and Kang [133] introduced a deep NN (DNN) based IDS designed for IVNs. The CAN payload was employed as the basis for feature generation, while mode and value information were utilized to reduce dimensionality. A distinct Deep Belief Network acquired the DNN model's initial weights. The authors employed a template-matching methodology to contrast the training sample and CAN packet to detect attack scenarios.Another study by Zhang et.al [134] proposed an IDS for the CAN bus that utilizes DNNs. Data is collected by directly connecting the CAN adapter to the CAN bus. KvaserCAN Leaf Light V2 is the data collection device for the CAN bus. However, discerning these values is unfeasible without the DBC file or familiarity with the CAN payload.

Lin et al. [135] proposed the utilization of DNN and incremental learning to develop an IDS tailored to the dynamic nature of driving environments and behavioral patterns. The labels for online model updates were derived from the predicted class labels of the DNN model. Boumiza et al. [136] proposed IDS to secure automotive networks using DNNs with Rectified Linear Units (ReLU) activation functions. This system is designed to detect vulnerabilities in the CAN. The DNN model employs ReLU to avoid saturation and promote better gradient flow, enhancing its learning capabilities. The dataset used in this work utilizes data collected from a 2012 Subaru Impreza through the OBD-II port. The authors Fenzl et al. [137] proposed a continuous field classification algorithm to detect the alignments of payload values. Subsequently, a DL methodology was employed to detect the atypical fields. The model's performance was evaluated using datasets from the Renault Zoe EV and manipulated signals.

Loukas et al. [74], proposed a cloud-centric cyber-physical IDS for autos that uses a mix of physical and digital quality. LSTM deep MLP and RNN architecture were the algorithms used in the research. Inspired by studies done by Cho and Shin [138] and Choi et al. [139], Xun et al. [140] presented VehicleEIDS, an inventive IDS that makes use of a vehicle's voltage signal. The used model uses the various voltage signals that ECUs emit. The authors used 14 time-domain characteristics to extract the data from the two cars. The deep support vector domain description (deep SVDD) model created the EV IDS. The detection of malicious message injections on the CAN bus was performed by Jedh et al. Jedh [141] conducted a study on identifying malicious message injections in the CAN bus. The authors utilized message sequence graphs of CAN identifiers at consecutive temporal intervals to calculate Pearson and Cosine similarities. These similarities were then employed as the characteristics of the LSTM model. The model performance was evaluated by utilizing real dataset of vehicles, which was enhanced by incorporating artificially generated messages related to RPM (revolutions per minute) and speed. Khan et al. [142] proposed a hybrid IDS for IoVs that detects internal and external attacks. A bloom filter and DNN bidirectional LSTM architecture identify zero-day attacks. The proposed IDS was evaluated utilizing CAN-based car hacking and UNSWNB-15 external vehicular network statistics. Zhu et al. [143] proposed an approach for IDS using a multidimensional LSTM framework to predict the next can message based on the received real-time message. This approach was developed to address the computational constraints of IVNs. Another IDS for IVN applications was proposed by Gao et al. [144]. This IDS leverages DL and a set of experience knowledge structures (SOEKS). Empirical findings from the analysis of a real vehicle dataset demonstrated that the utilization of SOEKS and information entropy yielded a notable enhancement in detecting attacks. To detect modifications in IVNs, Wasicek et al. [145] designed a CAID (context-aware IDS) framework utilizing ANN. Three components comprise CAID: the monitor module reads and compiles data, the detector module spots irregularities, and the reporter module establishes a connection with the user. Vehicle speed, engine RPM, fuel rate, and predicted load are features utilized in ANN models. This model was assessed using an actual vehicle for chip tuning and power boxing modifications. The authors in [145] proposed an ANN-based lightweight model. This model barely outperformed the baseline models. Tariq et al. [146] proposed a framework to detect CAN bus attacks that incorporates rule-based and DL (specifically, LSTM) models. The proposed model was evaluated using DoS, fuzzing, and replay attack techniques. The collective model exhibited superior accuracy compared to the individual rule-based or LSTM model for all types of attacks.

The anomaly detection capabilities of LSTM and One-Class SVM (OCSVM) were evaluated by Chockalingam et al. [138] in detecting anomalies in CAN frames. The researchers utilized an authentic dataset and generated erroneous packets by implementing fuzzing and misplaced non-anomalous packets. The optimization process of the non-linear kernel was time-consuming. The LSTM model exhibited superior performance compared to the OCSVM. Tomlinson et al. [147] employed a one-class compound classifier to detect attacks within the IVN. The analysis encompassed the payload values of three distinct CAN identification numbers. The researchers used fuzzing techniques to evaluate the efficacy of the classifier. The authors proposed ensemble detection techniques to address the challenges of relying on a single classifier to identify CAN IDs. Kang and Shen [148] proposed an IDS that utilizes an LSTM network. This IDS is capable to effectively identify both familiar and unfamiliar anomalous messages. The model is provided with CAN Identifier (CAN-ID) and the data field of CAN messages. Synthetic frames are generated using a GAN to train the LSTM network. Cheng et al. [149] present MKF-ADS, an IDS framework for IVN that employs a self-supervised learning approach. This model integrates a multi-knowledge fusion strategy combining spatial-temporal correlation with an attention mechanism, specifically using Conv1D and Bi-LSTM for feature extraction from CAN data. Tested across various simulated and real attack scenarios, the MKF-ADS demonstrates robust predictive capabilities with an impressive F1-score of 97.3%, confirming its effectiveness in anomaly detection. Xu et al. [150] also employed an MLP and a GRU to implement an IDS, which achieved a high detection rate of up to 99.5% detection rate and a false positive up to 0.05% on the KDD99 dataset. Anew work by Kishore et al. [151] proposed IDS for CAN bus using a Bidirectional LSTM (B_LSTM) model. This model utilizes bidirectional processing to enhance abnormality detection by analyzing data sequences forward and backward, thereby capturing intricate patterns and dependencies that may indicate intrusions. The system is trained and tested on the Car-Hacking: Attack and Defense Challenge-2020 dataset.

3) AUTOENCODER

Autoencoder is a form of unsupervised learning applied to raw traffic communications to acquire effective coding. This eliminates the need for expert labeling of these messages, which was necessary in previous supervised learning methods. Autoencoders have a high level of proficiency in several tasks, including dimensionality reduction, noise reduction, and anomaly identification [152]. These activities hold significant importance within the context of IDS. Autoencoder models have been widely employed in various fields due to their versatility. These disciplines include image denoising, image super-resolution, feature extraction [153], text generation, machine translation [154], as well as IDS [155].

In [156], the author introduced an IDS known as CANnolo. This IDS utilizes LSTM Autoencoders to detect abnormalities inside the CAN protocol effectively. During the training phase, CANnolo performs an automated analysis of the CAN streams and constructs a model representing the authorized data sequences. The presented framework generates a temporal succession of CAN payload data for individual CAN identifiers, adapting network hyperparameters to reduce the Mahalanobis distance between the reproduced sequence and the initial sequence. More significant discrepancies in reconstruction will be identified as probable anomalies. The model is assessed using gathered CAN frames obtained during vehicle operation under various environmental conditions, encompassing urban and highway settings. a NIDS framework outlined in [157] employs the LSTM autoencoder technique to address security breaches arising at the primary gateways of vehicular systems. This approach performs binary classification on arriving data flow, leveraging statistical metrics such as the mean and standard deviation computed over message sequences within defined time intervals. These features are then converted using normalized likelihood sequences before input into the network. The efficacy of this method was evaluated using both the UNSW-NB15 dataset, which pertains to external network communications, and the car hacking dataset, which focuses on in-vehicle communications. In their study, Kristianto et al. [158] introduce an IDS for IVN, leveraging automotive Ethernet. This IDS employs RNNs and Autoencoders (AEs) for unsupervised learning, optimizing its performance within the computational constraints of IVNs. The system notably reduces parameter counts, which decreases memory usage, training time, and energy consumption while maintaining accuracy comparable to traditional methods. The effectiveness of this lightweight IDS was validated using simulated attacks on the Car-Hacking dataset, highlighting its suitability for resource-constrained automotive environments.

The study empirically evaluated CANnolo using a publicly accessible dataset derived from real-world sources. The Attention Mechanism and Autoencoder for IDS (AMAEID) approach was presented by Wei et al. [159]. This method integrates a denoising autoencoder and attention mechanism. The hexadecimal CAN payload underwent conversion into binary format during the data preprocessing phase. Subsequently, Gaussian distribution-based noise was added, enhancing the model's robustness and generalizability. A single layer connected NN was used to derive the final prediction, indicating whether the message is normal or abnormal. The authors validated their methodology using the OTIDS dataset, demonstrating its superior performance. However, the evaluation was based solely on conventional ML techniques such as DT, KNN, and SVM. Furthermore, more comparative analysis with other literature utilizing autoencoder methods needs to be performed, which could provide additional insights into the results.

In their study, Oleksandr et al. [160] introduced an unsupervised approach for identifying anomalies in time series data. They used LSTM-based autoencoders to develop a model capable of accurately identifying the precise location of anomalies. The evaluation was performed using two distinct sets of data: fake signal datasets of diverse nature and a dataset designed explicitly for detecting unusual sound occurrences. The IDS in the CAN bus was proposed by Kukkala et al. [161] through recurrent autoencoder-based GRUs. The SynCAN dataset was designated the assessment dataset, and distinct autoencoder models were trained for each identification number. Anomalous signal values were identified using signal-level intrusion scores that compared predicted and actual signal values. The authors presented an effective DL-based IDS methodology employing the deep denoising autoencoder. This approach aims to capture latent sequential patterns inherent in CAN data. Additionally, an evolutionary-based optimization method is integrated to fine-tune the model parameters to enhance the effectiveness and accuracy of the IDS against adversary intrusions. The efficacy of this approach is evaluated using three datasets, including data collected from an unmodified licensed vehicle and two widely recognized anomaly detection datasets relevant to the CAN bus domain.

4) TRANSFORMERS

Transformers is a newly emerging powerful DL architecture [162] that has demonstrated exceptional proficiency in various language-related tasks, such as text classification, machine translation, and question and answer [163]. One notable distinction between transformer and RNN is the use of a self-attention mechanism, which employs attention matrices rather than recurrent connections [164], [165]. The models that have gained significant popularity in the field include Bidirectional Encoder Representations from Transformers (BERT) [166], Generative Pre-trained Transformer (GPT) v1-3 [167], [168], Robustly Optimized BERT Pre-training [169], and Text-to-Text Transfer Transformers [170]. The flexibility of transformer-based models has rendered them highly appealing for implementation in ML-based NIDSs. Nam et al. [171] used the GPT model to acquire knowledge of the regular pattern of a standard CAN ID sequence by treating it as a sentence composed of words. Anomalies in typical patterns were recognized as assaults. The researchers employed a bidirectional approach to merge two GPT networks. In [172], the authors proposed multi-class IDS for IVN CAN buses using a transformers-based attention network (TAN). The proposed TAN model removes RNNs and classifies attacks into multiple categories. It can also detect replay attacks by aggregating sequential CAN IDs. Experimental results show that the TAN model is more efficient than baselines for different input data types and datasets. The model can identify intrusion messages without requiring message labeling. The authors [173] presented an attention-based model for identifying breaches in IoV, explicitly focusing on detecting attacks on the CAN. This study utilizes the CAN attacks dataset for experimentation and evaluation. The attention-based approach devised by the authors draws inspiration from the widely used transformers architecture in the field of NLP. The work in [174] introduced CANBERT, a linguistic-based IDS model explicitly designed for CAN. The CANBERT system utilized transformers, particularly Bidirectional Encoder Representations from BERT, to identify and analyze malicious attacks targeting the CAN network. The authors used a dataset known as CAN, which encompasses both normal and malicious data derived from diverse attack scenarios, including DoS, fuzzing, and impersonation attacks.

Alkhatib et al. [175] proposed a CAN-BERT approach to detect cyber attacks on the CAN bus protocol. The authors applied the BERT model to learn the sequence of arbitration IDs in the CAN bus for anomaly detection. The authors used "Car Hacking: Attack & Defense Challenge 2020" dataset [102]. Xu emei Li and Huirong Fu [176] developed the CAN-SecureBERT and CAN-LLAMA2 models to improve CAN-based IDS. They created models for CAN IDS and attack categorization by modifying pre-trained transformer-based models, specifically BERT, SecureBERT, and LLAMA2. The models CAN-C-BERT, CAN-SecureBERT, and CAN-LLAMA2 are presented and evaluated against the most advanced models currently available. Nevertheless, the research is limited by constraints on computational resources. The authors utilized the CarHacking Dataset to assess the implemented models. In their work, Jinhui et al. [177] presented an IDS based on a self-supervised learning model for IVN called IVNSL. Employing the Message Prediction Model based on Hierarchical Transformers (MPMHit), this approach captures spatial and temporal message dependencies without labeled data. Designed to address concept drift through an online update mechanism supported by vehicle-cloud collaboration, the model was validated using the Car-Hacking dataset, demonstrating enhanced detection accuracy compared to traditional methods.

Cobilean et al. [178] developed the CAN-Former IDS, a transformer-based NN that enhances IDS in vehicular communications through the CAN bus. Advantage the transformer architecture for sequence-to-sequence predictions, this model processes CAN IDs and message payloads efficiently. It operates under a self-supervised training mode. The model's effectiveness was validated on a dataset from three vehicles, demonstrating its ability to detect anomalies by comparing predicted and actual communication sequences.

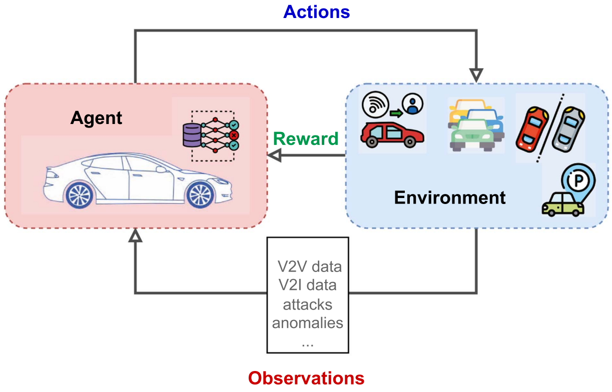


FIGURE 17. Deep Reinforcement Learning (DRL) for IVNs.

5) REINFORCEMENT LEARNING

In contrast to supervised ML, RL employs an intelligent agent to make decisions that optimize rewards to accomplish a specific objective [179]. RL exhibits similarities to the concept of dynamic programming. Furthermore, in contrast to supervised and unsupervised learning, RL employs distinct policies to facilitate the learning process. Fig. 17 depicts the conceptual framework of RL.

The primary goal is to acquire knowledge of a policy that enables an agent to make optimal decisions within a specified environment. An agent utilizes a reward-based learning approach to generate data and endeavors to optimize positive rewards through iterative interactions with an environment. The environment can be conceptualized as a Markov decision process, where determining rewards and probabilities of state transitions is contingent upon observations and the subsequent selection of actions.The primary objective of RL is to identify and select actions that optimize the accumulation of future rewards. An RL agent can improve its capabilities through iterative learning processes [180].

In recent years, a proliferation of RL-based IDS techniques has been proposed to offer autonomous cyber defense solutions in diverse contexts and for various application scenarios, including IoT [181], Wireless Networks [182], and Cloud [183]. The RL agent can incorporate self-learning capabilities throughout its learning process by relying solely on observations without supervision. This stands in contrast to traditional approaches that often rely on expert knowledge provided by humans [184]. Numerous NIDS techniques have been suggested, drawing on the concept of RL [185]. However, most current methodologies are plagued by the challenge of accurately identifying legitimate network traffic and need to improve their ability to handle large datasets. This is because an RL agent often faces the challenge of handling extensive learning states, which can lead to the state explosion problem.

a) Q-learning: Q-learning [186] is an RL algorithm that enables the agent to acquire the optimal policy through state transitions. Q-learning involves the iterative measurement and storage of estimated rewards in a tabular format for each state and potential action within that state. Q-learning utilizes the Bellman equation as a constraint to optimize the cumulative rewards [180]. The primary objective is to optimize the anticipated cumulative rewards by implementing a policy for action selection. In practical applications, Q-learning involves creating a lookup table to store a comprehensive set of actions and their corresponding expected rewards. This requires a more significant amount of memory and can occasionally result in inefficiency when a consecutive sequence of operations is applied to the data. As the cardinality of the set of states and actions increases, the cardinality of the table will correspondingly increase, posing challenges in storage and maintenance. The Deep Q-Network (DQN) concept was first introduced in [187], [188] to reduce space complexity. DQN refers to a hybrid approach that integrates conventional Q-learning with Deep Neural Networks (DNN). The input to the DQN consists of a state representing.

b) Deep reinforcement learning (DRL): DRL combines DL into a solution that assists the agent in RL in making the best possible choice from unstructured input and addresses the issue of manual state space engineering in RL. The key benefit of using DL in RL is due to the DNN's scalability in high-dimensional space. For example, the value function approximation uses DNN's data representation to express the highly compositional data distribution via end-to-end gradient-based optimization [189]. DRL algorithms are helpful in various applications, including IDS, video games, robotics, transportation, NLP, healthcare, computer vision, and finance [190]. They can also perform well for large-scale datasets. DRL policy is quick and straightforward and ideal for changing situations. It may be modified to stream data for quick reactions. It performs better than the other model in finding anomalies in high volume datasets, which is challenging for alternative unsupervised tasks [191].

In the past few years, there has been a growing interest in cyber-security research regarding the utilization of applied RL. This approach has been widely adopted in various security-related domains, including IDS [192], [193], [194], attack detection [195], and signal and authentication of devices [196], [197], [198]. This section provides an in-depth discussion of the RL techniques employed in recent studies within cyber-security.

In [192], a DRL algorithm called adversarial environment RL (AE-RL) was introduced for IDS. This algorithm utilizes Double Deep Q-Networks (DDQN) to achieve efficient inference and precise online training, particularly in class imbalance. The authors extended the AE-RL framework and introduced AESMOTE. This competitive DRL algorithm incorporates the Synthetic Minority Over-sampling Technique (SMOTE) to address the class imbalance issue. This approach was presented in [193]. In the current study, the authors successfully enhanced IDS accuracy. However, this improvement came at the expense of significantly longer training times. The authors in [199] have introduced a DDQN agent for IDS that relies on anomaly detection. The researchers compared DDQN and DQN and Policy Gradient and Actor-Critic frameworks. In [194], the authors introduced an anomalous NIDS that utilizes the Deep SARSA framework. This system aims to enhance the accuracy of attack detection in environments with a significant imbalance. In this study, the DRL agent assumes the role of an attack detector, in which distinct actions are assigned to various attacks or regular behavior. The authors conducted a comparative analysis between their proposed method and the current state-of-the-art approach. Their findings demonstrated the efficacy of Deep Sarsa in addressing classification problems characterized by significant class imbalance.

In their study, Sengupta et al. [200] introduced an approach that modifies the Q-learning algorithm to acquire optimal threshold values for a different characteristic of network traffic. The model exhibits a notable accuracy rate of 98% and demonstrates improved efficiency in processing real-time predictions. Furthermore, only a few studies have utilized RL-based IDS in distributed network environments. The application of RL for IDS in a network was carried out by Suwannalai et al. [201] introduced the Adversarial / Multi-Agent RL using DQN (AE-DQN) approach as a solution to network IDS challenges. Similarly, Sethi et al. [202] introduced an RL-based IDS that leverages Deep Q-Network in multiple distributed agents and incorporates an attention mechanism to classify network behaviors. In their study, Alavizadeh et al. [203] employed a collaborative approach that integrated Q-learning-based RL with a deep feed-forward neural network methodology. This approach aimed to mitigate the occurrence of malicious behaviors within network traffic.

Liu et al. [204] incorporated RL techniques to effectively address DDoS attacks in software-defined networking (SDN). By leveraging the state information of a switch, such as the count of received packets and the port number, the algorithm can mitigate the prevalence of attack traffic within the network by dynamically adjusting the network bandwidth of switches that exhibit abnormal behavior. Simpson et al. [205] introduced a method for detecting DDoS attacks using RL. This approach enables the system to make optimal decisions in the presence of various network topologies. The researchers devised a reward function based on evaluating legitimate traffic reception rates, upstream and downstream loads, and combined loads. This function effectively enhances the throughput of legitimate TCP traffic. This method requires legitimate traffic as the labeled data to train its model. Feng et al. [206] introduced a technique to detect DDoS attacks in the application layer. Their approach uses a DRL algorithm to acquire knowledge of appropriate actions to respond to varying network conditions [207]. In the event of an overwhelming DDoS attack, the agent's primary objective is to maintain the regular operation of the victim server by disconnecting a significant number of suspicious and malicious requests. Alternatively, the agent can prioritize mitigating DDoS attacks while minimizing the adverse impact on legitimate requests. To train the DDoS detection agent, it is necessary to have access to labeled data that can be used to determine the false positive rate, which is then utilized in the reward calculation. Additionally, Kurt et al. [208] proposed a comparable approach to detect attacks in a smart grid using RL. Furthermore, training the RL agent to detect DDoS attacks effectively requires considering the time required to launch such attacks.

The authors in [209] investigate the phenomenon of adversarial attacks on DRL algorithms. The study examined the effects of adversaries on a thoroughly trained DRL model for electric vehicle energy management. The attacks are initiated by utilizing the fast-gradient-sign method (FGSM). This method generates various assumptions targeting the DRL system, such as excessive fuel consumption or battery depletion. In a separate study, Wang et al. [210] studied the backdoor trojan attacks on DRL-based congestion control systems employed in autonomous vehicles. Before introducing it into the DRL training dataset, the authors examined several mechanisms to improve the covert nature of the attacks.

The authors in [211] proposed IDS for vehicular VANETs by leveraging Bayesian game theory and DRL techniques. This study presented GaDQN-IDS, which utilizes various theories and learning models to implement a self-adaptive IDS for VANETs. The study focuses on two key challenges encountered in IDS for VANETs: 1) identifying environmental changes as perceived by the IDS and 2) developing adaptability mechanisms for the IDS in various scenarios.

The study by Iftikhar et al. [212] explored the implementation of an ML methodology to improve the security and safety measures of the IoV systems. The authors utilize a DRL-based methodology, which incorporates LSTM and GAN models in their approach. LSTM is a specific variant of an RNN that can acquire and retain information across extended sequences. This characteristic makes it well suited for analyzing time-series data, such as sensor readings commonly encountered in AVs. In contrast, GANs comprise a pair of NN engaged in a competitive interaction within a zero-sum game structure. This framework can potentially generate efficient data that closely resemble real-world data.

Authors [213] proposed architecture for an IDPS for VANETs deployed in an Edge Computing (EC) environment. The authors acknowledged the sensitivity and criticality of IDS in VANETs for maintaining normal operations, utilizing RL throughout the architecture to deal with VANET dynamics, and making informed decisions based on the current state of VANETs. The goal is to achieve high detection accuracy.

Wang et al. [214] introduced an IDS in smart vehicular networks (SVNs) using DRL. The authors assert that conventional transportation networks can be conceptualized as SVNs, resulting in substantial improvements in traffic safety and convenience. The authors proposed an approach in the form of a DRL-based IDS, which aims to detect and classify abnormal network traffic patterns effectively. The proposed system utilizes a DQN model to enhance the effectiveness of IDS, thereby reducing the potential for erroneous assessments. In this study, the NSL-KDD dataset was used to train and assess the effectiveness of the proposed model.

Li et al. [215], presented an approach that uses a DDQN to detect DDoS attacks in the IoV context. The study proposed a methodology that employs an RL framework, augmented by a Kalman filter, to enhance the performance of DDoS detection in the DDQN algorithm while minimizing dependence on extensive labeled data. Furthermore, it utilizes the knowledge acquired from neighboring base stations with similar characteristics to accelerate the DDQN training process for a newly deployed base station. To conduct these simulations, the authors utilize the publicly available dataset, 'CIC-DDoS 2019', which encompasses various types of DDoS attack.

In their paper, Watts et al. [216] discussed the imperative of promptly identifying and isolating atypical or defective data to ensure the effective operation of CAVs. The proposed approach involves a dynamic method to adjust the threshold used in real-time IDS. This adjustment is crucial to effectively address fluctuations in anomaly rates and integrate feedback received during a trip to enhance algorithm performance. The proposed model comprises two layers, namely a CNN and a Kalman Filter (KF), and employs a DRL-Bayesian framework.

The work in [217] studied the cybersecurity issues associated with IoV. The authors suggested an IDS architecture that incorporates DL Engines (DLEs) to effectively identify and classify vehicular traffic. These Dynamic Learning Environments (DLEs) deploy on Multi-access Edge Computing (MEC) servers to cater to vehicles' mobility and the real-time demands of IoV networks.

The primary focus of the study conducted by Sagar et al. [218] is to develop and execute a DRL-based solution to promptly detect spoofing attacks. The authors employ the RL DQN model to effectively address GNSS spoofing attacks' dynamic and intricate characteristics. The DQN agent acquires decision-making abilities by interacting with an environment conceptualized as an MDP. The researchers employed the Honda Research Institute Driving Dataset to create two sets of data: one consisting of attack scenarios and the other composed of non-attack scenarios.

6) GENERATIVE ADVERSARIAL NETWORKS (GANS)

Generative adversarial networks (GANs) are a class of neural networks first introduced in [219] for generating realistic new images. A GAN is a two-stage network comprising a generator network and a discriminator network. The generator network is trained to produce new outputs in the target domain, and the discriminator is a binary classifier that classifies these outputs as real or fake. The generator aims to learn the true dataset by observing the discriminator's response to its generated samples. The ultimate goal is to make the generator output as realistic as possible. GANs are heavily used for image synthesis (e.g., RGB-to-Thermal image [220]) and image processing (e.g., image style transfer [221], image enhancement [222]).

Seu et al. [223] proposed a generative adversarial network intrusion-detection system (GIDS) for raw CAN traffic data.

A discriminator was first trained on real traffic data and then on real and fake data from the generator. The former produced 99% while the latter produced 98% accuracy over a synthetic dataset. Chen et al. [224] proposed an auxiliary classification GAN (ACGAN) to detect unknown attacks. The GAN generator is trained to generate negative samples (labeled as unknown) that reflect new attack types in the inference stage. Zhao et al. [225] proposed a cascaded two-stage classifier using ACGAN to detect unknown attacks. The GAN network generates new Out-of-Distribution(OOD) attack patterns that do not exist in the training dataset. The Car-hacking dataset is used with four types of known attacks to train the GAN network. New attack patterns are then generated to train the classifier. The performance is validated in four classification metrics. Yang et al. [226] introduced a single DNN with GAN to improve the detection accuracy over an IDS dataset. In [227], enhance the discriminator's ability to identify tampering attacks by incorporating a CAN communication matrix delineating the signal's maximum and minimum range. During data preprocessing, segment the CAN messages into five categories based on transmission mode, thereby minimizing misjudgments by the discriminator. Additionally, given the dynamic frame sequence in driving conditions, utilize 64 consecutive messages with identical IDs to formulate the CAN image instead of directly using varied traffic data with multiple CAN IDs. Hoang et al. [228] proposed a combination of an autoencoder and a GAN trained in a semi-supervised fashion. The model is trained first on a large number of unlabelled samples to learn the patterns in the data, and then a small number of labeled data samples are used to train the final model. The model is tested for DoS, fuzzy, spoofing, and unknown attacks, which achieved an F1-score up to 0.9984. Batzorig et al. [229] proposed CANPerFL, a framework that utilizes a concise Resnet architecture for classifying binary-encoded CAN IDs. The model creates a matrix that represents the temporal and geographical organization of the CAN ID sequence. CANPerFL development includes an FL technique. The framework attains a general precision of around 99%. In their study, Qin et al. [230] introduce the GPIDS system, an IDS for IVN using GAN to detect vehicle attacks such as bus-off, spoofing, and replay. This system employs a semi-supervised learning model that requires minimal training data, allowing for effective anomaly detection based on deviations from standard patterns. Extensive validation on four vehicles demonstrated GPIDS's capability to accurately identify threats with minimal latency, supported by a dataset derived from these actual vehicles.

7) FEDERATED LEARNING

FL is a decentralized learning mechanism that allows model training across multiple devices or servers without exchanging raw data. By bringing the model training process to the data sources, FL preserves data privacy. FL involves training a ML model on local devices, servers, or nodes. These local models work collaboratively to improve the global model by sharing model weights or gradients. The model updates and aggregation runs iteratively, and the resulting global model improves over time as the accuracy of the local models improves. FL is gaining traction in various industries [231], [232] including cyber security [165], [233], [234], [235] as a privacy-preserving solution. Yang et al. [236] proposed an IVN IDS based on the periodicity of the network message ID. ConvLSTM was used in FL using a client-server model. Clients are intelligent connected vehicles (ICVs), and the server is a mobile edge computing (MEC) server located at the base station. The model is optimized for the accuracy and system overhead of FL training. The model achieved 95% accuracy over the Car-hacking Attack & Defense dataset [102]. Driss et al. [237] also employed FL to detect attacks on IVN using an ensemble of Gated Recurrent Units (GRU) with an RF model. With an ensemble of just 5 GRUs and RF, authors could achieve more than 98% accuracy on the same dataset. Shibly et al. [238] presented an FL-based IDS method using supervised and non-supervised learning techniques to detect multiple types of attacks. Data from three different real vehicles is used in the FL setup to evaluate the proposed scheme, and an accuracy of up to 99.9% was reported. In [239], a graph neural network and a two-stage classifier cascade were used to construct the CAN bus IDS and identify all threats simultaneously. The approach is adaptable and has robust parallel processing and fault tolerance capabilities. However, it incurs substantial computational costs throughout the training model generation process. Evaluate the suggested IDS via thorough tests using various real-world datasets. Hoang et al. [240] proposed an FL scheme for CAN IDS using different car models from different manufacturers (KIA, BMW, and Tesla). The dataset was collected from the three cars with two types of attacks (fuzzing and replay). Aliyu et al. [241] proposed an SDN-enabled IDS for CAN bus using FL and random forest. Statistical features such as minimum, maximum, mean, standard deviation, and two high-order statistical (HOS) are extracted and used to train the RL model in an FL setup. The proposed method is implemented in SDN emulator Mininet and a high accuracy of up to 98% is achieved.

8) TRANSFER LEARNING

The concept of "Transfer Learning" holds significant importance in contemporary ML, specifically in the domain of AI [245]. Transfer learning uses information from a source domain to boost the learning process for a target job in a different domain. The transfer learning methodology offers a potential solution to address the challenge of limited data availability for model training [246]. The approach uses models trained on comparable data characteristics to project new data characteristics onto the same feature space as the original. In contrast to unsupervised and semi-supervised learning approaches, this technique leverages pre-existing knowledge to enhance IDS with less labeled data. Transfer learning is a mathematical framework that encompasses two fundamental concepts: domain and learning task. Typically, model-based

TABLE 5. Transfer Learning Approaches for IDS in IVNs

Category	Ref	Source Domain		Target Domain		Remarks
		DL Model	Dataset/Platform	DL Model	Dataset/Platform	
Cross-data TL	[251]	DenseNet (CNN)	HCRL	DenseNet (CNN)	HCRL+GAN	Knowledge transfer across datasets.
	[252]	CNNs	CICIDS2017	CNNs	CICIDS2017	Evaluate performance over CNN models.
	[253]	P-LeNet (CNN)	Synthetic data	P-LeNet (CNN)	Synthetic data	Improve accuracy in binary classification.
	[262]	SupCon ResNet	Car-hacking	SupCon ResNet	HCRL, Survival	TL from a rich dataset to a small dataset.
Cross-model TL	[254]	DBN	CICIDS2017, NSL-KDD	FF-ANN	CICIDS2017, NSL-KDD	Improve accuracy in IVNs.
	[260]	MobileNetV2	Car-Hacking	Lightweight CNN	CICIDS2017	TL with different data and models.
Cross-vehicle TL	[148]	LSTM	Sonata	LSTM	Soul and Spark	Improve accuracy in binary classification
	[250]	ConvLSTM	Soul, Sonata	ConvLSTM	Soul, Sonata	One-shot learning to detect new attacks

approaches are commonly integrated with DL models in the context of transfer learning. This integration allows for transferring the structure and parameters of pre-trained models, such as AlexNet, VGGNet, and ResNet, which have been trained on extensive datasets. The weights obtained from training on the large dataset are then utilized as the initial weights for the new task [247]. In contrast to DL, transfer learning can identify and extract previously undiscovered information. Transfer learning involves training a deep network structure on a comprehensive dataset. Subsequently, the model is applied to a smaller dataset by adjusting its parameters via a process known as fine-tuning. The characteristics derived from the pre-trained DL exhibit universality and may be used effectively for diverse datasets [246].

ML/DL-based IDS possess enhanced proficiency in handling substantial volumes of data and identifying unanticipated security risks. The primary objective is to classify network data as normal or abnormal by extracting features from network traffic to train a detection model. The initial ML/DL model is implemented during vehicle production and subsequent departure from the manufacturing facility. However, the model's performance would significantly decrease when new attacks with different feature distributions are launched. To address these limitations, the concept of transfer learning has been introduced. This approach involves leveraging either data or a pre-existing model from a source domain to train an ML/DL model specifically tailored to a new task in the target domain in Table V.

The study conducted in [148] represents the initial attempt to utilize transfer learning in analyzing CAN bus data. The researchers introduced an LSTM-based model to address the task of binary classification. The authors tested the proposed scheme on a small-sized survival dataset [248]. The transfer learning technique was applied to test the performance of the Kia Soul and Chevrolet Spark datasets. The Hyundai Sonata dataset was utilized to train the proposed model.

The IDS developed by Mehedi et al. [249] is based on a deep transfer learning model called the LeCun Network. The model has the following input features: CAN Identifier (CAN-ID), Data Length Code (DLC), and the data field of CAN messages. There is a lack of available data regarding the detection latencies associated with this particular method. The CAN Transfer model, proposed by the authors [250], the presented approach named CANTransfer, which leverages the transfer learning and an LSTM model for IDS on the CAN bus. CANTransfer was designed to minimize processing time, rendering it well-suited for real-time IDS. The researchers performed comprehensive experiments utilizing authentic datasets obtained from two distinct vehicles.

The authors in [251] proposed a transfer learning-based self-learning IDS (TLSIDS) for CANs. The TLSIDS uses a cascade detection approach to detect high-performing known and unknown attacks. It consists of four modules: basic detection, advanced detection, unknown attack classification, and self-learning. A public dataset evaluation showed that the TLSIDS has high effectiveness and robustness in detecting attacks. The work in [252] presented IDS designed specifically for IoV systems. The IDS utilizes CNNs, transfer learning, ensemble learning, and hyperparameter optimization techniques. The author aimed to develop IDS to identify and detect cyber-attacks in intra-vehicle and external vehicular networks. The authors employ two widely recognized public benchmark datasets about IoV security: the Car-Hacking dataset and the CICIDS2017 dataset. Another work in [253] proposed an approach for detecting illegal EV network infrastructure access. The authors proposed an IDS using deep transfer learning with the P-LeNet model to address security issues. Transfer learning helps the IDS adapt to the quickly changing threat environment in IVNs. The authors trained and validated the P-LeNet model using a randomly chosen training dataset and a validation dataset. The study [254] presented a cyberattack-detecting IDS for intra- and inter-vehicle communication networks. The infrastructure-independent IDS detects anomalies using a blacklist of threat signatures. A cloud-based security management system may update threat signatures in connected automobiles over the air. The detection engine uses Self-taught Transfer Learning (STL) to build DNNs using pre-trained DBN models. The work evaluates the model using actual datasets and emphasizes ICV cybersecurity. The transfer learning approach proposed by Li et al. [255] aims to enhance IDS capabilities for various attacks on the IoV. The experimental findings demonstrate that, compared to prevailing TML and DL approaches>The IDS proposed by Xu et al. [249] is based on DL and transfer learning. The implementation of transfer learning is employed in this study to enhance the efficiency and adaptability of the model. The experimental analysis demonstrates that the proposed model performs superior to conventional TML and DL methods in efficiency and robustness. The authors [256] proposed two model update approaches that use transfer learning to address new and developing threat types in the IoV. The first cloud-assisted updating strategy uses the IoV cloud to provide limited data. The IoV cloud cannot quickly deliver tagged data in the second technique. The local update approach uses pre-classifications to get pseudo-labels for unlabeled material in fresh assaults. Multiple cycles of transfer learning use these pseudo-labels. This allows the vehicle to update without annotated data from the Internet of IoV cloud. Simulations were performed on two AWID datasets [257]. The article [258] introduced TRLID, a deep transfer learning-based IDS model for the IoV. The model successfully transfers information from a source task to a target task using transfer learning features. The car-hacking dataset of OBD-II CAN packets trains the model for various attack scenarios. In their 2024 study, Hoang et al. [259] introduce an advanced IDS for vehicular networks utilizing a Supervised Contrastive ResNet (SupCon ResNet) model enhanced through transfer learning. The IDS utilizes a pre-trained SupCon ResNet. This method is initially trained on the Car-Hacking dataset and subsequently adapted using the Survival dataset. This approach markedly reduces false-negative rates and achieves high F1 scores, demonstrating superior performance and robustness compared to traditional IDS methods in the real-world automotive field. Ultimately, the model can adjust to limitations imposed by hardware, such as the amount of memory available and the time it takes to execute to be used on actual devices.

The authors [260] presented a lightweight IDS for protecting the information security of IoV. The proposed method uses the MobileNetv2 network as the backbone and combines transfer learning techniques and hyper-parameter optimization to detect attacks on IVNs and external vehicle networks (EVNs). The method achieves high accuracy, precision, and recall on both Car-Hacking and CICIDS2017 datasets representing IVNs and EVNs, respectively. Haddaji et al. [261] introduce a hybrid IDS that integrates FL with TL to improve the robustness and adaptability of IVN security systems, particularly against CAN bus attacks. The framework employs a trusted authority for secure communications and leverages a cloud server for model distribution and aggregation. Data collection is performed over the CAN bus, and the model training utilizes data selected using Maximum Mean Discrepancy (MMD) to ensure relevancy to the target domain, enhancing detection capabilities. This approach begins with standardized baseline models and allows each vehicle within the network to refine these models through TL, fostering a collective intelligence that continuously evolves to meet emerging cyber threats. The proposed solution has been evaluated and validated using OTIDS and Car-Hacking datasets.

C. SUMMARY AND DISCUSSION

The AI-based iIDS techniques have been compared following ML, DL, Transformers, transfer learning, and DRl techniques. IDS approaches are reviewed according to the essence of learning methodologies. Together, all the methods obtain higher prediction accuracy, and DL and Transfer learning show highly accurate results. Thus, AI-based techniques can be a potential technique for identifying and classifying attacks. In addition, the AI-based methods should be optimized for the latest attacks to improve the detection capability.

AI has assumed a pivotal role in identifying intrusions by delivering exceptional precision in IDS. AI-based models often emphasize accuracy as a primary performance parameter. However, they may only sometimes consider other significant metrics like F1-score, false acceptance rate (FAR), precision, and recall. Consequently, there exists a need to formulate a comprehensive framework that emphasizes these criteria, as mentioned earlier. Another concern with AI-based IDS is using publically accessible datasets for attack detection. These datasets are often extensive in size and may include noisy data, potentially impacting the system's overall performance. To tackle this issue, we can use a mechanism that may identify anomalies within the dataset. This mechanism can then be included in the existing framework to mitigate the problem of overfitting. Furthermore, a majority of frameworks fail to consider factors such as temporal complexity and CPU consumption, both of which have the potential to significantly influence the overall performance of a system. When considering these measures, it is possible to enhance the overall performance of the system. It is essential to acknowledge that despite the extensive body of research on IDS, practical implementation for this particular system still needs to be implemented.

Despite impressive results in automotive security applications, Section V demonstrated that ML has many limitations. There is also some discussion of ML-based studies of car security here. A fundamental limitation is the use of adversarial ML. There are various methods in which vehicles (adversaries) might trick the ML model, leading to subpar results. Feature poisoning and other purposeful attacks on supervised algorithms that employ static features and predetermined labels, known as adversarial training, may lead to inaccurate results for ML systems. There is a lack of research on unsupervised learning attacks on vehicular networks. Adversarial attacks may just as easily damage unsupervised algorithms. Therefore, reliable supervised and unsupervised algorithms with robust feature selection are required for security-sensitive vehicle networks. DL has shown exceptional capabilities in accurately detecting and predicting many phenomena. One notable advantage of DL is its ability to analyze raw data in its natural form, eliminating the need for feature engineering. This approach is suitable for analyzing non-linear data patterns and may be used in many learning scenarios, including supervised, partially supervised, or unsupervised settings. In the context of multi-dimensional data, CNNs have shown effective performance. However, in scenarios where understanding of temporal information is crucial, RNNs emerge as a more suitable alternative to CNNs. RNNs are designed to handle sequential and/or time-series data effectively. Nevertheless, it is impossible to generalize that the LSTM design is preferable to the CNN architecture or vice versa. The selection of the DL architecture is only one aspect of design considerations, and it is essential to recognize that other design choices could have a far more significant influence on the overall outcome than the specific choice between LSTM and CNN. An IDS that undergoes training via unsupervised learning may exhibit increased proficiency in identifying new types of attack. This is mainly because such an IDS is forced to prioritize distinguishing between normal and abnormal behaviors rather than only relying on specific patterns associated with a limited range of assaults. An IDS that incorporates analysis of the data field with the arbitration ID can potentially identify data tampering attempts. Conversely, an IDS that excludes the data field from analysis would be unable to detect such attacks. With the emergence of ML and DL methodologies, there is potential to enhance training effectiveness by using pre-processing techniques for the CAN bus system dataset. The majority of methodologies explored in the research, as mentioned above, primarily concentrate on enhancing the core and post-processing models while overlooking the analysis of pre-processing components. The performance of the IDS is significantly impacted by the volume of data, particularly in the case of the CAN, due to its high rate of packet broadcasting. It may be beneficial to consider doing a comparison analysis to evaluate the computational efficiency of the data pre-processing technique as a potential area of investigation for future research [263]. In addition, it is worth noting that these mechanisms have positive efficacy in countering unfamiliar IVN assaults. However, it is essential to acknowledge that their implementation requires a substantial allocation of computational and storage resources, rendering them unsuitable for deployment inside the IVN environment. However, in the context of IDSs, the quantity of normal samples often surpasses the number of intrusion samples, resulting in imbalanced data. This imbalance poses a challenge in the training process. This phenomenon may lead to the model exhibiting a bias towards normal samples, hence detrimentally impacting the efficacy of IDS. In addition, IDSs are confronted with a substantial volume of heterogeneous data, including network traffic, system logs, and system calls. Transforming this data into feature vectors appropriate for DL models might pose challenges. The efficacy of IDSs heavily relies on the criticality of feature extraction. Moreover, the issue of overfitting is often encountered in the field of DL, mainly when working with a restricted quantity of data. IDSs may experience a decline in generalization performance due to overfitting, resulting in the model being excessively tailored to the training data and failing to identify novel intrusions.

Transfer learning is a novel approach to learning methods operating with established ML models. In recent years, it has shown promising prospects in the domain of vehicle security. Deep Transfer Learning (DTL) in IDSs is intended to enhance the precision and efficiency of these systems by capitalizing on the knowledge acquired from analogous activities or domains.

When considering the DL-based IDS, the availability of tagged data may be limited or come at a high cost. The difficulty at hand may be efficiently tackled by DTL, which involves using information acquired from activities or domains that are closely related. This approach enables models to learn well even when working with limited datasets. Additionally, DTL has the potential to enhance the generalization capabilities of IDS by facilitating the transfer of acquired information from one domain to another.

This review is one of the first comprehensive reviews of the literature on the use of RL/DRL methods in IVN IDS. While there are reviews in the existing literature on the topic, research must adequately address these methodologies. This survey provides a comprehensive investigation of the use of DRL and RL methods in the context of IDS based on IVN. The research includes an in-depth analysis of the datasets employed in the experiments and an evaluation of the performance shown by each DRL/RL model. In recent times, DRL has demonstrated superior performance compared to DRL and ML across several domains. The primary methodologies used in DRL include Deep Q learning, policy gradient, deep auto-encoder Q learning, double deep Q learning, policy gradient, and actor-critic models. The DRL above models have shown superior performance to other DL/ML methodologies in anomaly detection across many applications. This survey demonstrates the applicability of a deep Q network for handling intrusion anomaly data. Deep policy gradient approaches have been used in constructing anomaly detection systems. The actor-critic approach has been seen in the context of intrusion detection. RL is a promising methodology for enhancing the capabilities of autonomous vehicles.

Despite advancements in the field, RL in autonomous systems can encounter several challenges. These challenges include misclassification of objects in perception systems, vehicle theft resulting from incorrect recognition of driver monitoring patterns by neural networks, compromised functional safety due to erroneous collection of vehicle data, and failure to detect attacks. In the context of RL, when an agent lacks past information and makes decisions based on long-term rewards, it is possible for the agent to inadvertently amplify rewards in a manipulated environment when subjected to an assault [264]. Furthermore, it is worth noting that the recovery period in RL algorithms tends to be somewhat lengthy. Consequently, several scholars have expressed apprehensions about the dependability of RL in applications that are crucial for security [265].

The amount of research publications on this topic needs to be increased since it is a relatively new technology introduced in 2017. This survey is limited to scholarly articles published in journals and conference proceedings that only use the RL and DRL frameworks for IoV research. Consequently, we have addressed IoV I IDSs, and UMV, which have similarities with the IDS used in IVN. This approach may provide valuable insights for researchers working on IVN IDSs. RL and its DL-assisted variations are crucial in enabling autonomous cars to make judgments during driving tasks [266] and IoV [267]. RL has been extensively used in developing IDS for UAVs within the context of smart cities [268]. In the domain of UAVs, RL algorithms may be used to train IDS to identify and effectively counteract various incursions. RL algorithms can undergo training processes that enable them to identify and classify many forms of assaults, including but not limited to illegal access, jamming, spoofing, and other similar instances. Furthermore, RL methods may be used to enhance the response of the IDS, assuring its optimal effectiveness. Using RL in IDS for UAVs inside smart city environments has shown significant efficacy. Its widespread adoption may be attributed to its inherent capacity for adaptive learning and continual enhancement.

FL is a new distributed paradigm with privacy-preserving benefits compared to traditional centralized (non-distributed) learning methods. However, FL faces challenges such as communication overhead, data imbalance, etc. [269]. The review of the recent works on FL in IVNs clearly shows the amount of work on FL is less compared to the vast amount of work using centralized learning. The results consistently report that FL can achieve comparable performance to traditional centralized learning models. The existing datasets used in these works are not curated for FL setup and thus have a high-class imbalance, which reduces the fairness of the FL methods proposed. The complexity involved in FL in the IVN environment is another challenge that needs to be addressed.

VI. BENCHMARK DATASETS AND EVALUATIONS

This section aims to summarize the most commonly used datasets and simulation tools.

A. BENCHMARK DATASETS

The popular datasets for IDS in IVNs are briefly described in this section. These datasets differ in several ways. The significant distinctions are the type of attacks, the number of features, the size of the datasets, and fidelity (whether actual or simulated data). The common attack types among all datasets are DoS and Spoofing attacks. The ORNL Automotive Dynamometer CAN intrusion dataset in the list contains the highest number of attacks (i.e., 10^2). However, the dataset has no labeling for attacks. Other datasets without attack labels include HCRL CAN, TU CAN, and SynCAN.

1) HCRL OTIDS [270]

The HCRL Open-Source Intrusion Detection System (OTIDS) dataset is created by the HCRL group, which is a meticulously curated dataset designed to facilitate the detection of intrusions in CAN systems, commonly referred to as the CAN dataset for IDS. This dataset consists of four features: Timestamp, CAN ID, DLC, DATA[0], and DATA, on benign and DoS attacks, fuzzy attacks, and impersonation (masquerade) attacks. It was collected using a Kia Soul vehicle. In contrast to the car hacking dataset, the attribute of labels (ground truth) is absent. The documentation provides attack injection intervals that appear erroneous and are inadequate for identifying fuzzy and impersonation attacks due to a lack of specific information regarding the injected IDs.

2) CRYSYS LAB DATASET

[271] The CrySyS Lab dataset (CrySyS CAN) and CAN log infector created by CrySyS Lab are related to the CAN communication protocol. This dataset comprises various elements such as CAN messages, message identifiers, timestamps, and corresponding signal values. It also includes benign driving scenarios, including but not limited to maintaining a constant velocity of 30 km/h, executing a lane change after driving at a velocity of 40 km/h, coming to a complete stop, and performing an emergency brake from a velocity of 60 km/h to 0.

3) HCRL CAR-HACKING DATASET

[270] The HCAR-CH dataset for intrusion detection is an extensive dataset intentionally developed to advance research and development in the intrusion detection domain in automotive systems. It was methodically curated by a group of scholars affiliated with the Hacking and Cybersecurity Research Lab (HCRL). The dataset was obtained during the execution of attacks on an actual vehicle. The dataset comprises a total of 500 seconds of benign data, which was gathered during the operation of a vehicle and is accompanied by four distinct attack types, comprising DoS, fuzzing, and two spoofing attacks, namely RPM and gear. Each attack consisted of 300 message injection intrusions that persisted for 3 to 5 seconds and were recorded for 30 to 40 minutes. The dataset comprises several attributes, including timestamp, CAN ID, Data Length Code (DLC), payload, and label, representing injected and normal messages.

4) HCRL SA

[270] The Survival Analysis dataset (HCRL SA) for automobile IDS is also provided by the HCLR group. The main objective of this dataset is to analyze the duration until an intrusion occurs in an automotive system while also comprehending the variables that play a role in the success or failure of the IDS. The singular publicly accessible CAN dataset encompasses authentic attacks on numerous vehicles. The pre-owned automobiles in the market comprise the Hyundai YF Sonata, Kia Soul, and Chevrolet Spark. The researchers gathered non-malicious information and three distinct forms of attacks, namely DoS flooding attacks, fuzzing attacks, and spoofing attacks causing malfunction, from every vehicle. The dataset under consideration comprises several attributes, including timestamp CAN ID, Data Length Code (DLC), payload, and label that denotes normal and injected messages.

5) AEGIS BIG DATA PROJECT [272]

The AEGIS Big Data Project Automotive CAN Bus dataset (AEGIS CAN) is an endeavor that concentrates on utilizing Big Data technologies to achieve advanced analytics and information security objectives. This endeavor aims to tackle the obstacles to handling and examining exceedingly voluminous datasets, commonly known as Big Data, while guaranteeing resilient information security protocols. The dataset in question is a benign collection of driving data spanning 20 hours. It contains various signal data, including but not limited to wheel speed, steering wheel angle, roll, pitch, and accelerometer values for each direction. GPS data is also accessible.

6) TU EINDHOVEN CAN BUS DATASET

[273] The TU Eindhoven CAN bus intrusion dataset (TU CAN v2) is intended for academic purposes. It has been specifically curated to facilitate research on intrusions in automotive systems via the CAN bus. The dataset was generated by a group of scholars at the Technical University of Eindhoven via a regulated experimental configuration. The experimental setup involved the integration of multiple sensors and devices onto an automotive testbed or vehicle to acquire communication data transmitted via the CAN bus. These devices comprise hardware interfaces, such as monitoring tools for the CAN bus or bespoke hardware, which facilitate the acquisition of CAN messages transmitted between the ECUs in the automobile. The benign data was collected using a CAN bus prototype with two vehicles, an Opel Astra and a Renault Clio. The simulated attacks encompass diagnostic, fuzzing, replay, suspension, and DoS attacks. Modifying CAN message timestamps during post-processing renders the dataset unsuitable for evaluating AI-driven CAN intrusion detection systems that rely on time as a key feature.

7) HCRL CAN SIGNAL EXTRACTION AND TRANSLATION

[270] The CAN Signal Extraction and Translation (HCRL-SET) dataset is a thorough collection of data that centers on retrieving and converting CAN signals within automotive systems. The development of the HCRL-SET dataset encompassed various technical procedures and deliberations. Initially, a varied assortment of vehicles that were equipped with CAN bus interfaces were utilized to gather data. The interfaces facilitated the acquisition of unprocessed CAN frames, encompassing the encoded communications transmitted among the ECUs within the automobiles. The dataset comprises 56 logs of CAN traffic, which were obtained by systematically transmitting OBD queries during controlled driving conditions. The aforementioned contains a total of 28 distinct CAN identification numbers. The dataset in question lacks both attack-related data and information pertaining to benign data.

8) SYNCAN DATASET

[274] The Synthetic CAN Bus dataset (SynCAN) is a scholarly asset intended to examine automotive cybersecurity, particularly on attacks and IDS based on the CAN bus. The resource offers an extensive compilation of fabricated CAN data that emulates authentic driving situations and encompasses diverse attack scenarios. The process of creating the dataset is a multifaceted procedure. A comprehensive comprehension of both automotive systems and CAN communication protocols is imperative. Utilizing this information, a software application is created to produce fabricated CAN messages that depict various automobile metrics, including velocity, acceleration, and engine condition. The purpose of this dataset is to train unsupervised CAN IDS. This dataset is extensively employed in academic literature for assessing unsupervised iIDS that rely on payload analysis. In contrast to previously discussed datasets, this dataset presents signal values without disclosing the raw CAN data. Therefore, it is appropriate to conduct testing on IDS that rely on signals. The dataset comprises a set of training data and six distinct test datasets. The dataset for testing includes a single normal dataset and five datasets specifically designed to simulate attacks. The five attack types are plateau, continuous, playback, suppress, and flooding.

9) HCRL CAR HACKING (HCRL-CH)

[102] The dataset is a scholarly pursuit that centers on investigating and scrutinizing susceptibilities in vehicular systems, with a specific emphasis on the possibility of car hacking attacks. This challenge aims to cultivate a more profound comprehension of the methods used by malevolent actors to breach automobile security and establish efficacious countermeasures to thwart such incursions. HCRL gathered the data by employing a Hyundai Avante CN7 vehicle, as part of a competition that sought to foster the creation of attack and detection methodologies for the CAN bus. The data attributes of timestamp, ID, DLC, payload, label, and SubClass (attack type) incorporate attacks such as benign, flooding (DoS), spoofing, replay, and fuzzing.

10) REAL ORNL

[73] The Real ORNL Automotive Dynamometer (ROAD) CAN intrusion dataset is a significant asset in automotive security for IDS in the CAN. This dataset was methodically generated via controlled experiments on an automotive dynamometer, a laboratory apparatus to replicate authentic driving scenarios. This dataset involves recorded unauthorized access or manipulation of the system. The dataset adeptly captures the intricacies and obstacles encountered within authentic automotive settings by implementing controlled conditions that replicate genuine driving scenarios. The dataset comprises 33 attacks, each equivalent to 30 minutes of driving, and 12 benign datasets encompassing various driving scenarios, totaling 3 hours. All data was collected using a single vehicle. While gathering attack data, the vehicle was on a dynamometer, which simulated driving conditions. The dataset comprises three types of attacks: (i) fuzzing attack that involves the injection of random IDs, (ii) targeted ID

attacks that come in four variations, namely correlated signal (alteration of the wheels' speed), max speedometer (display of false speed), max engine coolant temperature (activation of engine coolant warning light), and reverse light (misrepresentation of the gear status), and (iii) accelerator attacks that place the ECU in a compromised mode.

11) CICEV2023

[275] The dataset simulated DDoS attacks of different magnitudes in electric vehicles (EVs) charging infrastructure and consists of features such as packet access counts and system status information on charging facilities.

B. SIMULATION TOOLS

Simulators play a crucial role in developing AI-based IDS for IVNs by offering a testbed for cybersecurity solutions and providing valuable data for AI model training. This highlights the importance of cost-effective, easily configurable, high-performing simulators for efficient and effective IDS development. Below is a group of simulation tools used in vehicular environments to model real-world scenarios.

1) MATLAB

[277] is a high-performance language and software environment for technical computing and visualization, widely used in the field of vehicular technologies. It provides extensive tools and libraries for designing, simulating, and testing vehicle systems. Engineers can model the vehicle's physical characteristics, control systems, and embedded software within MATLAB. They can also develop advanced driver-assistance systems (ADAS), optimize vehicle powertrains, design vehicle dynamics and control systems, and conduct hardware-in-the-loop (HIL) testing. Furthermore, the toolboxes in MATLAB offer functionalities for developing autonomous driving systems, including sensor fusion, lidar and radar processing, and path planning. Thus, MATLAB is a comprehensive platform for the entire vehicle design and testing process.

2) VEINS (VEHICLES IN NETWORK SIMULATION) FRAMEWORK

[278] is a sophisticated tool that facilitates a comprehensive investigation of vehicular communications with a high degree of realism. From the standpoint of an automobile, it facilitates the emulation of diverse facets, such as communications between V2V and V2I. The simulation employs OMNeT++, a network simulator that manages wireless communications, and SUMO, a road traffic simulator, to replicate the movement patterns of a vehicle and its interactions with its surroundings. The VEINS system offers a security module encompassing a comprehensive collection of security mechanisms about Model-Based design (MBD) and safeguarding privacy. By integrating these simulations, VEINS facilitates realistic inter-vehicle and vehicle-infrastructure communication, adaptive response to dynamic traffic conditions, and assessment of diverse network protocols, all within a simulated, virtual environment.

3) ITETRIS

[279] is a comprehensive simulation tool that models cooperative Intelligent Transport Systems (C-ITS) from the viewpoint of a vehicle. The present platform, which is open-source in nature, integrates two traffic simulators, namely SUMO and NS-3, to simulate a diverse range of V2X interactions. These interactions include V2V, V2I, vehicle-to-pedestrian (V2P), and vehicle-to-network (V2N). The technology facilitates the ability of automobiles to engage with their environment and adapt to various traffic scenarios, thereby augmenting traffic efficacy, roadway security, and ecological viability. The iTETRIS platform enables efficient communication and collaboration between vehicles and other components within the transportation ecosystem, including digital traffic management systems, pedestrian crossings, and traffic lights. This facilitates the experimentation and advancement of novel C-ITS applications.

4) CARLA (CAR LEARNING TO ACT)

[280] platform is a highly advanced open-source simulation tool designed to research autonomous driving. From a vehicular standpoint, its environment is precise and authentic, allowing for the simulation of diverse driving circumstances such as varying weather patterns, interactions with pedestrians, and the behaviors of other vehicles on the road. The utilization of a simulator enables the examination and authentication of autonomous driving algorithms in a range of varied circumstances. CARLA offers comprehensive sensor models for various autonomous vehicle sensors, including LiDAR, cameras, GPS, IMU, and RADAR. These models enable the vehicles to accurately perceive and engage with their surroundings in a lifelike manner. The testing and refinement of autonomous vehicle systems in diverse and intricate scenarios aid researchers in developing safer and more dependable autonomous vehicles. The simulation tool lacks a V2X communication module. Nevertheless, specific extensions have successfully integrated a V2X module into CARLA.

5) THE VEHICULAR NETWORK OPEN SIMULATOR (VENTOS)

[281] is a comprehensive simulation tool that has been developed with the specific aim of supporting research endeavors in vehicular network systems, with a focus on the vehicles' perspective. Integrating network and traffic simulation results in a realistic setting that facilitates V2V and V2I communications. In the VENTOS system, automobiles are not solely passive objects that adhere to traffic regulations. Instead, they are intelligent entities that can interact with their surroundings and other vehicles. By utilizing authentic cartographic representations and actual traffic flow data, VENTOS facilitates the ability of automobiles to react to a diverse range of circumstances, including traffic build-up, collisions, or dynamic traffic situations. This renders VENTOS valuable for

TABLE 6. A Summary of Benchmarking Datasets for IVN IDSs

Dataset	Year	Fidelity	Environment	Attack Types	Format	Features	Port	Objective
HCRL OTIDS [270]	2017	Real	Testbed	DoS, fuzzing, impersonation	.csv	10	CAN/OBD-II	IDS
HCRL CH [270]	2018	Real	Testbed	DoS, Fuzzing, Spoofing	.csv	6	CAN/OBD-II	Driving profile
HCRL-SA	2019	Real	Testbed	Flooding, Fuzzy, Malfunction	.csv	10	CAN/OBD-II	IDS
TU CAN v2 [273]	2019	Real/synthetic	Testbed	diagnostic, fuzzing, replay, suspension, DoS	.txt	-	CAN/OBD-II	IDS
SynCAN [274]	2019	Synthetic	Simulation	plateau, continuous, playback, suppress, and flooding	.csv	7	CAN	IDS
HCRL A&D [102]	2020	Real	Testbed	Flooding, spoofing, replay, and fuzzing	.csv	6	CAN/OBD-II	IDS
ROAD [73]	2020	Real/synthetic	Testbed	fuzzing, targeted ID, accelerator attacks	.txt	-	CAN/OBD-II	IDS
AEGIS CAN [272]	2020	Real	Testbed	only benign data	.hdf	-	CAN/OBD-II	IDS
CrySyS Lab [271]	2021	Real	Testbed	benign data	.csv	-	CAN + GPS	IDS
HCRL-SET [270]	2021	Real	Testbed	-	.csv	-	Kvaser CAN	Driving profile
CICEV2023 [275]	2023	Synthetic	Simulation	DDoS	.csv	7	-	EV Charging IDS
CT&T [276]	2023	Real	Testbed	9 attacks (DoS, fuzzy, spoofing, etc.)	.csv	4	-	CAN IDS

exploring and advancing intelligent transportation systems and interconnected vehicular technologies.

6) ARTERY

[282] environment is a sturdy platform utilized to evaluate and execute vehicular communication systems, focusing on the vehicle's viewpoint. The ETSI ITS-G5 protocol stack, which is the European standard for V2X communications, enables vehicles to establish communication with both other vehicles and infrastructure. Artery facilitates the sharing of vehicle status, exchange of environmental information, and transmission of driver intentions among vehicles. Data exchange facilitates collaborative driving techniques, improving traffic efficacy, safety, and ecological implications. Artery utilizes the OMNeT++ and SUMO traffic simulators to facilitate the requisite network and traffic simulation functionalities. The vehicle's ability to simulate realistic network and traffic conditions is ensured by its compatibility with established platforms.

VII. OPEN PROBLEMS AND FUTURE WORK

Numerous unresolved matters have been identified within the domain of In-Vehicle NIDS (IVN IDSs). The following enumeration outlines five significant research directions.

A. DATASETS

The currently available datasets for evaluating IDS in IVNs are listed in Table VI. These datasets vary in different aspects, and the contributors have made a notable attempt to create more diverse datasets with new attack types and patterns. However, several limitations remain, such as sufficient diverse attack-free data from different sources (vehicle types, CAN bus configurations, etc.), new attack types, various attack patterns, and fidelity. IDSs are generally anomaly-based, classifying traffic as "normal" or "anomalous." During training, they establish a profile of "normal" traffic and flag deviations during testing. Thus, a diverse dataset with realistic automotive attacks and publicly available more diverse datasets with known and unknown attack combinations can expedite the research outcomes. The review of existing literature shows that the currently available public datasets are less challenging, and even simple ML models can achieve very high accuracy over these datasets. However, the performance of these ML/AI-based IDS in practical scenarios may not be guaranteed. Since IVNs require very high reliability, this may hinder real-world deployments of such schemes. Another issue with the current datasets is that most of these are collected from testbeds, and attacks are often simulated. This lack of fidelity is another shortcoming that can not extrapolate these IDSs to more challenging high-fidelity realistic scenarios.

B. ACCURACY REQUIREMENTS OF COMMERCIAL IDS

Improving the accuracy and rapidity of IDSs for IVNs is a pressing concern in the field of IoV IDS design. Identifying and differentiating between malevolent cyber assaults and strange occurrences such as sudden halts, collisions, and software upgrades within the context of an IVN will pose a formidable area of research. In the context of IDS techniques applied to the signal layer, such as frequency-based IDS, it is not feasible to differentiate between anomalous and malicious messages. The IDS implemented in the functional layer may address this particular concern. Integrating features into a forthcoming IDS design could be a viable approach to tackling this issue. This is because current IDS solutions are limited in their ability to address only certain types and scenarios of attacks.

C. DIVERSITY AND INTEROPERABILITY

The automotive industry's electronic components are currently sourced from various supply chain segments, with distinct vendors responsible for developing disparate distributed subsystems. The present scenario presents a formidable obstacle to implementing system security measures. Security vulnerabilities often manifest at the interfaces between code segments developed by disparate programmers. Establishing standardized protocols to manage and synchronize supply chains is imperative. For instance, the CAN bus implementation varies across different vendors; thus, an IDS system that performs well for one vendor may not perform similarly across all vendors' IVNs.

D. RELIABILITY AND ROBUSTNESS

The use of AI algorithms presents distinct benefits in implementing anonymous intrusion detection. Regrettably, two obstacles are encountered by the researchers. Firstly, the issue of deploying ML algorithms within an IVN system that has restricted computing resources. Secondly, the challenge of acquiring data sets that are conducive to effective training.

E. THE ROADMAP TO STANDARDIZED IDS

Future research endeavors should investigate the feasibility of implementing the scrutinized IDS methodologies for CAN in these recently developed protocols. It is possible that certain IDS approaches that have been reviewed could be potentially implemented in these networks. As the research in this domain advances, the malevolent actors and their assaults will also evolve. The aforementioned process necessitates ongoing revisions to threat models to detect emerging vulnerabilities and attacks, followed by corresponding modifications to IDS to mitigate them. Despite its inherent lack of security, the primary concern persists that CAN has become a contemporary standard for vehicular communication. This underscores the necessity of incorporating security measures throughout the entire design process. DRL showed significant results in such a non-standard atmosphere. DRL could be a good candidate for designing global IDS for IoVs protocols, which can be adapted to learn and achieve high accuracy in such an environment.

VIII. CONCLUSION

This survey analyzes the techniques utilized in implementing IDSs for safeguarding automotive systems. The survey includes an overview of the methods and a comprehensive discussion of their merits and demerits. Our endeavor involved an effort to disambiguate and consolidate the notion of anomalies and intrusion detection in the context of automotive security. The initial step involves identifying threat models on automotive security, focusing on recognizing threats that have a universal impact on all vehicles rather than being limited to a particular model. From a technical standpoint, IDSs can effectively identify intrusions on the CAN bus. Various implementations of anomaly detection techniques can identify distinct categories of anomalies. Contemporary methodologies prioritize identifying message injection attacks as they constitute the primary avenue for malicious actors seeking to manipulate vehicular behavior. Establishing a connection between detection and response is imperative to facilitate prevention. An efficient IDS for cyber-physical systems must be able to respond actively to cyberattacks. The methods for detecting attacks have been identified; however, further research is required to address the mitigation of said attacks after their detection.

With the development of additional communication protocols, including FlexRay, LIN, and Ethernet, the complexity of IVNs keeps growing [30]. Vehicles now have new vulnerabilities as a result of these new protocols. Future work should focus on determining whether the IDS strategies for CAN that were reviewed can be used with these new protocols. Some of the reviewed IDS techniques might hypothetically be utilized on these new networks. Attackers and their assaults will advance along with this area of survey. To discover new vulnerabilities and assaults in this evolution, threat models must be updated often. IDS must then be modified to counteract these changes. The core problem still exists in the fact that CAN, although fundamentally unsafe, is a current car standard, demonstrating the need to include security in all design phases.

ACKNOWLEDGMENT

The findings herein reflect the work, and are solely the responsibility of the authors. Open Access funding provided by the Qatar National Library.

REFERENCES

[1] S. Checkoway et al., "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. USENIX Secur. Symp.*, 2011, vol. 4, no. 447-462, Art. no. 2021.

[2] "Introduction to the LIN bus Kvaser," 2010. [Online].Available: https://www.kvaser.com/about-can/can-standards/linbus/

[3] R. Makowitz and C. Temple, "Flexray-A communication network for automotive control systems," in *Proc. IEEE Int. Workshop Factory Commun. Syst.*, 2006, pp. 207–212.

[4] A. Sumorek and M. Buczaj, "New elements in vehicle communication "media oriented systems transport" protocol," *Teka Komisji Motoryzacji i Energetyki Rolnictwa*, vol. 12, no. 1, 2012.

[5] 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. 21266–21289, 2019.

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

[7] F. Yu, D.-F. Li, and D. Crolla, "Integrated vehicle dynamics control–state-of-the art review," in *Proc. IEEE Veh. Power Propulsion Conf.*, 2008, pp. 1–6.

[8] S. Tsugawa, "Inter-vehicle communications and their applications to intelligent vehicles: An overview," in *Proc. IEEE Intell. Veh. Symp.*, 2002, vol. 2, pp. 564–569.

[9] H. Lenz, C. Wagner, and R. Sollacher, "Multi-anticipative car-following model," *Eur. Phys. J. B-Condens. Matter Complex Syst.*, vol. 7, pp. 331–335, 1999.

[10] M. Levi, Y. Allouche, and A. Kontorovich, "Advanced analytics for connected car cybersecurity," in *Proc. IEEE 87th Veh. Technol. Conf.*, 2018, pp. 1–7.

[11] E. Aliwa, O. Rana, C. Perera, and P. Burnap, "Cyberattacks and countermeasures for in-vehicle networks," *ACM Comput. Surv.*, vol. 54, no. 1, pp. 1–37, 2021.

[12] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Veh. Commun.*, vol. 23, 2020, Art. no. 100214.

[13] W. Wu, G. Zhang, C. Zou, L. Zhang, and Q. Wang, “IDH-CAN: A hardware-based ID hopping CAN mechanism with enhanced security for automotive real-time applications,” *IEEE Access*, vol. 6, pp. 54607–54623, 2018.

[14] M. Müter and N. Asaj, “Entropy-based anomaly detection for in-vehicle networks,” in *Proc. IEEE Intell. Veh. Symp.*, 2011, pp. 1110–1115.

[15] A. Tomlinson, J. Bryans, and S. A. Shaikh, “Towards viable intrusion detection methods for the automotive controller area network,” in *Proc. 2nd ACM Comput. Sci. Cars Symp.*, 2018, pp. 1–9.

[16] C. Young, J. Zambreno, H. Olufowobi, and G. Bloom, “Survey of automotive controller area network intrusion detection systems,” *IEEE Des. Test*, vol. 36, no. 6, pp. 48–55, Dec. 2019.

[17] G. Dupont, J.Den Hartog, S. Etalle, and A. Lekidis, “A survey of network intrusion detection systems for controller area network,” in *Proc. IEEE Int. Conf. Veh. Electron. Saf.*, 2019, pp. 1–6.

[18] S.-F. Lokman, A. T. B. Othman, and M.-H. Abu-Bakar, “Intrusion detection system for automotive controller area network (CAN) bus system: A review,” *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, pp. 1–17, 2019. [Online]. Available: https://api.semanticscholar.org/CorpusID:198119754

[19] W. Wu et al., “A survey of intrusion detection for in-vehicle networks,” *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 919–933, Mar. 2020.

[20] 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, 2022, Art. no. 1072.

[21] 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 Comput. Surv.*, vol. 55, no. 11, pp. 1–40, Feb. 2023.

[22] K. Arshad et al., “Deep reinforcement learning for anomaly detection: A systematic review,” *IEEE Access*, vol. 10, pp. 124017–124035, 2022.

[23] J. Nagarajan et al., “Machine learning based intrusion detection systems for connected autonomous vehicles: A survey,” *Peer-to-Peer Netw. Appl.*, vol. 16, pp. 2153–2185, 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:259695347

[24] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, “BPDS: A blockchain based privacy-preserving data sharing for electronic medical records,” *IEEE Global Commun. Conf. (GLOBECOM)*, pp. 1–6, 2018.

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

[26] A. M. Wyglinski, X. Huang, T. Padir, L. Lai, T. R. Eisenbarth, and K. Venkatasubramanian, “Security of autonomous systems employing embedded computing and sensors,” *IEEE Micro*, vol. 33, no. 1, pp. 80–86, Jan./Feb. 2013.

[27] M. Shavit, A. Gryc, and R. Miucic, “Firmware update over the air (FOTA) for automotive industry,” SAE, Warrendale, PA, USA, Tech. Rep. 2007-01-3523, 2007, p. 9. [Online]. Available: https://doi.org/10.4271/2007-01-3523

[28] T. L. Willke, P. Tientrakool, and N. F. Maxemchuk, “A survey of inter-vehicle communication protocols and their applications,” *IEEE Commun. Surv. Tut.*, vol. 11, no. 2, pp. 3–20, Secondquarter 2009.

[29] S. Sharma and A. Kaul, “A survey on intrusion detection systems and honeypot based proactive security mechanisms in VANETs and VANET cloud,” *Veh. Commun.*, vol. 12, pp. 138–164, 2018.

[30] J. Wang, J. Liu, and N. Kato, “Networking and communications in autonomous driving: A survey,” *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1243–1274, Secondquarter 2019.

[31] S. C. HPL, “Introduction to the controller area network (CAN),” Appl. Rep. SLOA101B, pp. 1–17, Aug. 2002.

[32] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, “A comprehensive survey on vehicular ad hoc network,” *J. Netw. Comput. Appl.*, vol. 37, pp. 380–392, 2014.

[33] O. Avatefipour and H. Malik, “State-of-the-art survey on in-vehicle network communication (CAN-bus) security and vulnerabilities,” 2018, *arXiv:1802.01725*.

[34] B. Groza and P.-S. Murvay, “Security solutions for the controller area network: Bringing authentication to in-vehicle networks,” *IEEE Veh. Technol. Mag.*, vol. 13, no. 1, pp. 40–47, Mar. 2018.

[35] R. Bosch et al., “CAN specification version 2.0,” Robert Bosch GmbH, Gerlingen, Germany, Tech. Rep., 1991.

[36] K.-T. Kim, J.-S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, “Cybersecurity for autonomous vehicles: Review of attacks and defense,” *Comput. Secur.*, vol. 103, 2021, Art. no. 102150.

[37] S. Abbott-McCune and L. A. Shay, “Intrusion prevention system of automotive network CAN bus,” in *Proc. IEEE Int. Carnahan Conf. Secur. Technol.*, 2016, pp. 1–6.

[38] C. Miller and C. Valasek, “CAN message injection,” *OG Dynamite Ed.*, 2016.

[39] T. Huang, J. Zhou, and A. Bytes, “ATG: An attack traffic generation tool for security testing of in-vehicle CAN bus,” in *Proc. 13th Int. Conf. Availability, Rel. Secur.*, 2018, pp. 1–6.

[40] A. Payne, “Fashion futuring in the anthropocene: Sustainable fashion as ‘taming’ and ‘rewilding’,” *Fashion Theory*, vol. 23, no. 1, pp. 5–23, 2019.

[41] S. A. Almalki and J. Song, “A review on data falsification-based attacks in cooperative intelligent transportation systems,” *Int. J. Comput. Sci. Secur.*, vol. 14, pp. 22–37, 2020.

[42] A. Derhab, M. Belaoued, I. Mohiuddin, F. Kurniawan, and M. K. Khan, “Histogram-based intrusion detection and filtering framework for secure and safe in-vehicle networks,” *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2366–2379, Mar. 2022.

[43] C. Miller and C. Valasek, “Remote exploitation of an unaltered passenger vehicle,” *Black Hat USA*, vol. 2015, no. S 91, pp. 1–91, 2015.

[44] K. Iehira, H. Inoue, and K. Ishida, “Spoofing attack using bus-off attacks against a specific ECU of the CAN bus,” in *Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf.*, 2018, pp. 1–4.

[45] F. Martinelli, F. Mercaldo, V. Nardone, and A. Santone, “Car hacking identification through fuzzy logic algorithms,” in *Proc. IEEE Int. Conf. Fuzzy Syst.*, 2017, pp. 1–7.

[46] D. S. Fowler, J. Bryans, M. Cheah, P. Wooderson, and S. A. Shaikh, “A method for constructing automotive cybersecurity tests, a CAN fuzz testing example,” in *Proc. IEEE 19th Int. Conf. Softw. Qual., Rel. Secur. Companion*, 2019, pp. 1–8.

[47] M. E. Verma et al., “A comprehensive guide to CAN IDS data and introduction of the road dataset,” *PLoS One*, vol. 19, no. 1, 2024, Art. no. e0296879.

[48] D. Zelle, T. Lauser, D. Kern, and C. Krauß, “Analyzing and securing SOME/IP automotive services with formal and practical methods,” in *Proc. 16th Int. Conf. Availability, Rel. Secur.,*, 2021, pp. 1–20. [Online]. Available: https://doi.org/10.1145/3465481.3465748

[49] M. Bozdal, M. Samie, S. Aslam, and I. Jennions, “Evaluation of CAN bus security challenges,” *Sensors*, vol. 20, no. 8, 2020, Art. no. 2364.

[50] T. Hoppe and J. Dittman, “Sniffing/replay attacks on CAN buses: A simulated attack on the electric window lift classified using an adapted CERT taxonomy,” in *Proc. 2nd Workshop Embedded Syst. Secur.*, 2007, pp. 1–6.

[51] C. Miller and C. Valasek, “Remote exploitation of an unaltered passenger vehicle,” in *Proc. Black Hat USA*, 2015, pp. 1–91.

[52] U. E. Larson and D. K. Nilsson, “Securing vehicles against cyber attacks,” in *Proc. 4th Annu. Workshop Cyber Secur. Inf. Intell. Res.: Developing Strategies Meet Cyber Secur. Inf. Intell. Challenges Ahead*, 2008, pp. 1–3.

[53] A. S. Siddiqui, Y. Gui, J. Plusquellic, and F. Saqib, “Secure communication over CANBus,” in *Proc. IEEE 60th Int. Midwest Symp. Circuits Syst.*, 2017, pp. 1264–1267.

[54] V. Verendel, D. K. Nilsson, U. E. Larson, and E. Jonsson, “An approach to using honeypots in in-vehicle networks,” in *Proc. IEEE 68th Veh. Technol. Conf.*, 2008, pp. 1–5.

[55] R. A. Kemmerer and G. Vigna, “Intrusion detection: A brief history and overview,” *Computer*, vol. 35, no. 4, pp. supl27–supl30, Apr. 2002.

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

[57] I. Nazakat and K. Khurshid, “Intrusion detection system for invehicular communication,” in *Proc. IEEE 15th Int. Conf. Emerg. Technol.*, 2019, pp. 1–6.

[58] V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection: A survey,” *ACM Comput. Surv.*, vol. 41, no. 3, pp. 1–58, 2009.

[59] S. Jin, J.-G. Chung, and Y. Xu, “Signature-based intrusion detection system (IDS) for in-vehicle CAN bus network,” in *Proc. IEEE Int. Symp. Circuits Syst.*, 2021, pp. 1–5.

[60] A. Bezemskij, G. Loukas, D. Gan, and R. Anthony, "Detecting cyberphysical threats in an autonomous robotic vehicle using Bayesian networks," in *Proc. IEEE Int. Conf. Internet Things, IEEE Green Comput. Commun., IEEE Cyber, Phys. Social Comput., IEEE Smart Data*, 2017, pp. 98–103.

[61] A. Broggi, P. Cerri, M. Felisa, M. C. Laghi, L. Mazzei, and P. P. Porta, "The vislab intercontinental autonomous challenge: An extensive test for a platoon of intelligent vehicles," *Int. J. Veh. Auton. Syst.*, vol. 10, no. 3, pp. 147–164, 2012.

[62] D. Wu et al., "ADDSEN: Adaptive data processing and dissemination for drone swarms in urban sensing," *IEEE Trans. Comput.*, vol. 66, no. 2, pp. 183–198, Feb. 2017.

[63] S. Martini et al., "Distributed motion misbehavior detection in teams of heterogeneous aerial robots," *Robot. Auton. Syst.*, vol. 74, pp. 30–39, 2015.

[64] B. Lampe and W. Meng, "A survey of deep learning-based intrusion detection in automotive applications," *Expert Syst. With Appl.*, vol. 221, 2023, Art. no. 119771.

[65] G. Loukas, Y. Yoon, G. Sakellari, T. Vuong, and R. Heartfield, "Computation offloading of a vehicle's continuous intrusion detection workload for energy efficiency and performance," *Simul. Modelling Pract. Theory*, vol. 73, pp. 83–94, 2017.

[66] L. Zhang and H. Han, "An admission control method for CAN networks based on voltage fingerprinting," in *Proc. SPIE*, 2023, vol. 12714, pp. 106–112.

[67] H. J. Jo and W. Choi, "A survey of attacks on controller area networks and corresponding countermeasures," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 6123–6141, Jul. 2022.

[68] A. Tomlinson, "Detecting cyber attacks on the automotive controller area network," Ph.D. dissertation, Coventry Univ., Coventry, U.K., 2020.

[69] L. Da Bernarda, L. Santos, R. L. Costa, and C. Rabadão, "Automotive controller area network intrusion detection systems," in *Proc. Inf. Secur. Privacy Smart Devices: Tools, Methods, Appl. IGI Glob.*, 2023, pp. 96–121.

[70] "Intrusion, anomaly, and attack detection in smart vehicles," *Microprocessors Microsystems*, vol. 96, 2023, Art. no. 104726.

[71] M. Weber, S. Klug, E. Sax, and B. Zimmer, "Embedded hybrid anomaly detection for automotive CAN communication," in *Proc. 9th Eur. Congr. Embedded Real Time Softw. Syst.*, 2018, pp. 1–10.

[72] 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.

[73] M. E. Verma, M. D. Iannacone, R. A. Bridges, S. C. Hollifield, B. Kay, and F. L. Combs, "Road: The real ORNL automotive dynamometer controller area network intrusion detection dataset (with a comprehensive CAN IDS dataset survey & guide)," 2012, *arXiv:2012.14600*.

[74] G. Loukas, E. Karapistoli, E. Panaousis, P. Sarigiannidis, A. Bezemskij, and T. Vuong, "A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles," *Ad Hoc Netw.*, vol. 84, pp. 124–147, 2019.

[75] Y. Wang, Z. Ye, P. Wan, and J. Zhao, "A survey of dynamic spectrum allocation based on reinforcement learning algorithms in cognitive radio networks," *Artif. Intell. Rev.*, vol. 51, no. 3, pp. 493–506, 2019.

[76] N. Abdi, A. Albaseer, and M. Abdallah, "The role of deep learning in advancing proactive cybersecurity measures for smart grid networks: A survey," *IEEE Internet Things J.*, vol. 11, no. 9, pp. 16398–16421, May 2024.

[77] A. Theissler, "Anomaly detection in recordings from in-vehicle networks," *Big Data Appl.*, vol. 23, pp. 23–35, 2014.

[78] V. N. Vapnik, "An overview of statistical learning theory," *IEEE Trans. Neural Netw.*, vol. 10, no. 5, pp. 988–999, Sep. 1999.

[79] D. M. Abdullah and A. M. Abdulazeez, "Machine learning applications based on SVM classification a review," *Qubahan Academic J.*, vol. 1, no. 2, pp. 81–90, 2021.

[80] T. Moulahi, S. Zidi, A. Alabdulatif, and M. Atiquzzaman, "Comparative performance evaluation of intrusion detection based on machine learning in in-vehicle controller area network bus," *IEEE Access*, vol. 9, pp. 99595–99605, 2021.

[81] M. Al-Saud, A. M. Eltamaly, M. A. Mohamed, and A. Kavousi-Fard, "An intelligent data-driven model to secure intravehicle communications based on machine learning," *IEEE Trans. Ind. Electron.*, vol. 67, no. 6, pp. 5112–5119, Jun. 2020.

[82] O. Avatefipour et al., "An intelligent secured framework for cyberattack detection in electric vehicles' CAN bus using machine learning," *IEEE Access*, vol. 7, pp. 127580–127592, 2019.

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

[84] Y.-Y. Song and L. Ying, "Decision tree methods: Applications for classification and prediction," *Shanghai Arch. Psychiatry*, vol. 27, no. 2, pp. 130–135, 2015.

[85] L. Yang, A. Moubayed, I. Hamieh, and A. Shami, "Tree-based intelligent intrusion detection system in internet of vehicles," in *Proc. IEEE Glob. Commun. Conf.*, 2019, pp. 1–6.

[86] M. L. Han, B. I. Kwak, and H. K. Kim, "Event-triggered interval-based anomaly detection and attack identification methods for an in-vehicle network," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, no. 2021, pp. 2941–2956, 2021.

[87] S. C. Kalkan and O. K. Sahingoz, "In-vehicle intrusion detection system on controller area network with machine learning models," in *Proc. IEEE 11th Int. Conf. Comput., Commun. Netw. Technol.*, 2020, pp. 1–6.

[88] D. Tian et al., "An intrusion detection system based on machine learning for CAN-bus," in *Proc. 3rd Int. Conf. Ind. Netw. Intell. Syst.*, 2018, pp. 285–294.

[89] S. S. Dhaliwal, A.-A. Nahid, and R. Abbas, "Effective intrusion detection system using XGboost," *Information*, vol. 9, no. 7, 2018, Art. no. 149.

[90] G. Kim, S. Lee, and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," *Expert Syst. With Appl.*, vol. 41, no. 4, pp. 1690–1700, 2014.

[91] A. R. Gad, A. A. Nashat, and T. M. Barkat, "Intrusion detection system using machine learning for vehicular ad hoc networks based on TON-IoT dataset," *IEEE Access*, vol. 9, pp. 142206–142217, 2021.

[92] A. Anjum, P. Agbaje, S. Hounsinou, and H. Olufowobi, "In-vehicle network anomaly detection using extreme gradient boosting machine," in *Proc. IEEE 11th Mediterranean Conf. Embedded Comput.*, 2022, pp. 1–6.

[93] J. Zhu and W. Hu, "Recent advances in Bayesian machine learning," *J. Comput. Res. Dev*, vol. 52, no. 1, pp. 16–26, 2015.

[94] I. Koch, K. Naito, and H. Tanaka, "Kernel Naive Bayes discrimination for high-dimensional pattern recognition," *Australian New Zealand J. Statist.*, vol. 61, no. 4, pp. 401–428, 2019.

[95] H. Zhang, N. Cheng, Y. Zhang, and Z. Li, "Label flipping attacks against Naive Bayes on spam filtering systems," *Appl. Intell.*, vol. 51, pp. 4503–4514, 2021.

[96] R. Islam, M. K. Devnath, M. D. Samad, and S. M. J. Al Kadry, "GGNB: Graph-based Gaussian Naive Bayes intrusion detection system for CAN bus," *Veh. Commun.*, vol. 33, 2022, Art. no. 100442.

[97] A. R. Nair, N. K. Jadav, R. Gupta, and S. Tanwar, "Ai-empowered secure data communication in V2X environment with 6G network," in *Proc. IEEE Conf. Comput. Commun. Workshops*, 2022, pp. 1–6.

[98] B. S. Bari, K. Yelamarthi, and S. Ghafoor, "Intrusion detection in vehicle controller area network (CAN) bus using machine learning: A comparative performance study," *Sensors*, vol. 23, no. 7, 2023, Art. no. 3610.

[99] O. Y. Al-Jarrah, O. A. Ramadan, B. Alsaify, and S. Alkhushayni, "Comparative evaluation of machine learning-based controller area network intrusion detection systems," in *Proc. IEEE 14th Int. Conf. Inf. Commun. Syst.*, 2023, pp. 978–986.

[100] H. Sun et al., "CCID-CAN: Cross-chain intrusion detection on CAN bus for autonomous vehicles," *IEEE Internet Things J.*, early access, Apr. 24, 2024, doi: 10.1109/JIOT.2024.3393122.

[101] E. Alalwany and I. Mahgoub, "Classification of normal and malicious traffic based on an ensemble of machine learning for a vehicle can-network," *Sensors*, vol. 22, no. 23, 2022, Art. no. 9195. [Online]. Available: https://www.mdpi.com/1424-8220/22/23/9195

[102] H. Kang, B. Kwak, Y. H. Lee, H. Lee, H. Lee, and H. K. Kim, "Car hacking: Attack & defense challenge 2020 dataset," *EEE Dataport*, IEEE Piscataway, NJ, USA, vol. 10, 2021.

[103] A. K. Dwivedi, "Anomaly detection in intra-vehicle networks," 2022, *arXiv:2205.03537*.

[104] S. Purohit and M. Govindarasu, "Ml-based anomaly detection for intra-vehicular CAN-bus networks," in *Proc. IEEE Int. Conf. Cyber Secur. Resilience*, 2022, pp. 233–238.

[105] D. Divya Raj, G. Renjith, and S. Aji, "A lightweight intrusion detection model for in-vehicular CAN networks," in *Proc. 3rd Int. Conf. Sustain. Expert Syst.*, 2023, pp. 665–678.

[106] S. C. Kalkan and O. K. Sahingoz, "In-vehicle intrusion detection system on controller area network with machine learning models," in *Proc. IEEE 11th Int. Conf. Comput., Commun., Netw. Technol.*, 2020, pp. 1–6.

[107] A. Alfardus and D. B. Rawat, "Intrusion detection system for CAN bus in-vehicle network based on machine learning algorithms," in *Proc. IEEE 12th Annu. Ubiquitous Comput., Electron., Mobile Commun. Conf.*, 2021, pp. 0944–0949.

[108] F. Amato, L. Coppolino, F. Mercaldo, F. Moscato, R. Nardone, and A. Santone, "CAN-bus attack detection with deep learning," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5081–5090, Aug. 2021.

[109] K. Gao, H. Huang, L. Liu, R. Du, and J. Zhang, "A multi-attention based CNN-BiLSTM intrusion detection model for in-vehicle networks," in *Proc. IEEE Int. Conf. Parallel Distrib. Process. With Appl., Big Data Cloud Comput., Sustain. Comput. Commun., Social Comput. Netw.*, 2023, pp. 809–816.

[110] P. Mansourian, N. Zhang, A. Jaekel, M. Zamanirafe, and M. Kneppers, "Anomaly detection for connected autonomous vehicles using LSTM and Gaussian Naïve Bayes," in *Wireless and Satellite Systems*, J. Zhao, Ed., Cham, Switzerland: Springer Nature Switzerland, 2023, pp. 31–43.

[111] M. Kneib and C. Huth, "Scission: Signal characteristic-based sender identification and intrusion detection in automotive networks," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, New York, NY, USA,, 2018, pp. 787–800.

[112] Y. Wu, D. Wei, and J. Feng, "Network attacks detection methods based on deep learning techniques: A survey," *Secur. Commun. Netw.*, vol. 2020, pp. 1–17, 2020.

[113] Y. Dong, K. Chen, Y. Peng, and Z. Ma, "Comparative study on supervised versus semisupervised machine learning for anomaly detection of in-vehicle CAN network," in *Proc. IEEE 25th Int. Conf. Intell. Transp. Syst. (ITSC)*, 2022, pp. 2914–2919.

[114] H. Teryak, A. Albaseer, M. Abdallah, S. Al-Kuwari, and M. Qaraqe, "Double-edged defense: Thwarting cyber attacks and adversarial machine learning in IEC 60870-5-104 smart grids," *IEEE Open J. Ind. Electron. Soc.*, vol. 4, pp. 629–642, 2023.

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

[116] W. Wang et al., "HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection," *IEEE Access*, vol. 6, pp. 1792–1806, 2018.

[117] Z. Tan, A. Jamdagni, X. He, P. Nanda, R. P. Liu, and J. Hu, "Detection of denial-of-service attacks based on computer vision techniques," *IEEE Trans. Comput.*, vol. 64, no. 9, pp. 2519–2533, Sep. 2015.

[118] J. Gu et al., "Recent advances in convolutional neural networks," *Pattern Recognit.*, vol. 77, pp. 354–377, 2018.

[119] D. Ariu, R. Tronci, and G. Giacinto, "HMMPayL: An intrusion detection system based on hidden Markov models," *Comput. Secur.*, vol. 30, no. 4, pp. 221–241, 2011.

[120] R. Hu, Z. Wu, Y. Xu, and T. Lai, "Multi-attack and multi-classification intrusion detection for vehicle-mounted networks based on mosaic-coded convolutional neural network," *Sci. Rep.*, vol. 12, no. 1, 2022, Art. no. 6295.

[121] J. Sekar, P. Aruchamy, H. Sulaima Lebbe Abdul, A. S. Mohammed, and S. Khamuruddeen, "An efficient clinical support system for heart disease prediction using TANFIS classifier," *Comput. Intell.*, vol. 38, no. 2, pp. 610–640, 2022.

[122] G. Baldini, "Intrusion detection systems in in-vehicle networks based on bag-of-words," in *Proc. IEEE Proc. 5th Cyber Secur. Netw. Conf.*, 2021, pp. 41–48.

[123] H. M. Song and H. K. Kim, "Self-supervised anomaly detection for in-vehicle network using noised pseudo normal data," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1098–1108, Feb. 2021.

[124] K. Desta, S. Ohira, I. Arai, and K. Fujikawa, "Rec-CNN: In-vehicle networks intrusion detection using convolutional neural networks trained on recurrence plots," *Veh. Commun.*, vol. 35, 2022, Art. no. 100470.

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

[126] M. E. Eddin et al., "Fine-tuned RNN-based detector for electricity theft attacks in smart grid generation domain," *IEEE Open J. Ind. Electron. Soc.*, vol. 3, pp. 733–750, 2022.

[127] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[128] A. Albaseer and M. Abdallah, "Fine-tuned LSTM-based model for efficient honeypot-based network intrusion detection system in smart grid networks," in *Proc. IEEE 5th Int. Conf. Commun., Signal Process., Appl.*, 2022, pp. 1–6.

[129] S. A. Althubiti, E. M. Jones, and K. Roy, "LSTM for anomaly-based network intrusion detection," in *Proc. IEEE 28th Int. Telecommun. Netw. Appl. Conf.*, 2018, pp. 1–3.

[130] M. Ezeddin, A. Albaseer, M. Abdallah, S. Bayhan, M. Qaraqe, and S. Al-Kuwari, "Efficient deep learning based detector for electricity theft generation system attacks in smart grid," in *Proc. IEEE 3rd Int. Conf. Smart Grid Renewable Energy*, 2022, pp. 1–6.

[131] A. R. Javed, S. U. Rehman, M. U. Khan, M. Alazab, and T. R. G, "CANintelliIDS: Detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1456–1466, Apr.–Jun. 2021.

[132] M. K. Putchala, "Deep learning approach for intrusion detection system (IDS) in the Internet of Things (IoT) network using gated recurrent neural networks (GRU)," Wright State Univ., 2017.

[133] M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PLoS One*, vol. 11, no. 6, 2016, Art. no. e0155781.

[134] J. Zhang, F. Li, H. Zhang, R. Li, and Y. Li, "Intrusion detection system using deep learning for in-vehicle security," *Ad Hoc Netw.*, vol. 95, 2019, Art. no. 101974.

[135] J. Lin, Y. Wei, W. Li, and J. Long, "Intrusion detection system based on deep neural network and incremental learning for in-vehicle CAN networks," in *Proc. Int. Conf. Ubiquitous Secur.*, 2021, pp. 255–267.

[136] S. Boumiza and R. Braham, "In-vehicle network intrusion detection using DNN with ReLU activation function," in *Proc. IEEE Int. Conf. Cyberworlds*, 2023, pp. 410–416.

[137] F. Fenzl, R. Rieke, and A. Dominik, "In-vehicle detection of targeted CAN bus attacks," in *Proc. 16th Int. Conf. Availability, Rel., Secur.* , 2021, pp. 1–7.

[138] K.-T. Cho and K. G. Shin, "Viden: Attacker identification on in-vehicle networks," in *Proc. Conf. Comput. Commun. Secur.*, 2017, pp. 1109–1123.

[139] 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 Trans. Inf. Forensics Secur.*, vol. 13, no. 8, pp. 2114–2129, Aug. 2018.

[140] Y. Xun, Y. Zhao, and J. Liu, "VehicleEIDS: A novel external intrusion detection system based on vehicle voltage signals," *IEEE Internet Things J.*, vol. 9, no. 3, pp. 2124–2133, Feb. 2022.

[141] M. Jedh, L. Ben Othmane, N. Ahmed, and B. Bhargava, "Detection of message injection attacks onto the CAN bus using similarities of successive messages-sequence graphs," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, no. 2021, pp. 4133–4146, 2021.

[142] I. A. Khan, N. Moustafa, D. Pi, W. Haider, B. Li, and A. Jolfaei, "An enhanced multi-stage deep learning framework for detecting malicious activities from autonomous vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 12, pp. 25469–25478, Dec. 2022.

[143] K. Zhu, Z. Chen, Y. Peng, and L. Zhang, "Mobile edge assisted literal multi-dimensional anomaly detection of in-vehicle network using LSTM," *IEEE Trans. Veh. Technol.*, vol. 68, no. 5, pp. 4275–4284, May 2019.

[144] L. Gao, F. Li, X. Xu, and Y. Liu, "Intrusion detection system using SOEKS and deep learning for in-vehicle security," *Cluster Comput.*, vol. 22, no. 6, pp. 14721–14729, 2019.

[145] O. Vinyals, C. Blundell, T. Lillicrap, K. Kavukcuoglu, and D. Wierstra, "Matching networks for one shot learning," in *Proc. Adv. Neural Inf. Process. Syst.*, 2016, pp. 3630–3638.

[146] S. Tariq, S. Lee, H. K. Kim, and S. S. Woo, "CAN-ADF: The controller area network attack detection framework," *Comput. Secur.*, vol. 94, 2020, Art. no. 101857.

[147] 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 *Proc. IEEE/IFIP 48th Annu. Int. Conf. Dependable Syst. Netw. Workshops*, 2018, pp. 231–238.

[148] L. Kang and H. Shen, “A transfer learning based abnormal CAN bus message detection system,” in *Proc. IEEE 18th Int. Conf. Mobile Ad Hoc Smart Syst.*, 2021, pp. 545–553.

[149] P. Cheng, Z. Wu, and G. Liu, “MKF-ADS: Multi-knowledge fusion based self-supervised anomaly detection system for control area network,” *IEEE Trans. Veh. Technol.*, vol. 1, no. 1, pp. 1–10, 2024.

[150] C. Xu, J. Shen, X. Du, and F. Zhang, “An intrusion detection system using a deep neural network with gated recurrent units,” *IEEE Access*, vol. 6, pp. 48697–48707, 2018.

[151] C. R. Kishore, D. C. Rao, J. Nayak, and H. S. Behera, “Intelligent intrusion detection framework for anomaly-based CAN bus network using bidirectional long short-term memory,” *J. Inst. Eng. (INDIA): Ser. B*, vol. 105, pp. 541–564, 2024. [Online]. Available: https://doi.org/10.1007/s40031-023-00987-9

[152] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, “Learning representations by back-propagating errors,” *Nature*, vol. 323, no. 6088, pp. 533–536, 1986.

[153] Y. Zhang, K. Li, K. Li, L. Wang, B. Zhong, and Y. Fu, “Image super-resolution using very deep residual channel attention networks,” in *Proc. Eur. Conf. Comput. Vis.*, 2018, pp. 286–301.

[154] Y. Duan, C. Xu, J. Pei, J. Han, and C. Li, “Pre-train and plug-in: Flexible conditional text generation with variational auto-encoders,” in *Proc. 58th Annu. Meeting Assoc. Comput. Linguistics*, 2020, pp. 253–262.

[155] W. Zhou, H. Fu, and S. Kapoor, “Canguard: Practical intrusion detection for in-vehicle network via unsupervised learning,” in *Proc. IEEE/ACM Symp. Edge Comput.*, 2021, pp. 454–458.

[156] S. Longari, D. H. N. Valcarcel, M. Zago, M. Carminati, and S. Zanero, “CANnolo: An anomaly detection system based on LSTM autoencoders for controller area network,” *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 2, pp. 1913–1924, Jun. 2021.

[157] 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 Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4507–4518, Jul. 2021.

[158] E. Kristianto, P.-C. Lin, and R.-H. Hwang, “Sustainable and lightweight domain-based intrusion detection system for in-vehicle network,” *Sustain. Comput.: Inform. Syst.*, vol. 41, 2024, Art. no. 100936.

[159] P. Wei, B. Wang, X. Dai, L. Li, and F. He, “A novel intrusion detection model for the CAN bus packet of in-vehicle network based on attention mechanism and autoencoder,” *Digit. Commun. Netw.*, vol. 9, no. 1, pp. 14–21, 2023.

[160] O. I. Provotar, Y. M. Linder, and M. M. Veres, “Unsupervised anomaly detection in time series using LSTM-based autoencoders,” in *Proc. IEEE Int. Conf. Adv. Trends Inf. Theory*, 2019, pp. 513–517.

[161] V. K. Kukkala, S. V. Thiruloga, and S. Pasricha, “INDRA: Intrusion detection using recurrent autoencoders in automotive embedded systems,” *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 39, no. 11, pp. 3698–3710, Nov. 2020.

[162] A. Vaswani et al., “Attention is all you need,” in *Proc. Adv. Neural Inf. Process. Syst.*, 2017, vol. 30.

[163] S. Edunov, M. Ott, M. Auli, and D. Grangier, “Understanding back-translation at scale,” in *Proc. Conf. Empirical Methods in Natural Lang. Process.*, 2018, p. 489.

[164] M. Al-Mehdhar, A. Albaseer, M. M. Abdallah, and A. Al-Fuqaha, “Charging ahead: A hierarchical adversarial framework for counteracting advanced cyber threats in EV charging stations,” in *Proc. IEEE 99th Veh. Technol. Conf.*, 2024, p. 6.

[165] H. N. C. Neto, J. Hribar, I. Dusparic, D. M. F. Mattos, and N. C. Fernandes, “A survey on securing federated learning: Analysis of applications, attacks, challenges, and trends,” *IEEE Access*, vol. 11, pp. 41928–41953, 2023.

[166] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, “Bert: Pre-training of deep bidirectional transformers for language understanding,” 2018, *arXiv:1810.04805*.

[167] T. Brown et al., “Language models are few-shot learners,” in *Proc. Adv. Neural Inf. Process. Syst.*, 2020, vol. 33, pp. 1877–1901.

[168] A. Radford et al., “Language models are unsupervised multitask learners,” *OpenAI blog*, vol. 1, no. 8, p. 9, 2019.

[169] Y. Liu et al., “RoBERTa: A robustly optimized BERT pretraining approach,” 2019, *arXiv:1907.11692*.

[170] C. Raffel et al., “Exploring the limits of transfer learning with a unified text-to-text transformer,” *J. Mach. Learn. Res.*, vol. 21, no. 1, pp. 5485–5551, 2020.

[171] M. Nam, S. Park, and D. S. Kim, “Intrusion detection method using bi-directional GPT for in-vehicle controller area networks,” *IEEE Access*, vol. 9, pp. 124931–124944, 2021.

[172] T. P. Nguyen, H. Nam, and D. Kim, “Transformer-based attention network for in-vehicle intrusion detection,” *IEEE Access*, vol. 11, pp. 55389–55403, 2023.

[173] A. NasrEldin, A. M. Bahaa-Eldin, and M. A. Sobh, “In-vehicle intrusion detection based on deep learning attention technique,” in *Proc. IEEE 16th Int. Conf. Comput. Eng. Syst.*, 2021, pp. 1–7.

[174] E. Nwafor and H. Olufowobi, “Canbert: A language-based intrusion detection model for in-vehicle networks,” in *Proc. IEEE 21st Int. Conf. Mach. Learn. Appl.*, 2022, pp. 294–299.

[175] N. Alkhatib, M. Mushtaq, H. Ghauch, and J.-L. Danger, “Can-bert do it? Controller area network intrusion detection system based on bert language model,” in *Proc. IEEE/ACS 19th Int. Conf. Comput. Syst. Appl.*, 2022, pp. 1–8.

[176] X. Li and H. Fu, “SecureBERT and LLAMA 2 empowered control area network intrusion detection and classification,” 2023, *arXiv:2311.12074*.

[177] J. Cao et al., “Anomaly detection for in-vehicle network using self-supervised learning with vehicle-cloud collaboration update,” *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 7, pp. 7454–7466, Jul. 2024, doi: 10.1109/TITS.2024.3351438.

[178] V. Cobilean, H. S. Mavikumbure, C. S. Wickramasinghe, B. J. Varghese, T. Pennington, and M. Manic, “Anomaly detection for in-vehicle communication using transformers,” in *Proc. IEEE 49th Annu. Conf. IEEE Ind. Electron. Soc.*, 2023, pp. 1–6.

[179] B. C. Stadie, S. Levine, and P. Abbeel, “Incentivizing exploration in reinforcement learning with deep predictive models,” 2015, *arXiv:1507.00814*.

[180] T. T. Nguyen and V. J. Reddi, “Deep reinforcement learning for cyber security,” *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 34, no. 8, pp. 3779–3795, Aug. 2023.

[181] B.-B. Li, J.-R. Song, Q.-Y. Du, and J.-J. He, “DRL-IDS:deep reinforcement learning based intrusion detection system for industrial Internet of Things,” *Comput. Sci.*, vol. 48, no. 7, pp. 47–54, 2021.

[182] K. Toyoshima, T. Oda, M. Hirota, K. Katayama, and L. Barolli, “A DQN based mobile actor node control in WSAN: Simulation results of different distributions of events considering three-dimensional environment,” in *Proc. Adv. Internet, Data Web Technol.: 8th Int. Conf. Emerg. Internet, Data Web Technol.*, 2020, pp. 197–209.

[183] K. Sethi, R. Kumar, D. Mohanty, and P. Bera, “Robust adaptive cloud intrusion detection system using advanced deep reinforcement learning,” in *Proc. 10th Int. Conf. Secur., Privacy, Appl. Cryptogr. Eng.*, 2020, pp. 66–85.

[184] K. Sethi, E. Sai Rupesh, R. Kumar, P. Bera, and Y. Venu Madhav, “A context-aware robust intrusion detection system: A reinforcement learning-based approach,” *Int. J. Inf. Secur.*, vol. 19, pp. 657–678, 2020.

[185] Q.-V. Dang and T.-H. Vo, “Reinforcement learning for the problem of detecting intrusion in a computer system,” in *Proc. 6th Int. Congr. Inf. Commun. Technol.*, 2022, pp. 755–762.

[186] N. Kumar, S. N. Swain, and C. S. R. Murthy, “A novel distributed Q-learning based resource reservation framework for facilitating D2D content access requests in LTE-A networks,” *IEEE Trans. Netw. Serv. Manag.*, vol. 15, no. 2, pp. 718–731, Jun. 2018.

[187] M. Roderick, J. MacGlashan, and S. Tellex, “Implementing the deep Q-network,” 2017, *arXiv:1711.07478*.

[188] V. Mnih et al., “Human-level control through deep reinforcement learning,” *Nature*, vol. 518, no. 7540, pp. 529–533, 2015.

[189] Y. Li, “Deep reinforcement learning: An overview,” 2017, *arXiv:1701.07274*.

[190] K. Arulkumaran, M. P. Deisenroth, M. Brundage, and A. A. Bharath, “A brief survey of deep reinforcement learning,” 2017, *arXiv:1708.05866*.

[191] A. Muneer, S. M. Taib, S. M. Fati, A. O. Balogun, and I. A. Aziz, “A hybrid deep learning-based unsupervised anomaly detection in high dimensional data,” *Comput., Mater. Continua*, vol. 70, no. 3, pp. 2363–2381, 2022.

[192] G. Caminero, M. Lopez-Martin, and B. Carro, "Adversarial environment reinforcement learning algorithm for intrusion detection," *Comput. Netw.*, vol. 159, pp. 96–109, 2019.

[193] X. Ma and W. Shi, "AESMOTE: Adversarial reinforcement learning with SMOTE for anomaly detection," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 943–956, Apr.–Jun. 2021.

[194] S. Mohamed and R. Ejbali, "Deep SARSA-based reinforcement learning approach for anomaly network intrusion detection system," *Int. J. Inf. Secur.*, vol. 22, no. 1, pp. 235–247, 2023.

[195] R. Cai, H. Li, S. Wang, C. Chen, and A. C. Kot, "DRL-FAS: A novel framework based on deep reinforcement learning for face anti-spoofing," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 937–951, 2021.

[196] A. Ferdowsi and W. Saad, "Deep learning for signal authentication and security in massive Internet-of-Things systems," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1371–1387, Feb. 2019.

[197] X. Lu, L. Xiao, T. Xu, Y. Zhao, Y. Tang, and W. Zhuang, "Reinforcement learning based PHY authentication for VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 3068–3079, Mar. 2020.

[198] A. Albaseer and M. Abdallah, "DRL-based federated uncertainty-guided semi-supervised learning for network traffic selection and threshold determination in ZSM," in *Proc. IEEE Glob. Commun. Conf.*, 2023, pp. 1253–1258.

[199] M. Lopez-Martin, B. Carro, and A. Sanchez-Esguevillas, "Application of deep reinforcement learning to intrusion detection for supervised problems," *Expert Syst. With Appl.*, vol. 141, 2020, Art. no. 112963.

[200] N. Sengupta, J. Sen, J. Sil, and M. Saha, "Designing of on line intrusion detection system using rough set theory and Q-learning algorithm," *Neurocomputing*, vol. 111, pp. 161–168, 2013.

[201] E. Suwannalai and C. Polprasert, "Network intrusion detection systems using adversarial reinforcement learning with deep Q-network," in *Proc. IEEE 18th Int. Conf. ICT Knowl. Eng.*, 2020, pp. 1–7.

[202] K. Sethi, Y. V. Madhav, R. Kumar, and P. Bera, "Attention based multi-agent intrusion detection systems using reinforcement learning," *J. Inf. Secur. Appl.*, vol. 61, 2021, Art. no. 102923.

[203] H. Alavizadeh, H. Alavizadeh, and J. Jang-Jaccard, "Deep Q-learning based reinforcement learning approach for network intrusion detection," *Computers*, vol. 11, no. 3, p. 41, 2022.

[204] Y. Liu, M. Dong, K. Ota, J. Li, and J. Wu, "Deep reinforcement learning based smart mitigation of DDoS flooding in software-defined networks," in *Proc. IEEE 23rd Int. Workshop Comput. Aided Model. Des. Commun. Links Netw.*, 2018, pp. 1–6.

[205] K. A. Simpson, S. Rogers, and D. P. Pezaros, "Per-host DDoS mitigation by direct-control reinforcement learning," *IEEE Trans. Netw. Service Manag.*, vol. 17, no. 1, pp. 103–117, Mar. 2020.

[206] S. Hu et al., "CVshield: Guarding sensor data in connected vehicle with trusted execution environment," in *Proc. 2nd ACM Workshop Automot. Aerial Veh. Secur.*, 2020, pp. 1–4.

[207] Y. Feng, J. Li, and T. Nguyen, "Application-layer DDoS defense with reinforcement learning," in *Proc. IEEE/ACM 28th Int. Symp. Qual. Serv.*, 2020, pp. 1–10.

[208] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang, "Online cyber-attack detection in smart grid: A reinforcement learning approach," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5174–5185, Sep. 2019.

[209] P. Wang, Y. Li, S. Shekhar, and W. F. Northrop, "Adversarial attacks on reinforcement learning based energy management systems of extended range electric delivery vehicles," 2020, *arXiv:2006.00817*.

[210] Y. Wang, E. Sarkar, W. Li, M. Maniatakos, and S. E. Jabari, "Stop-and-go: Exploring backdoor attacks on deep reinforcement learning-based traffic congestion control systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 4772–4787, 2021.

[211] J. Liang, M. Ma, and X. Tan, "GaDQN-IDS: A novel self-adaptive IDS for VANETs based on Bayesian game theory and deep reinforcement learning," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 12724–12737, Aug. 2022.

[212] I. Rasheed, F. Hu, and L. Zhang, "Deep reinforcement learning approach for autonomous vehicle systems for maintaining security and safety using LSTM-GAN," *Veh. Commun.*, vol. 26, 2020, Art. no. 100266.

[213] M. Xiong, Y. Li, L. Gu, S. Pan, D. Zeng, and P. Li, "Reinforcement learning empowered IDPs for vehicular networks in edge computing," *IEEE Netw.*, vol. 34, no. 3, pp. 57–63, May/Jun. 2020, doi: 10.1109/MNET.011.1900321.

[214] Z. Wang, D. Jiang, Z. Lv, and H. Song, "A deep reinforcement learning based intrusion detection strategy for smart vehicular networks," in *Proc. IEEE Conf. Comput. Commun. Workshops*, 2022, pp. 1–6.

[215] Z. Li, Y. Kong, and C. Jiang, "A transfer double deep Q network based DDoS detection method for Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 72, no. 4, pp. 5317–5331, Apr. 2023.

[216] J. Watts, F. Van Wyk, S. Rezaei, Y. Wang, N. Masoud, and A. Khojandi, "A dynamic deep reinforcement learning-Bayesian framework for anomaly detection," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 12,, pp. 22884–22894, Dec. 2022.

[217] T. Alladi, V. Kohli, V. Chamola, F. R. Yu, and M. Guizani, "Artificial intelligence (AI)-empowered intrusion detection architecture for the Internet of Vehicles," *IEEE Wireless Commun.*, vol. 28, no. 3, pp. 144–149, Jun. 2021.

[218] S. Dasgupta, T. Ghosh, and M. Rahman, "A reinforcement learning approach for global navigation satellite system spoofing attack detection in autonomous vehicles," *Transp. Res. Rec.*, vol. 2676, no. 12, pp. 318–330, 2022.

[219] I. Goodfellow et al., "Generative adversarial networks," *Commun. ACM*, vol. 63, no. 11, pp. 139–144, 2020.

[220] M. A. Khan, H. Menouar, and R. Hamila, "Multimodal crowd counting with Pix2Pix GANs," 2024, *arXiv:2401.07591*.

[221] T. Karras, S. Laine, and T. Aila, "A style-based generator architecture for generative adversarial networks," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, 2019, pp. 4401–4410.

[222] M. A. Khan, H. Menouar, and R. Hamila, "Crowd counting in harsh weather using image denoising with Pix2Pix GANs," in *Proc. IEEE 38th Int. Conf. Image Vis. Comput. New Zealand*, 2023, pp. 1–6.

[223] E. Seo, H. M. Song, and H. K. Kim, "GIDS: GAN based intrusion detection system for in-vehicle network," in *Proc. IEEE 16th Annu. Conf. Privacy, Secur., Trust*, 2018, pp. 1–6.

[224] M. Chen, Q. Zhao, Z. Jiang, and R. Xu, "Intrusion detection for in-vehicle CAN networks based on auxiliary classifier GANs," in *Proc. IEEE Int. Conf. High Perform. Big Data Intell. Syst.*, 2021, pp. 186–191.

[225] Q. Zhao, M. Chen, Z. Gu, S. Luan, H. Zeng, and S. Chakrabory, "CAN bus intrusion detection based on auxiliary classifier GAN and out-of-distribution detection," *ACM Trans. Embedded Comput. Syst.*, vol. 21, no. 4, pp. 1–30, 2022.

[226] Y. Yang, G. Xie, J. Wang, J. Zhou, Z. Xia, and R. Li, "Intrusion detection for in-vehicle network by using single GAN in connected vehicles," *J. Circuits, Syst. Comput.*, vol. 30, no. 01, 2021, Art. no. 2150007.

[227] G. Xie, L. T. Yang, Y. Yang, H. Luo, R. Li, and M. Alazab, "Threat analysis for automotive can networks: A GAN model-based intrusion detection technique," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4467–4477, Jul. 2021.

[228] T.-N. Hoang and D. Kim, "Detecting in-vehicle intrusion via semi-supervised learning-based convolutional adversarial autoencoders," *Veh. Commun.*, vol. 38, 2022, Art. no. 100520. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214209622000675

[229] M. Batzorig, Y. Koh, I. Oh, and K. Yim, "A novel attack scenario dataset collection for intrusion detection system in CAN network," in *Advances in Networked-Based Information Systems*, L. Barolli, Ed. Cham, Switzerland: Springer Nature Switzerland, 2023, pp. 130–141.

[230] J. Qin, Y. Xun, Z. Deng, and J. Liu, "GPIDS: GAN assisted contextual pattern-aware intrusion detection system for IVN," *IEEE Trans. Veh. Technol.*, early access, Apr. 01, 2024, doi: 10.1109/TVT.2024.3383449.

[231] M. Abaoud, M. A. Almuqrin, and M. F. Khan, "Advancing federated learning through novel mechanism for privacy preservation in healthcare applications," *IEEE Access*, vol. 11, pp. 83562–83579, 2023.

[232] D. Unal, M. Hammoudeh, M. A. Khan, A. Abuarqoub, G. Epiphaniou, and R. Hamila, "Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things," *Comput. Secur.*, vol. 109, 2021, Art. no. 102393.

[233] A. Albaseer and M. Abdallah, "Privacy-preserving honeypot-based detector in smart grid networks: A new design for quality-assurance

and fair incentives federated learning framework," in *Proc. IEEE 20th Consum. Commun. Netw. Conf.*, 2023, pp. 722–727.

[234] B. Ghimire and D. B. Rawat, "Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8229–8249, Jun. 2022.

[235] A. Albaseer, N. Abdi, M. Abdallah, M. Qaraqe, and S. Al-Kuwari, "FedPot: A quality-aware collaborative and incentivized honeypot-based detector for smart grid networks," *IEEE Trans. Netw. Service Manage.*, early access, Apr. 12, 2024, doi: 10.1109/TNSM.2024.3387710.

[236] J. Yang, J. Hu, and T. Yu, "Federated ai-enabled in-vehicle network intrusion detection for Internet of Vehicles," *Electronics*, vol. 11, no. 22, 2022, Art. no. 3658. [Online]. Available: https://www.mdpi.com/2079-9292/11/22/3658

[237] M. Driss, I. Almomani, Z. E. Huma, and J. Ahmad, "A federated learning framework for cyberattack detection in vehicular sensor networks," *Complex Intell. Syst.*, vol. 8, no. 5, pp. 4221–4235, 2022.

[238] K. H. Shibly, M. D. Hossain, H. Inoue, Y. Taenaka, and Y. Kadobayashi, "Personalized federated learning for automotive intrusion detection systems," in *Proc. IEEE Future Netw. World Forum*, 2022, pp. 544–549.

[239] H. Zhang, K. Zeng, and S. Lin, "Federated graph neural network for fast anomaly detection in controller area networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 1566–1579, 2023.

[240] T.-N. Hoang, M. R. Islam, K. Yim, and D. Kim, "CANPerFL: Improve in-vehicle intrusion detection performance by sharing knowledge," *Appl. Sci.*, vol. 13, no. 11, 2023, Art. no. 6369. [Online]. Available: https://www.mdpi.com/2076-3417/13/11/6369

[241] I. Aliyu, M. C. Feliciano, S. Van Engelenburg, D. O. Kim, and C. G. Lim, "A blockchain-based federated forest for SDN-enabled in-vehicle network intrusion detection system," *IEEE Access*, vol. 9, pp. 102593–102608, 2021.

[242] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," *Veh. Commun.*, vol. 21, 2020, Art. no. 100198. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214209619302451

[243] S. K. Sahu, D. P. Mohapatra, J. K. Rout, K. S. Sahoo, Q.-V. Pham, and N.-N. Dao, "A LSTM-FCNN based multi-class intrusion detection using scalable framework," *Comput. Elect. Eng.*, vol. 99, 2022, Art. no. 107720. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790622000362

[244] B. Cao et al., "Network intrusion detection technology based on convolutional neural network and BiGRU," *Comput. Intell. Neurosci.*, vol. 2022, no. 1, 2022, Art. no. 1942847.

[245] M. M. Leonardo, T. J. Carvalho, E. Rezende, R. Zucchi, and F. A. Faria, "Deep feature-based classifiers for fruit fly identification (diptera: Tephritidae)," in *Proc. IEEE 31st SIBGRAPI Conf. Graph., Patterns Images*, 2018, pp. 41–47.

[246] S. J. Pan and Q. Yang, "A survey on transfer learning," *IEEE Trans. Knowl. Data Eng.*, vol. 22, no. 10, pp. 1345–1359, Oct. 2010.

[247] K. Sahinbas and F. O. Catak, "Transfer learning-based convolutional neural network for COVID-19 detection with X-ray images," *Data Sci. COVID-19*, New York, NY, USA: Elsevier, 2021, pp. 451–466.

[248] L. Kang, H. Shen, M.-K. Han, B.-I. Kwak, and H.-K. Kim, "Anomaly intrusion detection method for vehicular networks based on survival analysis," *Veh. Commun.*, vol. 14, pp. 52–63, Oct. 2018.

[249] Y. Xu, "Intrusion detection based on fusing deep neural networks and transfer learning," in *Digital TV and Wireless Multimedia Communications*, G. Zhai, J. Zhou, H. Yang, P. An, and X. Yang, Eds. Singapore: Springer Singapore, 2020, pp. 212–223.

[250] S. Tariq, S. Lee, and S. S. Woo, "CANTransfer: Transfer learning based intrusion detection on a controller area network using convolutional LSTM network," in *Proc. 35th Annu. ACM Symp. Appl. Comput.*, 2020, pp. 1048–1055.

[251] Y. Wang, Y. Lai, Y. Chen, J. Wei, and Z. Zhang, "Transfer learning-based self-learning intrusion detection system for in-vehicle networks," *Neural Comput. Appl.*, vol. 35, no. 14, pp. 10257–10273, 2023.

[252] L. Yang and A. Shami, "A transfer learning and optimized CNN based intrusion detection system for internet of vehicles," in *Proc. IEEE Int. Conf. Commun.*, 2022, pp. 2774–2779.

[253] Q. Ahmed, A. Naveed, E. Haq, M. Imran, and B. Jan, "Deep transfer learning based intrusion detection system for electric vehicular networks," *Sensors*, vol. 21, no. 14, 2021, Art. no. 4736.

[254] Y. Otoum and A. Nayak, "Signature-over-the-air with transfer learning IDS for intelligent connected vehicles (ICV)," in *Proc. IEEE Globecom Workshops*, 2021, pp. 1–6.

[255] X. Li, Z. Hu, M. Xu, Y. Wang, and J. Ma, "Transfer learning based intrusion detection scheme for Internet of Vehicles," *Inf. Sci.*, vol. 547, pp. 119–135, 2021.

[256] X. Li, Z. Hu, M. Xu, Y. Wang, and J. Ma, "Transfer learning-based intrusion detection scheme for Internet of Vehicles," *J. Inf. Secur. Appl.*, vol. 52, 2020, Art. no. 102491.

[257] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset," *IEEE Commun. Surv. Tut.*, vol. 18, no. 1, pp. 184–208, Firstquarter 2016.

[258] A. Haddaji, S. Ayed, and L. C. Fourati, "A transfer learning based intrusion detection system for Internet of Vehicles," in *Proc. 15th Int. Conf. Developments eSyst. Eng.*, 2023, pp. 533–539.

[259] T.-N. Hoang and D. Kim, "Supervised contrastive ResNet and transfer learning for the in-vehicle intrusion detection system," *Expert Syst. With Appl.*, vol. 238, 2024, Art. no. 122181.

[260] Y. Wang et al., "A lightweight intrusion detection system for internet of vehicles based on transfer learning and MobileNetV2 with hyper-parameter optimization," *Multimedia Tools Appl.*, vol. 83, no. 8, pp. 22347–22369, 2023.

[261] A. Haddaji, S. Ayed, and L. C. Fourati, "A novel and efficient framework for in-vehicle security enforcement," *Ad Hoc Netw.*, vol. 158, 2024, Art. no. 103481.

[262] T.-N. Hoang and D. Kim, "Supervised contrastive ResNet and transfer learning for the in-vehicle intrusion detection system," *J. LATEX Class Files*, vol. 18, no. 9, 2021, Art. no. 122181.

[263] N. M. Nawi, A. S. Hussein, N. A. Samsudin, N. A. Hamid, M. A. M. Yunus, and M. F. Ab Aziz, "The effect of pre-processing techniques and optimal parameters selection on back propagation neural networks," *Int. J. Adv. Sci., Eng. Inf. Technol.*, vol. 7, no. 3, pp. 770–777, 2017.

[264] M. Ring and L. Orseau, "Delusion, survival, and intelligent agents," in *Proc. 4th Int. Conf. Artif. Gen. Intell.*, 2011, pp. 11–20.

[265] J. García, R. Majadas, and F. Fernández, "Learning adversarial attack policies through multi-objective reinforcement learning," *Eng. Appl. Artif. Intell.*, vol. 96, 2020, Art. no. 104021.

[266] S. So, P. Sharma, and J. Petit, "Integrating plausibility checks and machine learning for misbehavior detection in VANET," in *Proc. 17th IEEE Int. Conf. Mach. Learn. Appl.*, 2018, pp. 564–571.

[267] A. Qayyum, M. Usama, J. Qadir, and A. Al-Fuqaha, "Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the way forward," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 998–1026, Secondquarter 2020.

[268] F. A. Ghaleb et al., "Misbehavior-aware on-demand collaborative intrusion detection system using distributed ensemble learning for VANET," *Electronics*, vol. 9, no. 9, 2020, Art. no. 1411.

[269] O. A. Wahab, A. Mourad, H. Otrok, and T. Taleb, "Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 1342–1397, Secondquarter 2021.

[270] H. Kang, B. I. Kwak, Y. H. Lee, H. Lee, H. Lee, and H. K. Kim, "Car hacking: Attack & defense challenge 2020 dataset," IEEE Dataport, vol. 10, 2021. [Online]. Available: https://dx.doi.org/10.21227/qvr7-n418

[271] A. Gazdag, R. Ferenc, and L. Buttyán, "CrySyS dataset of CAN traffic logs containing fabrication and masquerade attacks," *Sci. Data*, vol. 10, no. 1, 2023, Art. no. 903.

[272] C. Kaiser, A. Stocker, and A. Festl, "Automotive CAN bus data: An example dataset from the AEGIS big data project," *OpenAIRE*, 2019.

[273] G. Dupont, A. Lekidis, J. J. den Hartog, and S. S. Etalle, "Automotive controller area network (CAN) bus intrusion dataset v2," 4TU.Centre for Research Data, 2019. [Online]. Available: https://data.4tu.nl/articles/_/12696950/2

[274] 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. 58194–58205, 2020.

[275] Y. Kim, S. Hakak, and A. Ghorbani, "DDoS attack dataset (CICEV2023) against EV authentication in charging infrastructure," in *Proc. IEEE 20th Int. Conf. Privacy, Secur., Trust*, 2023, pp. 1–9.

[276] B. Lampe and W. Meng, "Can-train-and-test: A curated CAN dataset for automotive intrusion detection," *Comput. Secur.*, vol. 140, pp. 103777, 2024.

[277] "Matlab, 9.7.0.1190202 (R2019b)," 2010. Accessed: Jun. 25, 2023. [Online]. Available: https://www.mathworks.com/products/matlab.html

[278] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved IVC analysis," *IEEE Trans. Mobile Comput.*, vol. 10, no. 1, pp. 3–15, Jan. 2011.

[279] M. Rondinone et al., "iTETRIS: A modular simulation platform for the large scale evaluation of cooperative its applications," *Simul. Modelling Pract. Theory*, vol. 34, pp. 99–125, 2013.

[280] A. Dosovitskiy, G. Ros, F. Codevilla, A. Lopez, and V. Koltun, "CARLA: An open urban driving simulator," in *Proc. Conf. Robot Learn.*, 2017, pp. 1–16.

[281] M. Amoozadeh, B. Ching, C.-N. Chuah, D. Ghosal, and H. M. Zhang, "VENTOS: Vehicular network open simulator with hardware-in-the-loop support," *Procedia Comput. Sci.*, vol. 151, pp. 61–68, 2019.

[282] "Artery simulation," 2020. Accessed: Jun. 25, 2023.

MOHAMMED ALMEHDHAR (Graduate Student Member, IEEE) received the B.Sc. degree from the Department of Computer Science, Hadhramout University, Al Mukalla, Yemen, and the M.Sc. degree in computer engineering from the Department of Computer Engineering, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia. He is currently working toward the Ph.D. degree with the Department of Computer Science and Engineering, Hamad Bin Khalifa University, Doha, Qatar. His research interests include AI for networking, AI for cybersecurity, software-defined networking, and electrical vehicle security.

ABDULLATIF ALBASEER (Member, IEEE) received the M.Sc. degree (with Hons.) in computer networks from the King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia, in 2017, and the Ph.D. degree in computer science and engineering from Hamad Bin Khalifa University, Doha, Qatar, in 2022. From 2022 to 2023, he was a Visiting Scholar with Texas A&M University in Qatar, Doha, Qatar. He is currently a Postdoctoral Research Fellow with Smart Cities and IoT Lab, Hamad Bin Khalifa University. He has authored or coauthored more than 30 journal and conference papers, mostly in IEEE Transactions. He also holds six U.S. Patents in the area of wireless network edge technologies. His research interests include AI for networking, AI for cybersecurity, distributed AI, and LLMs for networking. Dr. Albaseer was the Chair and Organizing Committee Member for international conferences. He is a reviewer for numerous prestigious IEEE journals and conferences. He has also presented at various international conferences and has participated in numerous academic and professional development activities.

MUHAMMAD ASIF KHAN (Senior Member, IEEE) received the B.Sc. degree in telecommunication engineering from the University of Engineering and Technology Peshawar, Peshawar, Pakistan, in 2009, the M.Sc. degree in telecommunication engineering from the University of Engineering and Technology Taxila, Taxila, Pakistan in 2013, and the Ph.D. degree in electrical engineering from Qatar University, Doha, Qatar, in 2020. He was a Research Mentor with Qatar University Young Scientists Center, Qatar Univesity. He is currently a Research Scientist with Qatar Mobility Innovations Center, Doha. He was the recipient of Postdoctoral Research Award from the Qatar National Research Fund, for his research work as a Postdoctoral Research Fellow with Qatar University. He has authored or coauthored more than 40 journal articles and conference papers including two book chapters. Dr. Khan is a member of IET and Chartered Engineer with the Engineering Council, London, U.K. He is an Associate Editor for IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, IEEE TRANSACTIONS ON TECHNOLOGY AND SOCIETY, and IEEE FUTURE DIRECTIONS TECHNOLOGY POLICY AND ETHICS NEWSLETTER. He serves on several IEEE committees including the TCCC, TCPAMI, MDA-TC, MMTC, IOT, and Sensors Council. He was a TPC member of numerous IEEE conferences including ICC, Globecom, CCNC, VTC, ICCE, BigData, Sensors, and GEM.

MOHAMED ABDALLAH (Senior Member, IEEE) received the B.Sc. degree from Cairo University, Giza, Egypt, in 1996, and the M.Sc. and Ph.D. degrees from the University of Maryland, College Park, MD, USA, in 2001 and 2006, respectively. From 2006 to 2016, he held academic and research positions with Cairo University and Texas A&M University in Qatar, Doha, Qatar. He is currently a Founding Faculty Member with the rank of Associate Professor with the College of Science and Engineering, Hamad Bin Khalifa University, Doha. He has authored or coauthored more than 150 journals and conferences and four book chapters and co-invented four patents. His research interests include wireless networks, wireless security, smart grids, optical wireless communication, and blockchain applications for emerging networks. He was the recipient of Research Fellow Excellence Award at Texas A& M University in Qatar in 2016, Best Paper Award in multiple IEEE conferences, including IEEE BlackSeaCom 2019, IEEE First Workshop on Smart Grid and Renewable Energy in 2015, and Nortel Networks Industrial Fellowship for five consecutive years, 1999–2003. He is an Associate Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS and IEEE OPEN ACCESS JOURNAL OF COMMUNICATIONS, Track Co-Chair of the IEEE VTC Fall 2019 Conference, Technical Program Chair of the 10th International Conference on Cognitive Radio-Oriented Wireless Networks, and Technical Program Committee Member of several major IEEE conferences.

HAMID MENOUAR (Senior Member, IEEE) received the Engineering degree (M.S.) in computer science from the University of Science and Technology Houari Boumediene, Algiers, Algeria, in 2003, the DEA (M.S.) degree in systems and information technologies from the University of Technology of Compiègne, Compiègne, France, in 2004, and the Ph.D. degree in computer science from Télécom ParisTech, Paris, France, in 2008. Before moving to Qatar in 2010, he worked for eight years with Hitachi Research Lab, Sophia Antipolis, France, where he contributed and led research and development activities related to connected vehicles. During his experience with Hitachi, he has heavily contributed to the development of connected vehicles communication standards in Europe through an active participation at ETSI, TC, ITS, and Car to Car Communication Consortium. He is currently a Senior Research and Development Expert with the Qatar Mobility Innovations Center, Doha, Qatar, where he leads the development of innovations in the area of smart cities and smart living.

SAIF AL-KUWARI (Senior Member, IEEE) received the Bachelor of Engineering degree in computers and networks from the University of Essex, Colchester, U.K., in 2006, and the two Ph.D. degrees in computer science from the University of Bath, Bath, U.K., and Royal Holloway, University of London, Egham, U.K., in 2011. He is currently a Faculty with the College of Science and Engineering, Hamad Bin Khalifa University, Doha, Qatar, and the Director with the Qatar Center for Quantum Computing, Hamad Bin Khalifa University. His research interests include quantum cryptography and quantum machine learning. He is IET and BCS Fellow, and ACM senior member.

ALA AL-FUQAHA (Senior Member, IEEE) received the Ph.D. degree in computer engineering and networking from the University of Missouri-Kansas City, Kansas City, MO, USA, in 2004. He is currently a Professor with Hamad Bin Khalifa University, Doha, Qatar. His research interests include the use of machine learning in general and deep learning in particular in support of the data-driven and self-driven management of large-scale deployments of IoT and smart city infrastructure and services, wireless vehicular networks, cooperation and spectrum access etiquette in cognitive radio networks, and management and planning of software defined networks. He is an ABET Program Evaluator. He is with the editorial boards of multiple journals, including IEEE COMMUNICATIONS LETTER and *IEEE Network* Magazine. He was the Chair, Co-Chair, and Technical Program Committee Member of multiple international conferences, including IEEE VTC, IEEE Globecom, IEEE ICC, and IWCMC.