A Survey of Cybersecurity Challenges and Mitigation Techniques for Connected and Autonomous Vehicles

Bhosale Akshay Tanaji and Sayak Roychowdhury

***Abstract*—Connected and autonomous vehicles (CAVs) are emerging as the future of the automotive industry for secure, efficient and sustainable mobility. CAVs are being rapidly adapted for passenger transportation, delivery of cargo, disaster management and military reconnaissance missions. CAVs for urban transportation are in line with the evolution of "smart cities." However, as CAVs belong to the family of cyber-physical systems (CPS), they inherit some of the generic cyber vulnerabilities of CPS. Due to the unique features of vehicular networks, establishing secure communication between vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) has remained a challenge for vehicular ad-hoc network (VANET) service providers. The vulnerabilities associated with the multitude of sensors and internal connectivity modules increase the threat of cyber-attack on CAVs by many folds. This necessitates clear identification of the potential threats and classify them in terms of attack mechanisms. Such classification will help in mapping the existing security solutions and exploration of new defense strategies for CAVs. This article has conducted a comprehensive survey of the cyber-attacks on CAVs and the ongoing research on the defense mechanisms. Here, the cyber-attacks are organized based on the attacker strategies, attack surfaces, and attack vectors. The mitigation strategies are categorized based on the underlying defense approaches such as cryptography, intrusion detection, access control, and authentication in relation to their effectiveness in mitigating different attack categories. In conclusion this review delves into the current challenges and explores future research directions in the domain of cybersecurity of CAVs.**

***Index Terms*—Connected and autonomous vehicles, cybersecurity, cyber-attacks, vehicular ad-hoc networks, intrusion detection, cryptography, machine learning.**

NOMENCLATURE

ABS	Anti-lock braking system.
ADAS	Advanced driving assistance system.
AODV	Ad hoc on-demand distance vector.
AVP	Automated valet parking.
CAN	Controlled area network.
CAV	Connected autonomous vehicle.
CDS	Cognitive dynamic system.
CIA	Confidentiality, integrity, availability.
CMT	Chronological Merkle Tree.
CNN	Convolutional neural network.
CPS	Cyber-physical system.
DDoS	Distributed denial of service.
DRL	Deep reinforcement learning.
DS	Doppler shift.
DSRC	Dedicated short-range communication.
ECDIS	Electronic chart display and information system.
ECU	Electronic control unit.
GPS	Global positioning system.
HVs	Human-driven vehicles.
IBC	Identity-based cryptography.
IDS	Intrusion detection system.
IMU	Inertial measurement units.
IoV	Internet of vehicle.
ITS	Intelligent transportation system.
IV	Intelligent vehicle.
LiDAR	Light detection and ranging.
LIN	Local interconnect network
MANET	Mobile ad-hoc network.
MITM	Man-in-the-middle.
MOST	Media oriented serial transport.
OBD	On-board device.
OSI	Open systems interconnection.
RADAR	Radio detection and ranging.
RKE	Remote keyless entry.
RMCs	Remote microclouds.
ROS	Robotic operating system.
RSU	Roadside unit.
SYN	Synchronize.
TPD	Tamper-proof device.
TPMS	Tire pressure monitoring system.
UAM	Urban air mobility.
UAV	Unmanned aerial vehicle.
UDP	User datagram protocol.
URLLC	Ultra-reliable and low-latency communication.
VANET	Vehicular ad-hoc network.
VCC	Vehicular cloud computing.
VSN	Vehicular social networking.
V2D	Vehicle to device.
V2I	Vehicle to infrastructure.
V2N	Vehicle to network.
V2P	Vehicle to pedestrian.
V2V	Vehicle to vehicle.
V2X	Vehicle to everything.
WAVE	Wire access in vehicular networks.

Received 5 October 2024; revised 30 October 2024; accepted 1 November 2024. Date of publication 7 November 2024; date of current version 21 November 2025. *(Corresponding author: Sayak Roychowdhury.)*

The authors are with the Department of Industrial and Systems Engineering, Indian Institute of Technology, Kharagpur 721302, India (e-mail: bhosaleakshay78@iitkgp.ac.in; sroychowdhury@iem.iitkgp.ac.in).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIV.2024.3493938.

Digital Object Identifier 10.1109/TIV.2024.3493938

I. Introduction

CONNECTED and autonomous vehicles (CAVs) have emerged as one of the key achievements in technology in the 21st century. They have a wide range of applications, spanning from military surveillance to disaster management, from futuristic public transport to quick delivery of goods. CAVs, which belong to the family of intelligent vehicles (IVs), promise to improve resource utilization efficiency, increase road safety, minimize infrastructure cost, and human effort in transporting passengers and cargo. As a result, technology giants such as Apple, Google, and car manufacturers such as Tesla, Renault, Audi, and Ford have invested heavily in developing autonomous cars. Recently, in Singapore, nuTonomy's driverless taxis successfully navigated an obstacle course [1]. In the logistics industry, autonomous trucks are being deployed in restricted areas such as mines and warehouses. Vehicle platooning trials with autonomous trucks have been conducted in countries like the USA and U.K. [2]. Not just above the ground, similar advancements in unmanned aerial [3], surface [4], [5], and underwater vehicles [6], [7] (UAV, USV, UUV) have enhanced remote sensing, reconnaissance, search, and rescue capabilities in the air, on the water surface and under water respectively. Dubai is in the process of adopting urban air mobility (UAM) using autonomous air taxis [8]. However, because of their heavy dependence on wireless communication and the internet, such technologies are susceptible to cyber-attacks and require robust cybersecurity mechanisms to remain functional. While the control mechanisms of ground AVs, UAVs, USVs and UUVs are different, the attack vectors which the cyber attackers can exploit are very similar [9]. This article seeks to review the important cybersecurity issues for autonomous vehicles and the research related to mitigate the same.

We have explored the attack vectors through which the attackers gain access to the vehicles, disrupt functionalities, and mitigation schemes to deal with the cyber-attack events. Over one hundred seventy five scientific articles are selected from electronic repositories viz. Scopus, IEEE Xplore, Google Scholar, ScienceDirect, and Springer. Fig. 1 provides the distribution of sources we have considered for this review in a pie-chart. The following search phrases are used to search for the relevant articles: *cybersecurity of autonomous vehicles, cyber physical system, attack vectors for autonomous vehicles, cyberattacks on an autonomous vehicle, machine learning and game theory for cybersecurity of autonomous vehicles, availability attack, confidentiality attack, integrity attack, cryptography, GPS spoofing, vehicle to vehicle (V2V), vehicle to infrastructure (V2I), intrusion detection in autonomous vehicles, Sybil attack, eavesdropping, and black-hole attack.*

A. Motivation

Autonomous vehicles are prime examples of cyber-physical systems (CPS). Fig. 2 shows the structural model of the cyber-physical system encompassing computation, communication, physical, and cyber components integrated for seamless operation. For better preparedness to secure CAVs, it is essential to have an overall understanding about the attackers' motivations,

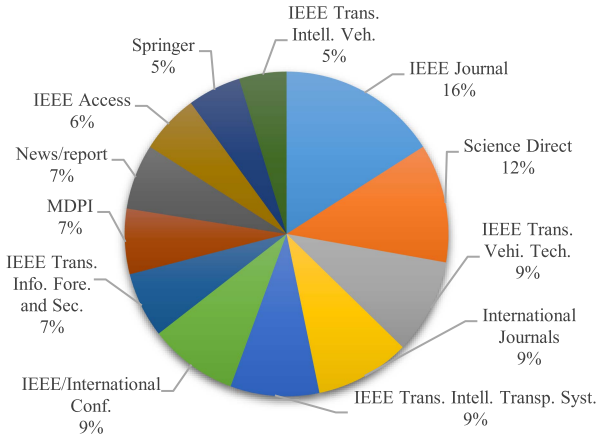

Fig. 1. Pie-chart of research articles reviewed.

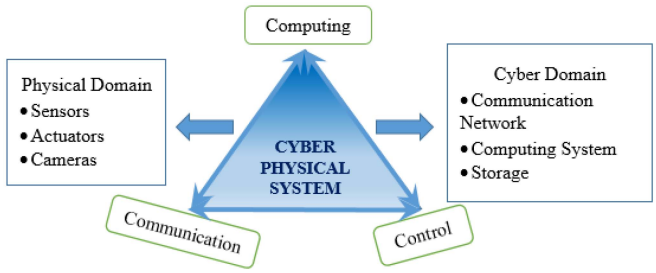

Fig. 2. Components of cyber-physical system (CPS).

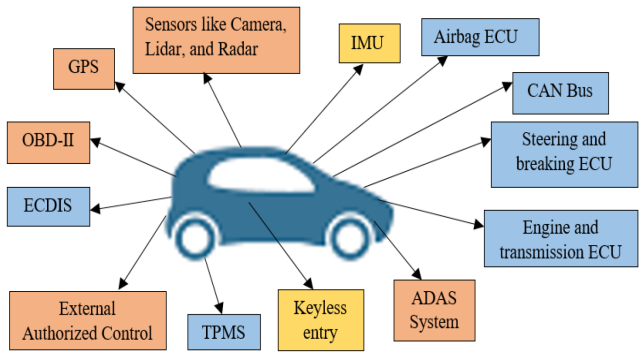

Fig. 3. Possible attack vectors present on autonomous vehicles.

existing and potential attack mechanisms, attack surfaces, interdependencies of the various components, exploitable system vulnerabilities, and the impact of such attacks. Some of the major attack surfaces present in CAVs are shown in Fig. 3.

The primary motivation of this article is to create a comprehensive overview about the cyber-attack mechanisms on CAVs and the mitigation strategies of the same. To substantiate this motivation, a few real-world incidents and experimental studies are mentioned below:

1) Miller and Valasek, in 2015 conducted a remote attack against a Jeep Cherokee via a vulnerability in Uconnect, the vehicle's Internet-connected entertainment system, by introducing malicious data into the CAN bus to control the vehicle's braking system [10].

TABLE I
SUMMARY OF LITERATURE REVIEW ARTICLES

Author (Year)	Year of latest reviewed article	Articles reviewed	Attack classification	Defense classification	Contributions	Research Gap
Cui et al. (2019)	2016	167	Availability, confidentiality, and integrity of data	NA	Classify attack and corresponding defense technique	Advance detection technique based on machine learning, and few defense measures are not discussed
Kim et al. (2021)	2019	151	autonomous control system, driving system components, V2X communication	Security architecture, intrusion detection, and anomaly detection	Provide systematic research on attacks and defense for AVs	Real incident of CAV attack or defense is not mentioned
Ju et al. (2022)	2021	189	Attack classified on attack position (intravehicle, intervehicle, sensor)	NA	Advantages of each attack detection method is mentioned	Advanced detection techniques and cyber-attack techniques are not discussed
Han et al. (2023)	2023	140	(Based on CIA) False data, information theft, privilege escalation, block communication, time delay	Standardisation efforts, authentication and verification, resilient strategies, digital forensic	Linkage of attack technique with defense measure is shown.	Future work is not explained elaborately
Islam et al. (2023)	2023	135	Influence on classifiers, security violation, and attack specificity	NA	Focus on sensor and perception system	Defense techniques are not explained
This Article	2024	175	Based on attack surfaces and CIA triad	Classify in encryption, IDS, and authentication	Focus on vehicular communication, AV platoons	Detailed description about vehicle component is not given

2) In January 2011, French intelligence services investigated possible Chinese involvement in the car manufacturer Renault hack to obtain electric vehicle technologies [11].
3) In 2024, engineers at Duke University demonstrated a Sybil attack situation by creating a system that dubbed phantom car to fool automotive radar sensors into believing almost anything is possible [12].
4) Tesla AV has been involved in multiple autopilot accidents that involved a Tesla Model S failed to identify the white side of the truck due to bright sky [13], an impact on the divider causing loss to personnel [14], an accident in Indianapolis causes loss of two people [15], Pwn2Own in 2024 hacked Tesla electric vehicle components, operating system using zero-day vulnerabilities [16].

Several survey articles published in recent years provide a general overview of cyber threats, their impact on autonomous vehicles, and potential mitigation techniques [17], [18], [19], [20]. Table I provides the comparative analysis of the existing literature reviews on this topic.

Ju et al. [21] highlight the different attack detection and resilience techniques for CAVs considering vehicle dynamics and control parameters in intra-vehicle networks, communication with sensors, and inter-vehicle networks. Thing et al. [22] discuss attack taxonomy related to autonomous vehicles based on attack vectors, vulnerable components in AVs, the attackers' motives, and the after-effects of the attacks.

The key contributions of this article are summarized below:

1) This article presents an overview of vulnerable components inside autonomous vehicles as well as within vehicular networks that can be exploited by attackers.
2) This article classifies the threats by considering the attack surfaces and information security bases (CIA triad) involved in the different cyber-attacks on CAVs. The corresponding defense mechanisms are also explained.
3) A comprehensive understanding of general preventive strategies is provided for securing CAVs based on the underlying defense mechanisms such as cryptography, intrusion detection, and authentication.
4) This article connects the attack categories with the appropriate mitigation strategies with an analysis on the effectiveness of the same.

The remaining paper is structured as follows: Section II presents characteristics of vehicular communication and modes of communication for CAVs. Section III surveys attack vectors and corresponding cyber-attacks on CAVs. Section IV focuses on defense strategies based on cryptography, intrusion detection, and authentication. Section V highlights game theory based decision strategy in cybersecurity of CAVs. Section VI summarizes the article with directions for potential future research.

II. VEHICULAR COMMUNICATION

In CAVs, a multitude of sensors, network systems, and on-board components take part to ensure seamless vehicular operation and communication. Attackers may use these components to gain unauthorized access to the system [22] either physically or through wireless communication.

A. Types of Communication Modes

The components of intra-vehicular, vehicle to everything (V2X), and vehicular cloud computing (VCC) communication are discussed below.

1) Intra-Vehicular Communication: A controlled area network (CAN) bus is a standard protocol for communication

TABLE II
CHARACTERISTICS OF DIFFERENT IN-VEHICLE COMMUNICATION TECHNOLOGIES

Characteristics	FlexRay	CAN Bus	MOST	LIN
Communication protocol	Time-triggered in-vehicle	Serial data	High-speed multimedia	Single-Wire Communication
Applications	x-by-wire systems, Active Cruise Control, and the Anti-lock Braking System (ABS)	ECU nodes, Powertrain (Engine, Transmission, ABS).	Distributed in-vehicle entertainment and infotainment systems.	Monitor battery and temperature sensors.
Advantages	Higher data throughput, more reliability, and less uncertainty	Broadcast transmission, no authentication, encryption, and the ID-based priority scheme	Easily scalable, plug-and-play, reduced electromagnetic interference, higher signal integrity	Easy to use, cheaper, and more reliable.
Maximum bandwidth/payload	10 Mb/s on a single channel and a payload size of 254 Bytes.	1 Mb/s, and the maximum 64-bit length payload.	150 Mb/s and a max 64-bit length payload.	20 Mb/s and a maximum payload of 8-bit length.
Cost	Higher cost	Low-cost	Higher cost	Low-cost

among electronic control units (ECU) in modern vehicles. The other alternatives are FlexRay, Local Interconnect Network (LIN), Automotive Ethernet (AE), and Media Oriented Serial Transport (MOST) [23]. CAN bus is susceptible to wireless network vulnerabilities that cause cyber-attacks in autonomous vehicles. Jo and Choi [24] categorize mitigation techniques against CAN attacks into preventive measures, intrusion detection, message validation, and post security. Liyanage et al. [25] report that the compromised element of the intra-vehicular system may consume excess network resources, insert fake messages into wireless networks, and generate counterfeit warnings to distract the driver and co-passenger inside the vehicle. FlexRay is used as an alternative to CAN for intra-vehicular communication.

The FlexRay protocol has static and dynamic segments within each communication cycle. The static segment is used for periodic safety-critical messages, whereas the dynamic segment primarily includes diagnostic information [26]. The characteristics of different in-vehicle communication technologies used in intra-vehicular communication is provided in Table II. Schneider et al. [27] propose an essential and easily accessible framework for communication of different fieldbus protocols. The framework is integrated into the Robotic Operating System (ROS) using FlexRay protocol as a real-world case.

2) Vehicle to Everything Communication (V2X): V2X communication encompasses V2V, V2I, vehicle to network (V2N), vehicle to pedestrian (V2P), and vehicle to device (V2D) communication for CAVs. In CAVs, V2V communication is used for lane changes, multiple road intersection crossings, and cooperative merging on highways [28]. V2V communication can be achieved by Vehicular Ad Hoc Networks or VANETs, which maintain communication between road side units (RSU) and the vehicles and among the vehicles. V2I is essential for broadcasting information about road conditions, safety measures, and signboard data using RSU. They also communicate with external communication networks via the internet [29]. VANETs generally adhere to the seven layers Open Systems Interconnection (OSI) model and inherit their usual vulnerabilities. Some available VANET standards include Dedicated Short Range Communication (DSRC), Wireless Access in Vehicular Networks (WAVE), and IEEE 802.11p. The WAVE architecture belongs to the IEEE 1609 family, consolidating the standards and protocols for V2V and V2I communications. Cellular network technology is also used as a communication platform for VANETs. Long Term Evolution (LTE) based V2X communication or LTE-V benefits from the cellular networks' high capacity and broad coverage. The comparison between different protocols used in vehicular network based on bit rate, application, and range is given in Table III.

TABLE III
COMPARISON BETWEEN DIFFERENT PROTOCOLS FOR VEHICULAR NETWORK

Protocol	Bit Rate	Range	Delay	Application	Standard	Security
DSRC	3-27 Mbps	< 1 km	<100 ms	V2V, V2I	IEEE 802.11 p	PKI-based
5G	10 Gbps	< 2 km	<1 ms	V2X	NA	Enhanced 5G security
LTE-V	1 Gbps	< 3 km	~20 ms	V2V, V2I, V2N, V2P	LTE-V	LTE-enhanced

Lai et al. [30] explain the infrastructure and cybersecurity challenges of advanced 5G vehicular networks, standardized by the Third Generation Partnership Project or 3GPP. 5G networks support high bandwidth at low latency, which is desirable for V2X communications, but they are susceptible to Sybil and DoS attacks. Spoofing, jamming, eavesdropping and trojans are some of the other attacks that can be administered on 5G enabled vehicular networks. The authors discuss preventive measures such as message authentication and secure group management in 5G communication.

In VANETs, the high mobility of the nodes create an induced Doppler Shift (DS) in the carrier frequency at the receiver end [31]. Alieiev et al. [32] propose a predictive communication algorithm to predict DS in dynamic environments, compensating for line-of-sight issues. The article also classifies the DS into three categories: constant shift, continuously varying shift, and disruptive shift. Chen et al. [33] explores the challenge of channel estimation in reconfigurable

intelligent surface (RIS) assisted millimeter-wave (mmWave) IoV systems, taking into account the detrimental impact of the DS. DS can be used for detection of spoofing attacks on LiDAR [41].

3) Vehicular Cloud Computing (VCC): VCC is the technology that provides cloud computing facilities to drivers and passengers using the communication, storage, and computational capabilities of VANETs. Liu et al. [36] explore edge computing systems to integrate all the functional and communication elements of autonomous driving in a secure and energy-efficient manner. Zhang et al. [37] establish a novel secure channel scheme to protect the confidentiality of task delivery in VCC. Bi et al. [38] propose an algorithm for the request distribution among vehicular clouds (VCs), remote micro-clouds, and remote clouds of the VCC system. The multiple VCs and remote microclouds (RMCs) assist remote clouds (RCs) in making decisions and processing requests, respectively.

B. Control and Communication Overhead

The different types of communication between vehicles and the environment increase the computational complexity and communication overhead. Sousa et al. [39] propose a distributed and low-overhead protocol for traffic congestion control (DisTraC) that detects, quantifies, and updates the traffic congestion map to find the vehicle's efficient route from source to destination. Mistareehi and Manivannan [40] develops the RSU aided message authentication and distribution scheme to reduce the communication overhead in different sub regions. Wang et al. [41] propose a novel authentication request scheme for a large number of on-board units (OBUs) using batch verification for VANETs, which uses two bilinear pairing operations to reduce the communication overhead and computational cost. The other techniques for secure authentication in V2I communication based on batch authentication and bilinear pairing are b-SPECS+ [42], LIAP [43], BASRAC [44], P2BA [45], CPP-HSC [46]. These methods help to reduce computational and control overhead for RSUs or trusted authority (TA) by using secret key generation.

Sewalkar and Seitz [47] develop a Multi-channel Clustering-based Congestion Control (MC-COCO4V2P) algorithm to reduce network congestion and signalling overhead for V2P communication. The MC-COCO4V2P algorithm forms pedestrian clusters based on pedestrian movement and achieves safety in V2X communication.

C. Ultra-Reliable and Low-Latency Communication (URLLC)

Low latency and high reliability are desirable features of wireless networks. Ge [48] employs Euclidean norm theory to study the combined impact of reliability and latency in 5G vehicular networks. The network slicing technique with service, function, and resources is proposed for URLLC between CAVs and other entities in VANET. Nalam et al. [49] introduce a low latency DRiVe mechanism based on joint probability distribution to identify malicious RSUs and provide data integrity for CAVs. Liu et al. [50] propose a ranking and foresight-integrated dynamic RFID scheme to prioritize resources. The technique achieves low latency and high reliability in directed acyclic graph (DAG) task scheduling for dynamic vehicular clouds.

D. VANETs Information Sharing

Attackers can gain access to private user information through vulnerabilities in VANETs, which can be exploited further for fraudulent activities. Xiao et al. [51] propose a perception task-oriented information sharing (PTOIS) network and a game-based resource allocation mechanism to achieve secure and efficient data sharing via V2X communications. Han et al. [52] introduce a reputation-driven reward and penalty system based on a repeated game (RPMBRG) framework, to enhance the reliability of information sharing. Sun et al. [53] present a Privacy-preserving Data Share Mechanism with Flexible Cross-domain authorization (PDSM-FC) for an intelligent autonomous platoon system, which comes with a new cipher text conversion technique and ensure information security.

III. Attack Mechanisms

This section provides an overview of the cyber-attack targeting CAVs. Table IV summarizes the list of cyber-attack surfaces in CAVs. Fig. 4 provides a taxonomy of different cyber-attack mechanisms on CAVs. The attacks can be broadly categorized based on the general CIA triad model of cybersecurity, viz. confidentiality, integrity, and availability [54], as described in the following subsections.

A. Confidentiality Attack

In a confidentiality attack, the attacker gains access to secure information in an unauthorized manner. Messages exchanged among the nodes in a VANET can be intercepted, leading to the disclosure of confidential information such as the location of a vehicle, its routes, and user's identity [55]. Threats that come under this category of such attacks are as follows.

1) Eavesdropping Attack: Eavesdropping is referred to as a passive or privacy leakage attack, which can be easily carried out on wireless networks like VANETs [55]. Since there is minimal effect on the network, this type of attack is difficult to detect. The attacker may be located in a vehicle which is part of the VANET, or may infiltrate an RSU [56]. Balakrishnan et al. [57] discuss the possible mechanisms of conducting eavesdropping attacks on 802.11ad mmWave systems. In autonomous vehicles, relay attacks, a form of eavesdropping attack, are among the most common due to the availability of inexpensive radio hacks. The relay attack requires two attackers to handle the Proxmark device closer to the near field communication (NFC) reader and one attacker read the device using smart device [58], [59].

2) Man-in-the-Middle Attack (MITM): In MITM attack, the attacker intercepts the information being exchanged between two users and modifies the same with malicious intent. Ahmad et al. [60] show the relationship of MITM with other attacks such as eavesdropping and black-hole attacks. Robust

TABLE IV
PRIMARY FUNCTIONS OF CAV COMPONENTS AND POTENTIAL ATTACK SURFACES

CAV Component	Primary function	Attack surfaces	Attack types
Physical Interfaces	Perceive the environment and provide interaction between various subsystems, external devices, and users	Sensors (cameras, LiDAR, radar, GPS), Ports (OBD-II, USB), Key entry system, Charging system	Jamming [78], Replay [79], Spoofing [68], [80], [81]
Software system	Processes data from sensors and integrates perception, planning, and control algorithms for real-time decisions	Operating system, Third-party application, Cloud service, Telematics and infotainment system (Bluetooth, Wi-Fi, cellular connection)	Code/Malware injection [72], [82], Jamming attack [83]
Control System	Implements driving decisions by managing the AV's actuators (steering, braking, and acceleration)	Electronic Control Units, Actuators, Dynamics, and powertrain control systems	Replay [67], [84], DoS [82], Spoofing [75]
Communication System	Ensures continuous and secure information flow between internal and external systems	Vehicle-to-Everything (V2X), Vehicle to Infrastructure (V2I), Vehicle to Vehicle (V2V), RSUs	Sybil [85], [86], Malware [71], Black hole attack [77], [87], Wormhole attack [88]
Networking System	Provides real-time control and monitoring through a communication network	Controller Area Network, Local Interconnect Network, Ethernet	DoS [62], [64], [89], MITM [60], Black hole attack [90], [91], Injection attack [67], Masquerading [68], [92], Eavesdropping attack [57]

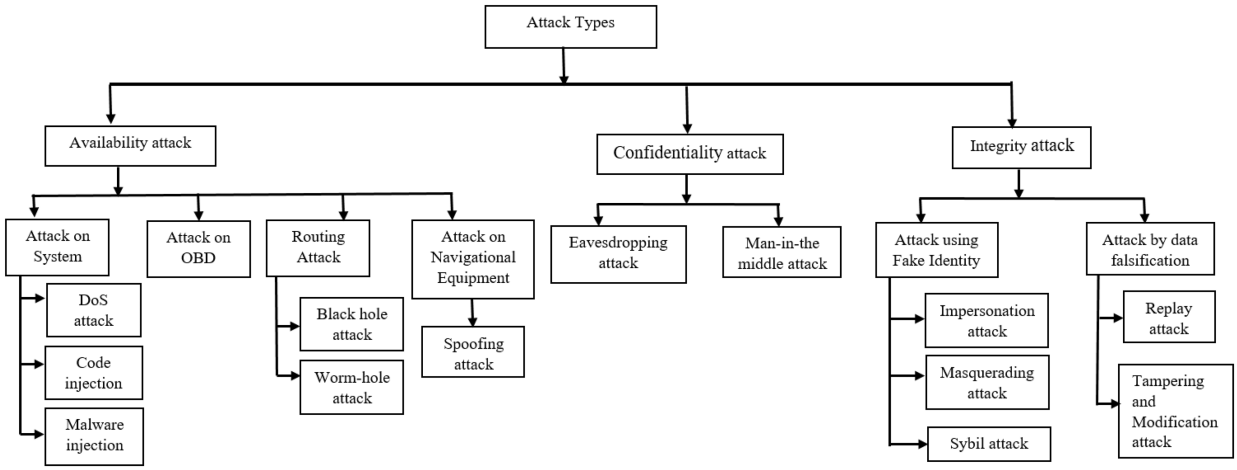

Fig. 4. Taxonomy of cyber-attacks in connected and autonomous vehicles.

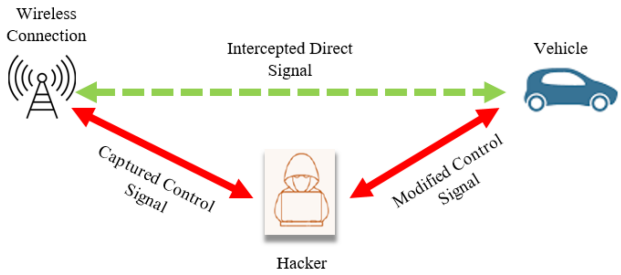

Fig. 5. Man-in-the-middle attack.

authorization techniques such as digital certificates and zero-knowledge proof are some of the proven cryptographic solutions against MITM attacks [55]. Santoso and Finn [61] propose convolutional neural network (CNN) based detection and reduction of MITM attacks in the robot operating system (ROS) for military robotic vehicles. As shown in Fig. 5, hackers manipulate or intercept the signal coming from the transmitter and send a modified signal to the receiver vehicle.

B. Availability Attack

Availability implies the effective functioning of communication networks, cyber-physical components, and information accessibility at any operating condition of CAVs. In availability attacks, attackers block communication or make the network unavailable from authorized users [55]. The following attacks are some of the examples of the availability attacks on CAVs:

1) Attacks on System:

a) Denial-of-service (DoS): Denial of service (DoS) attacks are executed through sending a large number of fraudulent data packets to vehicular networks, causing over-consumption of system resources [62], [63]. Fig. 6 shows a schematic of a Distributed Denial of Service (DDoS) attack, where the attacker compromises many systems or bots, to overwhelm the target. DDoS attackers may use numerous CAVs as bots to perform SYN/TCP flooding and UDP/ICMP flooding to disrupt operations.

Synchronize (SYN) and User Datagram Protocol (UDP) flooding are DoS attacks on intra-vehicular communication that leads to malfunctioning of vehicle control [25]. Tang et al.

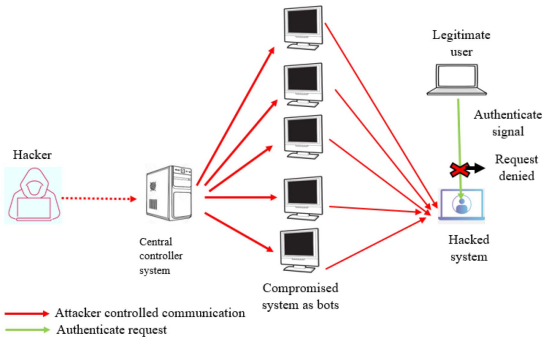

Fig. 6. Distributed denial of service attack (DDoS Attack).

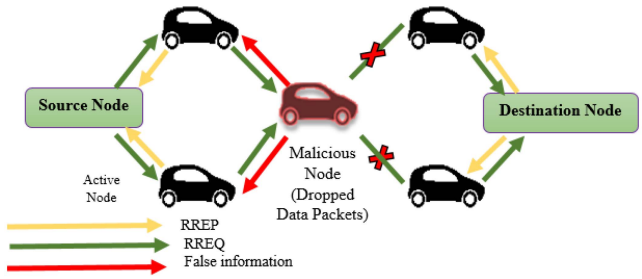

Fig. 7. Mechanism of black-hole attack.

[64] model bus-off attacks as one form of DoS attack in which attackers exploit the CAN error treatment function and turn the CAN bus into off state. Basiri et al. [65] describe a DoS attacker on vehicle platoons that blocks the link between two neighboring vehicles to disrupt inter-vehicular communication.

b) Code Injection: In code injection type of attacks, the attacker inserts a piece of malicious code into the control logic of an autonomous vehicle, which may disrupt normal vehicle operation. Thing et al. [22] mention that code injection can be administered on ECUs with harmful payloads such as malware, spyware, and Trojan Horse inserted into the CAV control systems. Alnabulsi and Islam [66] propose a technique to insert SQL and XSS code injection attacks through information exchange in ITS. They also implement attack detection using the Snort architecture, with signature terms such as UNION, SELECT, DELETE, INSERT, Alert, Document, and IMG. Zhang et al. [67] study CAN message architecture, processing and way of message suspension attack on CAN by compromising ECUs. They also provide different types of message injection, suspension, and falsification attack on CAN bus.

c) Malware Injection: Malware is software built intentionally to disrupt a computer system, software, server, or network. A human being can insert malware into the system, constituting a man-in-the-middle attack. Legitimate users may turn rogue and steal data, inject malware, update falsified firmware, or try to overload the system and stop functioning [68], [69]. Al-Sabaawi et al. [70] mention malware attacks on inter-vehicle communication systems that lead to DoS, GPS spoofing, masquerading, and Sybil attacks. In-vehicle infotainment (IVI) systems such as BMW's i-Drive, Jeep's uConnect, and Benz's Command, may be compromised remotely by the attackers, who can then take control of the vehicle operations [71]. The attackers may use vulnerable smartphone applications to infect the IVI [72]. Since IVIs are connected with the CAN bus to assist driving, such attacks may seriously compromise vehicular control and the safety of the passengers.

2) Attack on On-board Devices (OBD): Attackers may tamper with on-board devices by gaining physical access to the victim vehicle. For example, malicious components may be inserted into the vehicle's internal network using the OBD-II port, that has become standard in modern vehicles [73]. Woo et al. [74] demonstrate a long range wireless attack on CAN using smart phone. Physical tampering of sensors and equipment may also be carried out at various points in the vehicle supply chain. Software embedded in ECUs may also come under attack compromising vehicle safety [75], [18].

3) Routing Attacks:

a) Black-Hole Attack: In Black-hole attack, infected nodes in a vehicular network disrupt communication by dropping data packets or intentionally failing to relay information from source to destination nodes [76]. In Mobile ad-hoc networks (MANETs) or VANETs, a source vehicle may transmit information to a destination vehicle through intermediate nodes. In case of a black-hole attack, an infected node responds to the Route Request (RREQ) from the source node with a false Route Reply (RREP), offering the shortest route to the destination. When the communication is established through the infected node, it simply drops the data packets, creating a DoS like situation. Fig. 7 shows how the black-hole attack propagates on a vehicle network. In Fig. 7, the black vehicles are normal, and the red vehicles are malicious. When the data is transmitted from the source to the destination node, the malicious or black-hole node reroutes the data packet and drops data packets to the destination node. Delkesh et al. [77] introduce the idea of sending a fake RREQ message from the source node to detect the infected nodes in the vicinity. The RREQ message would contain a fake destination address, so any RREP received should come from black-hole node(s).

Tobin et al. [76] propose three-stage process of black-hole attack mitigation for using backtracking algorithm. They show the conventional mechanism of black-hole attack in the presence of only one malicious node. Kumar et al. [90] propose an AODV routing algorithm for black-hole attack detection in VANETs. Cherkaoui et al. [91] propose a black-hole attack detection method by monitoring network activity in VANETs and identifying possible anomalies using the Kolmogorov-Smirnov (K-S) normality test.

b) Wormhole attack: A wormhole attack requires at least two malicious vehicles that are spatially separated and connected through a communication channel called a *tunnel* [18], [88]. Legitimate users in a VANET can be fooled to trust these malicious nodes, seriously disrupting multi-hop message transmission. Wormhole attacks can be categorized as a type of DoS [55], but this mechanism can also be used for stealing information and breaching the confidentiality of the users [93]. The attack using outsider nodes is more difficult to execute due to the unavailability of system certificates and keys, whereas vehicles inside the VANET can launch such attacks more efficiently [88]. Packet leashes, statistical analysis, multi-path hop count

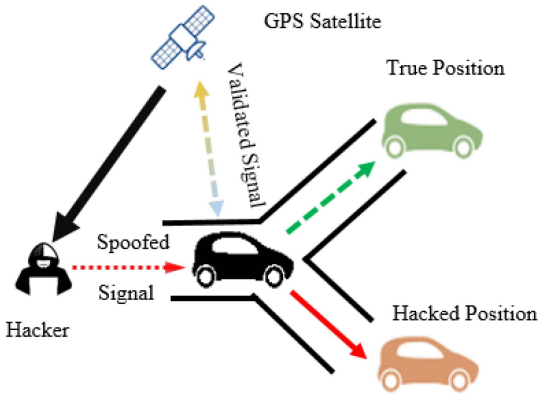

Fig. 8. GPS spoofing attack.

analysis, and delay-per-hop identification are known methods to prevent wormhole attacks [94].

4) Attack on Navigational Equipment:

a) Spoofing Attack: In AVs, the perception of the surrounding environment is developed using equipment such as LiDAR, radio detection and ranging (RADAR), camera, and OBD [95]. In June 2019, experts from Regulus Cyber successfully deceived the GPS navigation system of a Tesla Model 3 vehicle. Tesla Model 3 has autonomy level 2.5, where GPS makes several driving decisions. Raiyn [28] describes attacks on the recognition capabilities of cameras by hiding the signal images of traffic boards at critical locations and adding lines on a road to confuse lane detection. Attackers target LiDAR by replaying the original signal sent from a target vehicle's LiDAR system from another location to create a fake signal. Petit et al. [96] observe that jamming of LiDAR and RADAR is possible using inexpensive methods and should be regarded as a threat of high severity. Camera modules can be blinded by being subjected to bright lights, which is another affordable way to interrupt sensing capabilities.

GPS receivers are the key navigational equipment for connected vehicles. GPS jamming is a common way of disrupting the vehicular navigation system [80], [97]. Jammers broadcast high power signals to obscure the low power GPS original signal. Generally, if the GPS signal frequency is unknown, the jammers broadcast the jamming signal over a broad frequency spectrum, also called blanket jamming [98], [99]. Fig. 8 presents the effect of the GPS spoofing attack, showing the vehicle's displacement from its actual position. As shown in Fig. 8, the black vehicle is travelling to the true position presented by the green colour vehicle. The attacker transmits a fake GPS signal to the GPS receiver that causes the vehicle to change lanes and reach at the fake position shown by red car. In March 2019, at the Geneva Motor Show in Switzerland, GPS spoofing was demonstrated on cars of several brands, and the locations of the affected vehicles were shown to be in Buckingham, England, in the year 2036 [100].

C. Integrity Attack

The attacks that modify or tamper with the information being exchanged are categorized as integrity attacks. For CAVs, both V2V and V2I communication channels may be subjected to these types of attacks [55]. The different types of integrity attacks are discussed below.

1) Attack Using Fake Identity:

a) Impersonation Attack: An impersonation attack attempts to steal information or acquire control by pretending to be a trusted system. By implementing this attack, an attacker can gain access to the username and password of the target system. In VANETs, attacker nodes may impersonate legitimate RSUs, thereby tricking the other vehicles into revealing their authentication details [54]. Dolev et al. [101] present a scenario where the attacker may copy the visible static attributes of a target vehicle to impersonate the same. They propose a laser beam based dynamic attribute verification technique to block such attacks. Impersonation attacks on CAN buses can be prevented through periodic registration of ECUs [102].

b) Masquerading Attack: In a masquerading attack, the attacker aims to gain access to a system by faking a legitimate user identity [103], [104]. Gazdag et al. [92] generate a CAN dataset for masquerading and fabrication attacks on modern vehicles. The dataset improves the machine learning based anomaly detection for autonomous vehicles. In VANETs, the attacker may jam the network using fake identities leading to DDoS attacks [105]. Authentication based preventive techniques using MACs are discussed in [106]. Poudel et al. [107] point out that a malicious ECU can pretend to be a legitimate ECU to perform a masquerading attack. They propose an energy efficient ECU architecture that includes the security and dependability primitives. Jo et al. [108] perform masquerade attack by sending fabricated commands with fake CAN-IDs over the CAN bus by a compromised ECU.

c) Sybil Attack: Sybil attack is similar to a masquerading attack, but it involves many fake identities in the network that control the system [109]. In a VANET, a Sybil attack creates multiple fake vehicles called the Sybil nodes, which can disrupt the entire network through the exchange of fake messages. RSU based techniques [85] and location verification based [86], [110] methods are available for the prevention of Sybil attacks. Identity-based cryptography (IBC), Tamper-proof devices (TPD), and Multiplicative secret sharing (MSS) can also be used to avoid Sybil attacks [111]. Lim et al. [109] propose a scheme incorporating the advanced driver-assisting system (ADAS) to prevent Sybil attacks without requiring additional infrastructure. Du et al. [112] introduce a resilient distributed source localization algorithm for multi-vehicle systems in the presence of Sybil attacks by generating local reliable sets using inter-vehicle trust values

2) Attack By Data Falsification:

a) Replay Attack: In autonomous vehicles, a replay attack occurs when original messages are replaced with old or fake messages [20]. A series of pre-recorded valid frames may be fed to the ECU to perform a replay attack [113]. Often malicious users capture and replay expired beacon messages that lead to a recurrent illusion of an incident [114]. Greene et al. [79] discuss the threat of replay attacks on Remote Keyless Entry (RKE) systems of modern CAVs and propose a defense mechanism using timestamping and XOR encoding. Xu et al. [84] introduce

TABLE V
COMPARATIVE ANALYSIS OF DIFFERENT DEFENSE TECHNIQUES

Characteristics	Symmetric	Asymmetric	Signature based detection	Anomaly based detection	Supervised learning	Unsupervised learning	Reinforcement learning
Mechanism	Use single key	Use two separate keys (public key and private key)	Stores existing signatures of known attacks	Predefines the baseline, attack situation is beyond the baseline	Train an algorithm on labelled data	Train on unlabelled or raw data	Train by trial and error using the reward function.
Advantages	Simple, faster, reduces overhead	Slower for encryption of large data	Faster and efficient for known attacks	Computationally intensive and time-consuming	Time-consuming	Faster, automatic labeling	Learn a series of action
Disadvantages	Less secure for key distribution	More secure for authentication	High false negative rates, fails to detect new attacks	High false-positive rates, hard to determine the baseline	Human guidance and labeled dataset is require	Only classification is possible.	Excessive amount of data and computational power
Different algorithms	2FLIP, TESLA, RAISE, PACP, ECDSA	PPAA, PPGCV, TACKs, TARI, GSIS, SRAAC	RESTNet	CIDS, IDFV, AECFV, PES, OTIDS	TCAMs, PML-CIDS	CANet, LSTM, DNN, Deep Convolution Neural Network	Q learning, SARSA, DDQN, DQN
References	[17], [119], [121], [123]	[119], [124], [125], [123]	[69], [126], [127]	[128], [126], [129]	[89], [68], [61]	[68], [88], [130], [131], [129]	[83], [132], [133], [134], [135]

a speed synchronization control for motor-transmission power systems of CAVs in the presence of replay attack. A novel model predictive control (MPC) technique is used to obtain after-reset values to ensure adequate speed tracking performance and oscillation damping capability under replay attack.

b) Tampering and Modification Attack: Attackers may disrupt functioning systems by tampering or modifying the communicated information [115]. Jie et al. [116] show that the false modification of traffic data may lead to significant congestion. Equipment and sensors on board of the vehicle may be physically tampered for malicious purposes [117]. Duan et al. [118] propose a combination of the isolation forest method with data mass (MS-iForest) to detect data tampering attacks in CAVs.

IV. CYBER-DEFENSE TECHNIQUES FOR CAVS

So far, we have discussed the different types of attacks on CAVs, and instances of research related to the corresponding mitigation techniques The comparison of advantages, disadvantages, and algorithms used in different defense techniques is given in Table V. In this section, the different cyber defense mechanisms for CAVs are discussed which can be broadly classified into three categories: A) Encryption based methods, B) Intrusion detection, and C) Authentication-based defense, as shown in Fig. 9.

A. Encryption Based Methods

1) Cryptography: Cryptography is a method of secure communication between authorized entities that creates cipher text from plain text. Modern cryptography applies mathematical theories and models, computer science, electrical, and communication technology to enhance security mechanisms. Cryptographic hash functions create a short, bit-string digest for a long message, which can be helpful for creating a digital signature for the sender and quick verification by the receiver [119]. Cui et al. [120] implement a lightweight Blom key management technique for CAN bus in-vehicle security. In the proposed scheme, the Blom key provides a secure key to each communicating node and avoids the communication overhead. Fig. 10 explains the cryptography process used to protect data and secure communication in CAVs. As shown in Fig. 10, the transmitter sends an encrypted signal using a public key to the receiver vehicle. The receiving vehicle uses the private key to decrypt the message and extract the important information. Mejri et al. [55] review cryptographic solutions addressing cybersecurity challenges in VANETs.

Tangade et al. [121] have developed a hybrid cryptography trust management model for VANETs that uses asymmetric identity-based digital signature and symmetric hash message authentication. Xiong et al. [122] provide an edge assisted privacy preserving protocol using encryption and CNN for data sharing among CAVs.

B. Intrusion Detection System (IDS)

Intrusion is an illegitimate entry into a network without the authorized user's knowledge. IDS acts as a defensive measure to prevent the same. The IDS in CPS is used to detect compromised devices through scanning the sensors, control nodes, and actuators at optimal intervals. Machine learning models are prevalently used to develop IDSs, which can be broadly classified into two categories: anomaly-based detection and signature-based

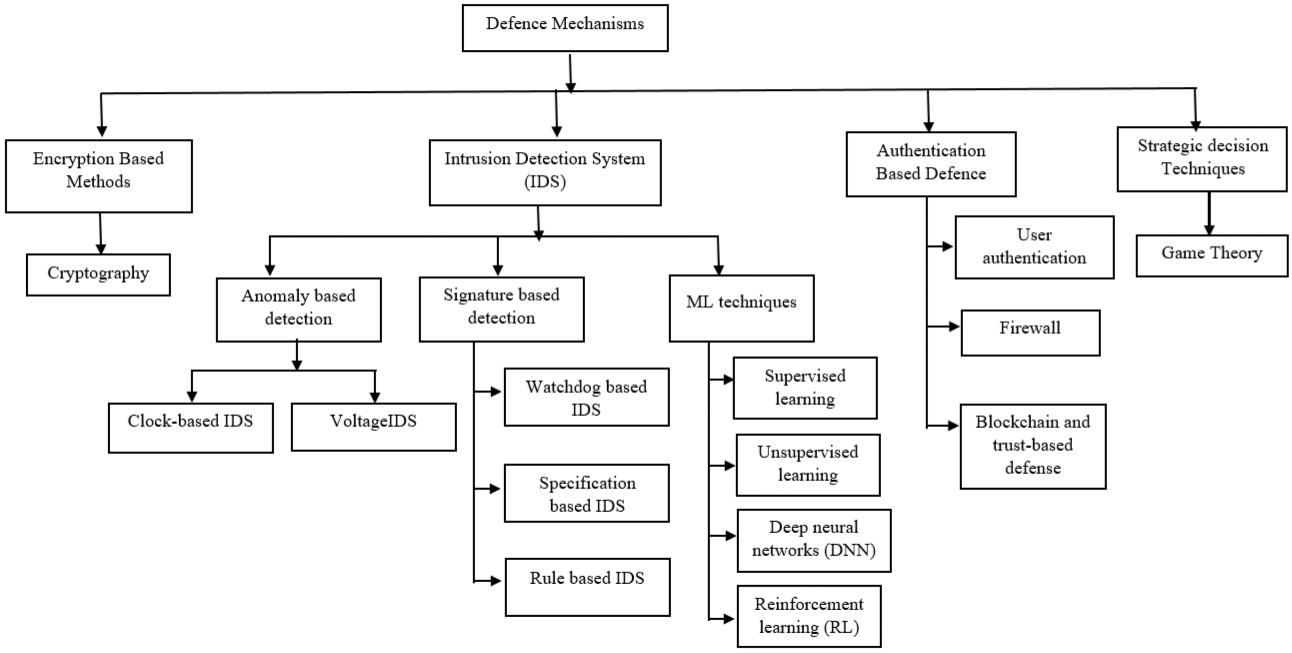

Fig. 9. Classification of defense mechanisms in connected and autonomous vehicles.

TABLE VI
DIFFERENT ATTACK CATEGORIES WITH DEFENSE MEASURES

Attacks ↓ Defense →	Cryptography	Machine learning	Anomaly detection	Signature based detection	User authentication	Firewall	Blockchain
DoS	✓	✓	✓	✓		✓	
Code/malware injection				✓	✓	✓	✓
Black hole		✓	✓				
Worm hole		✓	✓				✓
GPS spoofing	✓	✓				✓	
Eavesdropping	✓						
MITM	✓			✓	✓	✓	✓
Impersonation		✓			✓		
Sybil	✓		✓		✓		✓
Replay	✓	✓	✓	✓	✓		✓
Tampering	✓	✓	✓				✓

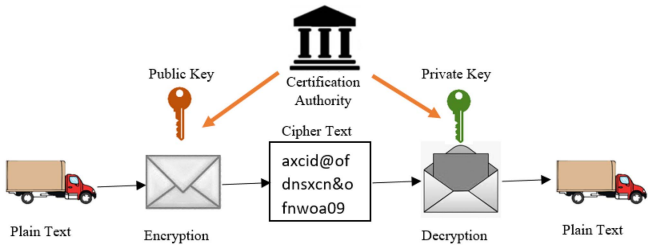

Fig. 10. Cryptography technique in CAVs.

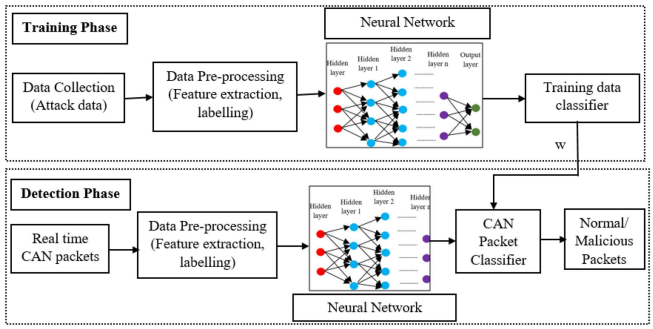

Fig. 11. The outline of an IDS by the deep neural network.

detection. The current state of research in the area of IVs in these two categories is elaborated in the next sections. Table VI presents the effective implementation of defense techniques for various types of cyber-attacks.

1) Machine Learning Techniques for IDS: Different machine learning (ML) techniques like supervised, unsupervised, and reinforcement learning are used to detect cyber-attack on autonomous vehicles [54]. Deep reinforcement learning (DRL) based defense techniques are also gaining prominence [132],

[133] in real-time detection of black-hole, traffic control, jamming, and spoofing attacks on CAVs. The deep neural network (DNN) based methods are applied to detect malicious data packets [131], [136]. Fig. 11 outlines the architecture of the DNN during both the training and testing phases. Cai et al. [89] have developed a mini-batch machine learning algorithm to mitigate network jamming and bandwidth exploitation issues arising from DoS attacks and improve service quality using constraint minimization by Lyapunov-Krasovskii functions (LKFs).

Toker et al. [137] propose an FFT-based digital signal processing (DSP) algorithm for detecting cyber-attack on 77 GHz automotive radar sensors. They extend the physical challenge response authentication (PyCRA) method propose by Shoukry et al. [138]. Clark et al. [139] examine the effectiveness of Q-learning control policies against adversarial data attacks on the robotic system of a Raspberry Pi-3 based AV model. Lin et al. [140] identify phantom attacks that cause fake perception of camera sensors. The attackers use devices like projectors and electronic displays to generate deceptive images in VANETs. Yao et al. [83] propose an anti-eavesdropping approach for securing a V2V communication network using Distributed Kalman Filtering (DKF) and DRL methods.

2) Anomaly-Based Detection: In anomaly detection, the normal behavior is first identified and compared with the actual behaviour of the vehicles [132]. This includes movement of vehicles as well as network traffic, sensors data and operating characteristics. Choi et al. [128] propose a novel IDS, named VoltageIDS, which incorporates a multi-class classifier (Linear SVM or Bagged Decision Tree) on electrical characteristics to detect masquerading attacks. Yang et al. [81] develop an anomaly detection module against GPS spoofing using learning from demonstrations implemented on CAVs.

Anomaly detection in VANETs is more challenging than in traditional wireless networks because of the fast movements of vehicles, topological variability, and the short-lived nature of the links [127]. Zhang et al. [67] provide an anomaly-based detection system created on a graph neural network to detect message injection, suspension, and fabrication in CAN buses. Tan et al. [129] have developed a certificationless authentication technique incorporating unsupervised learning using dynamic time warping. Laisen et al. [141] propose a spatio-temporal feature based technique for VANETs using a CNN. Machine learning based anomaly detection methods can potentially identify new types of attacks more effectively than traditional rule-based techniques. Deng et al. [142] propose a voltage-based IDS, IdentifierIDS, to provide security for in-vehicle networks. IdentifierIDS is a self-learning IDS that detect intrusions in ECU and IDs without the knowledge of confidential mapping between them.

3) Signature-Based Detection: Signature detection IDSs operate by matching the activities of participating nodes with known attack scenarios (signatures) stored in the database. In their review article, Sharma and Kaul [93] observe that although signature-based IDSs have high detection accuracy for known attacks, they are ineffective for zero-day exploits and are easy to evade with minor changes in the attack signature. A hybrid model of IDS for sensor data, which includes both anomaly (A_{ds}) and signature-based detection subsystems (S_{ds}) is proposed by Otoum et al. [143]. The signature-based subsystems distinguish normal traffic from malicious using Random Forest (RF). The anomaly-detection mechanism incorporates an enhanced DBSCAN algorithm for classification. Apart from anomaly-based, signature-based, and hybrid models, several other techniques are available for intrusion detection, e.g., watchdog-based [144], cross-layer based [145], [146], and honeypot-based techniques [147]. Watchdog-based IDS deploys a watchdog node, which monitors its nearby nodes to detect erroneous behaviour of vehicles [93]. The watchdog system evaluates the reputation of neighbouring vehicles by monitoring their network communications, allowing it to detect whether the observed vehicles are dropping or forwarding received packets.

C. Authentication Based Defense

1) User Authentication: User authentication is used frequently to mitigate access for unauthorized users. Raiyn [28] proposes a biometric-based iris recognition methodology for the security of autonomous vehicles. Huang et al. [148] propose a privacy-preserving reservation scheme for securing an automated valet parking (AVP) system against a "double-reservation attack." The method provides registration with real-time parking conditions to the user and generates a parking receipt for the vehicle. Rajput et al. [149] propose a hybrid detection approach using pseudonym-based and group signature-based features for privacy preservation in VANETs. The electrocardiogram (ECG) based authentication scheme, comprising QRS complex wave and T wave, helps to monitor the health features of users in VANETs[150], [151]. Jiang et al. [152] propose a cloud-centric three-factor authentication and key management protocol (CT-AKA) that secures communication in AVs and the cloud.

2) Firewall: A firewall is a network security technique that filters and controls incoming and outgoing network traffic having malicious features. Mitchell et al. [153] mention that data leak rate control can act as a countermeasure against the exfiltration failure of cyber-physical systems. Using rule-based techniques, firewalls can distinguish between legitimate and malicious networks in V2V/V2I communications [22].

3) Blockchain and Trust-Based Defense Mechanism: Blockchain is a type of distributed ledger technology (DLT) in which a digital ledger of the transactions are recorded with an immutable cryptographic signature (hash) that makes vehicle blockchain systems impossible to falsify. VANET blockchain-based systems ensure secure data sharing with additional features like decentralization, distribution, immutability, flexibility, and transparency [154]. Akhter et al. [154] propose a blockchain-based authentication system for VANETs that incorporates registration and classification of Internet of Vehicles (IoV), cooperative communication, and vehicular social networking (VSN). VSN plays a significant role in sharing critical information like emergency messages, accident scenarios, etc. Blockchain is also applied to preserve the privacy of users in VANETs. For example, Lu et al. [155] use the chronological Merkle Tree (CMT) and Merkle Patricia Tree (MPT) for privacy preservation

using blockchain. Lin et al. [156] suggest a conditional privacy-preserving authentication protocol using a public blockchain and key derivation algorithm to minimize the restoration of key pairs in vehicle OBUs. Li et al. [157] have developed a blockchain for certificates (CerBC) and requests (ReqBC) privacy protection. The CerBC helps in certificate registration, update, and revocation, whereas ReqBC records all query requests.

Different trust-based techniques for identification of threats have been proposed in the literature [121], [158]. Rathore et al. [123] present a novel Efficient Algorithm for secure Transmission (EAST) to solve a trust-based privacy model for IoV using encryption and steganography. Qi et al. [159] propose a trust-built data transmission security model for emergency messages in vehicular networks. Shen et al. [160] present a trust-based privacy protection technique integrating blockchain and a multi-party evaluation framework for IoV.

V. Game Theory Based Defense Mechanism

Game theory-based cyber-attack detection in autonomous vehicles has become an emerging topic. Game theory can be used for defense strategy selection, resource allocation, and cyber-attack feature selection in CAVs. The integration of game theory with machine learning [134], [161] or graph theory [162], [163] for CAVs cyber security is also an emerging area of research. Sedjelmaci et al. [164] classify different cybersecurity game techniques for intelligent transportation system (ITS). They also propose a Stackelberg security game framework for attack feature generation for zero-day attacks. Basiri et al. [165] propose an optimal placement of sensor nodes in vehicle platoons using a game theoretic approach for cyber-attack mitigation. This work combines game theory with directed and undirected weighted graphs to better understand platoon topology. Yan et al. [166] propose a multiple-vehicle game theory-based trajectory estimation framework for traffic safety and comfort in complex traffic scenarios. Three different types of game frameworks are included between AVs and human-driven vehicles (HVs). Zhang et al. [167] introduce a multi-target attacker-defender game where attackers possess multiple options to target various assets. Defenders allocate limited resources across different targets to minimize an exponential attack success function. Feng et al. [168] propose a Bayesian game theoretic approach for defenders to reduce the expected losses by optimizing the distribution of scarce defensive resources among multiple targets. Pan et al. [169] study a signal security game model for improvement in information security of urban traffic systems using the evolutionary game theory approach.

VI. Discussion And Future Directions

This article highlights the recent advancement in research related to the cybersecurity of CAVs. First, the different cyber-attack mechanisms that lead to road accidents, data breaches, traffic congestion, navigational errors, and service disruption at different levels are explored. Then, the mitigation strategies of these cyber-attacks are surveyed. The prevention strategies are categorized based on the underlying techniques, such as cryptography, intrusion detection, and user authentication. The rise of the electric CAVs also boosts V2X communication and promotes the development of intelligent infrastructure, enhancing safety and security in smart cities. Therefore, future research should focus on preventive defense, real-time monitoring, governmental policies, and secure communication protocols [82], [65], [170]. Trust management is one crucial aspect of securing vehicular networks. The rapid evolution of the communication platforms of VANETs necessitates the upgradation of vehicular trust management systems. Deep learning-based adversarial networks for testing the VANET security and identification of rogue vehicles are emerging areas of research [135], [171], [126]. VCC and edge computing platforms need further investigation to integrate with VANETs successfully. Issues such as the temporary nature of vehicular clouds and the involvement of single vehicles in multiple clouds have made the development of secure VCC architecture a challenging prospect [172].

Data privacy in VANETs can be further enhanced by advanced ML techniques like federated learning, in which data is not shared by the individual nodes. Integrating federated learning with conventional mitigation measures like blockchain and cryptography improves resource utilization making the CAV system both secure and sustainable [173]. In the development of VANETs, infrastructure plays a crucial role in ensuring better network connectivity. Detecting cyber-attacks in remote areas and at the internet blind spots presents a unique challenge. To resolve these issues, techniques such as behavior-based IDS, edge computing, computational offloading, and multi-layer redundancy need further refinement [112], [174]. For sustainable transportation, platooning with semi-autonomous vehicles is an emerging field of research [175]. Security aspects of cross-platform platooning, involving vehicles from different manufacturers should be studied in greater detail. Cyber resiliency for VANETs may be another field of research to be explored in future.

References

[1] S. Chng, S. Anowar, and L. Cheah, "To embrace or not to embrace? Understanding public's dilemma about autonomous mobility services: A case study of Singapore," *Case Stud. Transp. policy*, vol. 9, no. 4, pp. 1542–1552, 2021.

[2] "Autonomous vehicles self-driving chauffeur and AMoD reshuffle traditional supply chain," *FutureBridge*, 2020. [Online]. Available: https://www.futurebridge.com/mobility/autonomous-vehicles/

[3] L. V. N. Huy, X. Pham, H. M. La, and D. Feil-Seifer, "Autonomous UAV navigation using reinforcement learning," *Int. J. Mach. Learn. Comput.*, vol. 9, no. 6, pp. 756–761, 2019, doi: 10.18178/ijmlc.2019.9.6.869.

[4] P. S. Chib and P. Singh, "Recent advancements in end-to-end autonomous driving using deep learning: A survey," *IEEE Trans. Intell. Veh.*, vol. 9, no. 1, pp. 103–118, Jan. 2024.

[5] H. Huang, Z. Shen, C. Huang, Y. Wang, and F.-Y. Wang, "Intelligent vehicle carriers to support general civilian purposes," *IEEE Trans. Intell. Veh.*, vol. 8, no. 10, pp. 4292–4295, Oct. 2023.

[6] I. Bae and J. Hong, "Survey on the developments of unmanned marine vehicles: Intelligence and cooperation," *Sensors*, vol. 23, no. 10, 2023, Art. no. 4643.

[7] A. Anand, M. Y. Bharath, P. Sundaravadivel, J. P. Roselyn, and R. A. Uthra, "On-device intelligence for AI-enabled Bio-inspired autonomous underwater vehicles (AUVs)," *IEEE Access*, vol. 12, pp. 51982–51994, 2024.

[8] S. Wray, "Flying taxi trials in cities set to expand," *Cities Today*, Aug. 27, 2020. [Online]. Available: https://cities-today.com/cities-progress-flying-taxi-plans/

[9] M. Kumar and S. Mondal, "Recent developments on target tracking problems: A review," *Ocean Eng.*, vol. 236, 2021, Art. no. 109558.

[10] A. Drozhzhin, "Black Hat USA 2015: The full story of how that jeep was hacked," *Kaspersky daily*. [Online]. Available: https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/

[11] "Renault cars spy case: French intelligence investigates," *BBC News*, [Online]. Available: https://www.bbc.com/news/world-europe-12137714

[12] K. Kingery, "Engineers develop hack to make automotive radar hallucinate," Pratt School of Engineering, Jan. 31, 2024. [Online]. Available: https://pratt.duke.edu/news/engineers-develop-hack-to-make-automotive-radar-hallucinate

[13] J. K. Gurney, "Sue my car not me: Products liability and accidents involving autonomous vehicles," *U. Ill. JL Tech. Pol'y*, 247, 2013. [Online]. Available: https://ssrn.com/abstract=2352108

[14] J. Stewart, "No TitlTesla's autopilot was involved in another deadly car crashe," *WIRED*, 2023. [Online]. Available: https://www.wired.com/story/tesla-autopilot-self-driving-crash-california/

[15] M. Uzair, "Who is liable when a driverless car crashes?," *World Electr. Veh. J.*, vol. 12, no. 2, 2021, Art. no. 62.

[16] N. Nelson, "Pwn2Own 2024: Tesla hacks, dozens of zero-days in electrical vehicles," 2024. [Online]. Available: https://www.darkreading.com/ics-ot-security/pwn2own-2024-teslas-hacked-dozens-new-zero-days-evs

[17] K. 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.

[18] X. Sun, F. R. Yu, and P. Zhang, "A survey on cyber-security of connected and autonomous vehicles (CAVs)," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 6240–6259, Jul. 2022.

[19] M. Pham and K. Xiong, "A survey on security attacks and defense techniques for connected and autonomous vehicles," *Comput. Secur.*, vol. 109, 2021, Art. no. 102269.

[20] J. Han, Z. Ju, X. Chen, M. Yang, H. Zhang, and R. Huai, "Secure operations of connected and autonomous vehicles," *IEEE Trans. Intell. Veh.*, vol. 8, no. 11, pp. 4484–4497, Nov. 2023.

[21] Z. Ju, H. Zhang, X. Li, X. Chen, J. Han, and M. Yang, "A survey on attack detection and resilience for connected and automated vehicles: From vehicle dynamics and control perspective," *IEEE Trans. Intell. Veh.*, vol. 7, no. 4, pp. 815–837, Dec. 2022.

[22] V. L. L. Thing and J. Wu, "Autonomous vehicle security: A taxonomy of attacks and defences," in *Proc. IEEE Int. Conf. Internet Things; IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data*, 2016, pp. 164–170, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.52.

[23] S. Kim and R. Shrestha, *Automotive Cyber Security: Introduction, Challenges, and Standardization*. Berlin, Germany: Springer Nat., 2020.

[24] 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.

[25] M. Liyanage, P. Kumar, S. Soderi, M. Ylianttila, and A. Gurtov, "Performance and security evaluation of intra-vehicular communication architecture," in *Proc. IEEE Int. Conf. Commun. Work.*, 2016, pp. 302–308, doi: 10.1109/ICCW.2016.7503804.

[26] W. Xiong, D. W. C. Ho, and S. Wen, "A periodic iterative learning scheme for finite-iteration tracking of discrete networks based on FlexRay communication protocol," *Inf. Sci. (Ny).*, vol. 548, pp. 344–356, 2021.

[27] D. Schneider, L. Kastner, B. Schick, and D. Watzenig, "fROS: A generic fieldbus framework for ROS," *IEEE Trans. Intell. Veh.*, vol. 9, no. 10, pp. 6284–6297, Oct. 2024.

[28] J. Raiyn, "Data and cyber security in autonomous vehicle networks," *Transp. Telecommun.*, vol. 19, no. 4, pp. 325–334, 2018, doi: 10.2478/ttj-2018-0027.

[29] M. Islam, M. Chowdhury, H. Li, and H. Hu, "Cybersecurity attacks in vehicle-to-infrastructure applications and their prevention," *Transp. Res. Rec.*, vol. 2672, no. 19, pp. 66–78, 2018, doi: 10.1177/0361198118799012.

[30] C. Lai, R. Lu, D. Zheng, and X. S. Shen, "Security and privacy challenges in 5G-enabled vehicular networks," *IEEE Netw.*, vol. 34, no. 2, pp. 37–45, Mar./Apr. 2020, doi: 10.1109/MNET.001.1900220.

[31] M. N. Ahangar, Q. Z. Ahmed, F. A. Khan, and M. Hafeez, "A survey of autonomous vehicles: Enabling communication technologies and challenges," *Sensors*, vol. 21, no. 3, 2021, Art. no. 706.

[32] R. Alieiev, T. Hehn, A. Kwoczek, and T. Kürner, "Predictive communication and its application to vehicular environments: Doppler-shift compensation," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7380–7393, Aug. 2018.

[33] J. Chen, W. Shen, S. Luo, S. Ma, C. Xing, and L. Hanzo, "Estimation of dispersive high-doppler channels in the RIS-aided mmWave Internet of Vehicles," *IEEE Internet Things J.*, vol. 11, no. 1, pp. 677–691, Jan. 2024.

[34] X. Hu, T. Liu, T. Shu, and D. Nguyen, "Spoofing detection for LiDAR in autonomous vehicles: A physical-layer approach," *IEEE Internet Things J.*, vol. 11, no. 11, pp. 20673–20689, Jun. 2024.

[35] Z. Zhou, H. Li, Z. Chen, and M. Lu, "Velocity consistency checking based GNSS spoofing detection method for vehicles," *IEEE Trans. Veh. Technol.*, vol. 73, no. 2, pp. 1974–1990, Feb. 2024.

[36] S. Liu, L. Liu, J. Tang, B. Yu, Y. Wang, and W. Shi, "Edge computing for autonomous driving: Opportunities and challenges," *Proc. IEEE*, vol. 107, no. 8, pp. 1697–1716, Aug. 2019.

[37] R. Zhang, L. Zhang, Q. Wu, and J. Zhou, "Secure Channel Establishment scheme for task delivery in vehicular cloud computing," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 2865–2880, 2024.

[38] C. Bi, J. Li, Q. Feng, C.-C. Lin, and W.-C. Su, "Optimal deployment of vehicular cloud computing systems with remote microclouds," *Wireless Netw.*, vol. 30, pp. 5305–5317, 2023.

[39] R. S. De Sousa, A. Boukerche, and A. A. F. Loureiro, "A distributed and low-overhead traffic congestion control protocol for vehicular ad hoc networks," *Comput. Commun.*, vol. 159, pp. 258–270, 2020.

[40] H. Mistareehi and D. Manivannan, "A low-overhead message authentication and secure message dissemination scheme for vanets," *Network*, vol. 2, no. 1, pp. 139–152, 2022.

[41] T. Wang, L. Kang, and J. Duan, "A secure access control scheme with batch verification for VANETs," *Comput. Commun.*, vol. 205, pp. 79–86, 2023.

[42] S.-J. Horng et al., "b-SPECS+: Batch verification for secure pseudonymous authentication in VANET," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 11, pp. 1860–1875, Nov. 2013.

[43] S. Wang and N. Yao, "LIAP: A local identity-based anonymous message authentication protocol in VANETs," *Comput. Commun.*, vol. 112, pp. 154–164, 2017.

[44] S. Chen, Y. Liu, J. Ning, and X. Zhu, "BASRAC: An efficient batch authentication scheme with rule-based access control for VANETs," *Veh. Commun.*, vol. 40, 2023, Art. no. 100575.

[45] X. Feng, Q. Shi, Q. Xie, and L. Wang, "P2BA: A privacy-preserving protocol with batch authentication against semi-trusted RSUs in vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 3888–3899, 2021.

[46] I. Ali, T. Lawrence, A. A. Omala, and F. Li, "An efficient hybrid signcryption scheme with conditional privacy-preservation for heterogeneous vehicular communication in VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 11266–11280, Oct. 2020.

[47] P. Sewalkar and J. Seitz, "Mc-coco4v2p: Multi-channel clustering-based congestion control for vehicle-to-pedestrian communication," *IEEE Trans. Intell. Veh.*, vol. 6, no. 3, pp. 523–532, Sep. 2021.

[48] X. Ge, "Ultra-reliable low-latency communications in autonomous vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 5, pp. 5005–5016, May 2019.

[49] N. V. Abhishek, M. N. Aman, T. J. Lim, and B. Sikdar, "Drive: Detecting malicious roadside units in the internet of vehicles with low latency data integrity," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3270–3281, Mar. 2022.

[50] Z. Liu, M. Liwang, S. Hosseinalipour, H. Dai, Z. Gao, and L. Huang, "RFID: Towards low latency and reliable DAG task scheduling over dynamic vehicular clouds," *IEEE Trans. Veh. Technol.*, vol. 72, no. 9, pp. 12139–12153, Sep. 2023.

[51] Z. Xiao, J. Shu, H. Jiang, G. Min, H. Chen, and Z. Han, "Overcoming occlusions: Perception task-oriented information sharing in connected and autonomous vehicles," *IEEE Netw*, vol. 37, no. 4, pp. 224–229, Jul./Aug. 2023.

[52] H. Han, M. Zhang, Z. Xu, X. Dong, and Z. Wang, "Decentralized trust management and incentive mechanisms for secure information sharing in VANET," *IEEE Access*, vol. 12, pp. 124414–124427, 2024.

[53] J. Sun, G. Xu, T. Zhang, X. Cheng, X. Han, and M. Tang, "Secure data sharing with flexible cross-domain authorization in autonomous vehicle systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 7, pp. 7527–7540, Jul. 2023.

[54] M. Dibaei et al., "An overview of attacks and defences on intelligent connected vehicles," 2019. *arXiv:1907.07455*.

[55] M. Mejri, J. B.-O. Nidhal, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Veh. Commun.*, vol. 1, no. 2, pp. 53–66, 2014, doi: 10.1016/j.vehcom.2014.05.001.

[56] L. Chen, J. Zhu, Y. Yang, and S. Boichenko, "Physical layer security for RIS-V2V networks with different eavesdropper locations," *IEEE Internet Things J.*, vol. 11, no. 22, pp. 35791–35801, Nov. 2024.
[57] S. Balakrishnan, P. Wang, A. Bhuyan, and Z. Sun, "Modeling and analysis of eavesdropping attack in 802.11 ad mmWave wireless networks," *IEEE Access*, vol. 7, pp. 70355–70370, 2019.
[58] F. Lambert, "Tesla vehicles can be stolen with new relay attack, but there's a two-inch caveat," *Electrek*, Sep. 13, 2022. [Online]. Available: https://electrek.co/2022/09/13/tesla-vehicles-stolen-relay-attack-caveat/
[59] A. Greenberg, "Tesla can still be stolen with a cheap radio hack-despite new keyless tech," *WIRED*, 2024. May 22, 2024. [Online]. Available: https://www.wired.com/story/tesla-ultra-wideband-radio-relay-attacks/
[60] F. Ahmad, A. Adnane, V. N. L. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies," *Sensors*, vol. 18, no. 11, 2018, Art. no. 4040.
[61] F. Santoso and A. Finn, "Trusted operations of a military ground robot in the face of man-in-the-middle cyber-attacks using deep learning convolutional neural networks: Real-time experimental outcomes," *IEEE Trans. Dependable Secur. Comput.*, vol. 21, no. 4, pp. 2273–2284, Jul./Aug. 2024.
[62] H. Yang, S. Ju, Y. Xia, and J. Zhang, "Predictive cloud control for networked multiagent systems with quantized signals under DoS attacks," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 51, no. 2, pp. 1345–1353, Feb. 2021.
[63] D. Zhang, Y.-P. Shen, S.-Q. Zhou, X.-W. Dong, and L. Yu, "Distributed secure platoon control of connected vehicles subject to DoS attack: Theory and application," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 51, no. 11, pp. 7269–7278, Nov. 2021.
[64] J. Tang, S. Shao, J. Song, and A. Gupta, "Nash equilibrium control policy against bus-off attacks in CAN networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 980–990, 2023.
[65] M. H. Basiri, N. L. Azad, and S. Fischmeister, "Attack resilient heterogeneous vehicle platooning using secure distributed nonlinear model predictive control," in *Proc. IEEE 28th Mediterranean Conf. Control Automat.*, 2020, pp. 307–312.
[66] H. Alnabulsi and R. Islam, "Protecting code injection attacks in intelligent transportation system," in *Proc. 18th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./13th IEEE Int. Conf. Big Data Sci. Eng.*, 2019, pp. 799–806, doi: 10.1109/TrustCom/BigDataSE.2019.00116.
[67] 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.
[68] J. Ahmad et al., "Machine learning and blockchain technologies for cybersecurity in connected vehicles," *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.*, vol. 14, no. 1, 2024, Art. no. e1515.
[69] 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.
[70] A. Al-sabaawi, K. Al-dulaimi, E. Foo, and M. Alazab, *Addressing Malware Attacks On Connected and Autonomous Vehicles: Recent Techniques and Challenges*. Berlin, Germany: Springer, 2021.
[71] Q. Luo and J. Liu, "Wireless telematics systems in emerging intelligent and connected vehicles: Threats and solutions," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 113–119, Dec. 2018.
[72] S. Iqbal, A. Haque, and M. Zulkernine, "Towards a security architecture for protecting connected vehicles from malware," in *Proc. IEEE 89th Veh. Technol. Conf.*, 2019, pp. 1–5.
[73] A. Humayed, "An overview of vehicle OBD-II port countermeasures," in *Proc. Second Int. Conf. Innovations Comput. Res.*, 2023, pp. 256–266.
[74] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 993–1006, Apr. 2014.
[75] F. Kohnhäuser, D. Püllen, and S. Katzenbeisser, "Ensuring the safe and secure operation of electronic control units in road vehicles," in *Proc. 2019 IEEE Secur. Privacy Workshops*, 2019, pp. 126–131.
[76] J. Tobin, C. Thorpe, and L. Murphy, "An approach to mitigate black hole attacks on vehicular wireless networks," in *Proc. IEEE 85th Veh. Technol. Conf.*, 2017, pp. 1–7, doi: 10.1109/VTCSpring.2017.8108460.
[77] T. Delkesh, M. Ali, and J. Jamali, "EAODV : Detection and removal of multiple black hole attacks through sending forged packets in MANETs," *J. Ambient Intell. Humaniz. Comput.*, vol. 10, no. 5, pp. 1897–1914, 2019, doi: 10.1007/s12652-018-0782-7.
[78] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *Def Con*, vol. 24, no. 8, 2016, Art. no. 109.
[79] K. Greene, D. Rodgers, H. Dykhuizen, Q. Niyaz, K. Al Shamaileh, and V. Devabhaktuni, "A defense mechanism against replay attack in remote keyless entry systems using timestamping and XOR logic," *IEEE Consum. Electron. Mag.*, vol. 10, no. 1, pp. 101–108, Jan. 2021.
[80] G. Oligeri, S. Sciancalepore, O. A. Ibrahim, and R. Di Pietro, "GPS spoofing detection via crowd-sourced information for connected vehicles," *Comput. Netw.*, vol. 216, 2022, Art. no. 109230.
[81] Z. Yang et al., "Anomaly detection against GPS spoofing attacks on connected and autonomous vehicles using learning from demonstration," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 9, pp. 9462–9475, Sep. 2023.
[82] A. Chattopadhyay and K. Y. Lam, "Autonomous vehicle: Security by design," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 11, pp. 7015–7029, Nov. 2021, doi: 10.1109/tits.2020.3000797.
[83] Y. Yao, J. Zhao, Z. Li, X. Cheng, and L. Wu, "Jamming and eavesdropping defense scheme based on deep reinforcement learning in autonomous vehicle networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 1211–1224, 2023.
[84] X. Xu, X. Li, P. Dong, Y. Liu, and H. Zhang, "Robust reset speed synchronization control for an integrated motor-transmission powertrain system of a connected vehicle under a replay attack," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 5524–5536, Jun. 2021.
[85] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAP—Sybil attacks detection in vehicular ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 582–594, Mar. 2011.
[86] M. Baza et al., "Detecting sybil attacks using proofs of work and location in vanets," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 1, pp. 39–53, Jan./Feb. 2022.
[87] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan, and A. Aldegheishem, "Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles," *IEEE Access*, vol. 8, pp. 199618–199628, 2020, doi: 10.1109/access.2020.3034327.
[88] P. K. Singh, R. K. Gupta, S. K. Nandi, and S. Nandi, *Machine Learning Based Approach to Detect Wormhole Attack in VANETs*, vol. 927, Berlin, Germany: Springer, 2019.
[89] X. Cai et al., "Stability analysis of networked control systems under DoS attacks and Security Controller design with mini-batch Machine Learning Supervision," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 3857–3865, 2024.
[90] A. Kumar et al., "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm," *Microprocess. Microsyst.*, vol. 80, 2021, Art. no. 103352.
[91] B. Cherkaoui, M.-A. El Houssaini, M. Kasri, A. Beni-Hssane, and M. Erritali, "Kolmogorov-Smirnov based method for detecting black hole attack in vehicular ad-hoc networks," *Procedia Comput. Sci.*, vol. 236, pp. 177–184, 2024.
[92] 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.
[93] 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, doi: 10.1016/j.vehcom.2018.04.005.
[94] K. Stepień and A. Poniszewska-Marańda, "Analysis of security methods in Vehicular ad-Hoc network against worm hole and gray hole attacks," in *Proc. 2020 IEEE Intl Conf Parallel Distrib. Process. with Appl., Big Data Cloud Comput., Sustain. Comput. Commun., Social Comput. Netw. (ISPA/BDCloud/SocialCom/SustainCom)*, 2020, pp. 371–378.
[95] E. Ben Hamida, H. Noura, and W. Znaidi, "Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures," *Electronics*, vol. 4, no. 3, pp. 380–423, 2015, doi: 10.3390/electronics4030380.
[96] 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, doi: 10.1109/TITS.2014.2342271.
[97] P. Jiang, H. Wu, and C. Xin, "DeepPOSE: Detecting GPS spoofing attack via deep recurrent neural network," *Digit. Commun. Netw.*, vol. 8, no. 5, pp. 791–803, 2022.

[98] M. Liu, Z. Zhang, Y. Chen, J. Ge, and N. Zhao, "Adversarial attack and defense on deep learning for air transportation communication jamming," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 1, pp. 973–986, Jan. 2024.

[99] Q. Wu, F. Zhao, T. Zhao, X. Liu, J. Wang, and S. Xiao, "Stepped frequency chirp signal imaging radar jamming using two-dimensional nonperiodic phase modulation," *Front. Inf. Technol. Electron. Eng.*, vol. 24, no. 3, pp. 433–446, 2023.

[100] J. Hoffer, R. D. S. Lowande, P. Kreuser, and T. A. Youssef, "Educational review: GPS applications and vulnerability implications," in *Proc. 2020 SoutheastCon*, 2020, pp. 1–4.

[101] S. Dolev, Ł. Krzywiecki, N. Panwar, and M. Segal, "Dynamic attribute based vehicle authentication," *Wireless Netw.*, vol. 23, no. 4, pp. 1045–1062, 2017, doi: 10.1007/s11276-016-1203-5.

[102] A. Boudguiga, W. Klaudel, A. Boulanger, and P. Chiron, "A simple intrusion detection method for controller area network," in *Proc. 2016 IEEE Int. Conf. Commun.*, 2016, pp. 1–7, doi: 10.1109/ICC.2016.7511098.

[103] A. Anwar, A. Anwar, L. Moukahal, and M. Zulkernine, "Security assessment of in-vehicle communication protocols," *Veh. Commun.*, vol. 44, 2023, Art. no. 100639.

[104] G. Bendiab, A. Hameurlaine, G. Germanos, N. Kolokotronis, and S. Shiaeles, "Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 4, pp. 3614–3637, Apr. 2023.

[105] A. K. Malhi and S. Batra, "Genetic-based framework for prevention of masquerade and DDoS attacks in vehicular ad-hoc networks," *Secur. Commun. Netw.*, vol. 9, no. 15, pp. 2612–2626, 2016.

[106] A. Lotto, F. Marchiori, A. Brighente, and M. Conti, "A survey and comparative analysis of security properties of CAN authentication protocols," 2024. *arXiv2401.10736*.

[107] B. Poudel and A. Munir, "Design and evaluation of a reconfigurable ECU architecture for secure and dependable automotive CPS," *IEEE Trans. Dependable Secur. Comput.*, vol. 18, no. 1, pp. 235–252, Jan./Feb. 2021, doi: 10.1109/TDSC.2018.2883057.

[108] H. J. Jo, J. H. Kim, H.-Y. Choi, W. Choi, D. H. Lee, and I. Lee, "Mauth-CAN: Masquerade-attack-proof authentication for in-vehicle networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 2204–2218, Feb. 2020.

[109] K. Lim, T. Islam, H. Kim, and J. Joung, "A Sybil attack detection scheme based on ADAS sensors for vehicular networks," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf.*, 2020, pp. 1–5, doi: 10.1109/CCNC46108.2020.9045356.

[110] Y. Zhang, B. Das, and F. Qiao, "Sybil attack detection and prevention in VANETs: A survey," in *Proc. Future Technol. Conf.*, 2020, vol. 3, pp. 762–779.

[111] S. Abdus, A. Shadab, S. Mohammed, and B. Mohammad.Ubaidullah, "Internet of Vehicles (IoV) requirements, attacks and countermeasures," in *Proc. 5 Int. Conf. "Computing Sustain. Glob. Dev.*, 2018, pp. 4037–4040.

[112] Y. Du, F. Chen, J. Yuan, Z. Liu, and F. Yang, "Resilient distributed source localization for multi-vehicle systems under Sybil attacks," *IEEE Trans. Intell. Veh.*, vol. 9, no. 11, pp. 7392–7401, Nov. 2024, doi: 10.1109/TIV.2024.3397872.

[113] M. Scalas and G. Giacinto, "Automotive cybersecurity: Foundations for next-generation vehicles," in *Proc. IEEE 2019 2nd Int. Conf. New Trends Comput. Sci.*, 2019, pp. 1–6, doi: 10.1109/ICTCS.2019.8923077.

[114] M. A. Al-shareeda, M. Anbar, I. H. Hasbullah, S. Manickam, N. Abdullah, and M. M. Hamdi, "Review of prevention schemes for replay attack in vehicular ad hoc networks (VANETs)," in *Proc. 2020 IEEE 3rd Int. Conf. Inf. Commun. Signal Process.*, 2020, pp. 394–398.

[115] T. Limbasiya, K. Z. Teng, S. Chattopadhyay, and J. Zhou, "A systematic survey of attack detection and prevention in connected and autonomous vehicles," *Veh. Commun.*, vol. 37, 2022, Art. no. 100515.

[116] J. Lin, W. Yu, N. Zhang, X. Yang, and L. Ge, "Data integrity attacks against dynamic route guidance in transportation-based cyber-physical systems: Modeling, analysis, and defense," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8738–8753, Sep. 2018.

[117] B. Silverajan, M. Ocak, and B. Nagel, "Cybersecurity attacks and defences for unmanned smart ships," in *Proc. 2018 IEEE Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data*, 2018, pp. 1349–1354, doi: 10.1109/Cybermatics.

[118] X. Duan, H. Yan, D. Tian, J. Zhou, J. Su, and W. Hao, "In-vehicle CAN bus tampering attacks detection for connected and autonomous vehicles using an improved isolation forest method," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2122–2134, Feb. 2023.

[119] A. Braeken, "Public key versus symmetric key cryptography in client–server authentication protocols," *Int. J. Inf. Secur.*, vol. 21, no. 1, pp. 103–114, 2022, doi: 10.1007/s10207-021-00543-w.

[120] J. Cui et al., "Lightweight encryption and authentication for controller area network of autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 72, no. 11, pp. 14756–14770, Nov. 2023.

[121] S. Tangade, S. S. Manvi, and P. Lorenz, "Trust management scheme based on hybrid cryptography for secure communications in VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5232–5243, May 2020.

[122] J. Xiong, R. Bi, M. Zhao, J. Guo, and Q. Yang, "Edge-assisted privacy-preserving raw data sharing framework for connected autonomous vehicles," *IEEE Wirel. Commun.*, vol. 27, no. 3, pp. 24–30, Jun. 2020.

[123] M. S. Rathore et al., "A novel trust-based security and privacy model for internet of vehicles using encryption and steganography," *Comput. Electr. Eng.*, vol. 102, 2022, Art. no. 108205.

[124] W. Tiberti, R. Civino, N. Gavioli, M. Pugliese, and F. Santucci, "A hybrid-cryptography engine for securing intra-vehicle communications," *Appl. Sci.*, vol. 13, no. 24, 2023, Art. no. 13024.

[125] S. Safavat and D. B. Rawat, "On the elliptic curve cryptography for privacy-aware secure ACO-AODV routing in intent-based internet of vehicles for smart cities," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5050–5059, Aug. 2021.

[126] J. Shu, L. Zhou, W. Zhang, X. Du, and M. Guizani, "Collaborative intrusion detection for VANETs: A deep learning-based distributed SDN approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4519–4530, Jul. 2021.

[127] G. K. Rajbahadur, A. J. Malton, A. Walenstein, and A. E. Hassan, "A survey of anomaly detection for connected vehicle cybersecurity and safety," in *Proc. 2018 IEEE Intell. Veh. Symp.*, 2018, pp. 421–426.

[128] 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, doi: 10.1109/TIFS.2018.2812149.

[129] H. Tan, Z. Gui, and I. Chung, "A secure and efficient certificateless authentication scheme with unsupervised anomaly detection in VANETs," *IEEE Access*, vol. 6, pp. 74260–74276, 2018.

[130] N. Kabilan, V. Ravi, and V. Sowmya, "Unsupervised intrusion detection system for In-vehicle communication networks," *J. Saf. Sci. Resilience*, vol. 5, pp. 119–129, 2024.

[131] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, "Cloud-based cyber-physical intrusion detection for vehicles using deep learning," *IEEE Access*, vol. 6, pp. 3491–3508, 2017, doi: 10.1109/ACCESS.2017.2782159.

[132] R. V. J. Nguyen T. T., "Deep reinforcement learning for cyber security," *Reinf. Learn. Cyber-Phys. Syst.*, no. MI, pp. 155–168, 2019, doi: 10.1201/9781351006620-7.

[133] 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, doi: 10.1016/j.vehcom.2020.100266.

[134] J. Khoury and M. Nassar, "A hybrid game theory and reinforcement learning approach for cyber-physical systems security," in *Proc. 2020 IEEE/IFIP Netw. Operations Manage. Symp.*, 2020, pp. 1–9.

[135] F. O. Olowononi, D. B. Rawat, and C. Liu, "Trust-based adversarial resiliency in vehicular cyber physical systems using reinforcement learning," in *Proc. Int. Symp. Secur. Comput. Commun.*, 2020, pp. 139–151.

[136] 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, pp. 1–17, 2016, doi: 10.1371/journal.pone.0155781.

[137] O. Toker and S. Alsweiss, "Design of a cyberattack resilient 77 GHz automotive radar sensor," *Electronics*, vol. 9, no. 4, 2020, doi: 10.3390/electronics9040573.

[138] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "Attack resilience and recovery using physical challenge response authentication for active sensors under integrity attacks," 2016, *arXiv:1605.02062*.

[139] G. Clark, M. Doran, and W. Glisson, "A malicious attack on the machine learning policy of a robotic system," in *Proc. 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust.*, 2018, pp. 516–521, doi: 10.1109/TrustCom/BigDataSE.2018.00079.

[140] F. Lin et al., "PhaDe: Practical phantom spoofing attack detection for autonomous vehicles," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 4199–4214, 2024.

[141] L. Nie, Y. Li, and X. Kong, "Spatio-temporal network traffic estimation and anomaly detection based on convolutional neural network in vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 40168–40176, 2018.

[142] Z. Deng, J. Liu, Y. Xun, and J. Qin, "IdentifierIDS: A practical voltage-based intrusion detection system for real In-vehicle networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 661–676, 2024.
[143] S. Otoum, B. Kantarci, and H. T. Mouftah, "Detection of known and unknown intrusive sensor behavior in critical applications," *IEEE Sensors Lett.*, vol. 1, no. 5, Oct. 2017, Art. no. 7500804, doi: 10.1109/lsens.2017.2752719.
[144] J. Rupareliya, S. Vithlani, and C. Gohel, "Securing VANET by preventing attacker node using watchdog and bayesian network theory," *Procedia Comput. Sci.*, vol. 79, pp. 649–656, 2016.
[145] M. A. Shawky, M. Bottarelli, G. Epiphaniou, and P. Karadimas, "An efficient cross-layer authentication scheme for secure communication in vehicular ad-hoc networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 7, pp. 8738–8754, Jul. 2023.
[146] D. Kosmanos et al., "A novel intrusion detection system against spoofing attacks in connected electric vehicles," *Array*, vol. 5, 2020, Art. no. 100013.
[147] A. Hemida, C. Kiekintveld, C. Kamhoua, A. Sayed, A. Hemida, and C. Kiekintveld, "Strategic honeypot allocation in dynamic networks : A game-theoretic approach for enhanced cybersecurity Strategic honeypot allocation in dynamic networks : A game-theoretic approach for enhanced cybersecurity," p. –29, 2024.
[148] C. Huang, S. Member, R. Lu, and S. Member, "Secure automated valet parking : A privacy-preserving reservation scheme for autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11169–11180, Nov. 2018, doi: 10.1109/TVT.2018.2870167.
[149] U. Rajput, F. Abbas, H. Eun, and H. Oh, "A hybrid approach for efficient privacy-preserving authentication in VANET," *IEEE Access*, vol. 5, pp. 12014–12030, 2017.
[150] A. Santos et al., "ECG -based user authentication and identification method on VANETs," in *Proc. 10th Latin Amer. Netw. Conf.*, 2018, pp. 119–122.
[151] G. H. Choi, K. Lim, and S. B. Pan, "Driver identification system using normalized electrocardiogram based on adaptive threshold filter for intelligent vehicles," *Sensors*, vol. 21, no. 1, 2021, Art. no. 202.
[152] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, and K.-K. R. Choo, "Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 9, pp. 9390–9401, Sep. 2020.
[153] R. Mitchell and I. R. Chen, "Modeling and analysis of attacks and counter defense mechanisms for cyber physical systems," *IEEE Trans. Reliab.*, vol. 65, no. 1, pp. 350–358, Mar. 2016, doi: 10.1109/TR.2015.2406860.
[154] A. S. M. K. A. F. M. Suaib Akhter, Ahmet Zengin, Mohiuddin Ahmed, A. F. M. Shahen Shah, and A. Anwar, "A blockchain-based authentication protocol for cooperative vehicular ad hoc network," *MDPI*, vol. 21, no. 4, pp. 1–21, 2021.
[155] Z. Lu, Q. Wang, G. Qu, S. Member, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for VANETs," *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 27, no. 12, pp. 2792–2801, Dec. 2019, doi: 10.1109/TVLSI.2019.2929420.
[156] C. Lin et al., "BCPPA : A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 12, pp. 7408–7420, Dec. 2021, doi: 10.1109/TITS.2020.3002096.
[157] B. Li, R. Liang, D. Zhu, W. Chen, and Q. Lin, "Blockchain-based trust management model for location privacy preserving in VANET," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3765–3775, Jun. 2021, doi: 10.1109/TITS.2020.3035869.
[158] M. M. Mehdi, I. Raza, and S. A. Hussain, "A game theory based trust model for Vehicular ad hoc Networks (VANETs)," *Comput. Netw.*, vol. 121, pp. 152–172, 2017, doi: 10.1016/j.comnet.2017.04.024.
[159] J. Qi, N. Zheng, M. Xu, P. Chen, and W. Li, "A hybrid-trust-based emergency message dissemination model for vehicular ad hoc networks," *J. Inf. Secur. Appl.*, vol. 81, 2024, Art. no. 103699.
[160] Z. Shen, Y. Wang, H. Wang, P. Liu, K. Liu, and J. Zhang, "Trust mechanism privacy protection scheme combining blockchain and Multi-party evaluation," *IEEE Trans. Intell. Veh.*, vol. 9, no. 2, pp. 3885–3894, Feb. 2024.
[161] C. A. Kamhoua, C. D. Kiekintveld, F. Fang, and Q. Zhu, *Game Theory and Machine Learning For Cyber Security*. Hoboken, NJ, USA: Wiley, 2021.
[162] I. Kalderemidis, A. Farao, P. Bountakas, S. Panda, and C. Xenakis, "GTM: Game Theoretic methodology for optimal cybersecurity defending strategies and investments," in *Proc. 17th Int. Conf. Availability, Rel. Secur.*, 2022, pp. 1–9.
[163] L. Liu, C. Tang, L. Zhang, and S. Liao, "A generic approach for network defense strategies generation based on evolutionary game theory," *Inf. Sci. (Ny).*, vol. 677, 2024, Art. no. 120875.
[164] H. Sedjelmaci, M. Hadji, and N. Ansari, "Cyber security game for intelligent transportation systems," *IEEE Netw.*, vol. 33, no. 4, pp. 216–222, Jul./Aug. 2019, doi: 10.1109/MNET.2018.1800279.
[165] M. H. Basiri, M. Pirani, N. L. Azad, and S. Fischmeister, "Security of vehicle platooning: A game-theoretic approach," *IEEE Access*, vol. 7, pp. 185565–185579, 2019.
[166] Y. Yan et al., "A multi-vehicle game-theoretic framework for decision making and planning of autonomous vehicles in mixed traffic," *IEEE Trans. Intell. Veh.*, vol. 8, no. 11, pp. 4572–4587, Nov. 2023.
[167] X. Zhang, S. Ding, B. Ge, B. Xia, and W. Pedrycz, "Resource allocation among multiple targets for a defender-attacker game with false targets consideration," *Reliab. Eng. Syst. Safty*, vol. 211, 2021, Art. no. 107617, doi: 10.1016/j.ress.2021.107617.
[168] Q. Feng, H. Cai, and Z. Chen, "Using game theory to optimize the allocation of defensive resources on a city scale to protect chemical facilities against multiple types of attackers," *Reliab. Eng. Syst. Safty*, vol. 191, 2019, Art. no. 105900, doi: 10.1016/j.ress.2017.07.003.
[169] K. Pan, L. Wang, and L. Zhang, "A study on enhancing the information security of Urban traffic control systems using evolutionary game theory," *Electronics*, vol. 12, no. 23, 2023, Art. no. 4856, doi: 10.3390/electronics12234856.
[170] E. S. Dawam, X. Feng, and D. Li, "Autonomous arial vehicles in smart cities: Potential cyber-physical threats," in *Proc. IEEE 20th Int. Conf. High Perform. Comput. Commun. 16th Int. Conf. Smart City 4th Int. Conf. Data Sci. Syst. HPCC/SmartCity/DSS*, 2019, pp. 1497–1505, doi: 10.1109/HPCC/SmartCity/DSS.2018.00247.
[171] Z. Xiong, H. Xu, W. Li, and Z. Cai, "Multi-source adversarial sample attack on autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2822–2835, Mar. 2021.
[172] A. Masood, D. S. Lakew, and S. Cho, "Security and privacy challenges in connected vehicular cloud computing," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2725–2764, Fourthquarter 2020.
[173] V. P. Chellapandi, L. Yuan, C. G. Brinton, S. H. Żak, and Z. Wang, "Federated learning for connected and automated vehicles: A survey of existing approaches and challenges," *IEEE Trans. Intell. Veh.*, vol. 9, no. 1, pp. 119–137, Jan. 2024.
[174] C. Zhao, L. Zhang, Q. Wu, and F. Rezaeibagha, "Publicly accountable data-sharing scheme supporting privacy protection for fog-enabled VANETs," *IEEE Trans. Veh. Technol.*, vol. 73, no. 6, pp. 8487–8502, Jun. 2024.
[175] H. Guan, H. Wang, Q. Meng, and C. L. Mak, "Markov chain-based traffic analysis on platooning effect among mixed semi-and fully-autonomous vehicles in a freeway lane," *Transp. Res. Part B Methodol.*, vol. 173, pp. 176–202, 2023.

Bhosale Akshay Tanaji received the M.Tech. degree in operations research from the National Institute of Technology, Durgapur, India, in 2019. He is currently working toward the Ph.D. degree with the Department of Industrial and Systems Engineering, Indian Institute of Technology Kharagpur, India. His research interests include optimization, game theory, reinforcement learning, and cybersecurity.

Sayak Roychowdhury received the M.S. and Ph.D. degrees from the Department of Integrated Systems Engineering, The Ohio State University, Columbus, OH, USA, in 2014 and 2017, respectively. He is currently an Assistant Professor with the Department of Industrial and Systems Engineering, Indian Institute of Technology (IIT) Kharagpur, India. His areas of interest include statistical learning, operations research, reinforcement learning, quality engineering, and stochastic optimization. After finishing his doctoral studies, he worked for Netjets, Inc., as a Senior Operational Analyst for a year before joining IIT Kharagpur in 2018.