IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 29 November 2023, accepted 17 December 2023, date of publication 25 December 2023,
date of current version 3 January 2024.

Digital Object Identifier 10.1109/ACCESS.2023.3347200

SURVEY

Securing the Future: A Comprehensive Review of Security Challenges and Solutions in Advanced Driver Assistance Systems

ARYAN ALPESH MEHTA[1], ALI ASGAR PADARIA[1], DWIJ JAYESH BAVISI[1], VIJAY UKANI[1], PRIYANK THAKKAR[1], REBEKAH GEDDAM[1], KETAN KOTECHA[2], AND AJITH ABRAHAM[3,4], (Senior Member, IEEE)

[1]Computer Science and Engineering Department, Institute of Technology, Nirma University, Ahmedabad, Gujarat 382481, India
[2]Symbiosis Centre for Applied Artificial Intelligence, Symbiosis Institute of Technology, Symbiosis International University, Pune 411045, India
[3]School of Computer Science Engineering and Technology, Bennett University, Greater Noida, Uttar Pradesh 201310, India
[4]Center for Artificial Intelligence, Innopolis University, Innopolis, 420500 Republic of Tatarstan, Russia

Corresponding authors: Priyank Thakkar (priyank.thakkar@nirmauni.ac.in), Vijay Ukani (vijay.ukani@nirmauni.ac.in), and Ajith Abraham (abraham.ajith@gmail.com)

This work was supported by the Analytical Center for the Government of the Russian Federation in November 2021, under Grant 70-2021-00143 and Grant IGK 000000D730321P5Q0002.

ABSTRACT Advanced Driver Assistance Systems (ADAS) are advanced technologies that assist drivers with vehicle operation and navigation. Recent improvements and brisk expansion in the ADAS market, as well as an increase in the frequency of incidents such as sensor spoofing, communication interruption etc., in autonomous vehicles (AVs), have raised the need to research ADAS security technology. The security issues raised by incorporating these technologies into automobiles must be addressed to protect the privacy and safety of passengers and other road users. As a result, the purpose of this research is to investigate the security issues that arise from the integration of ADAS technologies. Addressing these challenges holds the potential to establish a foundation for enhanced safety and dependability within transportation networks amidst the ongoing advancements in vehicle technology. This paper starts by describing the vulnerabilities, threats, assaults, and defense mechanisms of the ADAS. It then delves into the attacks and countermeasures in three categories, namely VANET, Hardware, and Adversarial attacks. VANET attacks encompass threats targeting Vehicular Ad Hoc Networks, aiming to disrupt communication among vehicles or between vehicles and infrastructure. Hardware attacks focus on vulnerabilities within the physical components of ADAS, including sensors, processors, or communication modules. Adversarial attacks involve deliberate manipulations or perturbations introduced into machine learning models or algorithms utilized within ADAS. These attacks aim to deceive or undermine the functionality of AI-based systems, causing misclassification, compromising system integrity, and posing risks to user safety by exploiting vulnerabilities in the AI decision-making process. Finally, this study highlights potential areas for future research, such as the utilization of artificial intelligence (AI), the necessity of industry-wide standardization, and recommends specific future work tailored to each attack described in the corresponding sections.

INDEX TERMS Advanced driver assistance systems (ADAS), attacks, countermeasures, defences, security, threats.

I. INTRODUCTION

ADAS stands for ''Advanced Driver Assistance System''. It describes a group of electronic devices and technologies that help drivers operate their cars more safely and effectively. ADAS has numerous electrical and digital tools that aid drivers in minimizing errors and performing parking functions, among other things. The primary goal of this study is to lessen human mistakes and prevent accidents through technologies like automatic emergency braking, collision

The associate editor coordinating the review of this manuscript and approving it for publication was Lei Shu.

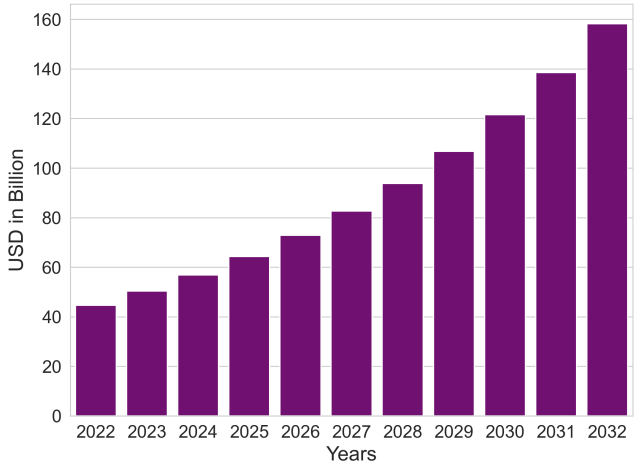

FIGURE 1. Estimated growth of ADAS market.

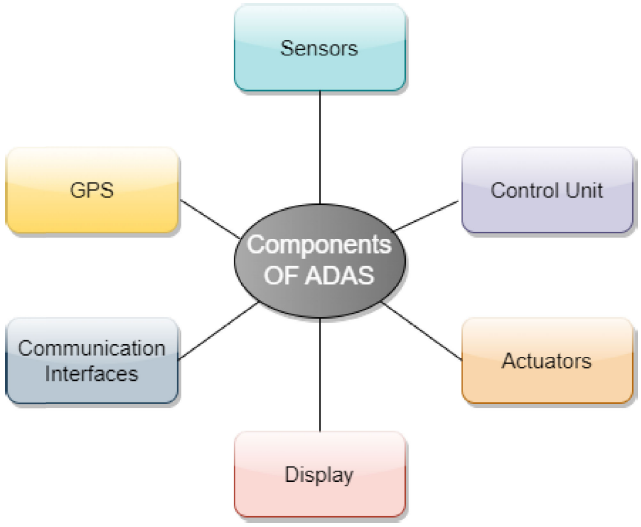

FIGURE 2. Components of ADAS.

avoidance, lane-keeping assistance, and autonomous cruise control. These features assist drivers in avoiding collisions and maintaining safe driving practices. The environment and vehicle safety are improved by ADAS thanks to its cutting-edge interface technology. It utilizes automated devices, such as cameras and sensors, to swiftly respond to driver errors or obstacles. The use of ADAS in vehicles is rising, as shown in Fig. 1 [1]. Unaware of it, some of us may use ADAS while operating our vehicles. The technology is based on data from cameras or other sensors with a wider field of view than a human. Given that self-driving cars utilize many of the technologies and principles of ADAS, it is thought that ADAS will be crucial in developing autonomous vehicles. A study by the American Automobile Association (AAA) [2] found that each year, 9.500 fatalities, 1.1 million injuries, and 2.7 million collisions can be avoided thanks to ADAS systems if installed on all vehicles. ADAS is also being incorporated into conventional automobiles to enhance driver safety and lower the probability of incidents on the road.

A. COMPONENTS OF ADAS

ADAS use various electronic components to provide various driver assistance features as shown by FIGURE 2. Here are some of the common components of ADAS:

1) SENSORS

Sensors are tools for detecting and measuring physical environmental variables. Cameras, radar, lidar, ultrasonic sensors, and combinations are all examples of sensors in the context of ADAS. Although radar, lidar, and ultrasonic sensors detect objects and estimate their distance from the vehicle, cameras record visual data. The data flow from the sensors to the ADAS system, which governs various vehicle components such as the steering wheel, acceleration, and braking, is illustrated in FIGURE 3. As a state-of-the-art approach,the paper [3] proposes a continuous and differentiable reference speed model for autonomous vehicles, using a hyperbolic tangent curve to improve passenger comfort by smoothing speed changes in various driving scenarios, achieving significant reductions in acceleration and jerk. Together, these sensors produce a 360-degree image of the area around the car and feed information to the ADAS control unit. Ziebinski et al. [4], studied and discussed a variety of sensors used as part of ADAS.

Continuous upgradation in technology and increased expectations from the automobile industry relating to driver support and safety have led to the development of ADAS based on various technologies. These systems can warn drivers of potential dangers or actively control the vehicle in emergencies. The study offers an overview of current ADAS capabilities and modules and proposes that there is still potential for further development, particularly through sensor fusion. The paper focuses on the potential application of sensor fusion to an autonomous mobile platform in the future.

The authors provide a general ADAS sensor error injection architecture in [5] for the System under Test (SuT)'s robustness testing. The paper proposed a modular sensor model design architecture for ADAS virtualization testing. The architecture was built on items that represented the environment around the car and were altered during the sensing process. A stochastic modification of the target object's position was used to create an example model.

2) CONTROL UNIT

The brain of the system, the ADAS control unit, is in charge of processing sensor data and making judgments based on it. The control unit analyses sensor data using algorithms and machine learning models to discover potential dangers, like objects in the path of the automobile or cars coming from the blind area. This analysis allows the control unit to decide whether to inform the driver or take action to prevent an accident. The authors of [6] researched the deterministic

architecture and middleware of domain control units and proposed a streamlined integration procedure for ADAS.

3) ACTUATORS

Actuators are crucial in ADAS, converting electrical signals into physical movement to control mechanical systems like brakes, steering, and suspension. They assist drivers in various ways, including adaptive cruise control, which uses the throttle and brakes to maintain a safe separation from the vehicle ahead of you. The paper [7] introduces a state-of-the-art innovative Adaptive Cruise Control (ACC) system integrated with weather adaptation, using dynamic reference signals and advanced control techniques to ensure high safety and comfort performance across various weather conditions. With lane departure warning systems, actuators can gently steer the car back into the right lane. In collision avoidance systems, actuators can apply the brakes or steer the vehicle to prevent an accident. They adjust the suspension for improved stability and handling in different driving conditions. Overall, actuators are essential for many ADAS functions and enhance the safety and performance of modern vehicles. Enders et al. [8] discussed the limitations of actuators in cars, including factors such as comfort, the maximum force, and the rate of change that can be experienced during a journey, among others.

4) DISPLAY

The driver is given information via displays, such as alerts or warnings. These may include audible or visible cues, like a flashing dashboard light or a warning sound. Screens can also provide details about the area around the car, such as a view of the blind spot or a camera feed from a backup camera. Many problems are possible due to the failure of display devices. In [9], the authors studied the effects of screen failure on driving performance in automated cars. They found that after the failure, objective trust declined, drivers took over more frequently, and lateral vehicle control was compromised.

5) COMMUNICATION INTERFACES

A communication interface allows different system components to exchange data and information. Multiple sensors, processors, control units, and actuators make up ADAS systems, all of which require real-time communication to function properly. Common communication interfaces used in ADAS include the Controller Area Network (CAN), FlexRay, Local Interconnect Network (LIN) and Ethernet. These interfaces allow processing units to exchange sensor data, such as that from cameras and radar, for analysis and decision-making. In order to carry out actions determined by the system analysis, they also facilitate communication between control units and actuators. A number of variables, including data bandwidth, real-time demands, system complexity, and security concerns, influence the selection of a communication interface.

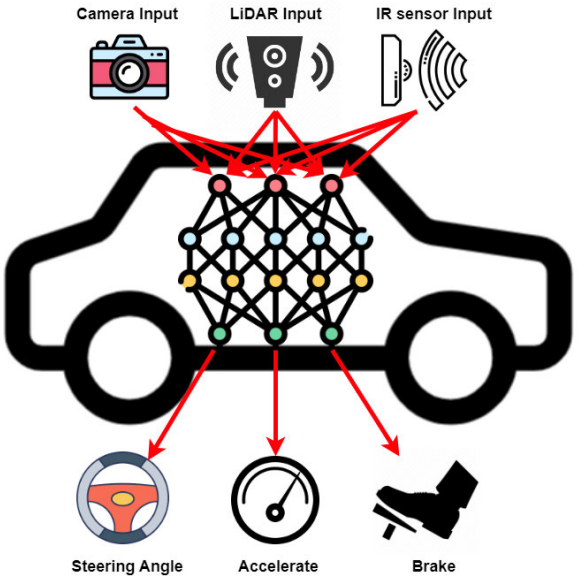

FIGURE 3. Sensors in ADAS.

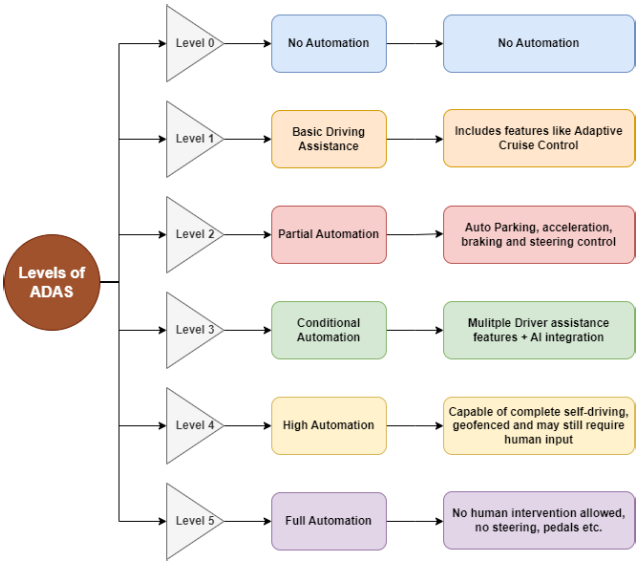

FIGURE 4. Levels of ADAS.

6) GLOBAL POSITIONING SYSTEM (GPS)

ADAS control unit has the capability to receive real-time data on the vehicle's precise position and speed through GPS (Global Positioning System) technology. This valuable input significantly enhances the accuracy and effectiveness of various ADAS functionalities, including adaptive cruise control, which utilizes GPS information to intelligently maintain a safe distance from surrounding vehicles on the road.

Adaptive cruise control, automated emergency braking, blind-spot monitoring, and parking assistance are just a few of the driver-aid features that ADAS may provide, thanks to the combination of the aforementioned components.

B. LEVELS OF ADAS

ADAS encompasses a range of automation levels with six distinct levels of advancement. These levels, ranging from 0 to 5, represent a spectrum of automation capabilities, from complete driver reliance to full automation. An in-depth discussion about the levels of ADAS has been presented in [10]. FIGURE 4 shows that ADAS systems can be divided into distinct levels:

Level 0: No Automation At this level, there are no ADAS functions in the car; therefore, the driver must do all driving duties. Seat belts, airbags, and anti-lock brakes are all basic safety equipment; however, they are not intended to aid with driving functions actively. As a result, the whole responsibility for maintaining a high level of situational awareness and exercising total control over the vehicle rests with the driver. To protect the safety and well-being of all passengers as well as other road users, this includes staying alert, responding quickly to changing road conditions, keeping an eye on the vehicle's performance, and making educated judgments at the moment.

Level 1: Driving Assistance The vehicle has basic ADAS technologies at this level of automation that help the driver with some aspects of driving. The features could include lane departure warning, which alerts the driver when the car veers out of its lane, or adaptive cruise control, which adjusts the speed of the car to preserve a suitable distance to follow from other vehicles. However, the driver is still primarily responsible for all driving-related activities and must remain vigilant.

Level 2: Partial Automation The vehicle is partially automated at this level and can drive in some situations, such as in low-speed or highway traffic. The vehicle may contain features like traffic jam assist, which may steer, brake, and accelerate the vehicle automatically in slow-moving traffic, or lane keeping assist, which can guide the vehicle to maintain it in its lane. However, the driver must always be alert and concentrated, prepared to take over at any time.

Level 3: Conditional Automation At this stage, the vehicles possess the ability to perceive their surroundings and autonomously make intelligent choices, such as overtaking a slow-moving vehicle. These vehicles may be equipped with advanced features like automated valet parking or traffic jam pilot, allowing them to navigate through traffic without requiring the driver's active involvement. However, there are instances when human intervention might be necessary, and as a result, the driver must remain vigilant and ready to assume control of the vehicle when required.

Level 4: High Automation In specific circumstances, such as on a highway or in a city, the vehicle can handle all aspects of driving. The vehicle may have capabilities like highway autopilot, which can operate from entry to exit on a highway, or urban autopilot, which may operate in city traffic. The majority of the time, the vehicle can drive itself; therefore, the driver may not always be prepared to take over. In the absence of driver intervention, the vehicle has the capability to perceive and respond to its environment autonomously.

Level 5: Full Automation A vehicle can operate autonomously in all driving situations at this level. There is no need for a human driver because the vehicle is entirely autonomous. Without the assistance of the driver, the vehicle can perceive and react to its surroundings. This level of automation is currently under development and not yet publicly accessible. The vehicle may operate without human input, and the driver can participate in other tasks while in the vehicle.

C. ETHICAL CONSIDERATIONS IN ADAS

1) DATA PRIVACY AND USER CONSENT

Ensuring user privacy is a cornerstone of responsible ADAS deployment. ADAS systems gather a wealth of data, ranging from driving patterns to personal information. Protecting this data involves robust encryption, anonymization techniques, and secure storage protocols. Moreover, respecting user consent is pivotal. Users must be informed about the data collected, how it's utilized, and provided with mechanisms to control their information. Transparency in data usage builds trust between users and ADAS systems.

2) RESPONSIBLE AI DEPLOYMENT

The integration of AI in vehicles mandates a responsibility to ensure the safety and reliability of these systems. Rigorous testing, validation, and continuous monitoring are essential to minimize risks associated with AI-driven decisions. It's imperative for developers and manufacturers to prioritize the safety of users while maintaining the functionality and efficacy of ADAS features.

3) ADDRESSING BIAS AND ENSURING FAIRNESS

AI algorithms powering ADAS systems can inadvertently perpetuate biases, potentially leading to unequal treatment among different demographic groups. Addressing and mitigating biases is a crucial ethical consideration. Efforts to ensure fairness in decision-making processes must be integral to the development lifecycle. Implementing techniques that actively detect and rectify biases helps in fostering a more equitable ADAS environment.

By incorporating these ethical considerations into the development and deployment of ADAS technologies, we can foster a safer, more transparent, and ethically conscious future for automotive advancements.

D. CONTRIBUTIONS

The following are the major contributions of this article.

- This paper provides an overview of ADAS and highlights the growing importance of security in ADAS.
- The paper provides a comprehensive overview of the security threats and vulnerabilities in ADAS systems, including attacks on VANET, hardware, and adversarial attacks.
- The paper identifies and discusses various countermeasures and defense mechanisms that can be employed to mitigate the impact of attacks on ADAS systems.

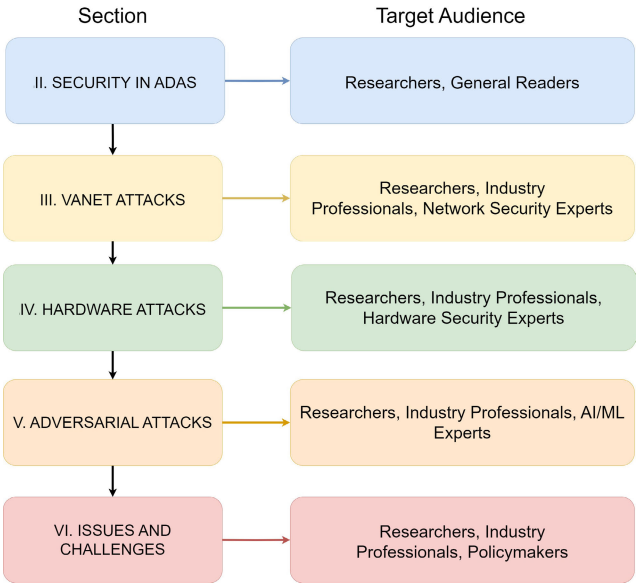

FIGURE 5. Section-wise target audience.

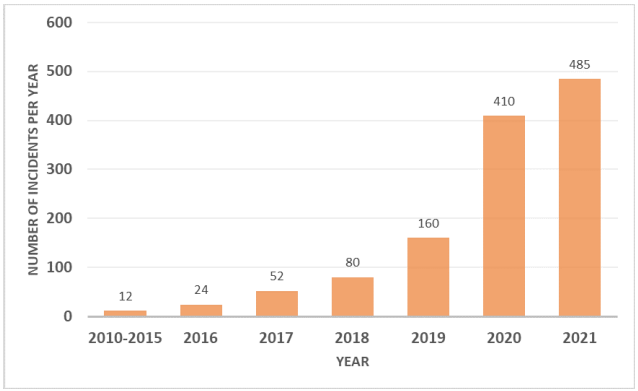

FIGURE 6. Rise in number of incidents in AV.

Furthermore, the complexities and limitations of countermeasures are also provided.

- The paper suggests future research directions for each discussed section on attacks, ie. VANET, Hardware, Adversarial attacks.

E. TAXONOMY

Further in this paper, Section III focuses on VANET attacks, discussing sub-types of attacks such as Sybil attacks and Distributed Denial of Service (DDoS) attacks, among others, along with their impacts on ADAS, prevention measures, and research direction. Section IV delves into hardware attacks, including but not limited to firmware attacks and jamming attacks, detailing their impacts on ADAS and hardware components and offering preventive measures and research direction. Section V explores adversarial attacks, such as patch attacks and training phase attacks, explaining their impacts on ADAS components like perception systems and machine learning models, prevention measures, and research direction. Section VI addresses four main challenges in ADAS: Cyber Threats, Errors and Malfunctions, human factors, and Supply Chain Security. Each challenge is discussed extensively, covering examples, impacts, and prevention strategies. The paper concludes in section VII by emphasizing the significance of understanding and addressing these vulnerabilities to develop robust security measures in ADAS.

FIGURE 5 illustrates the target audience for each section, indicating the specific audience for whom the content of that particular section is best suited.

II. SECURITY IN ADAS

ADAS has developed as a vital component of modern automobiles in today's fast-expanding automotive market. With advanced sensors, cameras, and clever algorithms, ADAS systems provide a wide range of benefits, including better safety, convenience, and driving comfort. However, as ADAS systems become more widely used, providing solid security measures within these systems becomes increasingly important. ADAS security protects the systems' integrity and performance, safeguards the safety and privacy of vehicle occupants, and mitigates potential financial risks. Let us explore the vulnerabilities, threats, attacks, and defenses related to ADAS security.

Vulnerabilities: ADAS systems have flaws in their network, software, and hardware components. Attackers may use ADAS systems' flaws to their advantage. For instance, a flaw might give a potential attacker remote access to the vehicle's system and command over its operations. Updates and patches that may not have been thoroughly evaluated before being applied may introduce vulnerabilities. In [11], the authors conducted several tests on an actual vehicle to see how vulnerable it is to potential assaults. The study also showed how an ADAS-equipped vehicle makes it possible for attackers to take over key modules. Many vulnerabilities in vehicles were studied and explored in [12], [13], [14], [15], [16], and [17].

Through the use of effective and affordable wired and wireless physical-layer relays, On the Passive Keyless Entry and Start (PKES) systems used in contemporary cars, Francillion et al. [12] showed relay attacks. These vulnerabilities allow attackers to start and enter a vehicle by relaying messages between the smart key and the vehicle. The authors offer rapid mitigation measures to lower the risk of relay assaults as well as techniques that might prevent relay attacks while keeping simplicity of use. It's possible that other PKES systems created using similar principles are similarly vulnerable to the relay attack because of how general it is.

Koscher et al. [14] in their paper experimentally evaluated the potential risks introduced by the digital transformation of modern automobiles. The researchers demonstrated the ability of an attacker to completely circumvent safety-critical systems and adversarially control various automotive functions, including disabling the brakes and stopping the engine. They also presented composite attacks leveraging

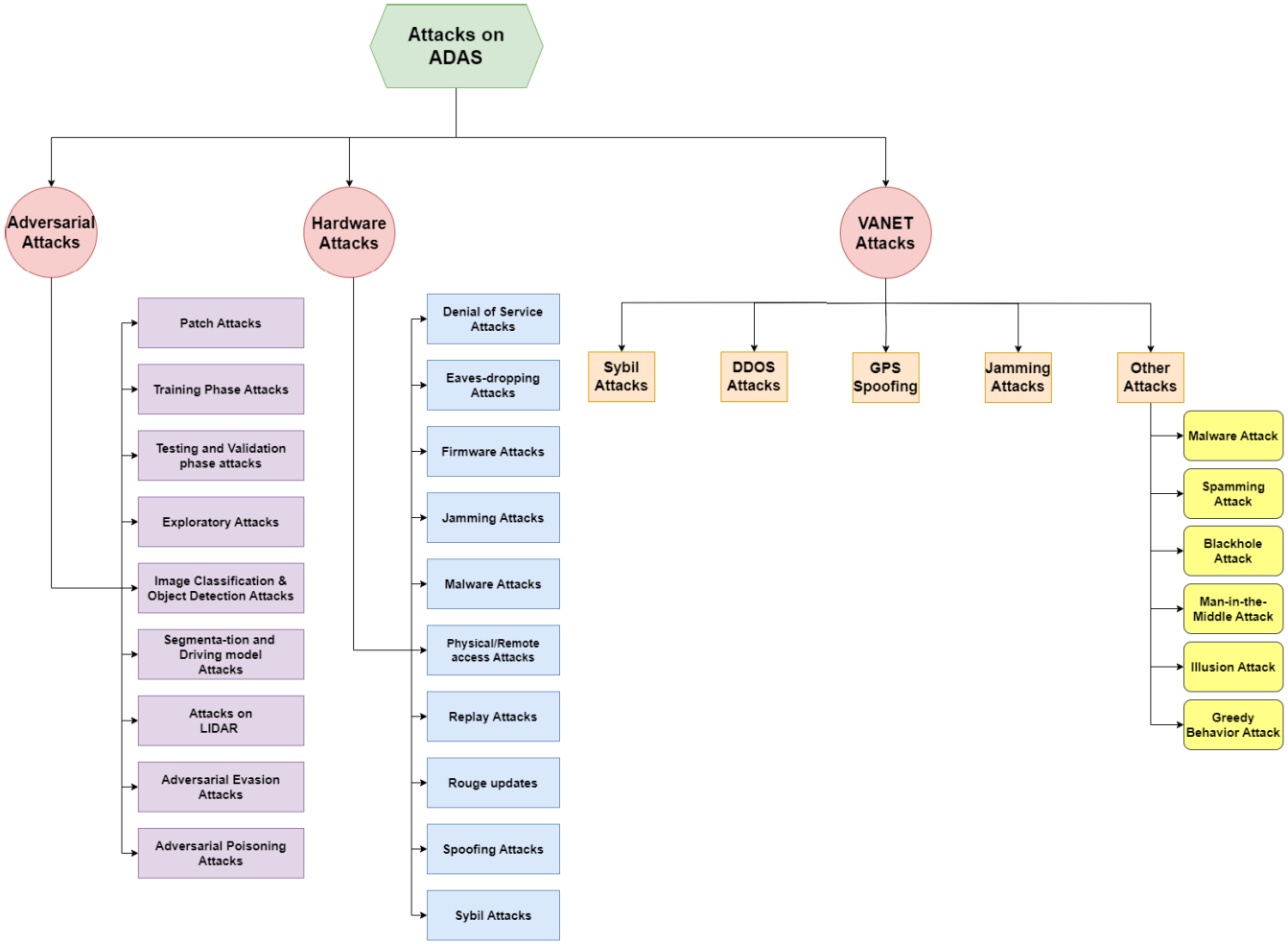

FIGURE 7. Taxonomy of paper.

individual weaknesses and discussed the challenges in addressing these vulnerabilities.

Real-life incidents underscore the dangers posed by vulnerabilities in Advanced Driver Assistance Systems (ADAS), such as the well-documented issue of phantom braking. These systems can sometimes misinterpret shadows or objects as pedestrians or vehicles, leading to sudden and unnecessary braking, especially on high-speed roads like motorways. In a 2021 incident in California, a Tesla Model 3 on autopilot collided with a parked police car when the vehicle unexpectedly engaged the brakes, even though there was no obstruction in its path. Another tragic incident occurred in Tempe, Arizona, where Elaine Herzberg, a pedestrian, was fatally struck by an autonomous Uber vehicle. These incidents underscore the imperative of continuous development and rigorous testing to address the limitations of ADAS and ensure their reliability in challenging conditions. Furthermore, they also highlight the necessity for ongoing research and development in this technology to improve overall road safety.

Various techniques can be used to find vulnerabilities in ADAS. These include information sharing and collaboration within the sector, close cooperation with manufacturers and suppliers, implementation of incident response plans and continuous monitoring, threat modeling to assess potential attack scenarios, risk assessments to prioritize security efforts, and security audits to ensure compliance with standards.

Threats: ADAS systems are subject to various threats. An attacker may, for instance, utilize a vulnerability to take over the car, steal financial or personal information from the computer inside, or use the vehicle as a launchpad for attacks on other systems. Natural calamities like a solar storm, which might interfere with or harm the vehicle's electronics, could also pose a threat. To protect the systems from threats, advanced threat assessment prediction models have been made possible recently by performance improvements in computer technology. In that case, the focus has shifted away from models based on kinematics, such as constant velocity [18], constant turn rate and acceleration [19], [20], or heuristics [21], and towards models based on learning that are trained on observed measurements. The applications of machine learning (ML) are to recognize lane changes [22],

forecast unintentional lane departures [23], [24], [25], [26], [27], predict the motion of nearby cars [28], [29], [30], predict the path of the individual vehicle [31], [32], [33], and predict the motion of adjacent vehicles, as well as for automatic driving (AD) [22]. This change has been prompted by the growing processing capability of the onboard computers and the ability of ML approaches to model complicated relationships between input and output data in a highly automated manner [34]. In Prediction-Uncertainty-Aware Threat Detection [35] the author proposed four threat-detection methods that leverage ML-based prediction models to improve advanced driver assistance systems' accuracy. The methods use real-time prediction uncertainty estimates to ensure trustworthy intervention decisions in challenging cases.

In transportation, platooning or flocking is a method for driving a group of vehicles together. It is meant to increase the capacity of roads via an automated highway system. However, platooning presents several challenges. Platooning problem of connected vehicles subject to communication interruptions and latency was investigated by the paper [36]. These shows real-world prevalence of such threats.

Attacks: Malware, phishing, social engineering, and physical attacks are a few ways ADAS systems might come under attack. An overview of the threats to self-driving cars was provided in [37]. For instance, an attacker may fool a user into downloading malware using a phishing email, which would then allow the attacker to take over the car's computer system. Physical assaults might involve interfering with the vehicle's electronics by using the wireless interface for communication with other equipment or an onboard diagnostic port. The authors of [38] investigated the common ADAS's resistance to safety-critical attacks that target the control system during various driving scenarios and result in accidents. According to their experimental findings, proposed context-aware attacks can successfully generate dangers with an 83.4 % success rate, 99.7 % of which happen without any prior notice.

More recent threats include exploitation of Buffer Overflow Vulnerabilities in ADAS [39]. BOFs are particularly dangerous because they can enable attackers to execute arbitrary code on a compromised system. This code can perform malicious actions, such as taking control of the system, stealing sensitive data, or launching other attacks.

Defense: To ensure the safety and security of the people inside the vehicle and other road users, defense against ADAS attacks is essential. Software updates and patches, secure coding techniques, encryption of critical data, and network segmentation are a few examples of defense mechanisms that can be used to reduce the impact of assaults. Access control techniques, intrusion detection and prevention systems, and firewalls are other possible defense measures. Wang et al. [40] have created two deep-learning models, a predictor-based model and an encoder-decoder-based model, to detect security attacks. The experimental findings highlight the relative advantages of different models and help provide a technique for creating learning-based intrusion detection approaches. Cho and Shin [41] proposed a method for detecting AV system intrusion by fingerprinting the clock skew of the ECUs and detecting those that differ from the authentic ones.

The discussion on the importance of cybersecurity in advanced automotive systems, particularly Advanced Driver Assistance Systems (ADAS), which play a crucial role in autonomous driving, was done in [42]. The paper highlights the need for cybersecurity measures beyond functional safety standards like ISO 26262 due to the growing use of connected technologies. The paper introduces ISO/SAE 21434 as a cybersecurity baseline for automakers and maps its requirements to traditional system design processes. It also presents a Threat Analysis and Risk Assessment approach and offers risk mitigation strategies. Overall, the paper emphasizes the significance of holistic cybersecurity engineering in automotive systems to address evolving cyber threats.

An introduction to cybersecurity analysis framework compliant with ISO/SAE 21434:2021 to address the growing cyber threats in modern automobiles were presented in [43]. The framework employs the STRIDE threat model, Attack Tree Analysis (ATA), and Common Vulnerability Scoring System (CVSS) to assess potential threats in Advanced Driver-Assistance Systems (ADAS). The framework identifies and addresses 199 potential threats across ADAS-related use cases, emphasizing the vulnerability of modern vehicles to cyberattacks and proposing security countermeasures.

Security for ADAS systems is a complicated subject requiring continual care and commitment. Manufacturers, software developers, and users must collaborate to find and fix vulnerabilities, guard against threats, and defend against assaults to guarantee ADAS systems' security and safety.

All the above-mentioned concerns are very important as ADAS systems are made to increase the vehicle's and its occupants' security. Thus, any flaw or attack that jeopardizes the system could have detrimental effects on everyone's safety. For instance, a perpetrator could take control of the vehicle and cause a collision or mechanical issue that results in harm or death. Also, sensitive information about the vehicle and its occupants, including location, speed, and driving style, is frequently collected and transmitted by ADAS systems. A vulnerability or attack compromising this data could result in privacy violations and other security problems. Due to the high installation and maintenance costs associated with ADAS systems, both vehicle owners and manufacturers are exposed to potential financial losses if the system experiences vulnerabilities or disruptions caused by attacks.

AI in ADAS: Previous sections have highlighted the multifaceted nature of Advanced Driver Assistance Systems (ADAS). It comprises of integral components such as longitudinal control, lateral control, driving vigilance

monitoring, and parking assistance, as elucidated in the study in [44]. Recent research, exemplified by Shruti et al. [45], underscores the substantial advantages derived from integrating diverse machine learning, deep learning, and vision algorithms into these systems. Their findings underscore the critical role of artificial intelligence (AI) in enabling the functionality of such systems, indicating that without AI integration, the development of these systems becomes considerably challenging.

Supervised machine learning methodologies offer versatile applications, particularly in the realms of lateral and longitudinal control, leveraging sensor data to formulate models that detect obstacles and ensure optimal driving safety. Hou et al. [46] showed this by devising a system facilitating mandatory lane changes at drop lanes. Their innovative approach combined decision-tree and Bayes classifiers. Similarly, Morris et al. [47] introduced a groundbreaking method employing the Relevance Vector Machine (RVM), an extension of Bayesian techniques within Support Vector Machines (SVM), to anticipate a driver's intent to change lanes.

Another AI methodology, Object detection, stands as a pivotal task within Autonomous Vehicles (AVs). Huval et al. [48] introduced a model leveraging a Convolutional Neural Network (CNN) specifically designed for the real-time detection of lanes and vehicles on highways. Additionally, Lee and Yeo [49] presented a system aimed at real-time Collision Warning, employing a Multi-Layer Perceptron Neural Network (MLPNN) for this purpose.

While these cases highlight the utilization of AI models within ADAS, a pressing concern emerges regarding the security implications tied to these AI-driven functionalities. The vulnerability arises from the potential for intruders to manipulate these models, posing significant risks to user safety. For instance, if the Collision Warning system is tampered with, its ability to accurately prevent collisions could be severely compromised, leading to misclassified scenarios. Consequently, users prompted by a compromised system might take incorrect actions, inadvertently resulting in accidents. Section V provides an in-depth exploration of Attacks on AI systems, shedding light on this critical issue.

A. CASES WHERE ADAS SYSTEMS ARE COMPROMISED

ADAS systems typically comprise distinct electronic control units (ECUs) linked via serial buses, communicating through a standardized protocol known as the Controller Area Network (CAN). Unlike traditional networks, CAN lacks a central primary node, as each node autonomously initiates t3ransmission and arbitration. Unfortunately, the CAN protocol doesn't incorporate inherent safeguards against traffic sniffing or spoofing, rendering it an appealing target for intruders. Moreover, the CAN-bus lacks a crucial security element: message identification [11]. Consequently, the interaction of ADAS systems with vital ECUs via the CAN bus exposes vehicles to heightened vulnerability against diverse attacks.

An article by McKinsey & Company [50] discussed the expected increase in demand for ADAS over the next decade and the technical challenges that need to be addressed. In the same year, an assessment of ADAS using real world scenarios [51] discussed the importance of testing and validation in developing future ADAS and Automated Driving Systems. The method developed in the paper was demonstrated by testing an Adaptive Cruise Control (ACC) system in scenarios where the predecessor of the ego vehicle is braking. This is a real-world scenario where the ACC system needs to respond appropriately to prevent a collision.

In 2017 and 2019, respectively, the BMW and Tesla autonomous vehicles received presentations on offensive security research from the security research lab Keen Lab of the Tancent Group [52]. Keen Lab also exploited browser and Wi-Fi vulnerabilities with 0-day attacks to take control of susceptible features in Tesla and BMW self-driving cars [53]. A person's life is severely disrupted when autonomous cars are tampered with like this.

A case was recorded in a research study [54] where a virus was created to manipulate messages transmitted through the controller area network (CAN) bus. This malware could remotely immobilise a car by intercepting the relevant signals of the central system and locking the doors. The presence of security vulnerabilities presents substantial risks to both driver safety and privacy.

The authors built the CarShark tool in [14] to oversee the data flow within the CAN bus system of a vehicle. By analysing and altering network packets, the tool was able to simulate a man-in-the-middle attack on the CAN network. By modifying the data packets, they were able to influence the sensor's values, showcasing that this threat could also pose a significant danger to self-driving vehicles.

Technological advancements have made it possible to utilise car hardware components, such as the Onboard Diagnostic (OBD) port, for multiple types of attacks. The article [55], for instance, shows how to successfully compromise several car types via the OBD port. Remote vehicle control is one of the possible outcomes of such breaches.

B. THE SIGNIFICANCE OF SECURITY IN ADAS

ADAS technologies are made to help drivers prevent collisions and increase traffic safety. Still, if these systems are corrupted, they can result in accidents or fail to stop them, endangering the lives of drivers and passengers. For instance, if a hacker takes over a car's braking system, it might accelerate or stop unexpectedly, resulting in a collision. A hacker might also cause a vehicle to veer off the road or collide with other vehicles if they take over the steering system.

Data about the vehicle and its occupants, such as location, speed, and driving style, are collected and transmitted by ADAS systems. This information may be sensitive. Thus, it has to be secured against unauthorized use or access. For

instance, if a hacker can access a vehicle's GPS data, they can track the vehicle's movements and possibly exploit this information for illegal activities. Similarly, suppose a hacker has access to a car's camera or microphone. In that case, they may be able to record video of the occupants of the vehicle or listen in on their discussions.

ADAS technology can also prevent theft by immobilizing the vehicle or warning the owner or authorities if the vehicle is moved without permission. Geofencing technology integrated into ADAS allows the creation of virtual boundaries for designated areas. The ADAS system can initiate an alert when the vehicle exceeds these pre-established boundaries. The vehicle can be stolen if these systems are exploited because they can be bypassed. For instance, if a hacker is able to get into a car's immobilizer system, they can turn it off and move the vehicle without intimating the owner.

A security flaw may cause an ADAS-equipped vehicle to be involved in an accident, in which case the manufacturer or provider may be held financially responsible. This danger can be reduced by making sure that these systems are secure. For instance, a manufacturer may be less likely to be liable if an accident occurs if they show that they took sufficient precautions to safeguard their ADAS systems.

Autonomous vehicles (AV) have been the target of numerous attacks over the past few years.:

- Researchers from Tencent's Keen Security Lab demonstrated a remote attack on a Tesla Model S that allowed them to use the autopilot function of the vehicle. They had access to the car's electronic brakes, door locks, and other features [56].
- The Jeep Cherokee's engine, gearbox, and brakes were all under the remote control of security experts Charlie Miller and Chris Valasek, because of which Fiat Chrysler decided to recall 1.4 million automobiles in order to fix the security flaw [57].
- Researchers from the University of Michigan and the University of California, Berkeley, tricked the Mobileye camera system used in ADAS. They altered traffic signs with stickers, leading to the system misinterpreting them and possibly resulting in hazardous driving conditions [58].

These examples demonstrate the potential dangers of ADAS attacks and the significance of creating strong security measures to counter these dangers. More vulnerabilities and dangers are likely to emerge as AV technology develops. Thus, it is crucial for vehicle manufacturers and suppliers to be cautious and proactive in addressing these risks.

The ADAS market's expected annual increase is shown in the FIGURE 1. The market for ADAS was estimated to be worth USD 44.62 billion in 2022 and is anticipated to increase to USD 158.24 billion by 2032, growing at a CAGR of 13.8% from 2023 to 2032. This visual representation of rapid growth allows us to discern a highly promising future for ADAS technology, as its implementation is expected to proliferate across a greater number of vehicles. The expanding adoption of such technologies necessitates an augmented focus on vehicle protection and security measures, as the increasing prevalence of these advancements exposes vehicles to a greater risk of potential threats. Furthermore, FIGURE 6 [59] provides insights into the approximate number of automotive hacking incidents reported between 2010 and 2021. Upstream, renowned for its extensive analysis of emerging automotive cybersecurity trends, has meticulously collected and curated the data presented in this figure. Spanning an 11-year timeframe, it is important to acknowledge that not all years yielded complete data points. However, despite this limitation, the available dataset reveals a discernible pattern, indicating an exponential growth trajectory within automotive cybersecurity. Considering the continuous escalation of such incidents on a yearly basis, it is imperative to adopt appropriate security measures to mitigate these risks effectively. As the automotive industry advances and incorporates new technologies, the proactive implementation of robust security protocols becomes increasingly paramount in safeguarding vehicles and preventing unauthorized intrusions.

Considering all the above facts, we can clearly see a need for strong and robust security measures.

III. VANET ATTACKS

The Vehicular Ad hoc Network (VANET) is a road-based mobile ad hoc network (MANET) that aims to enhance the safety of traffic, as well as the flow of traffic and the driving experience. Every vehicle is equipped with an onboard unit (OBU) that serves as a means of communication for interacting with other vehicles on the road. Additionally, roadside units (RSU) are network devices that are placed along the roadway where they are positioned. RSUs are equipped with network equipment necessary for dedicated short-range communication (DSRC), which allows them to establish a connection with the infrastructure of the network. The registration and management of RSUs and OBUs falls under the purview of the transportation authorities.

The authors in [60] highlight the increasing significance of Vehicle-to-X (V2X) in vehicular communication, emphasizing its growing importance in the field. VANETs are crucial for enabling V2X communications. The V2X paradigm encompasses various types of information sharing as described in [61], which include Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I),Vehicle-to-Network(V2N), Vehicle-to-Pedestrian (V2P), Vehicle-to-Roadside Units (V2R) and Vehicle-to-Self (V2S) [62]. These different forms of communication are integral to enhancing vehicular networks' efficiency, safety, and overall performance and these communications are represented in a visual manner in FIGURE 8

The dynamic nature of VANETs is primarily attributed to the high mobility exhibited by vehicles within the network. This inherent characteristic leads to rapid modifications in the network topology, consequently leading to frequent communication link failures among vehicles in the vehicular network. The fleeting nature of ties formed

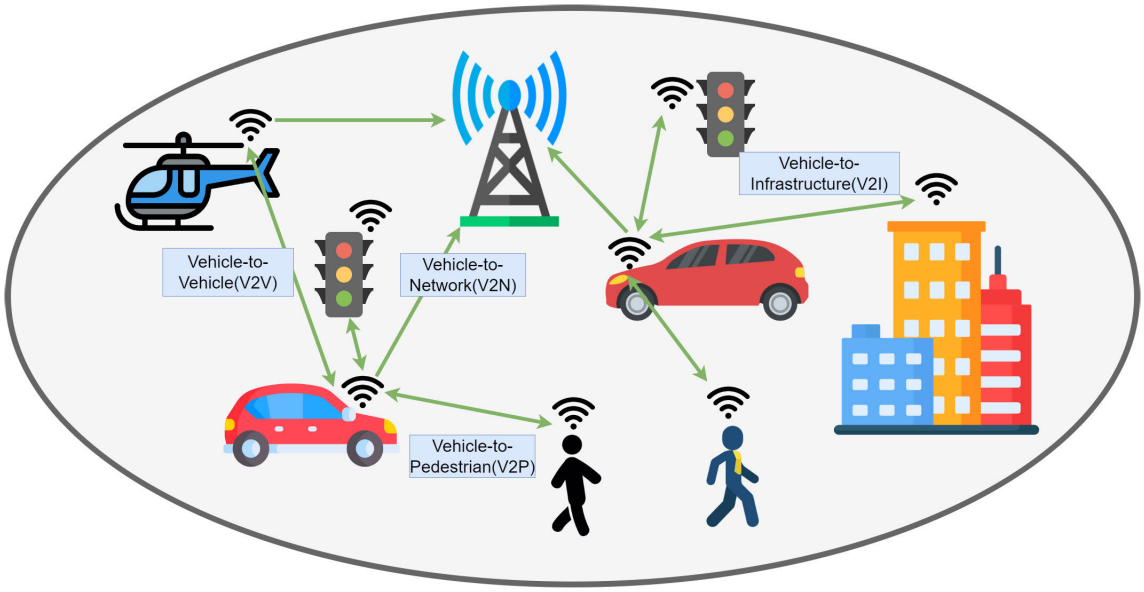

FIGURE 8. V2X communications in VANETS.

between cars moving in opposite directions, often only lasting a few seconds, is particularly notable. This transient connectivity imposes severe limitations on the duration for which vehicles can communicate with each other, leading to frequent disconnections within the vehicular network. These inherent challenges contribute to the heightened vulnerability of VANETs, rendering them more susceptible to malicious attacks. The transient and intermittent nature of communication links exacerbates the difficulties associated with identifying suspect vehicles within the network. As a consequence, the identification and mitigation of security threats in VANETs pose substantial challenges due to the constrained communication timeframes and rapid changes in network connectivity.

Particularly, in order to solve all security problems in VANETs, a complete understanding of risks and attacks is essential. In order to make VANET safer, Zaidi and Syed Faisal [63] had recognized that numerous security obstacles required study to advance. In their paper, the authors described critical analysis with regard to VANET components, security issues and challenges, assaults, and their remedies. Various VANET attacks were discussed in this section, along with their defenses against threats and attacks.

FIGURE 9 provides a general overview of different kinds of VANET attacks. TABLE 1 thoroughly examines diverse categories of VANET attacks, their impacts on various system aspects, and accompanying reference papers for additional exploration. The table's horizontal axis illustrates essential components such as communication channels, network availability, and data reliability, while the vertical axis enumerates specific types of VANET attacks. The marked cells indicate that the respective attacks influence the corresponding system aspect. Moreover, the table includes references to relevant papers utilized for this comprehensive review.

A. SYBIL ATTACKS

In order to prevent the network from operating normally, a hostile node willfully establishes numerous bogus identities. This is known as a Sybil attack.

Sheikh et al. [64] discussed that the attacker could manipulate the behavior of other vehicles and create the illusion of multiple vehicles by broadcasting multiple messages with fake IDs, causing traffic congestion and forcing them to take alternate routes. The network, as well as the safety of moving vehicles, may suffer significantly as a result of this.

It is critical for applications to require multiple vehicles to validate a specific piece of information before considering it legitimate. A malevolent vehicle that can impersonate several cars (a Sybil attack) and reinforce erroneous data, on the other hand, is a severe concern. If innocuous entities are unable to recognize this attack, they might accept the false information and make judgments based on it, leading them down a different path.

Prevention Measures: Zhou et al. [65] proposed various methods to combat such attacks in VANETs. They suggest a protocol that would allow a distributed collection of fixed nodes known as road-side boxes (RSBs) to passively overhear a malicious user pretending to be multiple (other) automobiles. Privacy is always safeguarded because no vehicle within the network must disclose its identity to recognize Sybil attacks in this manner. The proposed solution exposes only a small portion of the information while distributing the calculation strain from the DMV to RSBs via hash collisions. Another method for preventing Sybil attacks is to employ location verification techniques. Chen et al. [66] proposed a plan to prevent this attack that uses data collection to track the location of the vehicle from adjacent active nodes by collecting GPS data and using the signature.

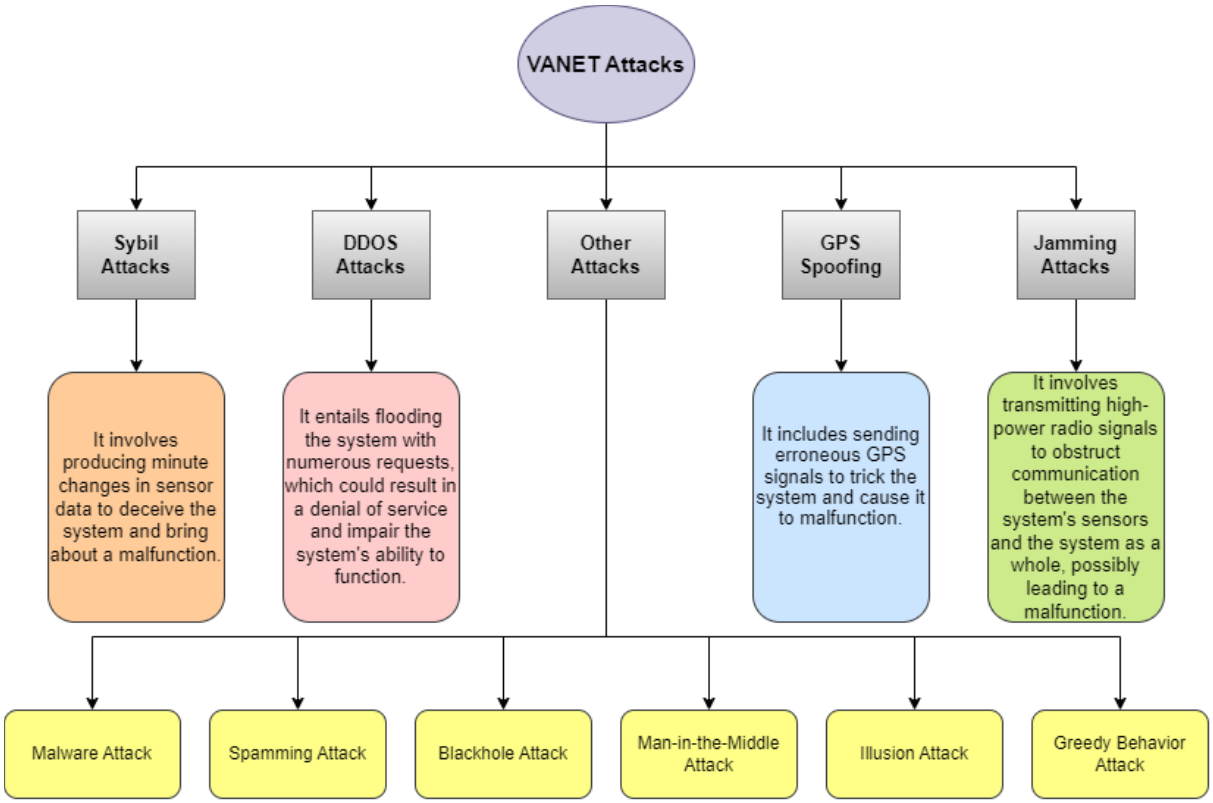

FIGURE 9. VANET attacks.

TABLE 1. Overview of VANET attacks on ADAS.

3*Possible threats	Affects						3*References
	Communication channels	network availability	data reliability	Data integrity	Location-based services	Hardware components	
Sybil Attacks			✓	✓	✓	✓	[64] [65] [66]
DDOS Attacks	✓	✓		✓		✓	[67] [68] [69] [70] [71] [72]
GPS Spoofing			✓	✓	✓	✓	[64] [73]
Jamming Attacks	✓	✓	✓		✓	✓	[74] [75] [76]–[78]
Malware Attack			✓	✓		✓	[64] [79]
Spamming Attack	✓	✓	✓				[67]
Blackhole Attack	✓	✓	✓	✓			[64] [67]
Man-in-the-Middle Attack	✓		✓	✓			[80]
illusion Attack		✓	✓				[81]

B. DOS & DDOS ATTACKS

A Denial of Service (DOS) attack can be initiated by internal or external vehicles within the network, a common threat in VANETs [67]. The attacker's goal is to disrupt the transfer of data between vehicles, effectively preventing any action. Network availability is critical in VANETs because all vehicles rely on it. One of the most dangerous kinds of network attacks is a DOS attack. Its main objective is to limit authorized users' access to services.

The attacker sends several fake messages to the network to attract attention, disrupt efficiency, or exploit the network. By blocking the physical channel or inducing "Sleep Deprivation," the attacker hopes to stop users from using resources and services. A DOS attack is a serious problem in VANETs because it prevents users from communicating in the network and passing information to other vehicles. In life-critical applications, this can have disastrous consequences.

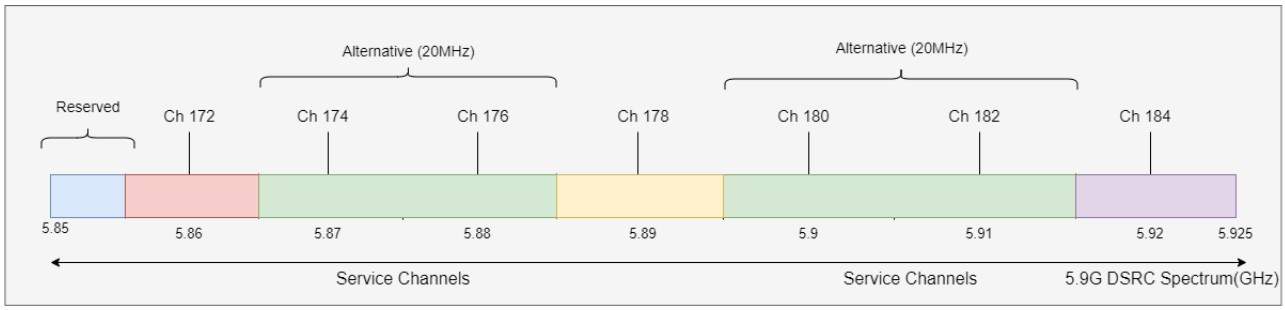

FIGURE 10. Channels in DSRC.

The Distributed Denial of Service (DDoS) attack is another type of DOS assault in which several attackers simultaneously hit a real vehicle from various locations. The severity of this attack in VANETs is significantly heightened due to the distributed nature of the mechanism. The attackers may send messages at different times of day, making it difficult to prevent or trace the attack. In a vehicular setting, according to Hasbullah et al. [68] and Biswas et al. [69], DoS attack can have a significant impact, but the severity escalates considerably with a DDoS attack, as the attack's mechanism operates across multiple points. In such instances, attackers launch simultaneous attacks from various locations, employing different attack types and time slots. This decentralized nature of the attack, coupled with variations in attack parameters and timing, further amplifies the detrimental effects, particularly with respect to V2V communication.

Prevention Measures: Raya and Hubaux [70] provided a thorough threat analysis and created a security architecture that is suitable for vehicular ad hoc networks. Stampoulis et al. [71]provided a survey of security in vehicular networks. Based on the work of Raya et al. and Stampoulis et al., Hasbullah et al. [68] have discussed various prevention measures:

Channel Switching: One method to mitigate these attacks is to switch between different channels or even communication technologies such as DSRC, cellular, or even Bluetooth for short range. DSRC provides multiple channels with a frequency range from 5.850GHz to 5.925GHz [82], divided into seven channels, each being 10MHz. DSRC allows data transfer at up to 27Mbps, making communication between nodes and infrastructure possible. The frequency spectrum and corresponding channels are shown in FIGURE 10. Among the seven channels, channel 172 and channel 184 are designated as safety-related channels, channels 174, channel 176, channel 180, and channel 182 as non-safety channels, and channel 178 as the control channel, which is typically used for safety-related applications, message broadcasting, and advertising services [83]. In case of an attack, when one channel is jammed, network availability can still be obtained by switching to other channels, thus denying a DOS attack.

Technology Switching: Various communication technologies like UMTS, Wi-MAX, Wi-Fi, and Zig-Bee can be used in VANET. The authors in [68] mentioned that the network can switch between these technologies to terminate an attack at a network type and prevent the overall network services from being affected. Depending on the severity of the attack, the system may be able to transition between different technologies thanks to their features [84]. If the attack intensity is low, a low-range technology is selected, while cellular technology is used when the level of the attacker or the DOS attack's range is high.

Frequency Hopping Spread Spectrum(FHSS): Multiple DSRC channels as shown in FIGURE 10 allow it to switch from one frequency channel to another when an attacker jams the communication channel, which lessens the attack [85]. Fast hopping and slow hopping are the two most common hopping approaches [83]. One or more data bits are transferred in a single hop using slow-frequency hopping. In contrast to the preceding technique, fast-frequency hopping divides one data bit into numerous hops. Sender and receiver nodes can communicate safely with one another because they already know the order of the hops, as pointed out by [68]. Attackers now find launching attacks impossible when the channels and frequencies are quickly adjusted.

C. GPS SPOOFING

Many applications rely on accurate location data. Hence location information is critical in VANETs. As a result, ensuring the integrity of location information is critical. In a location spoofing attack, the attacker generates fake GPS location information to deceive other network vehicles(shown in FIGURE 11). In order to do this, the attacker can generate false readings in GPS positioning system devices by employing a GPS satellite emulator, which generates signals that are more powerful than those from the actual satellite [64].

The GPS signal intensity measured at the Earth's surface is low, around −160dBw ($1 \times$ 10-16 Watts), which is similar to looking at a 25-Watt light bulb from 10,000 miles. As a result, by damaging or shielding the GPS receiver's antenna, the

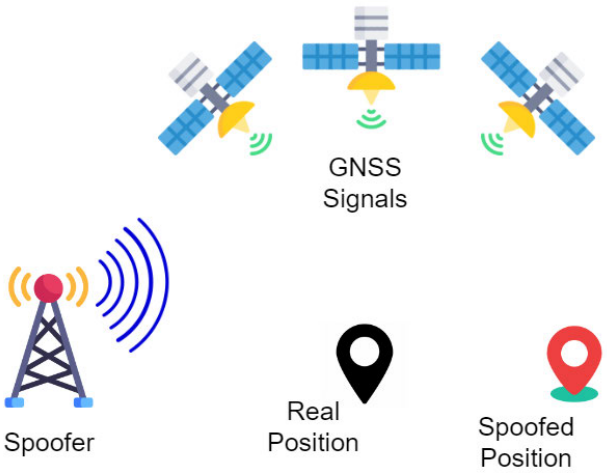

FIGURE 11. Location spoofing.

signal can be easily suppressed [73]. The GPS receiver will be aware it is not receiving the necessary signals to establish its position and time; therefore, blocking and jamming are not the most serious security issues. Instead, the danger stems from the attacker's ability to provide bogus GPS location data, which might deceive vehicles in the network and have potentially disastrous repercussions.

Countermeasures: In [86], the authors described a novel technique based on short-term information concealing and cross-correlation. The proposed method involved transmitting a hidden mark signal followed by a signed data signal to prevent GPS spoofing attacks. GPS receivers can differentiate between the original and replayed signals by measuring the delay between these signals. However, the method is vulnerable to relay attacks and less effective against selective delay attacks with highly directional antennas. Setting the power levels appropriately ensures a sufficient signal-to-noise ratio for signal recognition, while excessive noise power renders the broadcasted signal unrecognizable.

Also, redundancy [87] can be used to improve the resilience of GPS receivers against spoofing attacks. This can include using multiple GPS receivers [88] or integrating GPS with other navigation systems to provide backup in case of an attack. Equipping vehicles with multiple synchronized antennas improves positioning accuracy and availability. This system overcomes limitations caused by vehicle structure and cargo obstruction. By leveraging advanced algorithms, such as the Levenberg-Marquardt algorithm, it achieves decimeter-level accuracy and resilience against GPS spoofing. This preventive measure enhances positioning reliability even in challenging environments, making it an effective defense against GPS spoofing attacks.

D. JAMMING ATTACKS:

Jamming attacks are a common threat in VANETs. In these attacks, an attacker uses a radio frequency transmitter to flood the wireless communication channel with interference signals. This disrupts the normal operation of the VANET by preventing legitimate messages from being transmitted or received. Jamming assaults can have serious consequences. It is vital in safety-critical applications to guarantee that valid safety alarms are not disturbed. On the other hand, attackers can disrupt the communication channel by sending out high-powered signals at the same frequency. Within the same time frame as an incident, such acts can effectively reduce the signal-to-noise ratio(SNR) and block vital signals [74].

Jamming attacks are divided into four categories: persistent jamming, deceptive jamming, random jamming, and reactionary jamming. Persistent jamming sends random data over the channel without monitoring its condition. Deceptive jamming continuously injects a stream of random data with no gaps between packet transmissions. To conserve energy, random jamming alternates between jamming and sleeping modes [75], whereas reactive jamming jams only when it detects activity on the channel and is idle otherwise.

Countermeasures: There are various countermeasures to protect against Jamming attacks in VANETs. One strategy is to employ spread spectrum techniques [89] in which the transmitter disperses the signal across a wide frequency range, making it more challenging to jam any particular frequency. Here, the approach is to use frequency hopping and direct sequence spread spectrum techniques [76], [77], [78], where the transmitting device switches between multiple frequencies to avoid interference at any one frequency.

The use of directional antennas, which concentrate the transmission beam in a certain direction and make it more challenging for a jammer to interfere with the broadcast, is another defence strategy [90], [91].

E. OTHER ATTACKS

1) MALWARE ATTACK

The software elements that run the onboard and roadside equipment can be used to launch a malware attack against the system. The other parts of the VANET system could go down if the virus assault occurs in VANETs [64], [79].

2) SPAMMING ASSAULT

The attacker disrupts the VANET system by introducing a significant volume of unsolicited messages, generating excessive traffic. This increased traffic consumption consumes additional bandwidth and interferes with the smooth flow of essential data [67].

3) BLACKHOLE ATTACK

This Attack poses a significant threat to ad hoc networks and VANETs [64]. This malicious attack is typically executed by a registered VANET user who receives network packets but refuses to participate in the network's operations. As a result, the routing table may be altered, hindering critical communication with intended recipients and leading to non-functional scenarios [67].

4) MAN-IN-THE-MIDDLE ATTACK(MITM)

In VANETs, there exists a vulnerability where an attacker can manipulate messages during V2V conversations. Despite the belief in private communication, the attacker has complete access and control over the entire V2V communication, leading communicating entities to perceive direct interaction with each other erroneously.

MITM attacks pose a severe threat in VANETs, enabling hostile nodes to alter, drop, or delay critical information within the network. These attacks can be conducted passively or actively by adversaries. In passive attacks, the attacker eavesdrops on legitimate vehicles' communication channels. As discussed in [80], the attacker can actively manipulate received network information by dropping, delaying, or modifying its content.

5) ILLUSION ASSAULT

The illusion attack is a type of attack where data from antennas and sensors is gathered, including malicious data that produces fictitious traffic warning signals. This assault produces an illusion for nearby vehicles by taking advantage of the current road conditions, which could result in collisions and traffic jams [81]. By requiring extra bandwidth, the presence of such illusion attacks might have a negative influence on the VANET system's performance.

6) GREEDY BEHAVIOUR ATTACK

This attack is commonly directed toward the message authentication code (MAC) capability in VANETs. In this attack, a malicious vehicle exploits the MAC protocol to consume a significant amount of bandwidth, compromising the network's resources at the expense of other users. This leads to excessive traffic and collisions on the transmission channel, ultimately causing delays in the legitimate services of registered users.

TABLE 2 summarizes attacks and counter-techniques in VANETs. Key observations include the effectiveness of P2DAP in detecting Sybil attacks with low overhead and delay and RobSAD outperforming position verification. Counter-techniques such as channel switching and technology switching address channel congestion and enhance system resilience against DOS attacks. However, frequency hopping techniques face challenges from multiple jammers. Transmitting hidden mark signals improves GPS spoofing security, while directional antennas show higher efficiency in jammer detection. These observations emphasize the effectiveness and limitations of different counter-techniques in VANETs.

7) RESEARCH DIRECTION IN VANET ATTACKS

The research directions mentioned have been prioritized based on their critical importance for enhancing the overall security and functionality of VANETs.

1) **Mitigating DoS Attacks**: Research and implement adaptive algorithms capable of dynamically adjusting traffic filtering and rate-limiting mechanisms in real-time. Explore machine learning models to predict attack patterns and adjust mitigation strategies accordingly.
2) **Securing V2V and V2I Communications**: Conduct in-depth analysis and experimentation with post-quantum cryptography or homomorphic encryption to enhance the security of V2V and V2I communications. Evaluate the performance and resilience of these advanced encryption schemes in automotive environments.
3) **Anomaly-Based Intrusion Prevention**: Construct a robust anomaly detection framework using AI and machine learning algorithms trained on diverse and large-scale VANET data. Investigate the feasibility of deploying these models in real-time for efficient intrusion prevention.
4) **Enhancing Sybil Attack Detection**: Simulate various scenarios to test the effectiveness of current Sybil attack detection methods. Based on findings, propose and validate enhanced detection mechanisms, possibly leveraging blockchain or decentralized approaches to mitigate Sybil threats effectively.
5) **Optimized Routing Protocol Design**: Develop and validate routing algorithms specifically optimized for VANET security. Emphasize fault tolerance and adaptability to mitigate the impact of attacks while maintaining efficient communication among vehicles.

By elaborating on these recommendations with actionable strategies, researchers and industry professionals gain clearer insights into crucial steps needed to bolster the resilience and functionality of VANETs.

As we uncover the vulnerabilities in our vehicular networks, it becomes clearer how these intricacies might intertwine with hardware susceptibilities, a connection we'll explore in the following section.

IV. HARDWARE ATTACKS

ADAS relies on several hardware components, such as GPS, cameras, sensors, processors, and communication modules. The extent of usage of ADAS in modern vehicles was acknowledged by Kaye et al. [92]. Because of their complexity, they are also subject to attacks that could affect their dependability and security [93]. With the increasing prevalence of ADAS in modern vehicles [94], ensuring the security of those hardware components is of great importance. Hardware attacks refer to the deliberate exploitation of weaknesses in the physical elements of a system in order to gain unauthorised access, harvest confidential information, or disrupt normal operations. These vulnerabilities can be exploited by malicious individuals to gain control over the vehicle or manipulate the system's output, potentially leading to dangerous situations. This section aims to present a comprehensive overview of hardware attacks on ADAS, encompassing the various attack types, along with potential countermeasures to mitigate the associated risks. As depicted in FIGURE 12, an extensive overview of the diverse types

TABLE 2. VANET attacks.

Article	Attack	Counter-Technique	Description	Performance Metric	Outcomes
[65]	2*Sybil	P2DAP(Peer-to-Peer Distributed Accountable Protocols)	This method detects malicious users by passive overhearing by Road Side Units	computation/ communication overhead of the DMV, the privacy of the vehicles, and detection latency.	This method was effective with low overhead and delay while preserving the privacy of users.
[66]		RobSAD (Robust method of Sybil Attack Detection)	In this method, nodes independently compare the differences of neighboring node's digital signature vectors	Detection Rate	RobSAD achieved high detection rates (95-99%) with a low false positive rate (<10%) and outperformed position verification (98% detection rate vs. 75-96%).
[82], [83]	3*DOS	Channel Switching	Channel switching involves rapidly changing communication channels, making it difficult for attackers to target and overwhelm a specific channel.	Channel Congestion Metric	The issues of channel congestion control, broadcast performance improvement, and concurrent multichannel operation may be solved using a set of protocols based on differentiating routine and event safety messages.
[84], [68]		Technology Switching	Technology switching is the practice of changing the underlying technology or protocol to mitigate the impact of the attack.	-	The detailed features of these technologies were explained, including parameters such as standards, frequency bands, data rates, ranges, and primary uses. These features facilitated seamless technology switching within the system.
[83], [85]		Frequency Hopping	This technique employs frequent changes in the operating frequency, making it challenging for attackers to disrupt communication on any specific channel.	Packet Send Ratio (PSR), Packet Delivery Ratio (PDR), Jamming-to-Signal Ratio, Connectivity index	Frequency-hopping tactics were easily defeated by wide-band jammers and multiple jammers operating on several channels.
[86]	2*GPS	Transmitting Hidden Mark Signals	This method prevents GPS spoofing attacks by transmitting a hidden mark signal followed by a signed data signal, ensuring restricted access to the hidden mark signal until the signed data signal is received.	-	The counter technique provided added security but was still vulnerable to relaying attacks and selective delay attacks with highly directional antennas.
[87], [88]		Distributed Architecture for GPS antennas	This method employs redundancy by using multiple antennas for GPS to prevent spoofing	-	The proposed algorithm obtained a positioning accuracy close to the theoretical lower bound using coarse estimation.
[76]–[78]	2*Jamming	Frequency Hopping	This approach utilizes frequent variations in the operational frequency, posing difficulties for potential jammers in disrupting communication on a particular channel.	number of collisions and delay (time)	The proposed method ensured successful discovery between neighboring nodes despite jammers, as confirmed through theoretical analysis and simulations.
[90], [91]		Using Directional Antennas	This method employs redundancy by using multiple antennas for jammer detection	reachability, dissemination speed, uniformity, and efficiency	DSCF demonstrated higher efficiency compared to P-BCAST. The number of messages per delivery in DSCF was consistently smaller than in P-BCAST

of hardware attacks is presented, visually representing the subjects that will be expounded upon in detail in the forthcoming subsections. TABLE 3 provides a relation between possible hardware attacks and the corresponding affected components.

A. DENIAL OF SERVICE ATTACKS

In the section III-B, we have previously covered the topic of DOS attacks. However, in this subsection, we focus on exploring the specific hardware-related implications of DOS attacks. In [97], an exhaustive investigation of Distributed Denial of Service (DDoS) attacks over the network and their corresponding countermeasures was provided. The paper showed that those attacks could overwhelm the system's processing capacity, causing it to crash or malfunction.

1) AFFECTED COMPONENTS

The ECU is the brain of the ADAS system, which receives input from various sensors, including GPS, IMU, LIDAR, camera, TMU, and others. The system efficiently processes data and communicates instructions to the actuators, effectively managing and controlling the vehicle's behavior. Indeed, a successful DoS attack on the ECU can prompt the ADAS system to malfunction or completely shut down, potentially resulting in perilous situations for the driver and passengers. The ECU may be unable to receive input from the sensors, process the data, or send commands to the actuators, rendering the ADAS system ineffective.

2) COUNTERMEASURES

The Lane-Keeping Assist (LKA) system in autonomous vehicles was subjected to DoS attacks, leading to the proposal

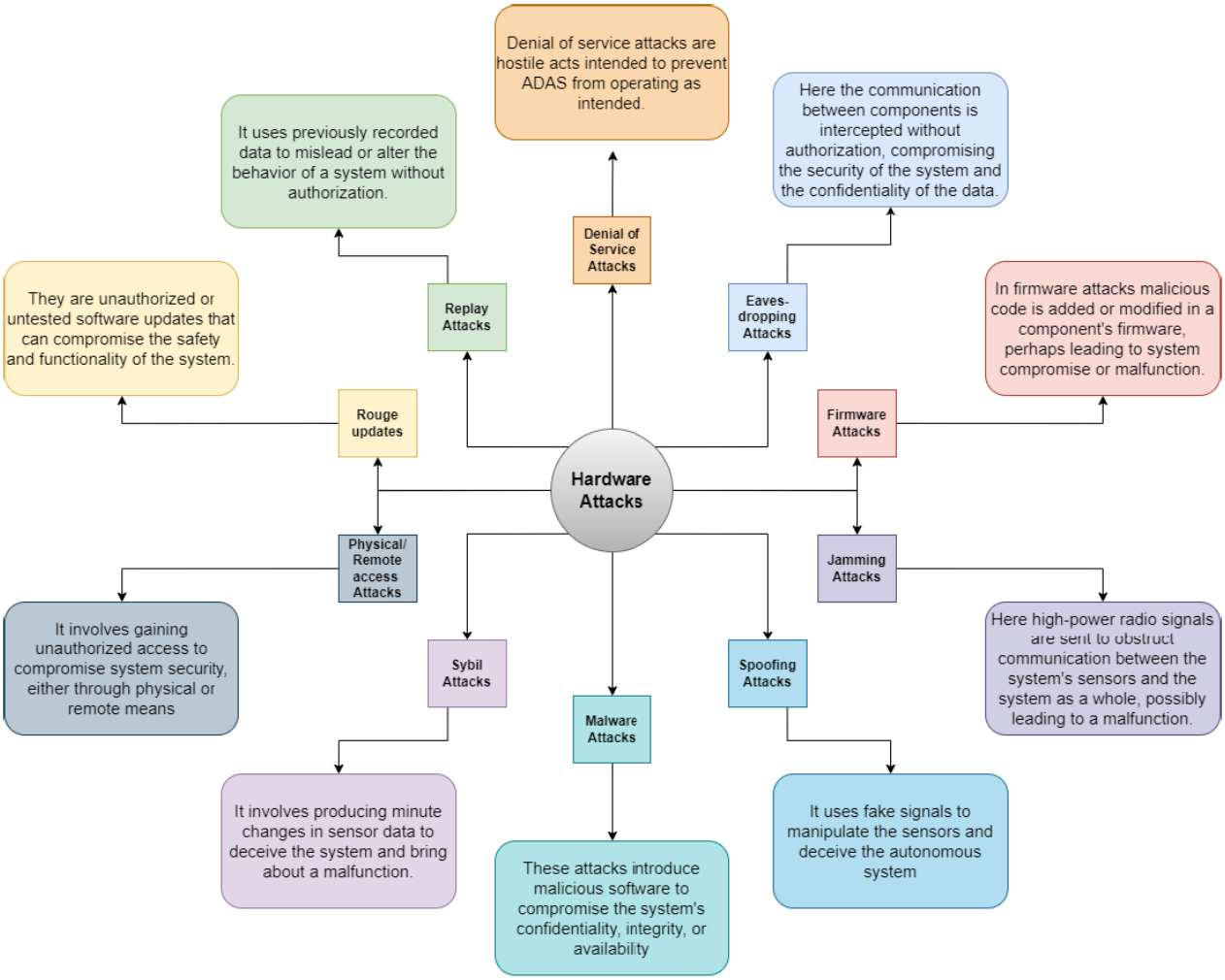

FIGURE 12. Hardware attacks.

TABLE 3. Overview of hardware attacks on ADAS.

2*Possible threats	Affected components						2*References
	GPS	IMU	LIDAR	Camera	TMU	ECU	
Denial of service attacks	✓	✓	✓	✓	✓	✓	[95] [96] [97] [98]
Eavesdropping attacks	✓	✓	✓	✓			[99] [100] [101]
Firmware attacks		✓	✓	✓	✓	✓	[102]
Jamming attacks	✓	✓	✓				[103] [104] [94] [105] [106]
Physical / remote access		✓	✓		✓	✓	[107] [108]
Spoofing attacks	✓	✓	✓	✓			[109] [110]
Sybil attacks	✓	✓	✓	✓	✓	✓	[64] [65] [66]

of a model-based detection approach by Kayser et al. [95]. Their system effectively detects the presence of the attack and subsequently alerts the human driver to regain control of the vehicle, ensuring safety during such adversarial events.

Djuitcheu et al. [96] proposed countermeasures using Machine Learning (ML) and Deep Learning (DL) approaches, in IoT networks, with potential applications in ADAS. Their research indicates that integrating ML and DL with technologies such as software-defined networking (SDN) presents the benefits of a highly promising approach for developing robust defenses against DDoS attacks.

Bouke et al. [98] proposed Gini index-based decision tree model for intelligent DDoS attack detection, which can

also be applied to ADAS systems. Their proposed method exhibits superior performance compared to baseline models employing more complex algorithms like Random Forest and XGBoost, achieving an impressive total accuracy of 98%. Only 13 out of 45 security characteristics may be chosen using their improved Gini index feature selection method, greatly lowering the dimensionality of the data and preventing overfitting problems. Additionally, only 2% of the testing events were incorrectly classified by their model, which has a lower false alarm rate.

B. EAVESDROPPING ATTACKS

Eavesdropping attacks intercept communication without consent, gaining access to sensitive information. This can result in privacy breaches, identity theft, and other malicious activities.

In the context of ADAS systems, eavesdropping attacks pose significant concerns, as they can compromise the security of the vehicle and the safety of the vehicle's occupants.

If an attacker successfully intercepts and eavesdrops on the communication between an ADAS system and its sensors or other components, they could acquire sensitive information regarding the vehicle's operation, including speed, location, or driver behavior.

Adversaries could exploit this acquired information to execute various attacks, including GPS spoofing or replay attacks. In such attacks, they send falsified or manipulated sensor data to the ADAS system, potentially leading to system malfunctions or erroneous decisions.

1) AFFECTED COMPONENTS

The components that are most susceptible to eavesdropping attacks are GPS, IMU, LIDAR, and camera. GPS, an acronym for Global Positioning System, is a system that uses satellites for navigation that offers precise location and time information to users. GPS signals can be intercepted and decoded by attackers, allowing them to track the location and movement of the vehicle. The Inertial Measurement Unit (IMU) serves as a sensor that gauges the vehicle's acceleration, orientation, and angular velocity. Attackers possess the capability to intercept and analyze IMU signals to deduce the vehicle's motion and direction. LIDAR (Light Detection and Ranging) operates as a sensor employing laser beams to generate a comprehensive 3D map of the environment. Attackers have the ability to intercept and analyze LIDAR signals, acquiring crucial information about the surrounding objects and terrain. The camera is another sensor that captures visual information about the environment. Attackers can intercept and analyze video signals from the camera to gain insights into the vehicle's location, speed, and direction. TMU (Traffic Management Unit) and ECU (Electronic Control Unit) are not typically susceptible to eavesdropping attacks, as they mainly process and control data within the vehicle's internal network.

2) COUNTERMEASURES

A countermeasure proposed by Biswas et al. [100] used cryptography-based techniques. The two main categories of cryptography-based techniques are encryption and authentication. Data integrity and secrecy are protected via encryption, which effectively shields against attackers listening in on transmissions of data.

Li et al. [101] introduced a defense mechanism utilizing blockchain and a zero-trust approach for smart electric vehicle chargers. The system adopts Hyperledger Fabric for key management and trust evaluation event storage to guarantee key and event validity, nonrepudiation, and tamper-proof attributes. Additionally, the application of zero trust helps safeguard critical assets and enforce identity and access management (IAM) for accessing entities. This technique demonstrated effective performance against eavesdropping attempts, which are relatively prevalent in electric vehicle charging.

C. FIRMWARE ATTACKS

Firmware attacks pose a security risk in various industries. Quick updates and potential testing gaps can leave devices vulnerable. Firmware attacks on ADAS systems are a significant threat as firmware is the low-level software that controls the system's hardware components, including the sensors, cameras, and other critical components. If an adversary successfully compromises the firmware, they could attain full control over the system and manipulate its operations entirely. Firmware attacks on ADAS systems can take various forms, including exploiting vulnerabilities in the firmware code, using malicious firmware updates, or manipulating firmware configurations to cause the system to behave unexpectedly.

1) AFFECTED COMPONENTS

The components most directly affected by firmware attacks are IMU, LIDAR, camera, TMU, and ECU. IMU, LIDAR, and camera sensors all have firmware that controls their operation. A firmware attack could modify the firmware to manipulate the sensor's output or cause it to malfunction, leading to inaccurate or misleading data. TMU (Traffic Management Unit) and ECU (Electronic Control Unit) are also susceptible to firmware attacks. The firmware of these components controls the vehicle's operation and communication with other ADAS components. An attacker could modify the firmware to send incorrect commands to the actuators, resulting in dangerous or unpredictable behavior. GPS (Global Positioning System) does not have firmware that a firmware attack can directly target,

2) COUNTERMEASURES

Emphasizing the importance of securing firmware in IoT devices, in paper [102], challenges and proposed solutions for firmware updates were identified for mitigating firmware-related vulnerabilities with potential applications in ADAS. In the work [111], the authors propose using

PUFs (Physical Unclonable Functions). PUFs (Physically Unclonable Functions) are hardware-based security elements that use a device's special physical characteristics to produce a distinctive identification or cryptographic key.

Firmware attack impact study and time series-based detection in microgrids were presented in paper [112]. These attacks can exploit vulnerabilities in the resource-constrained embedded controllers. This paper investigates the adversarial objectives of attackers attempting switching and controlling input modification attacks by manipulating firmware. The impact of such attacks is demonstrated using simulation, and the authors propose an effective countermeasure. To detect and prevent malicious firmware within controllers, the paper proposes the utilization of Time Series Classifiers (TSCs). The experimental results are promising, showing that the proposed countermeasure successfully identifies malicious firmware with high accuracy. This research is vital for enhancing the security and reliability of firmware in the face of evolving cyber threats.

D. JAMMING ATTACKS

While we have already discussed Jamming attacks in Section III-D, we will revisit them in this section from the perspective of their impact on the hardware components of the ADAS. As we know, jamming attacks involve disrupting the radio frequency (RF) signals used by ADAS sensors, preventing them from properly detecting and responding to the vehicle's surroundings [103], [104]. This can lead to dangerous situations, such as the failure of emergency braking systems, loss of vehicle control, or collisions. Consequently, it becomes imperative to conduct thorough investigations into potential risks and countermeasures against jamming attacks on ADAS, safeguarding the safety and security of drivers and passengers.

1) AFFECTED COMPONENTS

Jamming attacks can affect different components depending on the system being targeted. However, GPS and other communication systems are particularly vulnerable to jamming attacks. When a GPS system is jammed, it becomes difficult to determine the accurate position, velocity, and time information required for navigation [105]. IMUs and LIDAR systems, which rely on accurate positional data, can also be affected by jamming attacks. Cameras, Transmission Control Modules (TMU), and Engine Control Units (ECU) may not be directly impacted by jamming attacks. However, their operation could still be affected if the jamming causes the vehicle to lose its position or orientation, leading to potential safety hazards.

2) COUNTERMEASURES

Pelechrinis et al. [113] proposed and employed proactive Frequency Hopping (FH) as a method to effectively counteract jamming attacks in 802.11 networks, as described in their publication. In the study by Lee et al. [106], novel machine learning-based methods for jamming attack classification and effective defense techniques were introduced.

E. PHYSICAL/REMOTE ACCESS

Physical and remote access attacks targeting ADAS systems pose critical threats, potentially compromising the vehicle's and its occupants' safety and security. Recent incidents have revealed instances where sensors have been exploited for car and energy theft, financial fraud, and data compromise, among other illicit activities [107]. These occurrences have raised serious concerns about health and safety risks. Physical access attacks involve an attacker physically gaining access to the vehicle or its components. In contrast, remote access attacks involve an attacker accessing the system remotely, such as over the Internet. Physical access attacks on ADAS systems can take various forms, including stealing the vehicle, breaking into the vehicle's components, or tampering with the sensors or cameras. Once an attacker gains physical access to the system, they possess the potential to manipulate the system's operations or extract sensitive information, posing significant security risks. Remote access attacks on ADAS systems can take various forms, including exploiting vulnerabilities in the system's software or hardware, using phishing attacks to trick users into downloading malware or sharing login credentials, or using stolen or brute-forced login credentials to access the system. The repercussions of physical and remote access attacks on ADAS systems can be severe, encompassing the attacker's theft of sensitive information, manipulation of sensor data, and even complete control of the system. Such outcomes underscore the critical importance of implementing robust security measures to safeguard against such threats.

1) AFFECTED COMPONENTS

The components most directly affected by remote access attacks are the IMU, LIDAR, and TMU. Should an attacker manage to gain physical access to the ECU, they could potentially alter the code or install malicious software, resulting in hazardous situations for the driver and passengers. Likewise, if an attacker gains physical access to the TMU, they might intercept or modify the transmitted data between these components, causing the dissemination of inaccurate or misleading information. These scenarios underscore the importance of robust security measures to protect against physical access attacks. camera sensors are also vulnerable to remote access attacks if their software or firmware is compromised. An attacker could potentially manipulate the sensor's output or cause it to malfunction, leading to inaccurate or misleading data.

2) COUNTERMEASURES

The research paper [108] brought forward the security concerns of IoT and IIoT devices which are also applicable to advanced driver assistant systems (ADAS) due to their reliance on such devices. It comprehensively summarises several attack vectors, corresponding side effects, and attack

detection mechanisms. The paper's insights on addressing hardware vulnerabilities and implementing security mechanisms can help enhance the security of ADAS and prevent cyberattacks on these systems.

F. SPOOFING ATTACKS

Spoofing attacks are the intentional manipulation of signals, data, or other forms of communication to deceive or mislead a system or its users. In the context of autonomous vehicles, spoofing attacks pose a significant danger, as they can cause the vehicle to misinterpret its surroundings and make erroneous decisions, potentially leading to accidents or other hazardous situations. Ensuring robust defense mechanisms against spoofing attacks becomes crucial to guarantee the safety of autonomous vehicles and reliability of autonomous vehicles. To mitigate these risks, manufacturers of autonomous vehicles must implement robust security protocols [114].

1) AFFECTED COMPONENTS

Spoofing can potentially affect the GPS, IMU, LIDAR, and camera components, as these are all sensor-based technologies that rely on accurate and reliable data inputs to function properly. GPS spoofing, for example, can cause navigation systems to provide incorrect directions or lead a vehicle off course [110]. IMU spoofing can similarly affect navigation and positioning systems, as IMUs use gyroscopes and accelerometers to measure the orientation and movement of a vehicle. LIDAR and camera systems are used in ADAS for object detection and avoidance. Spoofing the data input from these sensors could cause a vehicle to make incorrect decisions, potentially leading to accidents. TMU and ECU are generally unaffected by spoofing, as they are responsible for controlling a vehicle's transmission and engine management systems and do not rely on sensor inputs for their operation.

2) COUNTERMEASURES

Preventing such attacks entails employing encryption-based technology, signal-process-based methods, and authenticated location information. These defense measures contribute to enhancing the security and resilience of the autonomous vehicle system against spoofing attacks.

G. SYBIL ATTACKS

Sybil attacks represent a form of cybersecurity attack wherein the attacker generates multiple fraudulent identities or nodes within a system to gain unauthorized access or manipulate the system's behavior. In the previous section III-A, we have covered Sybil attacks within the context of VANET attacks. Now, in this subsection, our focus shifts toward attacks specifically related to hardware.

1) AFFECTED COMPONENTS

Sybil attackers can create fake GPS signals or fake GPS devices, providing false or misleading location information to the ADAS system. This can result in incorrect positioning and navigation decisions, leading to compromised driving behavior. Sybil attackers can create fake IMU data, such as acceleration, orientation, and velocity, which the ADAS system can use for motion detection and estimation. Sybil attackers can create fake LIDAR signals or fake LIDAR devices, providing false or misleading 3D point cloud data to the ADAS system. Sybil attackers can create fake camera data, such as fake images or videos, which can be used to provide false or misleading information to the ADAS system. This can result in incorrect perception and decision-making, leading to compromised driving behavior. Sybil attackers can create fake TMU data, sending false or malicious traffic information to the ADAS system. This can result in incorrect traffic-related decisions, misleading traffic control commands, and compromised communication-based features. Sybil attackers can create fake ECUs or compromise legitimate ECUs, sending unauthorized or malicious commands to the ADAS system. This can result in unauthorized control of the vehicle, compromised driving behavior, and other safety risks.

2) COUNTERMEASURES

Researchers have presented diverse approaches to mitigate Sybil attacks in ADAS, one of which was the proposal by Zhou et al. [65]. Their approach introduced a privacy-preserving scheme grounded in authentication certificates to tackle the issue effectively. Another method by Chen et al. [66] for preventing Sybil attacks was to employ location verification techniques and proposed a plan that used data collection to track the location of the vehicle from adjacent active nodes by collecting GPS data and using the signature.

TABLE 4 summarizes various counter-techniques employed to mitigate hardware attacks, including denial of service, eavesdropping, firmware attacks, jamming, and Sybil attacks. Some notable observations include using model-based detection schemes for DoS attacks, the effectiveness of cryptography-based techniques and hybrid cryptography in strengthening security against eavesdropping, and the introduction of Physical Unclonable Functions (PUFs) for firmware attack prevention. Additionally, countermeasures like channel switching and frequency hopping enhance resilience against jamming attacks. The table also highlights the effectiveness of privacy-preserving schemes based on authentication certificates and location verification techniques in mitigating Sybil attacks. Quantitative information is provided in some cases, such as the high accuracy and low false positive rates achieved by certain models. The table showcases diverse approaches to address hardware attacks and their respective outcomes.

The future scopes of research based on the papers encompass a wide range of security and optimization challenges in various technological domains. Researchers can explore enhanced security measures to defend against denial of service attacks, jamming attacks, and Sybil attacks,

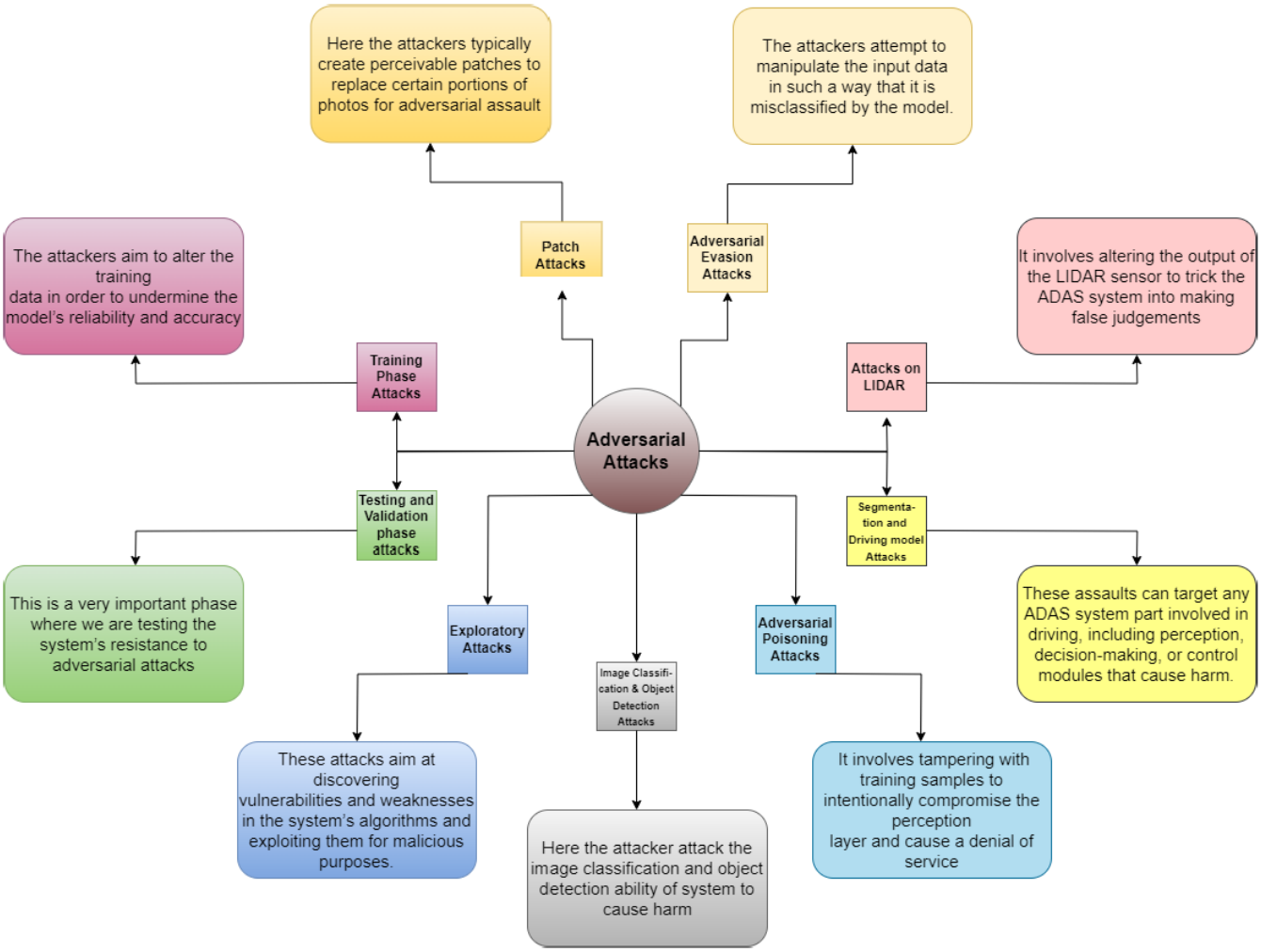

FIGURE 13. Adversarial attacks.

incorporating advanced machine learning algorithms, behavioral analysis, and adaptive defense mechanisms. Additionally, there is room for investigating standardized protocols for secure firmware over-the-air updates in IoT devices, ensuring data integrity and confidentiality, and exploring blockchain-based security models for smart systems. Optimizing techniques such as frequency hopping and feature selection can be further improved and applied to different domains to enhance efficiency and performance. Furthermore, the integration of cryptography and steganography can be explored in various communication and security systems for enhanced data transmission security. The integration of zero trust and blockchain technology can offer innovative solutions for secure data sharing and identity management. Finally, the potential of AI and machine learning in security domains, such as anomaly detection and intrusion prevention, holds promise for developing robust and real-time response systems.

Research Direction in Hardware Attacks: The outlined research directions in hardware attacks have been organized based on their pivotal role in ensuring the overall security of ADAS systems.

1) **Develop Integrated Security Frameworks:** Model and analyze the intricate interactions among various hardware components within ADAS systems. Develop comprehensive security frameworks integrating these models to offer robust protection against specific attack vectors, such as side-channel attacks or hardware trojans.
2) **Establish Secure Design Standards:** Conduct exhaustive vulnerability assessments during the design phase, leveraging threat modeling and penetration testing specific to ADAS hardware components. Establish and enforce stringent standards addressing potential vulnerabilities identified during these assessments.
3) **Explore Redundancy and Diversity:** Investigate dynamic redundancy strategies by employing reconfigurable hardware or runtime redundancy management. Experiment with diverse hardware

TABLE 4. Hardware attacks.

Article	Attack	Counter-Technique	Description	Outcomes
[95]	3*Denial of service attacks	Model-based detection scheme	This approach employs mathematical modeling to simulate a DoS attack on the system using the road's curvature for Lane-keeping Assistant (LKA).	The system used Simulink and a custom algorithm to alert the driver of attacks in the LKA system, enhancing safety.
[98]		Gini index based decision tree model	The Gini index is a statistical measure used in decision tree algorithms for feature selection. The model employs an improved Gini index feature selection technique to minimize data dimensionality and boost detection accuracy.	It outperformed baseline models with 98% overall accuracy and a 2% false alarm rate on the UNSW-NB15 dataset.
[96]		machine learning and deep learning approach	Software-defined networking (SDN) is an approach to network management and control that separates the control plane from the data plane, allowing for programmable and centralized management of network resources.	Authors found that combining ML, DL, and SDN offers promising defenses against DDoS attacks.
[100]	2*Eavesdropping attacks	Cryptography-based techniques	Cryptography techniques, including encryption algorithms like AES and RSA, secure data in electronic communication. Hybrid cryptography combines symmetric and asymmetric encryption, while digital signatures and integrity checking ensure data integrity. Steganography, particularly the LSB method, strengthens encrypted message security.	Hybrid cryptography improved security, steganography strengthened it, and message integrity checking was a notable feature. Successful simulations confirmed the algorithm's feasibility.
[101]		defense mechanism using blockchain	Blockchain is a decentralized and distributed ledger technology that securely records and verifies transactions across multiple participants, providing transparency and immutability. Zero trust is a security concept that assumes no implicit trust within a network and requires continuous verification and authentication for all entities and resources, regardless of their location.	The scheme successfully defended against replay and tampering attacks, ensuring secure data communication between systems.
[102]	Firmware attacks	Physical Unclonable Functions	These hardware-based security elements use a device's special physical characteristics to produce a distinctive identification or cryptographic key.	Experimental results verified the confidentiality of obfuscated data and the successful reconstruction of protocol keys solely by the original device.
[113]	2*Jamming attacks	Channel switching, frequency hopping	Channel switching is a technique used in wireless communication systems where the transmitter and receiver switch between different frequency channels to improve reliability and avoid interference. Frequency hopping is a specific form of channel switching that involves rapidly changing the frequency at which a signal is transmitted, enhancing security and resilience against jamming or interception.	Frequency hopping alone was found inadequate in safeguarding 802.11 networks against jamming, given the current spectrum allocations.
[106]		Jammer Classification and Effective Defense (JCED)	It utilizes machine learning (ML) techniques to classify jamming attacks and provides tailored defense responses based on the detected jammer type. The algorithm provides flexible response options, from straightforward retransmission to active battery-draining attacks.	Compared to Countermeasure Detection and Consistency Algorithm (CDCA), the JCED algorithm achieved a 24.9% higher effective throughput and 23.4% lower energy consumption.
[65]	2*Sybil attacks	privacy-preserving scheme based on authentication certificates	Authentication certificates are digital documents issued by an authority that verifies the identity of an entity, enabling secure communication and preventing impersonation or unauthorized access. They contain key information and cryptographic signatures to establish trust and ensure authenticity.	This technique worked well with little overhead and delay while protecting user privacy.
[66]		location verification techniques	Location verification techniques authenticate and validate reported physical locations using GPS, cellular networks, and sensors. They ensure accuracy for authentication, fraud prevention, and location-based services.	RobSAD achieved high detection rates (95-99%) with a low false positive rate (less than 10%) and outperformed position verification (98% detection rate vs. 75-96%).

implementations to mitigate single-point vulnerabilities, allowing systems to adapt to changing threat landscapes.

4) **Design Secure Communication Protocols:** Utilize formal verification techniques to ensure the resilience of communication protocols against hardware-based attacks. Explore zero-trust architectures and cryptographic methods specifically tailored to ADAS communication channels to prevent tampering or interception.

5) **Advanced Anomaly Detection with Deep Learning:** Investigate the feasibility of neural networks for hardware fingerprinting, enabling precise anomaly detection tailored to hardware behavior. Train deep learning models on hardware-specific features to distinguish between normal behavior and anomalous activities, enhancing detection accuracy while reducing false positives.

By exposing the weaknesses in our hardware components, we start to see the direct link between these physical vulnerabilities and potential adversarial exploits. This sets the stage for our exploration into the nuances of adversarial attacks within ADAS.

V. ADVERSARIAL ATTACKS

The deliberate modification of data that is input into a machine learning system with the intention of negatively influencing the decision-making process of the system is being referred to as an adversarial attack. These kinds of assaults could be particularly troublesome since they could potentially cause an increase in the probability of automobile accidents or other safety issues. An example of an adversarial assault could be the manipulation of the input data from sensors, such as cameras or lidars, on which the integrated driver assistance system (ADAS) relies in order to make driving decisions. Such an example is shown in FIGURE 14, wherein due to the addition of a noise, the output of the traffic sign classifier changes from the correctly classified "Bump Ahead" sign to "Right Turn" sign. An attacker may make the system misinterpret its surroundings and make bad decisions about things like steering, braking, or acceleration by making small alterations to the sensor data. Hence, addressing these attacks and finding ways to prevent and control them is very important. FIGURE 13 offers a comprehensive overview of the diverse types of adversarial attacks, visually illustrating the topics that will be expounded upon in detail in the forthcoming subsections.

A. PATCH ATTACKS

Another method for attacking neural network models is by perturbing a portion of the image with discernible noise. Attackers can typically create perceivable patches to replace certain portions of photos for adversarial assault. Patch attacks are this particular form of assault. A universal adversarial patch, for instance, can induce targeted misclassification of any item. Adversaries possess the capability to launch attacks on the autopilot system of autonomous vehicles by attaching stickers to traffic signs. The fact that most patch attack methods do not consider the issue of determining the ideal spot in an image to inject the patch is a significant restriction [115]. Current patch attack methods either learn patches that are universal across locations or use a fixed place as the patch site. While the random location patches don't have comparable attack success rates to the fixed location techniques, the fixed location approaches work well at some sites but poorly at others.

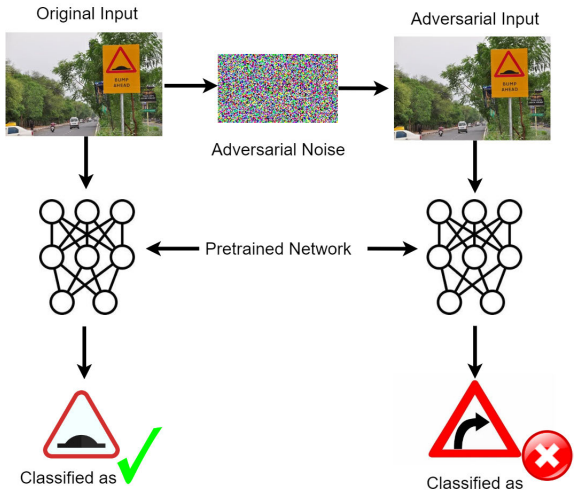

FIGURE 14. Adversarial attack on traffic sign detection.

Countermeasures: Levine and Feizi [116] proposed an approach that belonged to the large group of randomized smoothing robustness methods that offered certificates of high confidence in their probabilistic robustness. The authors improved robustness certificates against patch attacks by capitalizing on the constrained nature of these attacks compared to conventional sparse assaults.

Chiang et al. [117] extended interval bound propagation (IBP) on CIFAR10 to offer the first certifiable defense against patch assaults. In further work, tiny receptive fields or randomized smoothing were introduced to enhance CIFAR10 certification and scale to ImageNet.

Chen et al. [118] introduced Vision Transformer (ViT) into the framework of Derandomized Smoothing (DS) to move towards a practical certifiable defense technique for patch attacks.

B. TRAINING PHASE ATTACKS

A training phase attack takes place when a machine learning model is being trained. These attacks are directed toward modifying the training data to undermine the reliability and accuracy of the model. The primary objective of the attacker is to manipulate the training data so that the model exhibits inaccurate classification or prediction responses under specific inputs or circumstances. Chakraborty et al. [119] and Liu et al. [120] presented three significant categories, further segmenting the domain of adversarial attacks. The first type of assault, known as a data injection attack, is the introduction of adversarial data samples into the training dataset with the intention of tainting and changing its distribution. At the same time, the attacker is ignorant of the training dataset. The adversary deliberately alters or taints the training dataset in the second sort of assault, fully aware of their actions. In each of these attack scenarios, it is assumed that the adversary is unaware of the characteristics of the target model. The third type of attack is a logic corruption attack when the attacker

purposely tries to alter the target model. More sophisticated and exact manipulations are possible because the attacker in this situation fully understands and is familiar with the target model.

Countermeasures: Attacks during the training phase can be difficult to avoid. Limiting access to the dataset and making sure that only authorized individuals have access to it are two ways to stop data access threats. One strategy for poisoning attacks before using the training data to train the model is to rigorously check and clean the data. Using robust learning algorithms that are less vulnerable to poisoning assaults is a different strategy.

The author in [121] suggested changing the database defense technique, which entails changing the data used in both the training and testing phases and enhancing the models' robustness. The defensive strategies used in this method include input transformation [122], gradient hiding [121], [123] [124], and adversarial training [125].

C. TESTING AND VALIDATION PHASE

A crucial stage in the creation of ADAS is the testing and validation phase. In this step, the system's performance is tested and validated to ensure it complies with the requirements and safety standards.

One of the key testing methods employed is adversarial testing [126]. In this context, the ADAS is subjected to adversarial attacks, which can involve presenting the system with deceptive images or sensor data. This helps in assessing the system's resistance to such attacks. Another important aspect is the use of Generative Adversarial Networks (GANs) [127]. GANs can be used to generate synthetic intrusion traffic to test the influence of these attacks on the accuracy of machine learning-based Intrusion Detection Systems (IDSs). Moreover, research has been conducted on the practicality of adversarial attacks against ML-based network security entities. This includes an investigation of the impact of continuous training on adversarial attacks against IDS [126]. The findings indicate that continuous re-training, even without adversarial training, can reduce the effect of adversarial attacks.

During the validation phase, ADAS systems are subjected to a range of testing scenarios to evaluate their reliability, performance, and robustness.

One important aspect of validation is testing the system's resistance to adversarial attacks, which are malicious attempts to disrupt or compromise the system's functionality. The upcoming subsection offers a concise outline of Adversarial evasion attacks showing that the validation phase plays an important role in detecting evasion attacks at an early stage.

1) EVASION ATTACKS

Evasion attacks represent a specific category of adversarial attacks wherein an attacker manipulates input data to deceive the output of a machine learning model. The primary objective of an evasion attack is to induce the model to make incorrect predictions or misclassify the input data. These attacks pose significant concerns, especially in safety-critical domains like autonomous vehicles, where a single misclassification can potentially result in severe and catastrophic consequences. Evasion attacks can be designed to be imperceptible to the human eye, making them difficult to detect. Therefore, developing robust defenses against evasion attacks is crucial for ensuring the safety and reliability of machine learning models in critical applications. Evasion attacks try to trick existing models by providing carefully crafted adversarial inputs.

Early detection of evasion attacks plays a pivotal role in securing Advanced Driver Assistance Systems (ADAS). Evasion attacks have the potential to significantly undermine the accuracy of Intrusion Detection Systems (IDS), thereby allowing malicious traffic to be misclassified as benign [128]. This could have serious implications for the safety and operational efficiency of ADAS, which are heavily dependent on accurate and real-time data for decision-making. Furthermore, evasion attacks can bypass firewalls and defeat malware analysis, thereby exposing ADAS to a wider range of threats. In some instances, evasion attacks can even incapacitate a network security defense, leaving it vulnerable to subsequent targeted attacks. Consequently, the early detection of evasion attacks is of paramount importance in mitigating these risks and ensuring the safe and reliable operation of ADAS.

Girdhar et al. [129] presented a comprehensive literature review on Adversarial Attacks. In section V-G, we offer a concise outline of Adversarial evasion attacks.

Countermeasures: Various countermeasures can be implemented during the design and validation phases to protect ADAS from adversarial attacks. These include robustness testing to identify and mitigate vulnerabilities in the system, such as detecting and rejecting adversarial inputs. Chernikova et al. [130] produced research that illuminates Deep Neural Networks' security implications in the setting of self-driving cars, particularly concerning steering angle prediction. The study presented a case study wherein adversarial testing phase attacks resulted in misclassification, emphasizing the vulnerabilities of DNNs in self-driving systems.

Another countermeasure is incorporating security mechanisms such as encryption and authentication to prevent unauthorized access and manipulation of the system. Additionally, anomaly and intrusion detection can be used to identify and respond to potential attacks. Finally, ongoing monitoring and updating of the ADAS can help to address newly discovered vulnerabilities and stay ahead of potential threats.

D. ATTACKS ON IMAGE CLASSIFICATION AND OBJECT DETECTION MODELS

In ADAS, cameras serve as prevalent sensors to capture images of the surrounding environment. These images are

subsequently subjected to processing through image classification and object detection models, facilitating the identification of various objects, including vehicles, pedestrians, and traffic signs. These models are crucial in allowing ADAS capabilities, which include crucial duties like autonomous emergency braking, lane departure warning, and forward collision warning. However, adversarial attacks on these models can lead to misclassification of objects or detection of non-existent objects, which can result in incorrect or delayed responses by ADAS systems. Such errors can cause accidents and pose a significant risk to the safety of drivers and passengers. Hence, it becomes imperative to assess the susceptibility of image classification and object detection models to adversarial attacks and to devise robust defense mechanisms to ensure the safety and dependability of ADAS systems.

DeepFool represents an adversarial attack technique designed to produce perturbations capable of deceiving deep neural networks [131]. The methodology relied on approximating the decision boundary of a neural network linearly, specifically within the proximity of the input image. Subsequently, the algorithm computes perturbations by identifying the shortest distance from the input image to the decision boundary within this linearized space.

The DeepFool algorithm has been shown to be effective against various deep neural networks, including Convolutional Neural Networks and Recurrent Neural Networks. It is also fast and computationally efficient, making it a popular choice for generating adversarial examples.

In their investigation [131], the researchers devised an adversarial attack targeting the traffic sign recognition model in autonomous vehicles (AV). The attack generates adversarial examples outside the training and testing data distribution, constituting an out-of-distribution attack. The model's limitation in classifying inputs within its trained distribution is exploited, making it susceptible to misclassification when presented with images of logos or custom signs. Remarkably, this attack demonstrates effectiveness in both real-world and virtual scenarios.

In the same research study, the authors introduced a lenticular printing attack, capitalizing on the optical phenomenon of distinct viewing angles. This exploit manipulates a CNN-based traffic sign identification model by producing deceptive images that project different signs depending on the viewer's position. As elucidated by the researchers, the discrepancy in viewing angles between the human driver and the camera mounted on the vehicle's top creates an opportune environment for executing this attack.

In another research endeavor [132], the investigation delved into adversarial attacks on image classification in ADAS, concentrating on three distinct attack methodologies: Adversarial Attack on Traffic Sign Recognition, Square Attack on Image Classification Model, and Adaptive Square Attack.

The Adversarial Attack on Traffic Sign Recognition perturbs traffic sign images, inducing misclassification by the image classifier, which may result in erroneous actions by the ADAS system. The Square Attack on Image Classification Model involves the introduction of minute perturbations in the form of squares to the input image. These perturbations can cause misclassification of the image by the model. This employs two sampling distributions specific to the l_2 and l_∞ -attack, both motivated by the image processing techniques used in neural networks with convolutional filters. The l_2-attack technique entails generating adversarial examples by introducing small perturbations to the input image, measured in the l_2-norm sense. Conversely, the l_∞-attack involves perturbing the image in the l_∞-norm sense, which quantifies the maximum magnitude of the perturbation over all pixels in the image. The Adaptive Square Attack (ASA) represents an extension of the Square Attack, wherein it incorporates an adaptive distribution π with a learnable parameter ω instead of a uniform distribution used in traditional l_∞ and l_2 square attacks. The adaptive distribution is strategically designed to learn an efficient sampling strategy, necessitating fewer queries while attaining a heightened attack success rate. By sampling from this adaptive distribution, ASA constructs perturbations that prove more effective in evading the image classification system.

Countermeasures: Madry et al. [133] proposed a method called Adversarial Training to prevent adversarial attacks on image classification models. Adversarial Training involves training a model on a combination of normal training data and adversarial examples generated by intentionally perturbing the input images to cause misclassification. By incorporating these adversarial examples during training, the model learns to become more robust to such attacks during testing. In the paper, Madry et al. [133] showed that adversarial training significantly improves the model's accuracy on adversarial examples while maintaining good performance on normal inputs. They also demonstrate that their adversarial training method is more effective than other proposed defense mechanisms, such as input preprocessing or adversarial detection. Overall, the paper suggested that adversarial training can be an effective preventive measure against adversarial attacks on image classification models.

Papernot et al. [134] extensively investigated the transferability of adversarial attacks across diverse machine learning models. They further propose several preventive measures to mitigate such attacks' impact. The transferability of adversarial samples represents a noteworthy concern for machine learning models, as adversarial examples designed to deceive one model can effectively mislead other models trained for the same task. To counteract such attacks, it is imperative to deploy robust preventive strategies. Enhancing the accuracy and efficiency of substitute model learning algorithms presents one viable approach, exemplified by utilizing reservoir sampling to bolster training procedures. Developing effective substitute models through deep neural

networks (DNNs) or logistic regression (LR) can reduce the vulnerability of various classifiers to black-box attacks. Additionally, validation mechanisms for input data should be implemented to detect and filter out potential adversarial samples. Further research is needed to explore defenses against adversarial samples and investigate the impact of poisoning attacks during training. Implementing these preventive measures is essential for augmenting the security and dependability of machine learning systems, effectively safeguarding them against potential adversarial threats.

Xie et al. [135] presented a novel approach named AdvProp to address adversarial attacks. Diverging from the conventional emphasis on enhancing model robustness against such attacks, the authors advocate utilizing adversarial examples as individual data points to improve the overall model performance. The presented study introduced a distinct viewpoint in countering adversarial attacks, harnessing them as a means to enhance model performance. By acknowledging the distinct underlying distributions of normal and adversarial data, the authors advocate employing a dedicated auxiliary batch normalization for adversarial examples. The study provides improved protection mechanisms against adversarial attacks by adopting these suggested strategies, simultaneously improving the model's overall performance.

The paper [136] proposed a defense strategy against adversarial attacks through the utilization of a high-level representation-guided denoiser. The conventional denoiser is often susceptible to the error amplification effect, wherein minor residual adversarial noise is amplified, leading to inaccurate classifications. The High-level representation Guided Denoiser (HGD) efficiently reduces the error amplification phenomena by using a loss function to assess the difference between the target model's clean image-activated outputs and the denoised image. Comparing this approach to ensemble adversarial training, the current state-of-the-art defense strategy for large-scale images reveals three significant benefits. The main benefit of using HGD as a defense method is that it makes the target model more resistant to black-box and white-box adversarial attacks. Furthermore, HGD exhibits the advantage of successfully generalizing additional images and unknown classes, even when trained on a limited dataset. Lastly, HGD has the versatility to defend models other than the ones guided by it.

E. ATTACKS INTRODUCED ON SEGMENTATION AND DRIVING SIMULATION MODELS

Segmentation divides an image or video stream into various segments or areas depending on features like color, texture, or motion. Segmenting sensor data, such as pictures or video feeds from cameras or lidar sensors, is used in ADAS to identify objects and areas of interest. For instance, segmentation may be used in a standard ADAS system to recognize people, cars, and other objects in a camera stream and follow their movement over time. Other ADAS components, such as collision avoidance or lane departure warning systems, can use this information to determine how to operate the car afterward. On the other hand, driving simulation models are digital representations of how a vehicle would behave in various driving situations. These models often incorporate variables like vehicle mass, friction, and aerodynamics and are based on physical concepts like Newtonian mechanics. Driving simulation models are used in ADAS to forecast how a vehicle will behave in various circumstances and to test and assess the effectiveness of ADAS algorithms and systems. The effectiveness of a collision avoidance system under various driving scenarios, for instance, or the way a lane departure warning system responds to bends and twists in the road, might be tested using a driving simulation model. In order to create and execute ADAS, segmentation and driving simulation models are essential. These models aid in increasing the safety and dependability of ADAS systems and preventing traffic accidents by precisely recognizing objects and areas of interest in sensor data and simulating a vehicle's behavior in various driving scenarios. Xu et al. [137] presented an adversarial attack on segmentation models in AVs using an iterative projected gradient-based method. The DeepLab-V3+ segmentation model was used for their investigation. The untargeted attack achieved a D-mIoU(Drop-in mean interaction over-union) rate of around 65% during the evaluation, and the attack became more effective with an increase in the number of iterations. The researchers also proposed an adversarial training method based on their observations to mitigate such attacks on segmentation models.

Countermeasures: Gradient Hiding serves as a potent defense strategy against gradient-based attacks and adversarial crafting techniques, such as the Fast Gradient Sign Method (FGSM). As elucidated by Qiu et al. [121], this method effectively conceals model gradient information from potential adversaries, thereby rendering gradient-based attacks ineffective in cases where the model is non-differentiable, such as with decision trees, nearest neighbor classifiers, or random forests.

In order to lessen the effects of potential adversarial disturbances in images, Wang et al. [138] suggested the introduction of a special data conversion module. They noticed a small but notable improvement in the resilience of the network model in opposition to adversarial assaults by including data expansion approaches, such as the use of Gaussian randomization processing during the training phase.

F. ATTACKS ON LIDAR

LiDAR represents an advanced technology that leverages lasers to ascertain the distance to objects by precisely measuring the round-trip travel time of light as it reflects off the target and returns to a specialized receiver. It can also create 3D maps of terrain and ocean floors based on the differences in the way the laser light is reflected. In the context of vehicle perception systems, accurate recognition of

TABLE 5. Adversarial attacks.

Article	Attack	Counter-Technique	Description	Outcomes
[117]	Patch	Interval Bound Propagation (IBP)	Interval bound propagation is a simple verifier that uses layer-wise interval arithmetic to produce a certificate.	On the 5X5 MNIST dataset, the certified accuracy was 60.4% with a clean accuracy of 92%. On the 5X5 CIFAR dataset, the certified accuracy was 30.3% with a clean accuracy of 47.8%.
[116]		A method based on randomized smoothing	The idea of randomized smoothing is to add random noise to the input data to make the model's predictions more stable and resilient to adversarial perturbations	The proposed model outperformed [117] with faster training and improved results. It achieved certified accuracy of 52.44% (clean accuracy 96.54%) on 5X5 MNIST, 57.58% (clean accuracy 83.82%) on 5X5 CIFAR, and 13.9% certified accuracy (clean accuracy 44.6%) on 42X42 ImageNet.
[118]		Vision Transformers(ViT) for Derandomized Smoothing	ViT achieves CNN-like performance by employing self-attention and patch-based modeling for images.	On ImageNet, the proposed method achieved a certified accuracy of 41.70% and a clean accuracy of 78.58% under 2% area patch attacks.
[122]	Training Phase	Barrage of Random Transforms (BaRT)	BaRT is a technique in computer vision that applies a sequence of random transformations to training data to enhance model robustness and generalization	The proposed method achieved a remarkable up to 24-fold improvement in accuracy compared to previous work, extending its effectiveness to a previously untested maximum adversarial perturbation of epsilon=32.
[121], [123], [124]		Gradient Hiding	This technique hides gradient information of the target model from the adversaries	It was shown that the method could be easily fooled in certain scenarios by training a proxy black-box model using gradients and generating adversarial samples.
[125]		Adversarial Training	Adversarial Training involves training a model on a combination of normal training data and adversarial examples, which are generated by intentionally perturbing the input images to cause misclassification	A family of fast methods was introduced to generate adversarial examples for training, aiming to decrease test set error. It was also shown that adversarial training resulted in regularization, providing even stronger regularization than dropout.
[133]	Attacks on Image Classification and Object Detection Models	Adversarial Training		Compared to normal networks, adversarially trained networks' final loss values were noticeably lower.
[135]		AdvProp	The authors proposed an enhanced adversarial training scheme that treats adversarial examples as new examples to prevent overfitting	Their proposed model achieved a top-1 accuracy of 85.5% on ImageNet without using any additional data.
[136]		high-level representation guided denoiser (HGD)	This technique is used in image-denoising tasks to enhance the quality of denoised images. This method turned to be very robust against both white-box and black-box attacks.	The suggested approach performed better than the state-of-the-art ensemble adversarial training in a number of ways. It was more effective in defending against both white-box and black-box attacks, needed less time and training data, generalized well to additional photos and undiscovered classes, and could be applied to other target models.
[121]	Attacks introduced on segmentation and driving simulation Models	Gradient Hiding	Gradient hiding is an effective defense strategy that protects against gradient-based attacks and adversarial crafting techniques such as the Fast Gradient Sign Method (FGSM). It involves concealing the model's gradient information from potential adversaries.	The method was shown to be easily fooled in certain scenarios by training a proxy black-box model using gradients and generating adversarial samples.
[138]		Using a Data Transformation Module	The proposed approach integrates a non-parametric dimensionality reduction method called LLE with a DNN, enhances the DNN's resistance to adversarial samples	The results demonstrated that their approach generally provided superior classification performance and resistance compared to state-of-the-art solutions.
[139]	Lidar	sensor fusion	Sensor fusion techniques combine data from multiple sensors, such as LiDAR, RADAR, and cameras, to enhance perception and improve the accuracy and reliability of autonomous systems.	The paper discussed and compared various fusion techniques for sensors, highlighting their respective advantages, disadvantages, and application areas.
[140]		Quantization Index Modulation(QIM)	It is a data-hiding technique that embeds a binary watermark into sensor data, such as LiDAR, for the purpose of real-time integrity verification and tamper detection in autonomous vehicles.	The 3D FCN deep-learning model achieved good object detection accuracy with step sizes up to 30 cm, but higher step sizes resulted in deviations from the ground truth.
[125] [133]	Adversarial Evasion Attacks	Adversarial training	As discussed above, this method involves training a model on a combination of normal training data and adversarial examples.	Unlike normal networks, adversarially trained networks' final loss values were noticeably lower.
[141]		Defensive Distillation	Defensive distillation is a technique that trains a model to mimic the soft target labels provided by a teacher model, making the model more robust against adversarial attacks by smoothing decision boundaries.	Empirical findings demonstrated that defensive distillation significantly reduced the success of attacks against DNNs while maintaining the accuracy rates of the original models.
[123]		Ensemble model	Ensemble modeling in adversarial training combines multiple models to enhance robustness against attacks. It leverages diverse perspectives to reduce vulnerabilities and provide a stronger defense.	The introduced technique enhanced the robustness of models against black-box attacks on ImageNet. Additionally, this technique demonstrated promising outcomes in transferring the ability to withstand attacks from other models.

obstacles, tracking, and positioning is crucial for safe driving. Lidar provides a way to create detailed 3D representations of the environment, with the obstacle point cloud being denser than the background.

Recent advances in detection and segmentation technology have allowed Lidar to efficiently detect pedestrians and vehicles using 3D bounding boxes or point clouds. The 3D point cloud is generated by sensors that collect data points through Lidar. Each data point is a dot that represents a reflection of the laser light and is used to create a comprehensive 3D image of the environment.

While adversarial instances for 2D pictures and CNNs have received a great deal of study, 3D data like point clouds have received less attention [142]. Investigating the influence of adversarial point clouds on established deep 3D models assumes paramount importance in numerous safety-critical 3D applications, notably in the domain of autonomous driving [143]. A key component of the attack method against 3D models is the creation of 3D adversarial point clouds. This significance arises from the common practice of representing 3D objects through point clouds, which serve as the fundamental data format acquired from 3D sensors, such as depth cameras and LIDARs.

There are various innovative techniques for conducting adversarial attacks on point clouds, primarily falling into two categories: adversarial point perturbation and adversarial point generation. These attacks aim to create perturbations or generate points in a way that is imperceptible to humans or is hidden from human perception [142].

Concerning adversarial point perturbation, the approach involves making minimal shifts or adjustments to the positions of existing points within the point cloud. Experimental findings consistently highlight the remarkable success rate of generating adversarial point clouds through this technique.

Regarding adversarial point generation, this approach encompasses the generation of independent points or small clusters of points in the vicinity of the original object. The methodology revolves around the identification of ''vulnerable'' regions within the object and subsequently optimizing the positions and shapes of the generated points or clusters. The generation process is subject to constraints, considering factors such as point sizes, distances to the object surface, and the maximum number of shapes placed to ensure the stealthy and effective nature of the adversarial attack.

Countermeasures: Sensor fusion and redundancy are critical for fortifying LIDAR-based perception systems against such attacks [139]. Sensor fusion is a fundamental aspect of data integration in various domains, encompassing the synthesis of information derived from multiple sensors like LIDAR, cameras, and radar. This amalgamation facilitates the acquisition of an extensive and dependable comprehension of the surrounding environment, enhancing the overall system's performance and reliability. This integration of different sensor modalities enhances object detection, tracking, and scene understanding capabilities, reducing the impact of potential attacks. Additionally, redundancy techniques involving duplicate or overlapping LIDAR sensors provide backup options in case of sensor failures or malicious attacks. Cross-validating information from multiple LIDAR sensors allows the system to maintain accurate perception even when one or more sensors are compromised. Leveraging sensor fusion and redundancy in LIDAR-based systems is crucial for robust and secure perception, particularly in the face of attacks targeting the LIDAR sensor.

In their work [140], the researchers introduced an innovative approach involving semi-fragile data hiding, specifically employing 3-dimensional quantization index modulation (QIM), as an effective technique for securing LiDAR sensor data. The novel approach enables the detection of tampering and real-time integrity verification within the autonomous vehicle's decision-making unit. The experimental evaluation, conducted on a benchmark LiDAR dataset, substantiated the efficacy of the proposed approach in detecting and localizing tampering attacks. The paper highlighted the significance of fortifying against insider attacks on raw sensor data and proposed potential avenues for future research and extensions.

G. ADVERSARIAL EVASION ATTACKS

Evasion attacks manifest during the inference stage of the model, where malevolent entities endeavor to manipulate the input data in a manner that induces misclassification by the model [144]. The goal is to design input data that appears normal to human perception but can exploit the model's weaknesses and produce incorrect results. This attack seeks to cause a misclassification at inference time through manipulation of the inputs. Some Evasion attacks are:

FGSM Attack: FGSM, which stands for Fast Gradient Sign Method [125], [145] is a popular evasion technique that involves adding a minor perturbation to the input data that is proportional to the gradient of the loss with respect to the input. The aforementioned perturbation typically exhibits minimal visibility to the human visual perception; however, its presence can induce erroneous classification of the input within the model.

DeepFool Attack: DeepFool, as introduced by Moosavi-Dezfooli et al. [131], represents an iterative adversarial attack methodology predicated on linearization principles to ascertain the minimal perturbation required for input to traverse a decision boundary. The attack algorithm entails the computation of the decision function's gradient at the present data point, subsequently iteratively adjusting the input in the direction of the decision boundary until a misclassification is achieved.

Universal Adversarial Perturbation: A UAP [146], [147] refers to a minute perturbation that possesses the unique property of being universally applicable to any input data, regardless of its specific characteristics, thereby inducing

TABLE 6. Limitations and complexities of the discussed counter methods.

Reference	Method Name	Complexity	Limitations
[65]	P2DAP(Peer-to-Peer Distributed Accountable Protocols)	Medium	While the paper proposes involving the DMV for centralized management during detection, it doesn't address the limitations of relying on a central authority. In real-world scenarios, central authorities may be prone to single points of failure and may introduce latency or privacy concerns.
[86]	Transmitting Hidden Mark Signals	High	The suggested system remains susceptible to relay attacks, and the document highlights its vulnerability to selective-delay attacks that require a minimum of four high-gain directional antennas.
[90]	Using Directional Antennas	Medium	The paper's emphasis on a simplified two-dimensional road model may not adequately capture the intricacies and difficulties present in actual three-dimensional road systems, which encompass features like bridges, tunnels, and intricate intersections.
[116]	Random Smoothing for Adversarial Perturbation	High	Although the paper discusses improved performance compared to existing methods, it does not elaborate on the computational resources required to implement the defense. This could be a limitation in resource-constrained environments.
[121]	Gradient Hiding	Medium	It was shown that the method could be easily fooled in certain scenarios by training a proxy black-box model using gradients and generating adversarial samples
[139]	Sensor fusion	Low	Multi-Sensor Fusion (MSF) is widely adopted for perception in autonomous vehicles, particularly for the task of 3D object detection with camera and LiDAR sensors. However, MSF-based perception can be compromised by physically-realizable, adversarial 3D-printed objects that mislead an system to fail in detecting them.
[113]	Frequency Hopping	Medium	Traditional Frequency Hopping Spread Spectrum (FHSS) uses a fixed hopping pattern. Both the transmitter and receiver should pre-share the fixed hopping sequence in the presence of a jammer. Hopping from one channel to another can result in a throughput loss.
[95]	Machine learning and deep learning approach	High	ML/DL models are dependent on the quality and quantity of the data they are trained on and often require powerful and costly hardware infrastructure. Some methods are dependent on the network topology and may not be effective in different network environments. There is a lack of consensus, making it challenging to establish standard practices.
[100]	Cryptography based techniques	Varies: Medium to High	ADAS systems often require real-time performance. Cryptographic operations can be computationally intensive, leading to increased latency, which might not be acceptable in real-time systems. ADAS systems are also typically embedded systems with limited computational resources. Implementing robust cryptographic systems on such platforms can be challenging. Scalability of the cryptographic solutions can become a challenge.

a model to misclassify the perturbed inputs. UAPs are generated by optimizing a perturbation over a large dataset or by combining multiple perturbations.

Boundary Attack: The Boundary Attack is an iterative attack that searches for the decision boundary of a model [148]. The attacker starts with an input that is correctly classified by the model and then iteratively moves the input toward the decision boundary until it is misclassified.

Carlini and Wagner Attack: The Carlini and Wagner Attack (C&W) [149] constitutes an optimization-driven adversarial attack technique designed to create perturbations with specific objectives. By employing an optimization process, this attack generates perturbations that minimize the distance between the input data and a predefined target class and maximize the confidence associated with that target class. This simultaneous pursuit of two objectives enables the crafted perturbation to be effective in evading the target model's classification while increasing the likelihood of successful misclassification into the intended target class.

Countermeasures: Countering adversarial attacks is a challenging task, but there are several techniques that can be used to mitigate their impact. Here are some ways to prevent such attacks:

Similar to our previous discussion, where adversarial training was explored as a solution, it can also be leveraged as a preventive measure in the current problem. Adversarial training is a technique in machine learning where models are retrained using adversarial examples, aiming to enhance their robustness against potential attacks [125], [133].

The authors in [141] introduce defensive distillation as a preventive measure against adversarial samples in deep neural networks (DNNs). Defensive distillation is a technique that reduces the effectiveness of adversarial attacks by training DNNs with softened probability vectors, making them less susceptible to manipulation. Analytical and empirical evaluations demonstrate the significant reduction in the success rate of adversarial attacks achieved through defensive distillation, highlighting its potential as a practical

and effective defense mechanism for securing DNN-based systems.

Furthermore, an additional effective method, as suggested by Tramer et al. [123] in their work on ensemble models, involves combining multiple models to mitigate the impact of adversarial attacks. By employing an ensemble model approach, where multiple diverse models are trained, and their outputs are aggregated, the system becomes more resilient to adversarial perturbations. Subsequently, attackers would be confronted with the formidable task of devising adversarial examples with the capacity to deceive all the constituent models within the ensemble simultaneously. This cooperative defense mechanism increases the difficulty of successful attacks, further enhancing the security of the system against adversarial samples.

TABLE 5 summarizes various techniques used to counter adversarial attacks. It covers different types of attacks and their corresponding defense mechanisms. Notable observations include the effectiveness of adversarial training in improving model robustness, the vulnerability of gradient hiding techniques in certain scenarios, the superior performance of randomized smoothing compared to interval-bound propagation, and the successful application of sensor fusion in enhancing autonomous systems. Quantitative results indicate varying levels of success for each technique, with some achieving high certified accuracies and outperforming previous methods. The table provides valuable insights into the approaches employed to mitigate adversarial attacks and their corresponding outcomes.

In TABLE 6, we present an overview of the methods discussed in the preceding sections, which encompass a range of attacks, including those targeting VANETs, hardware, and adversarial scenarios. This table provides a comprehensive evaluation of each methodology, considering both the limitations inherent in the proposed countermeasures and the associated complexity. We categorize complexity into three levels: low, medium, and high.

Research Direction in Adversarial Attacks: The outlined research directions in adversarial attacks have been organized based on their paramount importance in ADAS security

1) **Advanced Defensive Techniques:** Research and implement dynamic adversarial training methods that continuously evolve defensive strategies against various attack types. Develop mechanisms to maintain high classifier accuracy while ensuring robustness against adversarial manipulations.
2) **Synergistic Defense Strategies:** Explore the combination of diverse defense tactics, such as input transformations, adversarial training, and robust model architectures. Investigate the strategic integration of randomness and variability to create synergistic defenses resilient to sophisticated attacks.
3) **End-to-end Training Approaches:** Develop frameworks for end-to-end training incorporating online adversarial attack generation. Investigate techniques that adaptively update models in real-time, enhancing resilience to dynamic adversarial threats encountered during operation.
4) **Scalable Certified Defense Techniques:** Enhance certified defense techniques to scale efficiently for larger and more complex datasets akin to ImageNet. Optimize verification methods to maintain effectiveness and computational efficiency while ensuring robustness at scale.
5) **Addressing Potential Pitfalls and Privacy Concerns:** Investigate strategies to balance robustness guarantees with user privacy. Develop mechanisms to mitigate system overconfidence while ensuring user data privacy remains uncompromised within the context of defense mechanisms.

Each direction represents a crucial avenue for further exploration, requiring in-depth investigations to fortify ADAS security against adversarial attacks while addressing concerns related to system reliability and user privacy.

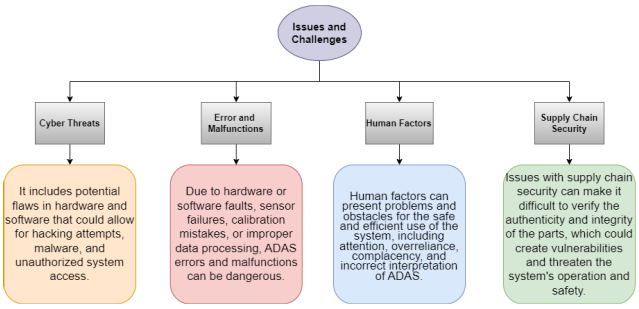

FIGURE 15. Issues and challenges.

VI. ISSUES AND CHALLENGES

In contemporary automobiles, ADAS are becoming more and more prevalent. By automating several driving processes, such as lane departure warnings, automatic emergency braking, etc., these technologies are intended to increase safety and convenience. But as technology is used in cars more and more, ADAS security has grown to be a significant issue. Some of the major problems and obstacles in ADAS security are shown in FIGURE 15.

A. CYBER THREATS

Hackers might leverage the infotainment system, the OBD connector, or even wireless signals used for V2I and V2V communications to gain access to the target vehicle's network and compromise ADAS systems. If these attackers successfully turned off the ADAS systems or even took over the vehicle, the security of the passengers and other drivers could be jeopardized. Gordan and Ford [150] mentioned that computers, networks, smart gadgets, and other electronic equipment may be used to facilitate or carry out cyberattacks in which they act as agents, facilitators, or targets. Further, the authors look at the range of computer-based crime and discuss cybercrimes with a strong technological component and cybercrime with a stronger human component.

Mller [151] discussed in their paper that the complexity of vehicular systems has increased due to the widespread use of cyber-physical systems (CPS) in the numerous vehicle ADAS, which require their sophisticated software algorithms to carry out the required tasks. Moller et al. [152] have mentioned that the cyber devices or physical devices of vital and important vehicle components are becoming more and more susceptible to various range of security issues, threats, malicious cyber-attacks, and intrusions as a result of their scale and complexity. The aforementioned interfaces can potentially generate additional attack vectors that expose internal onboard sensors utilised in autonomous driving to internal and external cyberattacks with the ability to tamper with sensor data. Changalvala and Malik [140] claimed that failing to secure the sensor data could lead to false assessments and possibly fatal accidents because the control algorithms that govern the behavior of the autonomous vehicle depend on the data from several onboard sensors, including LiDAR, camera, and RADAR.

B. ERROR AND MALFUNCTIONS

The proper operation of ADAS systems depends on a variety of sensors, cameras, and algorithms. Yet malfunctions and faults can also be brought on by hardware issues, software problems, or outside influences like bad weather. These flaws could result in the ADAS system making poor decisions or failing to recognize dangers, which could cause accidents. Ensuring that the system fault in ADAS systems doesn't hurt people is crucial. The improper execution of software may cause malfunctions. Goswami et al. [153] stated that there are numerous methods available to detect systematic SW errors throughout development. Yet, it is hard to ensure a fail-safe system without run-time monitoring.

One of the problems that the ISO 26262 functional security standard, [154] aims to lessen or prevent is the failure of the ADAS MPSoC. As SW complexity rises, the standard strongly emphasizes testing and verification of application SW components at every level of the product life cycle, including deployment in the field. Many kinds of methods have been developed to find systematic SW mistakes when creating SW for ADAS applications [155]. A fail-safe system cannot be assured if there is no way to monitor and notify the application's status, even when it malfunctions or crashes.

C. HUMAN FACTORS

Although ADAS systems are intended to help drivers, they nonetheless necessitate active attention from the driver. However, some drivers might rely too heavily on ADAS devices, leading to complacency or distraction and raising the possibility of accidents. Also, it's possible that drivers will not completely comprehend how to use or interpret the data offered by ADAS systems, which could cause confusion or incorrect interpretation.

Even though the ADAS system has advanced significantly, it still depends on the driver to oversee and control various aspects of the car. It has been observed [156], [157] driver errors that result in collisions and disputes can be caused by these interventions and supervision needs, which can cause drivers to go "out of the driving loop," acquire unfavorable behavioral adaptations and experience mode confusion.

Driver errors may also occur in human-machine interactions for a variety of reasons, including improper decision-making brought on by rule-based or knowledge-based mistakes or because users have misconceptions about the systems as a result of holes in their mental models, i.e., an intricate and rich structure that represents the user's comprehension of the system's contents, operation, and underlying idea and logic [158], [159].

Driver errors thus play a significant influence in auto accidents, especially when taking into account safety-critical systems.

D. SUPPLY CHAIN SECURITY

Supply chain security refers to safeguarding the components and processes involved in the development, manufacturing, and distribution of ADAS, including hardware, firmware, software, and other components, to ensure that they are free from vulnerabilities or malicious activities that could compromise the security of the ADAS. Supply chain security is critical for ADAS as these systems are complex and often rely on components and software from multiple vendors, which may introduce potential vulnerabilities or weaknesses in the system if not properly secured. Any compromise in the supply chain, such as tampering with components, insertion of malware or malicious code, or unauthorized access to sensitive information, can pose significant risks to the security and functionality of the ADAS.

Hassija et al. [160] outlined the crucial supply chain security application areas and thoroughly examined the security problems with the current architecture. Additionally, it considers cutting-edge technologies like blockchain, ML, and physically unclonable functions (PUFs) as viable remedies for the supply chain infrastructure vulnerabilities that are now present.

In a systematic literature review [161] of credible research on blockchain for environmentally conscious supply chain management, it was discovered that blockchain's highly safe framework and distributed consensus have benefits for increasing the sustainability of supply chains. The review identified notable journals, authors, organizations, and countries that have contributed to the subject, as well as the primary themes of blockchain for sustainable business operations, blockchain for decision support systems, and blockchain for intelligent transportation systems.

Significance of standardizing and maintaining transparency in naming conventions, designs, and operations of advanced driver-assistance systems (ADAS) functions, extending from modern ADAS to fully autonomous driving features are highlighted in [162]. The study systematically reviews user manuals from various automakers, conducting critical analyses of common ADAS functions. The findings

reveal substantial variations in terminologies, operational conditions, and control procedures among manufacturers, leading to driver confusion and underutilization of ADAS features. The paper suggests the need for industry-wide consensus and guidelines to improve ADAS transparency, benefiting both users and future AI-driven self-driving functions.

VII. CONCLUSION AND FUTURE SCOPE

A. CONCLUSION

The vital security concerns raised by the incorporation of ADAS technologies in AVs have been examined in this research paper. Throughout the study, we have outlined and examined the potential threats, attacks, and vulnerabilities that ADAS technologies may experience. Additionally, we covered defense strategies to lessen these dangers and improve passenger and other road user privacy and safety. The article examined three types of assaults and their defenses in the quest for safer and more dependable transportation networks: VANET attacks, Hardware attacks, and Adversarial attacks. For the purpose of protecting AVs from malicious intent, it is essential to comprehend these potential risks and effective responses. Our study has highlighted the pressing need to solve ADAS security issues as the field of automotive technology continues to advance quickly. The knowledge gathered from this research will help make ADAS technology more secure to use, advancing the development of AVs while safeguarding user welfare and public safety. The study also discusses some intriguing future research directions in ADAS security that merit further investigation. We can open the door to a safer and more dependable future of transportation by tackling the security issues raised by ADAS integration and doing ongoing research in this area. This will ensure that people and society can have faith in AVs.

B. FUTURE SCOPE

The future scope of ADAS security is large, necessitating ongoing research to keep up with emerging threats and weaknesses. Some of the issues and potential solutions to ensure the security and safety of ADAS systems were emphasized in the study. More study is needed, however, to develop more robust and complex security systems, such as the use of artificial intelligence and machine learning techniques to detect and prevent assaults. Furthermore, industry-wide standards and regulations are required to enable consistent implementation of security measures across different ADAS systems.

Since several manufacturers and developers are involved in ADAS, a common architecture is necessary to ensure that strong security measures are implemented consistently. Standardisation ensures interoperability and promotes collaboration across disparate systems by giving security protocols a uniform language. This strategy not only improves security but also makes it easier to adopt best practises. Attaining universal standardisation across the sector necessitates cooperative initiatives from various stakeholders, such as manufacturers, regulatory entities, and security specialists. Industry associations and joint research projects can help establish clear standards, enabling adaptation to address evolving challenges and developments in ADAS. Advocating for standards is primarily focused on cultivating a secure ecosystem that places user safety, privacy, and innovation as top priorities.

As ADAS systems grow more common, it is critical to keep looking for new ways to protect drivers, passengers, and other road users from potential security concerns.

Specific study directions for each area on attacks, namely VANET (Sec. III), Hardware (Sec. IV), and Adversarial (Sec. V), are listed at the end of their respective parts. In summary, suggestions are to work on defenses against attacks, as many existing given measures may have flaws or modest limits that may provide the attackers with an edge.

REFERENCES

[1] (2022). *Advanced Driver Assistance Systems (ADAS) Market*. Accessed: Mar. 15, 2023. [Online]. Available: https://www.precedence research.com/advanced-driver-assistance-systems-market

[2] A. Gross. (2018). *Drivers Rely Too Heavily on New Vehicle Safety Technologies in Spite of Limitations*. Accessed: Jul. 7, 2023. [Online]. Available: https://newsroom.aaa.com/2018/09/drivers-rely-heavily-new-vehicle-safety-technologies/

[3] S. M. Mohtavipour, T. Z. Ehsan, H. J. Abeshoori, and M. Mollajafari, "Smooth longitudinal driving strategy with adjustable nonlinear reference model for autonomous vehicles," *Int. J. Dyn. Control*, vol. 11, no. 5, pp. 2320–2334, Oct. 2023.

[4] A. Ziebinski, R. Cupek, H. Erdogan, and S. Waechter, "A survey of ADAS technologies for the future perspective of sensor fusion," in *Proc. Int. Conf. Comput. Collective Intell.* Cham, Switzerland: Springer, Sep. 2016, pp. 135–146.

[5] T. Hanke, N. Hirsenkorn, B. Dehlink, A. Rauch, R. Rasshofer, and E. Biebl, "Generic architecture for simulation of ADAS sensors," in *Proc. 16th Int. Radar Symp. (IRS)*, Jun. 2015, pp. 125–130.

[6] G. Niedrist, "Deterministic architecture and middleware for domain control units and simplified integration process applied to ADAS," in *Fahrerassistenzsysteme 2016*. Cham, Switzerland: Springer, 2018, pp. 235–250.

[7] M. H. Shojaeefard, M. Mollajafari, S. Ebrahimi-Nejad, and S. Tayebi, "Weather-aware fuzzy adaptive cruise control: Dynamic reference signal design," *Comput. Electr. Eng.*, vol. 110, Sep. 2023, Art. no. 108903.

[8] E. Enders, G. Burkhard, and N. Munzinger, "Analysis of the influence of suspension actuator limitations on ride comfort in passenger cars using model predictive control," *Actuators*, vol. 9, no. 3, p. 77, Aug. 2020.

[9] W. Payre, J. Perelló-March, and S. Birrell, "Under pressure: Effect of a ransomware and a screen failure on trust and driving performance in an automated car simulation," *Frontiers Psychol.*, vol. 14, p. 822, Mar. 2023.

[10] C. Rödel, S. Stadler, A. Meschtscherjakov, and M. Tscheligi, "Towards autonomous cars: The effect of autonomy levels on acceptance and user experience," in *Proc. 6th Int. Conf. Automot. User Interface Interact. Veh. Appl.*, Sep. 2014, pp. 1–8.

[11] A. Kurbanov, S. Grebennikov, S. Gafurov, and A. Klimchik, "Vulnerabilities in the vehicle's electronic network equipped with ADAS system," in *Proc. 3rd School Dyn. Complex Netw. Appl. Intellectual Robot. (DCNAIR)*, Sep. 2019, pp. 100–102.

[12] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2011, pp. 1–11.

[13] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," *Black Hat USA*, vol. 2014, p. 94, Aug. 2014.

[14] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *Proc. IEEE Symp. Secur. Privacy*, May 2010, pp. 447–462.

[15] D. K. Nilsson, U. E. Larson, and P. H. Phung, "Vehicle ECU classification based on safety-security characteristics," in *Proc. IET Road Transp. Inf. Control Conf. ITS United Kingdom Members' Conf. (RTIC)*, 2008, pp. 1–7.

[16] D. F. Oswald, "Wireless attacks on automotive remote keyless entry systems," in *Proc. 6th Int. Workshop Trustworthy Embedded Devices*, Oct. 2016, pp. 43–44.

[17] P. Kleberger, T. Olovsson, and E. Jonsson, "Security aspects of the in-vehicle network in the connected car," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2011, pp. 528–533.

[18] J. Jansson, "Collision avoidance theory: With application to automotive collision mitigation," Ph.D. thesis, Dept. Elect. Eng., Linköping Univ. Electron. Press, Linköping, Sweden, Tech. Rep., 2005.

[19] N. Brouwer, H. Kloeden, and C. Stiller, "Comparison and evaluation of pedestrian motion models for vehicle safety systems," in *Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2016, pp. 1–6.

[20] A. Houenou, P. Bonnifait, V. Cherfaoui, and W. Yao, "Vehicle trajectory prediction based on motion model and maneuver recognition," in *Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst.*, Nov. 2013, pp. 4363–4369.

[21] M. Brännström, E. Coelingh, and J. Sjöberg, "Model-based threat assessment for avoiding arbitrary vehicle collisions," *IEEE Trans. Intell. Transp. Syst.*, vol. 11, no. 3, pp. 658–669, Sep. 2010.

[22] Y. Xing, C. Lv, H. Wang, D. Cao, and E. Velenis, "An ensemble deep learning approach for driver lane change intention inference," *Transp. Res. C, Emerg. Technol.*, vol. 115, Jun. 2020, Art. no. 102615.

[23] J. M. Ambarak, H. Ying, F. Syed, and D. Filev, "A neural network for predicting unintentional lane departures," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, Mar. 2017, pp. 492–497.

[24] J. Dahl, G. Rodrigues de Campos, and J. Fredriksson, "Performance and efficiency analysis of a linear learning-based prediction model used for unintended lane-departure detection," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 9115–9125, Jul. 2022.

[25] J. Dahl, R. Jonsson, A. Kollmats, G. R. de Campos, and J. Fredriksson, "Automotive safety: A neural network approach for lane departure detection using real world driving data," in *Proc. IEEE Intell. Transp. Syst. Conf. (ITSC)*, Oct. 2019, pp. 3669–3674.

[26] J. Dahl, G. R. de Campos, and J. Fredriksson, "A path prediction model based on multiple time series analysis tools used to detect unintended lane departures," in *Proc. IEEE 23rd Int. Conf. Intell. Transp. Syst. (ITSC)*, Sep. 2020, pp. 1–7.

[27] W. Wang, D. Zhao, W. Han, and J. Xi, "A learning-based approach for lane departure warning systems with a personalized driver model," *IEEE Trans. Veh. Technol.*, vol. 67, no. 10, pp. 9145–9157, Oct. 2018.

[28] V. Ilic, D. Kukolj, M. Marijan, and N. Teslic, "Predicting positions and velocities of surrounding vehicles using deep neural networks," in *Proc. Zooming Innov. Consum. Technol. Conf. (ZINC)*, May 2019, pp. 126–129.

[29] K. Min, D. Kim, J. Park, and K. Huh, "RNN-based path prediction of obstacle vehicles with deep ensemble," *IEEE Trans. Veh. Technol.*, vol. 68, no. 10, pp. 10252–10256, Mar. 2019.

[30] H. Cui, T. Nguyen, F.-C. Chou, T.-H. Lin, J. Schneider, D. Bradley, and N. Djuric, "Deep kinematic models for kinematically feasible vehicle trajectory predictions," in *Proc. IEEE Int. Conf. Robot. Autom. (ICRA)*, May 2020, pp. 10563–10569.

[31] A. Zyner, S. Worrall, and E. Nebot, "Naturalistic driver intention and path prediction using recurrent neural networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 4, pp. 1584–1594, Apr. 2020.

[32] X. Mo, Y. Xing, and C. Lv, "Interaction-aware trajectory prediction of connected vehicles using CNN-LSTM networks," in *Proc. 46th Annu. Conf. IEEE Ind. Electron. Soc.*, Oct. 2020, pp. 5057–5062.

[33] K. Messaoud, I. Yahiaoui, A. Verroust-Blondet, and F. Nashashibi, "Attention based vehicle trajectory prediction," *IEEE Trans. Intell. Vehicles*, vol. 6, no. 1, pp. 175–185, Mar. 2021.

[34] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.

[35] J. Dahl, G. R. de Campos, and J. Fredriksson, "Prediction-uncertainty-aware threat detection for ADAS: A case study on lane-keeping assistance," *IEEE Trans. Intell. Vehicles*, vol. 8, no. 4, pp. 2914–2925, Apr. 2023.

[36] G. Guo, J. Kang, H. Lei, and D. Li, "Finite-time stabilization of a collection of connected vehicles subject to communication interruptions," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 10627–10635, Aug. 2022.

[37] J. M. Qurashi, M. J. Ikram, K. Jambi, F. E. Eassa, and M. Khemakhem, "Autonomous vehicles: Security challenges and game theory-based countermeasures," in *Proc. 1st Int. Conf. Adv. Innov. Smart Cities (ICAISC)*, Jan. 2023, pp. 1–6.

[38] X. Zhou, A. Schmedding, H. Ren, L. Yang, P. Schowitz, E. Smirni, and H. Alemzadeh, "Strategic safety-critical attacks against an advanced driver assistance system," in *Proc. 52nd Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2022, pp. 79–87.

[39] Y. Li, M. Liu, C. Cao, and J. Li, "Communication-Traffic-Assisted mining and exploitation of buffer overflow vulnerabilities in ADASs," *Future Internet*, vol. 15, no. 5, p. 185, May 2023.

[40] S.-L. Wang, S.-Y. Wu, C.-C. Lin, S. Boddupalli, P.-J. Chang, C.-W. Lin, C.-S. Shih, and S. Ray, "Deep-Learning-Based intrusion detection for autonomous vehicle-following systems," in *Proc. IEEE Int. Intell. Transp. Syst. Conf. (ITSC)*, Sep. 2021, pp. 865–872.

[41] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in *Proc. USENIX Secur. Symp.*, vol. 40, 2016, pp. 911–927.

[42] F. Siddiqui, R. Khan, S. Y. Tasdemir, H. Hui, B. Sonigara, S. Sezer, and K. McLaughlin, "Cybersecurity engineering: Bridging the security gaps in advanced automotive systems and ISO/SAE 21434," in *Proc. IEEE 97th Veh. Technol. Conf. (VTC-Spring)*, Jun. 2023, pp. 1–6.

[43] Z. Abuabed, A. Alsadeh, and A. Taweel, "STRIDE threat model-based framework for assessing the vulnerabilities of modern vehicles," *Comput. Secur.*, vol. 133, Oct. 2023, Art. no. 103391.

[44] A. Moujahid, M. ElAraki Tantaoui, M. D. Hina, A. Soukane, A. Ortalda, A. ElKhadimi, and A. Ramdane-Cherif, "Machine learning techniques in ADAS: A review," in *Proc. Int. Conf. Adv. Comput. Commun. Eng. (ICACCE)*, Jun. 2018, pp. 235–242.

[45] S. Shruti, M. Shravya, S. Mohan, Y. Suhail, and R. Radha, "AI-based solutions for ADAS," in *Proc. 6th Int. Conf. Intell. Comput. Control Syst. (ICICCS)*, May 2022, pp. 1009–1012.

[46] Y. Hou, P. Edara, and C. Sun, "Modeling mandatory lane changing using Bayes classifier and decision trees," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 2, pp. 647–655, Apr. 2014.

[47] B. Morris, A. Doshi, and M. Trivedi, "Lane change intent prediction for driver assistance: On-road design and evaluation," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2011, pp. 895–901.

[48] B. Huval, T. Wang, S. Tandon, J. Kiske, W. Song, J. Pazhayampallil, M. Andriluka, P. Rajpurkar, T. Migimatsu, R. Cheng-Yue, F. Mujica, A. Coates, and A. Y. Ng, "An empirical evaluation of deep learning on highway driving," 2015, *arXiv:1504.01716*.

[49] D. Lee and H. Yeo, "Real-time rear-end collision-warning system using a multilayer perceptron neural network," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 11, pp. 3087–3097, Nov. 2016.

[50] D. W. S. Choi, F. Thalmayr and F. Weig. (2016). *Advanced Driver-Assistance Systems: Challenges and Opportunities Ahead*. Accessed: Nov. 25, 2023. [Online]. Available: https://www.mckinsey.com/industries/semiconductors/our-insights/advanced-driver-assistance-systems-challenges-and-opportunities-ahead

[51] E. de Gelder and J.-P. Paardekooper, "Assessment of automated driving systems using real-life scenarios," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2017, pp. 589–594.

[52] Z. Cai, A. Wang, W. Zhang, M. Gruffke, and H. Schweppe, "0-days & mitigations: Roadways to exploit and secure connected BMW cars," *Black Hat USA*, vol. 2019, no. 39, p. 6, 2019.

[53] 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, Apr. 2021, Art. no. 102150.

[54] A. J. Kerns, K. D. Wesson, and T. E. Humphreys, "A blueprint for civil GPS navigation message authentication," in *Proc. IEEE/ION Position, Location Navigat. Symp.*, May 2014, pp. 262–269.

[55] Y. Zhang, B. Ge, X. Li, B. Shi, and B. Li, "Controlling a car through OBD injection," in *Proc. IEEE 3rd Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)*, Jun. 2016, pp. 26–29.

[56] (2016). *Car Hacking Research: Remote Attack Tesla Motors*. Accessed: Mar. 19, 2023. [Online]. Available: https://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/

[57] F. Chrysler. (2015). *Fiat Chrysler Recalls 1.4 Million Cars After Jeep Hack*. Accessed: Mar. 21, 2023. [Online]. Available: https://www.bbc.com/news/technology-33650491

[58] K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, C. Xiao, A. Prakash, T. Kohno, and D. Song, "Robust physical-world attacks on deep learning visual classification," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, Jun. 2018, pp. 1625–1634.

[59] E. Juliussen. (2022). *Automotive Cyberattacks Grow More Varied Despite Improving Defenses*. Accessed: Jul. 7, 2023. [Online]. Available: https://www.embedded.com/automotive-cyberattacks-grow-more-varied-despite-improving-defenses/

[60] A. Ghosal and M. Conti, "Security issues and challenges in V2X: A survey," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107093.

[61] G. E. M. Abro, S. A. B. M. Zulkifli, K. Kumar, N. E. Ouanjli, V. S. Asirvadam, and M. A. Mossa, "Comprehensive review of recent advancements in battery technology, propulsion, power interfaces, and vehicle network systems for intelligent autonomous and connected electric vehicles," *Energies*, vol. 16, no. 6, p. 2925, Mar. 2023.

[62] W. Tong, A. Hussain, W. X. Bo, and S. Maharjan, "Artificial intelligence for vehicle-to-everything: A survey," *IEEE Access*, vol. 7, pp. 10823–10843, 2019.

[63] T. Zaidi and S. Faisal, "An overview: Various attacks in VANET," in *Proc. 4th Int. Conf. Comput. Commun. Autom. (ICCCA)*, Dec. 2018, pp. 1–6.

[64] M. S. Sheikh, J. Liang, and W. Wang, "A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs)," *Sensors*, vol. 19, no. 16, p. 3589, Aug. 2019.

[65] 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.

[66] C. Chen, X. Wang, W. Han, and B. Zang, "A robust detection of the Sybil attack in urban VANETs," in *Proc. 29th IEEE Int. Conf. Distrib. Comput. Syst. Workshops*, Jun. 2009, pp. 270–276.

[67] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): Status, results, and challenges," *Telecommun. Syst.*, vol. 50, no. 4, pp. 217–241, Aug. 2012.

[68] H. Hasbullah and I. A. Soomro, "Denial of service (DoS) attack and its possible solutions in VANET," *Int. J. Electron. Commun. Eng.*, vol. 4, no. 5, pp. 813–817, 2010.

[69] S. Biswas, J. Mišić, and V. Mišić, "DDoS attack on WAVE-enabled VANET through synchronization," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2012, pp. 1079–1084.

[70] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, 2007.

[71] A. Stampoulis and Z. Chai, "A survey of security in vehicular networks," Project CPSC, Washington, DC, USA, Tech. Rep., 534, 2007.

[72] R. Prasad, R. Kanjee, and H. Zui, "Pishro 'DSRC accident warning system at intersection,'" UMass Amherst, Amherst, MA, USA, Tech. Rep., Oct. 2006.

[73] H. Wen, P. Y.-R. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," in *Proc. 18th Int. Tech. Meeting Satell. Division Inst. Navigat.*, 2005, pp. 1285–1290.

[74] S. Malebary and W. Xu, "A survey on jamming in VANET," *Int. J. Sci. Res. Innov. Technol.*, vol. 2, no. 1, pp. 1–10, 2015.

[75] S. D. Babar, N. R. Prasad, and R. Prasad, "Jamming attack: Behavioral modelling and analysis," in *Proc. Wireless VITAE*, Jun. 2013, pp. 1–5.

[76] A. M. Malla and R. K. Sahu, "Security attacks with an effective solution for dos attacks in VANET," *Int. J. Comput. Appl.*, vol. 66, no. 22, pp. 45–49, 2013.

[77] V. Nallarasan and K. Kottursamy, "Cognitive radio jamming attack detection using an autoencoder for CRIoT network," *Wireless Pers. Commun.*, vol. 127, no. 3, pp. 2267–2283, Dec. 2022.

[78] R. Zhang, J. Sun, Y. Zhang, and X. Huang, "Jamming-resilient secure neighbor discovery in mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5588–5601, Oct. 2015.

[79] M. S. Al-kahtani, "Survey on security attacks in vehicular ad hoc networks (VANETs)," in *Proc. 6th Int. Conf. Signal Process. Commun. Syst.*, Dec. 2012, pp. 1–9.

[80] F. Ahmad, A. Adnane, V. 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, p. 4040, Nov. 2018.

[81] N.-W. Lo and H.-C. Tsai, "Illusion attack on VANET applications—A message plausibility problem," in *Proc. IEEE Globecom Workshops*, Nov. 2007, pp. 1–8.

[82] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, "Design of 5.9 GHz DSRC-based vehicular safety communication," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 36–43, Oct. 2006.

[83] A. Yahya, O. Sidek, and J. Mohamad-Saleh, "Design and develop wireless system using frequency hopping spread spectrum," *Eng. Lett.*, vol. 13, no. 4, 2006.

[84] S. RoselinMary, M. Maheshwari, and M. Thamaraiselvan, "Early detection of DOS attacks in VANET using attacked packet detection algorithm (APDA)," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Feb. 2013, pp. 237–240.

[85] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 2, pp. 245–257, 2nd Quart., 2011.

[86] M. G. Kuhn, "An asymmetric security mechanism for navigation signals," in *Proc. Int. Workshop Inf. Hiding*. Cham, Switzerland: Springer, 2004, pp. 239–252.

[87] J. Magiera and R. Katulski, "Detection and mitigation of GPS spoofing based on antenna array processing," *J. Appl. Res. Technol.*, vol. 13, no. 1, pp. 45–57, Feb. 2015.

[88] X. An, S. Zhao, X. Cui, Q. Shi, and M. Lu, "Distributed multi-antenna positioning for automatic-guided vehicle," *Sensors*, vol. 20, no. 4, p. 1155, Feb. 2020.

[89] M. Simon, J. Omura, R. Scholtz, and B. Levitt, *Spread Spectrum Communications Handbook*. New York, NY, USA: McGraw-Hill, 2002.

[90] S. Kuribayashi, Y. Sakumoto, H. Ohsaki, S. Hasegawa, and M. Imase, "Performance evaluation of epidemic broadcast with directional antennas in vehicular ad-hoc networks," in *Proc. IEEE/IPSJ Int. Symp. Appl. Internet*, Jul. 2011, pp. 260–265.

[91] G. Noubir, "On connectivity in ad hoc networks under jamming using directional antennas and mobility," in *Proc. Int. Conf. Wired/Wireless Internet Commun.* Cham, Switzerland: Springer, 2004, pp. 186–200.

[92] S.-A. Kaye, S. Nandavar, S. Yasmin, I. Lewis, and O. Oviedo-Trespalacios, "Consumer knowledge and acceptance of advanced driver assistance systems," *Transp. Res. F, Traffic Psychol. Behav.*, vol. 90, pp. 300–311, Oct. 2022.

[93] I. J. Reagan, J. B. Cicchino, E. R. Teoh, and A. E. Cox, "New and used vehicle buyers' awareness, understanding, and trust in advanced driver assistance systems," *Transp. Res. F, Traffic Psychol. Behav.*, vol. 92, pp. 44–55, Jan. 2023.

[94] J. Ayoub, Z. Wang, M. Li, H. Guo, R. Sherony, S. Bao, and F. Zhou, "Cause-and-Effect analysis of ADAS: A comparison study between literature review and complaint data," in *Proc. 14th Int. Conf. Automot. User Interface Interact. Veh. Appl.*, Sep. 2022, pp. 139–149.

[95] S. Kayser, F. Heybetli, and M. S. Ayas, "Model based detection scheme for denial of service attack on lane keeping assist system," in *Proc. Int. Congr. Hum.-Comput. Interact., Optim. Robotic Appl. (HORA)*, Jun. 2022, pp. 1–6.

[96] H. Djuitcheu, M. Debes, M. Aumüller, and J. Seitz, "Recent review of distributed denial of service attacks in the Internet of Things," in *Proc. 5th Conf. Cloud Internet Things (CIoT)*, Mar. 2022, pp. 32–39.

[97] P. Kumari and A. K. Jain, "A comprehensive study of DDoS attacks over IoT network and their countermeasures," *Comput. Secur.*, vol. 127, Apr. 2023, Art. no. 103096.

[98] M. A. Bouke, A. Abdullah, S. H. ALshatebi, M. T. Abdullah, and H. E. Atigh, "An intelligent DDoS attack detection tree-based model using Gini index feature selection method," *Microprocessors Microsyst.*, vol. 98, Apr. 2023, Art. no. 104823.

[99] H. Chen, J. Liu, J. Wang, and Y. Xun, "Towards secure intra-vehicle communications in 5G advanced and beyond: Vulnerabilities, attacks and countermeasures," *Veh. Commun.*, vol. 39, Feb. 2023, Art. no. 100548.

[100] C. Biswas, U. D. Gupta, and Md. M. Haque, "An efficient algorithm for confidentiality, integrity and authentication using hybrid cryptography and steganography," in *Proc. Int. Conf. Electr., Comput. Commun. Eng. (ECCE)*, Feb. 2019, pp. 1–5.

[101] P. Li, W. Ou, H. Liang, W. Han, Q. Zhang, and G. Zeng, "A zero trust and blockchain-based defense model for smart electric vehicle chargers," *J. Netw. Comput. Appl.*, vol. 213, Apr. 2023, Art. no. 103599.

[102] S. El Jaouhari and E. Bouvet, "Secure firmware over-the-air updates for IoT: Survey, challenges, and discussions," *Internet Things*, vol. 18, May 2022, Art. no. 100508.

[103] A. Benslimane and H. Nguyen-Minh, "Jamming attack model and detection method for beacons under multichannel operation in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 6475–6488, Jul. 2017.

[104] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 767–809, 2nd Quart., 2022.
[105] E. Elezi, G. Çankaya, A. Boyaci, and S. Yarkan, "A detection and identification method based on signal power for different types of electronic jamming attacks on GPS signals," in *Proc. IEEE 30th Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2019, pp. 1–5.
[106] S.-J. Lee, Y.-R. Lee, S.-E. Jeon, and I.-G. Lee, "Machine learning-based jamming attack classification and effective defense technique," *Comput. Secur.*, vol. 128, May 2023, Art. no. 103169.
[107] Z. Muhammad, Z. Anwar, B. Saleem, and J. Shahid, "Emerging cybersecurity and privacy threats to electric vehicles and their impact on human and environmental sustainability," *Energies*, vol. 16, no. 3, p. 1113, Jan. 2023.
[108] N.-F. Polychronou, P.-H. Thevenon, M. Puys, and V. Beroulle, "A comprehensive survey of attacks without physical access targeting hardware vulnerabilities in IoT/IIoT devices, and their detection mechanisms," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 27, no. 1, pp. 1–35, Jan. 2022.
[109] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles," *Ad Hoc Netw.*, vol. 90, Jul. 2019, Art. no. 101823.
[110] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proc. 18th ACM Conf. Comput. Commun. Secur.*, Oct. 2011, pp. 75–86.
[111] M. A. Prada-Delgado, A. Vázquez-Reyes, and I. Baturone, "Trustworthy firmware update for Internet-of-Thing devices using physical unclonable functions," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2017, pp. 1–5.
[112] I. Zografopoulos, A. P. Kuruvila, K. Basu, and C. Konstantinou, "Time series-based detection and impact analysis of firmware attacks in microgrids," *Energy Rep.*, vol. 8, pp. 11221–11234, Nov. 2022.
[113] K. Pelechrinis, C. Koufogiannakis, and S. V. Krishnamurthy, "On the efficacy of frequency hopping in coping with jamming attacks in 802.11 networks," *IEEE Trans. Wireless Commun.*, vol. 9, no. 10, pp. 3258–3271, Oct. 2010.
[114] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.
[115] X. Li and S. Ji, "Generative dynamic patch attack," 2021, *arXiv:2111.04266*.
[116] A. Levine and S. Feizi, "(De) randomized smoothing for certifiable defense against patch attacks," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 33, 2020, pp. 6465–6475.
[117] P.-Y. Chiang, R. Ni, A. Abdelkader, C. Zhu, C. Studer, and T. Goldstein, "Certified defenses for adversarial patches," 2020, *arXiv:2003.06693*.
[118] Z. Chen, B. Li, J. Xu, S. Wu, S. Ding, and W. Zhang, "Towards practical certifiable patch defense with vision transformer," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2022, pp. 15127–15137.
[119] A. Chakraborty, M. Alam, V. Dey, A. Chattopadhyay, and D. Mukhopadhyay, "Adversarial attacks and defences: A survey," 2018, *arXiv:1810.00069*.
[120] X. Liu, L. Xie, Y. Wang, J. Zou, J. Xiong, Z. Ying, and A. V. Vasilakos, "Privacy and security issues in deep learning: A survey," *IEEE Access*, vol. 9, pp. 4566–4593, 2021.
[121] S. Qiu, Q. Liu, S. Zhou, and C. Wu, "Review of artificial intelligence adversarial attack and defense technologies," *Appl. Sci.*, vol. 9, no. 5, p. 909, Mar. 2019.
[122] E. Raff, J. Sylvester, S. Forsyth, and M. McLean, "Barrage of random transforms for adversarially robust defense," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2019, pp. 6521–6530.
[123] F. Tramèr, A. Kurakin, N. Papernot, I. Goodfellow, D. Boneh, and P. McDaniel, "Ensemble adversarial training: Attacks and defenses," 2017, *arXiv:1705.07204*.
[124] N. Papernot, P. McDaniel, I. Goodfellow, S. Jha, Z. B. Celik, and A. Swami, "Practical black-box attacks against machine learning," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, Apr. 2017, pp. 506–519.
[125] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," 2014, *arXiv:1412.6572*.
[126] M. E. Shehaby and A. Matrawy, "Adversarial evasion attacks practicality in networks: Testing the impact of dynamic learning," 2023, *arXiv:2306.05494*.
[127] B. Darvish Rouani, M. Samragh, T. Javidi, and F. Koushanfar, "Safe machine learning and defeating adversarial attacks," *IEEE Secur. Privacy*, vol. 17, no. 2, pp. 31–38, Mar. 2019.
[128] Md. A. Ayub, W. A. Johnson, D. A. Talbert, and A. Siraj, "Model evasion attack on intrusion detection systems using adversarial machine learning," in *Proc. 54th Annu. Conf. Inf. Sci. Syst. (CISS)*, Mar. 2020, pp. 1–6.
[129] M. Girdhar, J. Hong, and J. Moore, "Cybersecurity of autonomous vehicles: A systematic literature review of adversarial attacks and defense models," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 417–437, 2023.
[130] A. Chernikova, A. Oprea, C. Nita-Rotaru, and B. Kim, "Are self-driving cars secure? Evasion attacks against deep neural networks for steering angle prediction," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2019, pp. 132–137.
[131] S.-M. Moosavi-Dezfooli, A. Fawzi, and P. Frossard, "DeepFool: A simple and accurate method to fool deep neural networks," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2016, pp. 2574–2582.
[132] Y. Li, X. Xu, J. Xiao, S. Li, and H. T. Shen, "Adaptive square attack: Fooling autonomous cars with adversarial traffic signs," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6337–6347, Apr. 2021.
[133] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards deep learning models resistant to adversarial attacks," 2017, *arXiv:1706.06083*.
[134] N. Papernot, P. McDaniel, and I. Goodfellow, "Transferability in machine learning: From phenomena to black-box attacks using adversarial samples," 2016, *arXiv:1605.07277*.
[135] C. Xie, M. Tan, B. Gong, J. Wang, A. L. Yuille, and Q. V. Le, "Adversarial examples improve image recognition," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2020, pp. 816–825.
[136] F. Liao, M. Liang, Y. Dong, T. Pang, X. Hu, and J. Zhu, "Defense against adversarial attacks using high-level representation guided denoiser," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, Jun. 2018, pp. 1778–1787.
[137] X. Xu, J. Zhang, Y. Li, Y. Wang, Y. Yang, and H. T. Shen, "Adversarial attack against urban scene segmentation for autonomous vehicles," *IEEE Trans. Ind. Informat.*, vol. 17, no. 6, pp. 4117–4126, Jun. 2021.
[138] Q. Wang, W. Guo, K. Zhang, A. G. Ororbia II, X. Xing, X. Liu, and C. L. Giles, "Learning adversary-resistant deep neural networks," 2016, *arXiv:1612.01401*.
[139] J. Fayyad, M. A. Jaradat, D. Gruyer, and H. Najjaran, "Deep learning sensor fusion for autonomous vehicle perception and localization: A review," *Sensors*, vol. 20, no. 15, p. 4220, Jul. 2020.
[140] R. Changalvala and H. Malik, "LiDAR data integrity verification for autonomous vehicle using 3D data hiding," in *Proc. IEEE Symp. Ser. Comput. Intell. (SSCI)*, Mali, Dec. 2019, pp. 1219–1225.
[141] N. Papernot, P. McDaniel, X. Wu, S. Jha, and A. Swami, "Distillation as a defense to adversarial perturbations against deep neural networks," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 582–597.
[142] C. Xiang, C. R. Qi, and B. Li, "Generating 3D adversarial point clouds," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2019, pp. 9128–9136.
[143] A. Kloukiniotis, A. Papandreou, A. Lalos, P. Kapsalas, D.-V. Nguyen, and K. Moustakas, "Countering adversarial attacks on autonomous vehicles using denoising techniques: A review," *IEEE Open J. Intell. Transp. Syst.*, vol. 3, pp. 61–80, 2022.
[144] B. Flowers, R. M. Buehrer, and W. C. Headley, "Evaluating adversarial evasion attacks in the context of wireless communications," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1102–1113, 2020.
[145] A. Kurakin, I. J. Goodfellow, and S. Bengio, "Adversarial examples in the physical world," in *Artificial Intelligence Safety and Security*. Boca Raton, FL, USA: CRC Press, 2018, pp. 99–112.
[146] J. H. Metzen, M. C. Kumar, T. Brox, and V. Fischer, "Universal adversarial perturbations against semantic image segmentation," in *Proc. IEEE Int. Conf. Comput. Vis. (ICCV)*, Oct. 2017, pp. 2774–2783.
[147] H. Liu, R. Ji, J. Li, B. Zhang, Y. Gao, Y. Wu, and F. Huang, "Universal adversarial perturbation via prior driven uncertainty approximation," in *Proc. IEEE/CVF Int. Conf. Comput. Vis. (ICCV)*, Oct. 2019, pp. 2941–2949.
[148] W. Brendel, J. Rauber, and M. Bethge, "Decision-based adversarial attacks: Reliable attacks against black-box machine learning models," 2017, *arXiv:1712.04248*.
[149] N. Carlini and D. Wagner, "Towards evaluating the robustness of neural networks," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2017, pp. 39–57.

[150] S. Gordon and R. Ford, "On the definition and classification of cybercrime," *J. Comput. Virol.*, vol. 2, no. 1, pp. 13–20, Aug. 2006.
[151] D. P. Mller, *Guide to Computing Fundamentals in Cyber-Physical Systems: Concepts, Design Methods, and Applications*. Cham, Switzerland: Springer, 2016.
[152] D. P. F. Möller, I. A. Jehle, and R. E. Haas, "Challenges for vehicular cybersecurity," in *Proc. IEEE Int. Conf. Electro/Inf. Technol. (EIT)*, May 2018, pp. 0428–0433.
[153] P. Goswami, K. Chitnis, B. Jadav, A. Kapania, and S. Sivasankaran, "Software framework for runtime application monitoring of fail-safe multi-processor ADAS SoCs," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2017, pp. 39–42.
[154] M. A. Gosavi, B. B. Rhoades, and J. M. Conrad, "Application of functional safety in autonomous vehicles using ISO 26262 standard: A survey," in *Proc. SoutheastCon*, Apr. 2018, pp. 1–6.
[155] L. Verhoeff, D. J. Verburg, H. A. Lupker, and L. J. J. Kusters, "VEHIL: A full-scale test methodology for intelligent transport systems, vehicles and subsystems," in *Proc. IEEE Intell. Vehicles Symp.*, Feb. 2000, pp. 369–375.
[156] A. L. Medina, S. E. Lee, W. W. Wierwille, and R. J. Hanowski, "Relationship between infrastructure, driver error, and critical incidents," in *Proc. Hum. Factors Ergonom. Soc. Annu. Meeting*, vol. 48. Los Angeles, CA, USA: Sage, 2004, pp. 2075–2079.
[157] N. A. Stanton and P. M. Salmon, "Human error taxonomies applied to driving: A generic driver error taxonomy and its implications for intelligent transport systems," *Saf. Sci.*, vol. 47, no. 2, pp. 227–237, Feb. 2009.
[158] M. R. Endsley, "Situation awareness: Operationally necessary and scientifically grounded," *Cognition, Technol. Work*, vol. 17, no. 2, pp. 163–167, May 2015.
[159] T. W. Victor, E. Tivesten, P. Gustavsson, J. Johansson, F. Sangberg, and M. L. Aust, "Automation expectation mismatch: Incorrect prediction despite eyes on threat and hands on wheel," *Hum. Factors, J. Hum. Factors Ergonom. Soc.*, vol. 60, no. 8, pp. 1095–1116, Dec. 2018.
[160] V. Hassija, V. Chamola, V. Gupta, S. Jain, and N. Guizani, "A survey on supply chain security: Application areas, security threats, and solution architectures," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6222–6246, Apr. 2021.
[161] S. Sahoo, S. Kumar, U. Sivarajah, W. M. Lim, J. C. Westland, and A. Kumar, "Blockchain for sustainable supply chain management: Trends and ways forward," *Electron. Commerce Res.*, vol. 2022, pp. 1–56, May 2022.
[162] M. Murtaza, C.-T. Cheng, M. Fard, and J. Zeleznikow, "The importance of transparency in naming conventions, designs, and operations of safety features: From modern ADAS to fully autonomous driving functions," *AI Soc.*, vol. 38, no. 2, pp. 983–993, Apr. 2023.

ARYAN ALPESH MEHTA is currently pursuing the B.Tech. degree in computer science and engineering with Nirma University, Ahmedabad, India. His research interests include machine learning, deep learning, security, and computer vision. With a passion for innovation, he aims to contribute to the advancement of these fields through insightful research and practical applications.

ALI ASGAR PADARIA is currently pursuing the B.Tech. degree in computer science and engineering with Nirma University. His research interests include deep learning, blockchain, NLP, computer vision, and security. With plans to pursue the master's degree in computer science, he is committed to driving innovation in these fields through insightful research and practical and applications.

DWIJ JAYESH BAVISI is currently pursuing the B.Tech. degree in computer science and engineering with the Institute of Technology, Nirma University, India. With a keen interest in the fields of deep learning and security, he is passionate about exploring innovative solutions to challenges in these fields. As an Aspiring Researcher, he aims to contribute meaningfully to these fields through insightful research and practical applications.

VIJAY UKANI received the Ph.D. degree in multimedia transmission in wireless sensor networks from Nirma University. He is currently an Associate Professor with the Computer Science and Engineering Department, Nirma University, Ahmedabad, India. His research interests include wireless sensor networks, the Internet of Things, machine learning, and network protocol design. He was a recipient of a Research Grant from GUJCOST, SAC, ISRO, and the Science and Engineering Research Board (SERB), and worked on a consultancy project with Johnson Control Hitachi Ltd.

PRIYANK THAKKAR received the Ph.D. degree from Nirma University. He is currently an Associate Professor with the Computer Science and Engineering Department, Institute of Technology, Nirma University, Ahmedabad, India. He is also coordinating the Centre of Excellence in Data Science activities at the CSE Department, Institute of Technology, Nirma University. He has more than 22 years of teaching experience. His research interests include data and web mining, machine learning, soft computing, deep learning, and their applications in various domains.

REBEKAH GEDDAM received the B.Tech. degree in computer engineering from JNTU, Hyderabad, the M.Tech. degree in computer engineering from KU, Karnataka, and the Ph.D. degree in computer engineering from the GL School of Doctoral Research Innovations. She is currently an Assistant Professor with the Computer Science and Engineering Department, Nirma University, Ahmedabad, India. She has academic experience of more than 14 years. She has completed two projects on cognitive computing with Gujcost, India. Her research profile includes 12 Scopus publications in the area of digital decision for healthcare such for diseases, like Parkinson detection, epilepsy, autism, and attention deficient hyper disorder (ADHD) using machine learning algorithms. Her research interests include embedded systems, the Internet of Things (IoT), augmented reality, brain–computer interface, and machine learning.

KETAN KOTECHA is currently an Administrator and a Teacher with the Symbiosis Centre for Applied Artificial Intelligence, Symbiosis International (Deemed University), Pune, India. He has expertise and experience in cutting-edge research and projects in AI and deep learning for the last 25 years. He has published more than 200 articles in several excellent peer-reviewed journals on various topics ranging from cutting-edge AI, education policies, teaching-learning practices, and AI. He has published three patents and delivered keynote speeches at various national and international forums, including the Machine Intelligence Laboratory, USA, IIT Bombay, under the World Bank Project; and the International Indian Science Festival organized by the Department of Science and Technology, Government of India. His research interests include artificial intelligence, computer algorithms, machine learning, and deep learning. He was a recipient of the two SPARC projects worth INR 166 lakhs from the MHRD Government of India in AI in collaboration with Arizona State University, USA, and The University of Queensland, Australia. He was also a recipient of numerous prestigious awards, such as the Erasmus+ Faculty Mobility Grant to Poland, the DUO-India Professors Fellowship for research in responsible AI in collaboration with Brunel University, U.K., the LEAP Grant at Cambridge University, U.K., the UKIERI Grant with Aston University, U.K., and a Grant from the Royal Academy of Engineering, U.K., under Newton Bhabha Fund. He is an Associate Editor of IEEE Access.

AJITH ABRAHAM (Senior Member, IEEE) received the B.Tech. degree in electrical and electronic engineering from the University of Calicut, in 1990, the M.Sc. degree from Nanyang Technological University, Singapore, in 1998, and the Ph.D. degree in computer science from Monash University, Melbourne, Australia, in 2001. He is currently the Pro-Vice Chancellor with Bennett University, New Delhi, responsible for the University's Research and International Academic Affairs. Prior to this, he was the Dean of the Faculty of Computing and Mathematical Sciences, FLAME University, Pune, and the Founding Director of Machine Intelligence Research Labs (MIR Labs), USA, a not-for-profit scientific network for innovation and research excellence connecting industry and academia. He also held two International University Professorial appointments: a Professor of artificial intelligence with Innopolis University, Russia, and the Yayasan Tun Ismail Mohamed Ali Professorial Chair of artificial intelligence with UCSI, Malaysia. He works in a multidisciplinary environment. He has authored/coauthored more than 1,400 research publications out of which there are more than 100 books covering various aspects of computer science. One of his books was translated into Japanese and a few other articles were translated into Russian and Chinese. He has more than 52,000 academic citations (H-index of more than 107 as Per Google Scholar). He has given more than 150 plenary lectures and conference tutorials (in more than 20 countries). He was the Chair of the IEEE Systems Man and Cybernetics Society Technical Committee on Soft Computing (which has over more than 200 members), from 2008 to 2021, and served as a Distinguished Lecturer for the IEEE Computer Society representing Europe, from 2011 to 2013. He was the Editor-in-Chief of *Engineering Applications of Artificial Intelligence* (EAAI), from 2016 to 2021, and serves/served on the editorial board for over 15 international journals indexed by Thomson ISI.