A Review of Cybersecurity Challenges and Solutions for Autonomous Vehicles

Lasseni Coulibaly[1], Damien Hanyurwimfura[2], Evariste Twahirwa[3], Abubakar Diwani[4]
African Center of Excellence in Internet of Things, University of Rwanda, Kigali, Rwanda[1, 2, 3]
Department of Computer Science and IT, The State University of Zanzibar, Zanzibar, Tanzania[4]

***Abstract*—With the continuously increasing demand for new technologies, many concepts have emerged in recent decades and the Internet of Things is one of the most popular. IoT is revolutionizing several aspects of human life with a large range of applications including the transportation sector. Based on IoT technologies and Artificial Intelligence, new-generation vehicles are being developed with autonomous or self-driving capabilities to handle transportation in future smart cities. Regarding human-based errors such as accidents, traffic congestion, and disruptions, autonomous vehicles are presented as an alternative solution to increase traffic safety, efficiency, and mobility. However, by transferring from a human-based to a computer-based driving style, the transportation area is inheriting existing cyber-security challenges. Due to their connectivity and data-driven decision-making, the security of autonomous vehicles is a high-level concern since it involves human safety in addition to economic losses. In this paper, a comprehensive review is conducted to discuss the security threats and existing solutions for autonomous vehicles. In addition to that, the open security challenges are discussed for further investigations toward trusted and widespread deployment of autonomous vehicles.**

Keywords*—Internet of Things; smart transportation; autonomous vehicles; cybersecurity

I. Introduction

Ashton, in 1999, introduced the idea of connecting Radio Frequency Identification (RFID) Tags to the Internet which enabled the interconnection of conventional objects to handle autonomous tasks, and therefore, led to the new concept of the Internet of Things (IoT) [1]. With the help of IoT technologies, the transportation area is having a significant evolution from conventional mechanical vehicles to next-generation smart vehicles capable of collecting environmental data, process and communicating them, to make intelligent driving decisions without human assistance [2], [3]. Due to this new orientation toward intelligent transportation systems (ITS), the transport sector has become attractive for various interdisciplinary researchers and industries to work in the industrialization and deployment processes of autonomous vehicles (AV).

An AV is a computer on wheels that is equipped with a multitude of software and electronic components (such as sensors, processing units, and transmission modules), and capable of performing driving tasks on its own. In 2021, the Society of Automotive Engineers (SAE) provided an official updated reference which describes the evolution of vehicles in five automation levels, known as Level 1: driver-assistance; Level 2: partial-automation; Level 3: conditional-automation; Level 4: high-automation; and Level 5: full-automation [4]. In level 1, the human driver has full control over the vehicle's driving mode, but some computing systems are embedded to assist the driver in monitoring the environment (e.g. measuring of distance between vehicles to produce collision alerts, over-speeding alerts, …). In level 2, the human driver has partial control over the vehicle's driving mode, where some vehicular functions are controlled by automated systems (e.g. executing steering and acceleration functions). In level 3, most of the vehicle's driving functions are automated to enable a self-driving mode, but the human driver must necessarily respond to feature requests and take driving control in some situations. In level 4, the vehicle is highly automated and capable of handling driving functions without requiring much intervention from the human driver. In level 5, the human driver has no control over the vehicle's driving mode, and all the driving functions are performed by computing systems in all situations.

The main objective of introducing AVs is to avoid human-based errors that are mostly the cause of traffic issues like accidents, and therefore, to increase traffic safety, mobility, and efficiency [5], [6]. However, the transfer of the driving mode from human hands to computer systems also exposes vehicles to existing cybersecurity challenges, where attackers can gain access to AVs and control them for malicious ends making it urgent to consider their security at a high level for trustworthy developments and deployments. In this paper, a comprehensive review is conducted to give a state of the art of vehicular security, which provides the following key contributions:

- First, it describes the architecture of AVs, highlighting the role of different components, their security and privacy requirements, and the threats and vulnerabilities that can affect their normal operations.
- Second, it explores the literature to identify the reported attack methods against AV components as well as existing solutions that can be used to mitigate attacks.
- Third, it discusses the existing countermeasures to highlight their advantages and limitations, points out open challenges then proposes research directions for further investigations.

In the rest of this paper, Section II provides an overview of the architecture of AVs. The literature review is reported in Section III. Section IV discusses the existing security methods

for AVs. Section V proposes new research directions that can be considered to provide efficient security methods for AVs. The paper is concluded in Section VI.

II. Architecture of Autonomous Vehicle: Overview

The internal components of AVs can be classified into three main layers including the input layer, processing and control layer, and communication layer as depicted in Fig. 1. The input components collect data from the environment which are used by processing components to make decisions for controlling the vehicular functions. The communication components serve as interfaces allowing the interaction between different internal components and also between the vehicle and external entities such as other vehicles, personal devices, and infrastructures.

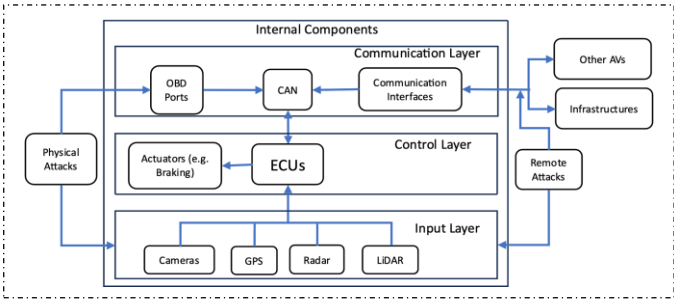

Fig. 1. Components of autonomous vehicles.

A. The Input Layer

AVs are equipped with a large number of sensors to collect specific data from the environment serving as input for control units [7]. Some commonly used sensors are Cameras, "Light Detection and Ranging (LiDAR), Global Positioning System (GPS), Radio Detection and Ranging (Radar), Ultrasonic", etc.

LiDAR sensors are used to detect surrounding objects by sending light waves and calculating the distance based on reflected signals [8]. In the same logic, Radar sensors measure the distance and speed of objects by sending electromagnetic waves in the radio domain and sense the reflected signals. Used for obstacle detection, the Radar works better in bad weather compared to the LiDAR and both are most used for long-range detection whereas ultrasonic sensors are preferable for short-range measurements based on sound waves. No matter the performance of obstacle detection sensors, they cannot identify the colour of a traffic light. Therefore, image sensors (cameras) are used to provide vision capability to the AV and identify different entities in the environment. GPS sensors operate by receiving radio signals from three or more satellites to determine the geographical location [9]. Therefore, GPS sensors are necessary for AVs to localize them and find routes between different locations. These sensors are useful in many applications and serve in AVs to observe the environment and make intelligent decisions to control the vehicle for safe driving and efficient navigation as illustrated in Fig. 2.

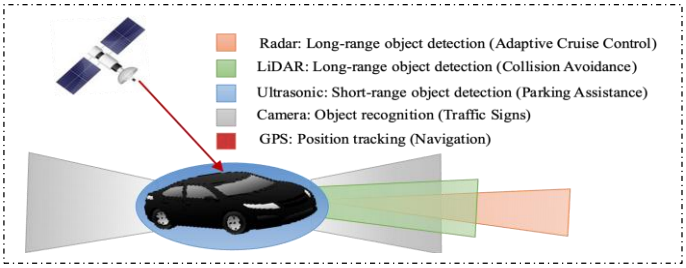

Fig. 2. Use of sensors in AVs.

B. The Control Layer

Electronic Control Units (ECU) represent the brain of AVs. ECUs are embedded systems that receive input signals from other components mainly sensors, process them, and decide the behaviour of vehicular functions [10]. As illustrated in Fig. 3, several types of ECU are used in AVs to perform specific tasks ensuring that vehicular functionalities are well-controlled and operational [11]. These include engine control, speed control, body control, tire-pressure monitoring, transmission modules also called telematics ECUs, and other internal measurement systems [12]. The ECUs can work together or independently based on the required action to take. For example, after detecting a pedestrian or other obstacles, the braking and speed control systems can collaborate to avoid collisions.

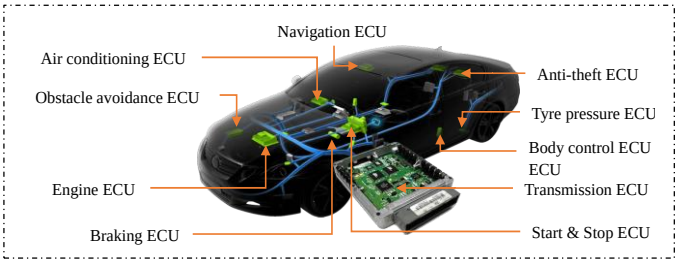

Fig. 3. Embedded ECUs in AV.

C. The Communication Layer

The internal components of AVs such as sensors, ECUs, and actuators, are interconnected through the in-vehicle network also known as "Controller Area Network (CAN)", where they exchange data to perform tasks together [7]. Short-range technologies are mostly privileged for in-vehicle communications to establish wireless connections between sensors and ECUs to reduce complex wiring. Also, external devices can be physically connected to the vehicle through onboard diagnostic (OBD) ports to access the CAN data for diagnostics on components or firmware updates [13]. The OBD ports can be found in any modern vehicle including existing AVs and are commonly used to access and update embedded software in the vehicle's control units.

For external communications, multiple AVs can form a network following the paradigm of vehicular ad-hoc networks (VANET) [14], where each AV can communicate with others and with surrounding communications infrastructures such as roadside units (RSU) as illustrated in Fig. 4.

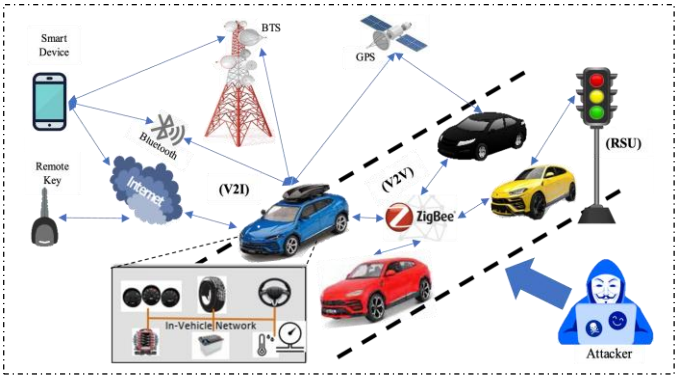

Fig. 4. Network of autonomous vehicles.

Typically, VANETs achieve four main types of communication listed as follows:

- Vehicle-to-Vehicle (V2V) communication: This allows vehicles to share traffic safety information and their status information like speed, position, and direction, to maintain good and safe driving conditions [15].
- Vehicle-to-Infrastructure (V2I) communication: This allows vehicles to interact with RSUs (V2R) for traffic safety information such as accidents, congestion alerts, and various warning messages. In this phase, vehicles can also communicate with other infrastructures such as satellite and Cellular for receiving their navigation-related data and other remote communications [16].
- RSU to RSU (R2R) communication: This allows nearby RSUs to interact and share network status information.
- Vehicle to Everything (V2X) communication: The V2X represents all the vehicular interactions with a large range of communication entities, such as smart devices, smart homes, pedestrians, clouds, computers, cellular networks, etc. [17]. This also includes V2V and V2I.

The vehicular interactions use different types of wireless communications protocols including short-range technologies (e.g. ZigBee, Bluetooth, and ultra-wideband (UWB)); medium-range technologies (e.g. Wi-Fi and "dedicated short-range communication (DSRC)"); and long-range technologies (e.g. Cellular Communications) [18]. The DSRC also known as "Wireless Access in Vehicular Environments (WAVE)" is adopted for V2V and V2R communications whereas cellular technologies are preferable for other V2I communications [19]. In addition to that, the AV uses the WIFI interface to interact with cloud and mobile applications for remote control [20].

D. Security and Privacy Requirements for AVs

The input, processing, and communication layers work together to create a well-functioning driving capability for AVs and their communication environments [21], but compromising any layer can destabilize the vehicle leading to harmful damage with direct consequences on human safety and economy [22]. Therefore, the security of AVs is a high priority and should cover all their internal and external interaction aspects. Some common security requirements are given as follows:

1) Availability: The internal components of AVs must remain accessible for collecting, processing, or transmitting data to ensure continuous operability. Also, the vehicular networks must stay available for receiving and sending safety-related information even during critical conditions such as high mobility. Therefore, AVs must be secured against attacks that can result in availability issues.

2) Authentication: This is a primary security measure where each node must be able to identify the source node that has sent a given message before going through further interactions. Therefore, vehicular networks must be secured against intrusions of malicious nodes to prevent attacks. For the sake of real-time requirements, rapid authentication methods are preferable to minimize communication delays.

3) Confidentiality and integrity: The exchanged messages between different nodes must only be accessible by the authorized members and each node must be able to verify that the received message was not modified or altered during transmission. The cryptographic algorithms are commonly used to achieve confidentiality and integrity requirements, but again, rapid encryption methods are necessary for vehicular applications to avoid added communication delay.

4) Privacy and anonymity: As a large amount of data is collected by AVs, processed, or transmitted over the network, the private information of users must not be exposed to unauthorized parties. This requires strict protection of identification information against potential privacy leakages.

5) Monitoring: In presence of multiple attacks, vehicular networks must be controlled to identify malicious nodes and actively remove them from vehicular communications through an appropriate authority. Therefore, real-time monitoring methods are required to efficiently prevent potential attacks.

E. Security and Privacy Threats Against AVs

Depending on the attack opportunity, attackers can reach AV components using remote interfaces or through physical access [23]. In the remote attack, any component capable of interacting with the surroundings can be vulnerable where an attacker can perform different types of attack aiming to steal information, to control a vehicular function, or to interrupt an operation [9]. In the physical access attack, the attacker can inject malicious codes into the vehicle's system using the onboard ports, physically damage a component, or insert an additional fake component to transmit wrong data into the vehicle's system [24], [25]. Some common attack vectors on AV components and communications are given as follows:

1) Sensor spoofing: The attacker manipulates and generates fake signals stronger enough to force sensors to detect and transmit wrong data [26]. This attack aims to control the decision-making of a targeted ECU which will receive the collected data and make wrong decisions. For example, if the GPS sensor detects stronger signals from the attacker, the navigation ECU of the vehicle can decide to

follow a different trajectory which is intended by the attacker as illustrated in Fig. 5.

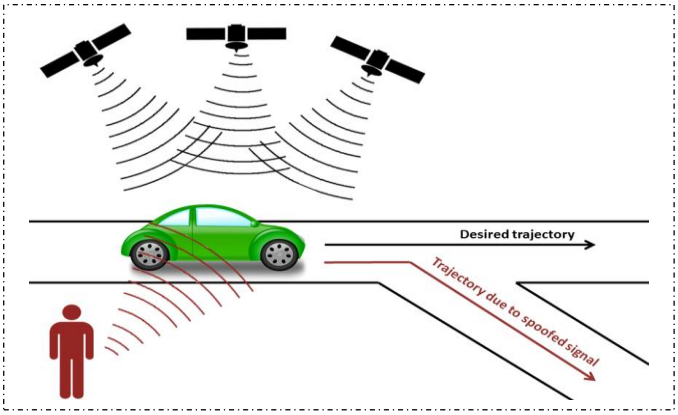

Fig. 5. Illustration of AV's GPS spoofing attacks [27].

2) Sensor jamming: It consists of blocking the sensor's perception by sending noise signals to interfere with normal signals [28]. This attack can interrupt operations of an ECU that depends on data from the targeted sensor. For example, if obstacle detection sensors are not able to collect data, the speed control ECU can decide emergency braking which can lead to accidents and traffic congestion as illustrated in Fig. 6.

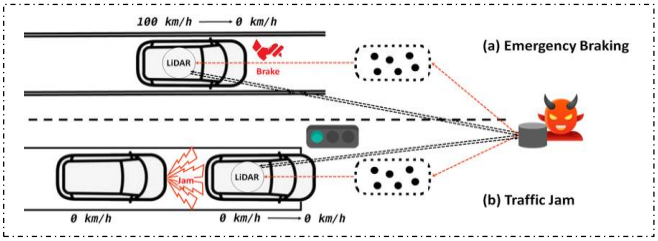

Fig. 6. Illustration of AV's sensor jamming attacks [29].

3) Blinding and adversarial images: The attacker can use strong light beams to blind or confuse the perception of the targeted camera [22]. Adversarial images generally target the machine learning models that are used for image recognition, where attackers manipulate images with adversarial samples that appear to be normal to human eyes but can cause huge confusion to the model producing incorrect outputs [30]. For example, if the attacker manipulates a stop road sign, the vehicle can misinterpret the captured image as a speed limitation and therefore speed up instead of slowing down, which can lead to harmful accidents as illustrated in Fig. 7.

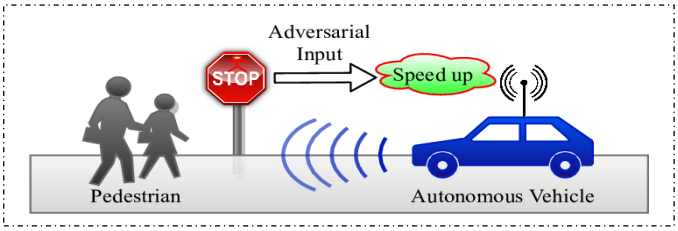

Fig. 7. Illustration of AV's camera attacks [31].

4) Malware and message injection: The attacker runs malicious code in the AV's system using the OBD ports, by flashing into its memory or through the process of firmware updates [32]. Also, the attacker can inject fake information through vehicular communications and force vehicles to take action on wrong data performing the intended activities [33]. These attacks aim to execute a specific task in a targeted ECU or interrupt its normal functionality as illustrated in Fig. 8.

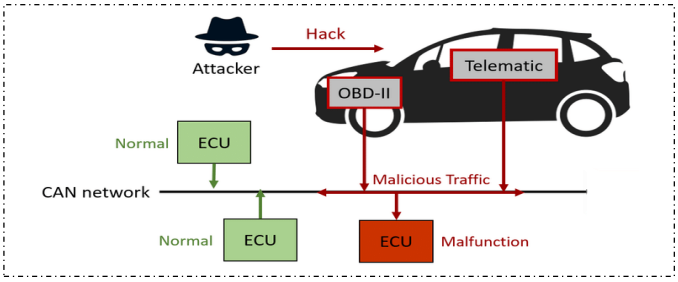

Fig. 8. CAN network attacks [34].

5) OBD Attack: Historically, dedicated handheld tools are used to scan information through OBD ports but most modern OBD devices such as Telia Sense [35] and AutoPi [36], allow connection with personal computers and smartphones for self-diagnostics purposes. As shown in Fig. 9, an attacker can use a compromised OBD device to access the vehicle's system which can allow executing a malicious program in targeted ECUs to control the vehicular functions.

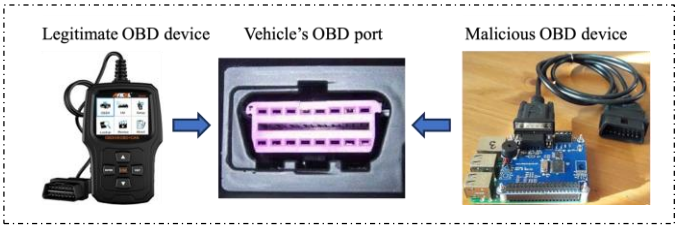

Fig. 9. OBD attacks.

6) DoS (Denial of Service) and DDoS (Distributed DoS): This attack aims to create unavailability of a service. It can target protocols and networks by sending excessive bad traffic packets to disrupt communications [37]. This attack can isolate a targeted vehicle from communicating with others or block the entire vehicular network leading to unwanted traffic conditions. The DoS and DDoS attacks can target AVs in both the internal and external communication aspects.

7) Eavesdropping: The attacker can intercept the exchanged information between different entities and secretly analyse or modify them to serve a malicious goal [37], [38]. The Man in The Middle attack is a typical example where the attacker modifies data between different entities and lets them believe that they are communicating with each other. This attack aims to access private information or to gain control over the vehicle's behaviour.

8) Message replay: The attacker can retransmit the past traffic status information in the vehicular network to mislead vehicles into believing that the action is currently happening

[28]. This attack can create traffic disorder and allow attackers to attempt their goal causing accidents or congestions.

9) Black hole: The attacker can manipulate the network informing other nodes that the malicious node has the shortest path to their destination [39]. After receiving packets, the malicious node will drop all of them to cause data loss blocking other nodes from receiving safety information. This attack can disrupt vehicular communications with the illusion of a normal driving environment.

10) Sybil: This attack consists of creating multiple fake identities in the network known as Sybil nodes which are used to transmit fake information to other nodes [28], and therefore, provoke the illusion of a busy network.

11) Physical damage: The attacker can target a specific component in the vehicle and destroy it [21]. This attack aims to interrupt the normal operations of the targeted component.

III. Literature Review

With the rapid development of connected and autonomous vehicles, several studies and hypothetical demonstrations in the literature have raised security weaknesses. In recent studies reported in [40] and [41], connected vehicles were targeted by more than 1300 reported cyberattacks from 2010 to 2023 and the analysis has shown that the attack frequency increased by 225% from 2018 to 2021, where 85% of attacks used remote interfaces and 54.1% were done by malicious actors leading to system control, vehicle theft, and unauthorized access to private data of users. This section exposes attack methods against AVs and the proposed countermeasures.

A. Sensors: Attacks and Defences

In general, sensors simply collect data and transmit them for further processing without authentication [21]. This fact makes sensors vulnerable to spoofing and jamming attacks.

1) LiDAR Sensors

Attacks: Authors in study [42] reported a successful jamming attack on a LiDAR sensor, the "ibeo LUX3 model", which consisted of sending higher intensity light to the LiDAR and blocking the acquisition of legitimate reflected light waves. Two variations of attack against LiDAR sensors were also demonstrated in study [43], where authors first showed the possibility of manipulating different LiDAR sensors of the same AV to perceive objects farther or closer than their real locations, by recording signals sent from one LiDAR sensor and then relaying those signals to the other LiDAR sensor. The second attack was to send fake signals to the targeted LiDAR sensor and make the vehicle believe that it was approaching a large obstacle. Authors in study [44] also performed this second attack on a LiDAR sensor, the "VLP-16 model", and explained that most LiDAR sensors are vulnerable to this attack especially those with large receiving angles.

Defences: Authors in study [45] proposed a new LiDAR scheme to detect jamming attacks based on random modulation of light waves. This modulation creates four polarization states (horizontal, vertical, diagonal, and anti-diagonal) for the photon and the jamming attack is detected based on a comparison of distances measured from the states. However, the authors acknowledged that their proposed scheme cannot filter jamming signals out of legitimate signals. Authors in study [46] proposed a method to detect fake input signals from LiDAR sensors by using the previous data frames to build a momentum model. However, building this model would require high computational power and time which is not adequate for real-time and resource-constraint applications such as AVs. The use of multiple LiDAR sensors was proposed in [44], to have overlapping views of the vehicle's surroundings or to reduce the signal-receiving angle for each sensor. This technique can reduce attack chances by preventing spoofing attacks on all the sensors at the same time, but requires a high number of LiDAR devices to cover all the vehicle's surroundings and therefore increases the cost. Authors in study [47] also proposed embedding identification data onto LiDAR's light waves by modulating them together, which allows sensor nodes to authenticate the received signals and therefore prevent LiDAR spoofing attacks. An experiment was conducted in [48], and the authors concluded that it becomes more difficult to succeed in LiDAR spoofing attacks when object detection is based on machine learning (ML) models. Authors in study [49], also confirmed the effectiveness of using ML models to detect LiDAR spoofing attacks. A LiDAR spoofing mitigation algorithm was proposed in [50] to detect adversarial objects and non-existing obstacle attacks where authors claimed correct attack detection based on simulation results.

2) Radar sensors

Attacks: A spoofing attack on a Radar device, the "Ettus Research USRP N210 model", was experimented with [51], by recording the broadcasted Radar signals to modify their phases and re-broadcast them to Radar sensors. This caused incorrect distance calculations and resulted in perceiving objects at a 15-meter distance while the real distance was 121 meters. Authors in study [52] demonstrated that it was possible to manipulate an object's velocity together with distance using spoofing attacks on FMCW Radar sensors, by designing an adversarial Radar to simulate two scenarios of attack provoking emergency braking and acceleration in a victim vehicle. Authors in [53] performed a similar attack on an FMCW Radar using a semi-passive modulated transponder and reported that it is possible to confuse a radar perception with ghost targets at different distances and velocities by simply changing the modulation frequency of the transponder without the need to use complex techniques. Also, authors in [54] demonstrated a jamming attack on Radar sensors for manned and unmanned aerial vehicles (UAV) where the attacker can modify the amplitude and the frequency of the recorded signals and then re-broadcast them to the Radar sensor to cause failure in object detection.

Defences: To mitigate spoofing and jamming attacks, a "physical challenge-response authentication (PyCRA)" was proposed in study [55], which sends random signals called challenging signals in the Radar sensing environment and detects fake signals based on a noise threshold. The PyCRA shuts down the sensing signals at random times, which was criticized to potentially affect AV safety-critical components by the authors in [56], who proposed an alternative method

called "Spacio-Temporal Challenge-Response (STCR)" and claimed to achieve better performance by transmitting challenging signals in random directions together with sensing signals instead of shutting them down. Once a malicious signal is detected, the reflected challenging signals are used to identify the attack directions and exclude them. Authors in [57] experimented with an unsupervised deep-learning method on Radar system data to detect manipulation attacks and found an accuracy of 88% detection rate. They defended that their technique could be used in AV's Radar systems to mitigate spoofing attacks, by learning the correlation between categorical and numerical features from Radar signals.

3) GPS Sensors

Attacks: The GPS spoofing attacks were analysed in study [58], where authors explained how it can be easy for an attacker to carry out GPS spoofing attacks by using hardware capable of generating stronger GPS signals, broadcasting them to GPS receivers in a chosen environment to force them to switch from legitimate satellite signals and manipulate their location calculations. In 2013, a man was arrested in New Jersey for using a GPS device that was interfering with GPS ground-based receivers of Newark's Liberty Airport [59]. This device was able to block surrounding GPS receivers from receiving legitimate GPS signals and he claimed using it in the company truck simply to hide from his employer. In [60], authors demonstrated a successful GPS attack using a low-cost device assembled from conventional components and were able to manipulate the navigation data of 38 real cars out of 40 participants to follow a wrong predetermined destination without being noticed. The authors discussed that this attack may not succeed when the driver is familiar with the location but it represents a high risk for self-driving vehicles. Authors in study [61] also demonstrated a new approach to GPS attacks that can succeed in manipulating navigation routes on vehicles where security mechanisms are used such as internal navigation system (INS). The technique consists of exploiting existing navigation data between the vehicle's start and destination points to identify similar routes with the original trajectory using an algorithm and then forcing the vehicle to follow the most similar trajectory. The authors claim that this attack can be successfully executed due to the negligible inconsistencies between the original and the spoofed routes. Also, authors in study [62] proposed a spoofing generator that cancels all legitimate GPS signals and allows surrounding GPS receivers to collect the attacker's generated signals. The authors defended that their spoofing generator can cover all open-sky satellites making this attack difficult to detect based on a comparison of signal consistency from different GPS receivers.

Defences: To prevent GPS attacks, the use of multiple antennas was proposed in study [63], to receive GPS signals and measure their phase differences to detect spoofing attacks but this technique would be inefficient under attack methods as presented in study [62]. Authors in study [64], proposed the use of coding in GPS systems to reduce jamming attacks where GPS signals are encoded and modulated by the satellite before transmitting to receivers that will then demodulate and decode to recover the original GPS signals. However, this method requires changes in GPS satellites which is very difficult and also, the authors acknowledged that their method is less effective when the jamming signals are too strong than the legitimate ones. In many applications, a technique known as "Receiver autonomous integrity monitoring (RAIM)" is used in which, the observed GPS signals are compared with the expected signals to determine the integrity of the received signals [65]. The RAIM uses a pseudo-ranging measurement to produce several GPS positions based on redundant signals [66]. However, the Advanced RAIM (ARAIM) used as an extension for other navigation systems beyond GPS, was criticised in study [67], for having availability issues when one or more satellites cannot be reached. Later, authors in [68] proposed a solution to improve the availability of ARAIM up to 98.75%. Authors in study [69], proposed integrating transmission signatures into GPS satellites which will allow GPS receivers to authenticate the received signals. This method can easily help to detect spoofing attacks but it would involve higher costs for changes in satellites. A rotation-based technique was proposed in study [70], for GPS receivers that can help to determine the angle of arrival of GPS signals from different satellites and compare them to detect spoofing attacks. Authors in study [71], proposed a GPS spoofing detection technique for vehicular GPS receivers based on the Doppler Shift associated with them. In their approach, authors intentionally perturbed the vehicle's velocity and observed the changes in Doppler Shift value if they were consistent with velocity variations or not. Due to the unpredictability of these variations, spoofing signals cannot follow the changes. A GPS spoofing mitigation technique was proposed in study [72], based on the Isolation Forest that consists of detecting the attack and isolating the compromised GPS receiver before correcting it using the location data of roadside units. The authors claimed to achieve good results but this method would require the use of multiple GPS receivers to avoid service interruption. Authors in study [73] and study [74], demonstrated through simulation that machine learning and deep learning algorithms can achieve detection of both GPS spoofing and jamming attacks with high accuracy.

4) Image Sensors (Cameras)

Attacks: A blinding attack was experimented in study [43], on a car's camera (MobilEye C2-270) where authors projected different light beams on it. First, an LED matrix of 940nm 5*5 and an LED spot of 850nm were used and able to blind the camera from perceiving images which took 5 seconds to recover later. A 650nm laser was then used on it to achieve the same results but the camera never recovered again. Authors in [75] conducted similar experiments to permanently blind a camera and concluded that both LED and Laser beams can blind cameras with enough intensity but infrared beams can make exceptions due to their narrow frequency band. Attackers can also use other methods such as manipulating images to cause incorrect predictions of road signs by ML-based algorithms as described in studies [76], [77], [78], [79]. In 2017, Google researchers created stickers with patterns and attached them to some important road objects such as speed limitations and stop signs [80]. The authors claimed that the stickers were able to provoke incorrect predictions in the used algorithms. Authors in study [81], experimented with similar attacks by decorating stop signs with many black-and-white stickers and found a failure of 100% of the algorithm to

recognize the stop signs with a fixed camera and 84.8% with a moving camera on a vehicle. Authors in study [82], experimented with a blinding attack using electromagnetic waves to interfere with cameras and were able to cause incorrect observation of stop signs. This attack is hard to detect because it does not require a physical modification. A similar experiment was conducted in study [83], using invisible infrared lights which affected the captured image's pixels with a magenta colour in ambient light. The authors succeeded in perturbating cameras on the Tesla Model 3 using off-the-shelf IR light sources and confirmed the effectiveness of their attack in various settings.

Defences: To mitigate camera blinding attacks, the authors in [43] proposed two solutions. The first consists of using multiple cameras in the AV to capture redundant images and avoid single-camera failure. This strategy makes it difficult to attack all cameras simultaneously due to the limited beam widths of LED and Laser spots but can increase the cost according to the number of cameras. The second solution is to integrate a light filter into cameras that can cut near-infrared lights. This strategy can be implemented at a low cost but lacks experiments to confirm its effectiveness. The authors in [83], proposed to implement infrared light filter-based software on cameras as mitigation to their attack. Authors in [84], proposed the use of ML algorithms to predict images and compare them with the captured images and claimed that this technique can help to detect blinding attacks and take the required actions before any damage. The use of machine learning models as a solution against adversarial image attacks has also been discussed in the literature. In these models, three major aspects are considered including pre-processing input images as detailed in [85], [86], [87], [88], training with adversarial image samples as proposed in [89], [90], [91], and detecting adversarial inputs using run-time information as described in study [92]. These models can be integrated into ECUs which receive their input images from cameras for the AV's vision.

B. Control and Processing Units: Attacks and Defences

The internal components of the AV can exchange information through the CAN network, where ECUs receive their input data from the different sensors, communication interfaces, and/or other ECUs [93], [94], [95]. Therefore, any failure from the input source can directly influence the ECU to give incorrect output. Also, attackers can observe the CAN messages and inject malicious data through OBD ports or telematic interfaces to target a specific ECU.

1) ECU Attacks: Authors in study [96] experimented with an attack by connecting a laptop to a vehicle's OBD port to access the CAN network and run a custom code named CarShark in targeted ECUs, which was able to compromise their initial functions. They warned that no security measures were applied during vehicle software updates through the OBD port. Authors in study [97] have also shown that an attacker can develop a malicious program and let a vehicle owner download it as a self-diagnostic application which will allow the control of ECUs through OBD connexions. Authors in study [98], were able to access a vehicle's ECUs through Bluetooth and long-range connections allowing them to analyse the firmware and execute their codes. The authors reported that an attacker can use the same process to remotely inject malicious codes in a targeted ECU and compromise its functions. In Black Hat 2015, some researchers demonstrated a successful attack on a Jeep Cherokee ECUs using remote interfaces [99]. The authors were able to control the vehicle's braking, steering, and acceleration systems. Authors in study [100], focused a study on discovering weaknesses in the deployed access control and communication mechanisms on Tesla vehicles, the "P85 and P75 models", and demonstrated how ECUs can be remotely controlled by sending malicious packets to the CAN via wireless technologies. Authors experimented with their attack, to remotely control the steering ECU of the Tesla Model S 75 [101]. Authors in study [102], demonstrated CAN vulnerabilities using experimental fuzzy-testing and reported that an attacker can easily access the CAN network and control a targeted ECU of the vehicle with necessary protocol analysis tools.

2) ECU Defences: Many mitigation solutions have been proposed in the literature to prevent ECU attacks. Authors in [103], proposed an attack detection technique which calculates entropy during normal and abnormal CAN communications to detect suspicious activities. The authors in study [104], proposed a technique to monitor all messages in the CAN network where each ECU will use a flag to indicate a message transmission time, and therefore, detect unauthorized messages based on the time threshold. This method was criticized in study [105], because it requires modifications in every ECU in the vehicle, then proposed to use identity checking of ECUs and observe the frequency of their message transmissions. If a significant change in frequency is detected from an ECU, then it can be considered compromised. A similar technique was proposed in stuy [106], to detect abnormal massages based on interval measurements of periodic CAN messages. Authors in study [107], proposed to use a machine learning-based device that can be connected to OBD ports to detect malicious patterns from the CAN traffic data and disable the messages when an attack is detected to prevent ECUs from being compromised. Authors in study [108], proposed to implement a hardware-based protocol that can achieve both CAN access authentication and message encryptions. Authors in [109], proposed a technique to monitor the correlations between ECU messages and estimate the behaviour of the vehicle. In this method, a specific ECU is detected as compromised when there is a sudden change in its messages but a sudden change in the vehicle's behaviour would mean multiple ECU attacks. Authors in study [110], proposed an Intrusion Detection System (IDS) to detect CAN network attacks based on ML algorithms. They experimented with their model using a CAN dataset and claimed to successfully classify DoS and Fuzzing attacks with high accuracy. Authors in study [111], proposed a secure boot scheme based on cryptographic algorithms that can protect the CAN network from malicious software being executed by the

vehicle's ECUs. After experiments, the authors claimed to achieve good performances with the Cipher-based MAC (CMAC) and the elliptic curve digital signature (ECDS) algorithms in terms of authentication and execution speed. Authors in study [112], also proposed an ML-based anomaly detection for CAN networks using the deep autoencoder method and claim to achieve high detection accuracy of up to 99.98%.

C. Vehicular Communications: Attacks and Defences

Vehicles are mobile and their interactions with various external entities make them vulnerable to several cyberattacks.

Attacks: Authors in study [113] conducted a simulation on a group of cooperative driving AVs where they experimented with an attack to compromise one of the vehicles and then used it to transmit false information in the vehicular network, which resulted in sudden disturbances in vehicles' speeds. A DoS attack was also experimented in study [114], by saturating a V2I network channels with excessive noise messages through simulation, where authors showed that this kind of attack in practice, can block all vehicles from sending messages in the network and therefore interrupt the vehicles' cooperation. In study [40], a group of researchers conducted a study to explore the security of automotive APIs, telematic systems, and the infrastructures that support them. The authors discovered multiple vulnerabilities across 19 major global suppliers and original equipment manufacturers (OEM) and exploited them to remotely control vehicles and access sensitive data.

1) Authentication defence mechanisms: Authors in study [115], proposed an authentication method for V2V communications in VANET, where vehicles periodically broadcast their presence information to others and record the received announcements to determine a neighbouring group, and then identify malicious nodes by sharing the composition of groups. Authors in study [116] proposed a V2I authentication method called "Security Credential Management System". The method was based on a public-key infrastructure and claimed to provide good privacy protection, but it suffers from high computation and communication delays.

Authors in study [117] proposed an authentication method to achieve group signatures for short-term communications in VANET based on the Boneh-Shacham algorithm. Authors in study [118] also proposed an authentication system for VANET which generates pseudonyms based on vehicles' IDs through public key cryptography and then uses these pseudonyms in the authentication processes for privacy-preserving purposes. They used an ID-based signature for V2I authentication and an ID-based online/offline signature for V2V authentication and defended the feasibility and efficiency of their method in vehicular networks based on performance evaluations.

Authors in study [119] proposed a lightweight authentication method for handover in V2X communications where each vehicle can be allocated a temporary identity from its home network and then use that identity when moved to a new network. The authors claimed to achieve better performance with low computation overhead through simulations. Authors in [120] proposed a security technique for vehicular LTE networks which can mutually authenticate vehicle nodes and preserve their privacy. They evaluated their method to have better performances in terms of communication cost, security level, and less computation. A privacy management algorithm based on hybrid cryptography was proposed in study [121], to ensure trusted communication between vehicles. The authors used an asymmetric identity-based digital signature and claimed to achieve better performances in terms of communication latency, computation and storage overheads.

Authors in study [122] proposed a self-checking authentication method for VANET where vehicles and RSUs can verify each other without including a Trusted Authority (TA). Initially, the TA is responsible for the registration of all vehicles and RSUs before they join the vehicular network environment and therefore TA will intervene in the vehicle's authentication process through RSUs. This method proposed to allocate a group signature to vehicles at their first authentication from one RSU domain and then use the same signature for authentication in other domains without going through the whole process. Authors claim that this method meets security requirements and benefits from faster authentication.

Authors in study [123] proposed a multifactor authentication process for AVs and claimed to achieve good security checks without revealing sensitive information of users. Authors in study [124] also proposed a multifactor authentication for remote vehicle diagnosis and maintenance which requires both biometric and password verifications from the vehicle's owner or the Service Centre to ensure legitimate access to the system. Through performance analysis of the technique, the authors claimed that it achieves a robust security level. An edge-based vehicular authentication architecture was proposed in study [125], where different vehicles can be grouped to form a vehicular cloud. The authors claim easier attack detections using deep learning algorithms in this technique that offer a lightweight authentication of vehicles for secure V2V communications.

Authors in study [126] proposed an identity-based cryptographic method for V2V authentications and security key agreement, where the ID of each vehicle is used as its public key, which can expose this method to privacy leakage. A Blockchain-based One-Time authentication method was proposed in study [127], for V2X communications. In this method, the identities of nodes are encrypted before sharing instead of revealing the real identities, and different proofs are generated to authenticate nodes which are verified through a noninteractive blockchain. Based on security analysis, the authors claim to achieve secure V2X authentications with reduced delay. Authors in study [128], proposed an aggregate and continuous authentication technique using federated learning for VANET applications. Based on the edge devices as learning centre between vehicles and RSUs, the authors claimed to achieve a secure and privacy-preserving authentication with reduced communication overheads.

2) Confidentiality defence mechanisms: In study [129], a "cryptographic mix-zone (CMIX)" algorithm was proposed to secure exchanged data in vehicular networks. In CMIX, the encryption process is based on a group secret key, where the same key is shared between all the vehicle nodes in the network to save time from individual key sharing. However, all the security is compromised when an attacker can intercept the encryption key during its broadcasting.

Authors in study [130] proposed a game theory technique known as the Markovian game to achieve secure communication, where each vehicle in the network is considered a player and players are either data holders (DH) or data requesters (DR). In this game, each vehicle earns income according to the provided services and uses that income to buy access to private data. If a DR node wants to access private data from a DH node, it will propose a motivation price then the DH will decide a privacy concession according to its satisfaction. The problem with this game is that the DH cannot verify if the DR is a malicious node or not before privacy concession. Therefore, the algorithm should consider other parameters to prevent network intrusion.

Authors in study [131] proposed a secure V2X communication method based on a hash chain of secret key cryptography and claimed to provide secure messaging between vehicles at low cost. The authors in [132] proposed a batch verification method using the "Paillier cryptographic algorithm" to solve privacy issues in VANETs, in which, vehicles can cooperate to identify malicious users without disclosing sensitive information. This method can achieve privacy-preserving communications but does not guarantee the confidentiality of exchanged data.

3) Network monitoring defence mechanisms: Authors in study [133], proposed a security algorithm to detect malicious vehicles based on their behaviours in the network and then isolate them from the rest of entities. This method can reduce the chances of successful sybil attacks but isolating a vehicle node from the network as a prevention technique can represent a danger in some situations, especially in complex traffic. Authors in study [134] proposed an intrusion detection system to detect attack scenarios against vehicular networks including packet duplication, selective forwarding, resource exhaustion, wormhole, black hole, and Sybil attacks. After simulation, the authors claim that the proposed algorithm can provide good attack detection accuracy with minimum detection time.

Authors in study [135] proposed an intrusion detection system for vehicular networks based on "deep neural network (DNN)" to detect attacks. Using an unsupervised training, the DNN algorithm could accurately classify normal packets and attacked packets and able to detect malicious events against the vehicle as a result. Therefore, this method can perform better in vehicular networks when many attacked packets from different attack scenarios are used in the training process of the DNN.

Authors in study [136] proposed a voting technique to identify rogue nodes in VANET. In this method, two vehicles vote for each other when they can communicate without any security issues. The trust level of a vehicle in the network is evaluated according to the number of gathered votes, where a vehicle with a small value of a vote is considered a rogue node and a potential source of attack. This method can achieve good performance in a fixed number of nodes since it is an experience-based system but does not perform in scalable network scenarios like vehicular networks, where vehicles can join a locale network and leave at any time due to their mobility. Authors in study [137] proposed a coalitional security game to detect malicious nodes in vehicular networks based on Dempster-Shafer's theory. The game consists of building trusted relationships between vehicles based on their reputation, experience, and knowledge. However, attackers can target a vehicle with experience and a good reputation and use it to perform attacks in the network. Also, vehicles can be in new environments at any time due to their mobility without previous experience gained from that environment.

Authors in study [138] proposed an intrusion detection system using ML models to detect "Distributed Denial of Service (DDoS)" attacks in V2I communications. The authors claimed to achieve good detection accuracy after various testing. The same approach was proposed in study [139] based on the Support Vector Machine algorithm where authors achieved high DDoS detection performances through simulations. Authors in study [140] proposed an attack detection mechanism for AVs that works both in online and offline modes. The offline phase is used to establish parameters based on which, the detection of attacks and responses are executed in the online phase.

IV. Discussion

Security is a very active research area for information technologies, and the introduction of AVs has increased the interest where each newly published work can offer fresh approaches to system security problems. However, most of the existing security standards are still facing challenges in addressing issues in this cutting-edge technology where additional critical parameters are being considered regarding real-time communication, resource constraint computation, user privacy, fault detection, network scalability, quality of service, etc. [141]. The previous security mechanisms presented in the literature are discussed in this section to point out the open security challenges for further investigations.

A. Sensors

Sensors represent the perception elements that collect data for AVs and are used to make decisions. Therefore, the security of sensors is crucial and the proposed attack mitigation methods should consider some requirements including:

- Detection of adversarial signals such as spoofing and jamming attack signals, and filter them to allow good perception of legitimate signals under attack situations;
- Availability: the solution should not disrupt other services during its execution and should have faster execution to meet the real-time functionality of AVs;

The defence strategies related to the security of sensors are discussed in Table I.

B. The In-Vehicle Network

In the internal network of the vehicle, the components interact to perform driving tasks together, and any successful attack or dysfunction can compromise the vehicle's normal operations. Therefore, the security measures should include the following requirements:

- Authentication: Every component should be identified and trusted before accessing the CAN network;
- Attack detection: suspicious activities in the CAN network should be identified, and compromised nodes should be excluded from sending data in the CAN.
- Availability: the solution should not disrupt other services during its execution and should have faster execution to meet the real-time functionality of AVs;

The defence strategies related to the security of CAN networks are discussed in Table II.

TABLE I. DISCUSSION OF SECURITY METHODS FOR SENSORS

Attack Types	Target components	Proposed Defense Strategies	Contributions	Limitations
Sensor Spoofing and Jamming	LiDAR, Radar, GPS	1) "Prevention of spoofing and jamming attacks" using multiple sensors [44], [63]. 2) "Detection of spoofing and jamming attacks" based on signals' directions [55], [56]. 3) "Detection of spoofing and jamming attacks" using the ML models [48], [49], [48], [49], [50], [57], [73], [74]. 4) "Detection of spoofing and jamming attacks" based on signals' authentication [45], [47], [64], [69].	1) The use of multiple sensors provides an overlapping coverage of the vehicle's surroundings, which can therefore reduce attack chances since it becomes difficult to compromise all sensors together. 2) The detection of attack directions can help to reject signals arriving from them and therefore prevent attacks. 3) The ML models increase the detection accuracy of spoofing and jamming signals. 4) The authentication of signals through modulation or signature methods, helps to identify attack signals from legitimate ones.	1) The main challenge with the use of multiple sensors to mitigate spoofing or jamming attacks is its implementation increases the cost. 2) The detection of attack signals based on their directions can be performed when the nodes are fixed, which makes it inefficient for vehicular applications due to the mobility of vehicles. 3) The ML-based attack detection methods lack experiments to determine their efficiency in realistic AV environments. 4) The authentication of signals requires computational modifications in sensor nodes, which represents a high implementation cost and also involves higher computational delays.
		Open challenges: The spoofing and jamming attacks against sensors remain a serious challenge in the context of AVs. Most of the existing solutions aim to detect spoofing and jamming signals, but there is a lack of efficient methods to filter them and allow sensors to correctly collect legitimate signals in attack situations. Therefore, further investigations are needed to guarantee the security of sensors for AV applications.		
Sensor Blinding and Adversarial images	Cameras	1) Prevention of blinding attacks using multiple cameras [43]. 2) Prevention of blinding attacks using light filters in cameras [43], [83]. 3) Detection of blinding and adversarial image attacks using ML models [84], [85], [86], [87], [88], [89], [90], [91], [92].	1) Multiple cameras provide overlapping views of the vehicle's surroundings to capture redundant images, which makes it difficult to blind all cameras together, and therefore, reduce attack chances. 2) The integration of light filters into cameras can help to cut near-infrared lights and therefore prevent blinding attacks. 3) The ML models increase the detection accuracy of adversarial image attacks.	1) The main challenge with the use of multiple cameras to mitigate blinding attacks is that it represents a high implementation cost. 2) The implementation of light filters needs to be experimented on real cameras to validate their effectiveness for AV applications. 3) Complex and adequate dataset of adversarial examples are still needed to train ML models and extensively experiment them on realistic cameras to determine their effectiveness.

TABLE II. DISCUSSION OF SECURITY METHODS FOR THE CAN NETWORK

Attack Types	Target components	Proposed Defense Strategies	Contributions	Limitations
Malware and Message Injection	CAN network, ECUs	1) "Detection of CAN network attacks" based on entropy calculation [103]. 2) "Detection of CAN network attacks" based on message transmission time [104]. 3) "Detection of CAN network attacks" based on message frequency [105], [106], [109]. 4) "Detection of CAN network attacks" based on authentication of ECUs [105]. 5) "Detection of CAN network attacks" based on ML models [107], [110], [112]. 6) "Prevention of	1) The changes in entropy can identify irregular activities, which can be useful in detecting CAN traffic anomalies. 2) The of message transmission times comparison is useful in identifying malicious data if the transmission time is higher than expected, which can particularly prevent message replay attacks without heavy computations. 3) The frequency of messages can help to determine the behaviour of different nodes in the CAN network, and therefore, detect abnormal actions. 4) The authentication of ECUs can prevent other ECUs from receiving malicious data from unidentified or illegitimate nodes. 5) The ML models can detect complex attacks with high accuracy. They can analyze large volumes of data and easily adapt to evolving attack patterns using updated datasets. This can monitor the CAN network in real-time. 6) The encryption of messages can prevent unauthorized access to data and guarantee	1) The main challenge with entropy calculation is its high sensitivity to data distribution, which must be well modelled to provide meaningful entropy values. Also, small changes in data distribution can lead to significant changes in entropy values making it practically inefficient for vehicular security. 2) The use of message transmission time can negatively impact the network in some unexpected situations such as transmission delays due to congestions or routing issues can falsely flag legitimate messages as malicious. Also, this can be vulnerable when the attacker manipulates the time. 3) The attack detection based on the frequency of messages may only be useful for the security of sensors, which collect data at a regular rate. However, this method is inefficient for ECUs that randomly transmit messages based on the needs. 4) The authentication of ECUs requires computational modifications in each ECU of the vehicle, which represents a high implementation cost and also involves higher delays. 5) The challenge with ML models is that their Training and deployment require significant computational resources, which may not be feasible in constrained environments like ECUs. Also, there is a lack of experiments to determine the effectiveness of the ML models on realistic CAN networks. 6) Many existing CAN networks lack built-in support for encryption, which requires significant hardware or software

		CAN network attacks" using encryption techniques [108], [111].	the integrity of exchanged information in the CAN network.	upgrades. Also, it would be challenging to implement and execute encryption algorithms in CAN networks because of their limited processing power and memory.
		Open challenges: The AVs remain vulnerable to malware and message injection attacks through OBD ports or telematics. Traditionally, the OBD ports are protected by a physical lock, which does not guarantee effective security. However, no security method was found in the literature that can distinguish legitimate OBD devices from malicious OBD devices when connected to the OBD port. Therefore, further investigations are needed to guarantee the security of ECUs for vehicular applications.		

C. Vehicular Communications

Each AV is an autonomous system susceptible to joining a network environment where it will interact with everything using wireless interfaces. The exchanged information between the vehicle with the outside world will determine its driving behaviour in traffic, making it vulnerable to various attacks. Therefore, the V2X communications protocols should include the following requirements:

- Authentication: Every entity including vehicles, smart devices, and RSUs, should be identified and verified as trusted before accessing the vehicular network;
- Data protection: Exchanged information between entities in the vehicular network should be authentic and confidential to avoid unauthorized access;
- Attack detection: The vehicular network should be controlled to detect suspicious activities, and exclude compromised entities from sending data in the network;
- Compatibility: The solution should not disrupt other services during its execution.
- Computational efficiency: The solution should have faster execution with low implementation cost to meet real-time and resource-constraint functionality of AVs;
- Scalability: The solution should accept the changes in the number of network entities.

The defence strategies related to the security of V2X communications are discussed in Table III.

TABLE III. DISCUSSION OF SECURITY METHODS FOR VEHICULAR COMMUNICATIONS

Attack Types	Target components	Proposed Defense Strategies	Contributions	Limitations
Network Intrusion attacks (identity theft, Sybil, replay, …) Eavesdropping (man in the middle, data manipulation, …),	Communication Protocols	1) Collaborative vehicular authentication [115], [125]. 2) Public key-based vehicular authentication [116], [118], [121], [126]. 3) Group signature-based vehicular authentication [117], [122]. 4) Identity-based vehicular authentication [119], [120]. 5) Multifactor-based vehicular authentication [123], [124]. 6) Blockchain-based vehicular authentication [127].	1) The collaborative authentication is decentralized and reduces the risk of single-point vulnerabilities. As multiple entities validate a vehicle's credentials, this technique can help balance the load of authentication tasks and identify malicious nodes more effectively. 2) The public key authentication uses strong encryption algorithms suitable for large-scale networks like vehicular networks, to ensure the integrity and authenticity of exchanged messages. 3) The group signature cancels the need for individual authentications, reducing communication delays. It also allows vehicles to authenticate themselves without revealing their specific identity, which enhances user privacy. 4) The identity-based authentication uses simple structures rather than complex and heavy cryptographic algorithms, which reduces computation and communication delays, making it suitable for time-sensitive applications. Also, it is easier to integrate identity-based methods across different vehicular networks to meet specific security requirements. 5) Combining multiple authentication factors (e.g., password/PIN, biometric data, cryptographic keys) makes it significantly harder for attackers to compromise the system. 6) The blockchain provides robust cryptographic security and immutability, making it difficult for attackers to alter authentication records. 7) The ML models gain from the high	1) The challenge with collaborative authentication is that it involves multiple messages exchanged among vehicles or nodes, leading to increased network traffic, and therefore introducing communication delays. Also, this method can lead to security and privacy breaches because of the exchange of vehicles' identity that can be intercepted and manipulated by attackers to have access to the network. 2) The public key operations (e.g., encryption, decryption, and signature verification) are computationally intensive, which can introduce delays and may affect the real-time requirements of vehicular networks. Also, this method can put the security of the entire network at risk, when the private keys or the certificate authority that it relies on, are compromised. 3) Generating and verifying group signatures can be computationally intensive, especially in a large number of group participants, which can impact real-time applications and reduce the network performance in real-world vehicular environments. 4) While promising, identity-based methods are less commonly deployed compared to certificate-based systems, limiting their effectiveness in verification and interoperability with existing infrastructures. 5) The authentication based on factors like biometrics can frequently fail due to mismeasurements or environmental conditions (e.g., dirt affecting fingerprint scanners). Also, authenticating multiple factors can take additional computation time, which may affect real-time applications like collision avoidance or emergency communications. 6) Blockchain transactions can require significant time to be validated and added to the ledger, which may not meet the real-time requirements of vehicular networks. Also, the increase in the number of vehicles and authentication transactions can lead to blockchain bloat, requiring more storage and computational resources.

Network saturation (DoS and DDoS)		7) ML-based intrusion detection [128], [134], [135], [138], [139].	accuracy of attack detection capable of analyzing large volumes of data to detect complex attacks with the ability to adapt to evolving attack patterns by retraining with updated datasets. This can monitor vehicular communications on a real-time basis.	7) The challenge with ML models is that their training and deployment require significant computational resources, which may become intensive for vehicles in case of the implementation of multiple ML algorithms. Also, there is a lack of experiments to determine the effectiveness of the ML models on realistic vehicular networks
		8) Game theory-based intrusion detection [130], [136], [137].	8) The game theory models allow the system to predict and counteract attacker strategies effectively by making the cost of an attack higher than its potential benefit. A well-designed game-theoretic approach can enhance the precision of attack detection when the attacker's behaviour patterns are incorporated.	8) The main challenge with game theory-based security methods is that they require detailed knowledge of attacker and defender behaviours to create a realistic game-theoretic model. Due to this dependency on accurate input data, such as network traffic patterns and known attack strategies, the game theory model can easily fail to detect an attack effectively if the attacker uses strategies outside the modelled game.
		9) Data protection based on cryptographic algorithms [129], [131], [132].	9) Cryptographic algorithms provide robust protection against unauthorized access and ensure data confidentiality throughout its lifecycle, even when transmitted over insecure channels. They can be implemented across various systems including vehicular networks.	9) Cryptographic algorithms can be resource-intensive, leading to delays in real-time systems like vehicular networks. Choosing a stronger encryption algorithm often involves a trade-off between security and performance, particularly in resource-constrained environments like IoT-based systems.
		Open challenges: Due to the high mobility of vehicles, they are permanently vulnerable to attacks through interactions with potentially compromised entities. Therefore, strong, efficient, and lightweight security protocols are still needed to defend vehicular networks from different intrusion, eavesdropping, and saturation attacks.		

V. Proposed Security Measures

To achieve good security and privacy requirements for vehicular applications while gaining from low computation and efficient implementation, we propose the use of powerful and innovative techniques. First, the cryptographic hashing algorithm is used for identity-based authentication, which achieves complex mathematical operations with faster computation. Secondly, homomorphic encryption is to be used to protect sensitive data communication between network entities for enhanced privacy and confidentiality. Finally, to build a Machine Learning based intrusion detection system using the transfer learning technique for multiple attack detection capability with efficient implementation.

A. Authentication Protocol

The proposed authentication protocol includes vehicles and their respective users, RSUs, and TA as illustrated in Fig. 10. First, each vehicle should be used by a legitimate user who is authenticated before the vehicular authentication in the network. The user authentication phase will protect user information to preserve privacy and avoid malicious traceability. Secondly, every vehicle and RSU is registered by the TA before being allowed in the vehicular network. In this registration phase, TA protects the privacy of vehicles and RSUs and provides secure authentication parameters for them. Third, vehicles are authenticated by RSUs to be admitted in their respective communication ranges, and vehicles authenticate each other to communicate among themselves. The authentication phase is based on mutual authentication where entities can identify each other and securely agree on a communication key. In this phase, each entity uses a pseudonym identity and other parameters received from TA during the registrations phase which avoid sharing the real identity and therefore preserve their privacy in the network. Finally, the authenticated or legitimate entities can securely participate in vehicular communications.

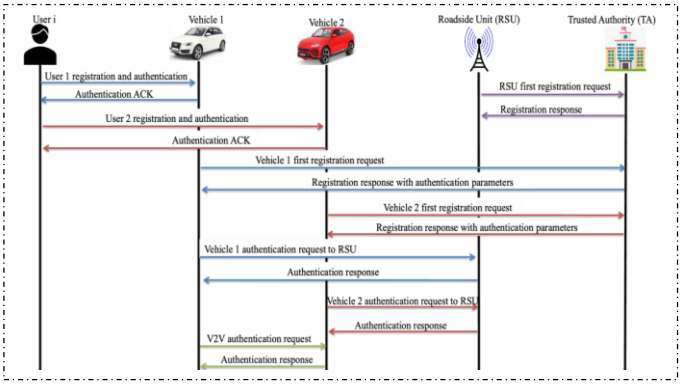

Fig. 10. Vehicular network authentication.

B. Privacy and Confidentiality

The proposed privacy and confidentiality mechanism for secure communication between vehicles, is based on homomorphic encryption as illustrated in Fig. 11. The homomorphic encryption offers the possibility to perform complex computations and data analysis on encrypted information without the need to decrypt them before [142], [143]. This represents a powerful solution for maintaining confidentiality and privacy during the transmission and processing of sensitive data. In the context of vehicular networks, each node can be a potential malicious node trying to collect private information. The homomorphic encryption can prevent unauthorized access to valuable information and therefore reduce the risk of data manipulation and breaches. Also, it enables traffic data analysis by the traffic authority and transportation companies without compromising the privacy of vehicular users and passengers.

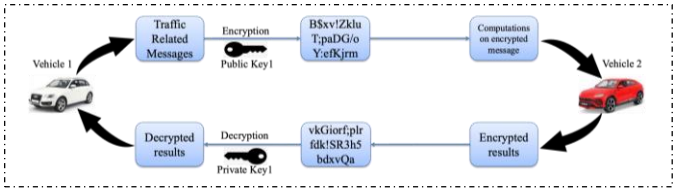

Fig. 11. Vehicular homomorphic encryption.

C. Intrusion Detection System

The proposed intrusion detection system for monitoring vehicular communications is based on transfer learning techniques as illustrated in Fig. 12. The transfer learning makes it possible to train a machine learning model using different datasets while gaining knowledge from all of them [144]. In this process, the model is trained with a starting dataset then the pre-trained model is trained again with a new dataset. Instead of implementing different models in the same device to detect individual types of attacks, transfer learning allows the accumulation of knowledge in a single model to save time and resources which is therefore suitable for vehicular applications.

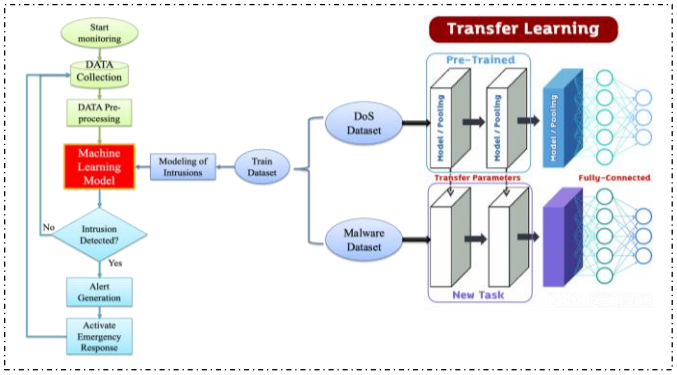

Fig. 12. Intrusion detection system based on transfer learning.

VI. Conclusion

Future transportation is expected to improve the quality of living by providing more safer and reliable mobility. While the introduction of autonomous vehicles has been presented to achieve this goal, it is also opening a new space for cyberattacks. Therefore, the cybersecurity concerns in the transportation area have raised interest from researchers and security experts to investigate and propose security measures for a trusted deployment. This paper reviewed the state of the art of cybersecurity issues defence strategies for AVs based on existing experiments and discussed methods in the literature. The review is organized by grouping attack methods and proposed defence techniques according to the target AV components. Based on this review, three major attack scenarios against AVs have been identified: 1) the attacker can target a component to interrupt its operations; 2) the attacker can target a component to have control over its operations without interrupting it; 3) the attacker can observe exchanged information without interrupting or controlling a component's operations. In response to the attacks, different defence approaches were proposed, which can also be categorised into three aspects including authentication, data protection, and intrusion detection. The authentication consists of identity verification and communication establishment to ensure that only trusted and legitimate entities are interacting. Data protection ensures that data transmitted between legitimate entities are trusted and secured from third parties. And, intrusion detection focuses on monitoring the interaction environment of legitimate entities to detect suspicious activities. The existing defence strategies were discussed to highlight their benefits in securing autonomous vehicles and also to show their limitations in satisfying critical requirements of vehicular networks, such as real-time and resource constraint applications, which can motivate further investigations. Furthermore, this paper presents some research directions that can be used to develop robust, efficient, and lightweight security measures, and therefore, contribute to building a trustworthy autonomous transportation ecosystem.

Acknowledgment

This work has been supported by the "Partnership for Skills in Applied Sciences, Engineering and Technology - Regional Scholarship and Innovation Fund (PASET-RSIF) through the African Centre of Excellence in Internet of Things (ACEIoT)".

References

[1] P. Suresh, J. V. Daniel, and R. H. Aswathy, "A state of the art review on the Internet of Things (IoT) History , Technology and fields of deployment," in *International Conference on Science, Engineering and Management Research (ICSEMR 2014)*, IEEE, 2014.

[2] P. Liu, "Internet of Thing Based Vehicular Network System and Application," in *Advances in Intelligent Systems Research*, 2018, pp. 298–302.

[3] F. Zhu, Y. Lv, Y. Chen, X. Wang, G. Xiong, and F. Y. Wang, "Parallel Transportation Systems: Toward IoT-Enabled Smart Urban Traffic Control and Management," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 10, pp. 4063–4071, 2020, doi: 10.1109/TITS.2019.2934991.

[4] SAE International, "Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor J3016_202104." Accessed: Dec. 14, 2023. [Online]. Available: https://www.sae.org/standards/content/j3016_202104/

[5] J. Wang, J. Liu, and N. Kato, "Networking and Communications in Autonomous Driving: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1243–1274, Apr. 2019, doi: 10.1109/COMST.2018.2888904.

[6] S. Muthuramalingam, A. Bharathi, S. Rakesh kumar, N. Gayathri, R. Sathiyaraj, and B. Balamurugan, "IoT Based Intelligent Transportation System (iot-its) for Global Perspective: A Case Study," *Internet of Things and Big Data Analytics for Smart Generation*. Springer Nature Switzerland AG 2019, pp. 279–300, 2019. doi: 10.1007/978-3-030-04203-5_13.

[7] A. O. Al Zaabi, C. Y. Yeun, and E. Damiani, "Autonomous Vehicle Security: Conceptual Model," in *2019 IEEE Transportation Electrification Conference and Expo, Asia-Pacific (ITEC Asia-Pacific)*, IEEE, May 2019, pp. 1–5. doi: 10.1109/ITEC-AP.2019.8903691.

[8] B. K. Ren, Q. Wang, C. Wang, Z. Qin, and X. Lin, "The Security of Autonomous Driving : Threats , Defenses , and Future Directions," *Proceedings of the IEEE*, pp. 1–16, 2019, doi: 10.1109/JPROC.2019.2948775.

[9] 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, p. 102150, Apr. 2021, doi: 10.1016/j.cose.2020.102150.

[10] X. Sun, F. R. Yu, and P. Zhang, "A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs)," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 6240–6259, Jul. 2022, doi: 10.1109/TITS.2021.3085297.

[11] Y. Takefuji, "Connected Vehicle Security Vulnerabilities [Commentary]," *IEEE Technology and Society Magazine*, vol. 37, no. 1, pp. 15–18, Mar. 2018, doi: 10.1109/MTS.2018.2795093.

[12] K. Rudd, "Security of Autonomous Systems Employing Embedded Computing and Sensors," pp. 80–86, 2013.

[13] M. Kalmeshwar and K. S. Nandini Prasad, "Development of On-Board Diagnostics for Car and it's Integration with Android Mobile," in *2017 2nd International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS)*, IEEE, Dec. 2017, pp. 1–6. doi: 10.1109/CSITSS.2017.8447540.

[14] A. Rizwan *et al.*, "Simulation of IoT-based Vehicular Ad Hoc Networks (VANETs) for Smart Traffic Management Systems," *Wirel Commun Mob Comput*, vol. 2022, pp. 1–11, May 2022, doi: 10.1155/2022/3378558.

[15] M. M. A. Muslam, "Enhancing Security in Vehicle-to-Vehicle Communication: A Comprehensive Review of Protocols and Techniques," *Vehicles*, vol. 6, no. 1, pp. 450–467, Feb. 2024, doi: 10.3390/vehicles6010020.

[16] S. Adnan Yusuf, A. Khan, and R. Souissi, "Vehicle-to-everything (V2X) in the autonomous vehicles domain – A technical review of communication, sensor, and AI technologies for road user safety," *Transp Res Interdiscip Perspect*, vol. 23, p. 100980, Jan. 2024, doi: 10.1016/j.trip.2023.100980.

[17] A. Chattopadhyay and K. Lam, "Security of Autonomous Vehicle as a Cyber-Physical System," 2017.

[18] M. N. Ahangar, Q. Z. Ahmed, F. A. Khan, and M. Hafeez, "A Survey of Autonomous Vehicles: Enabling Communication Technologies and Challenges," *Sensors*, vol. 21, no. 3, p. 706, Jan. 2021, doi: 10.3390/s21030706.

[19] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of DSRC and Cellular Network Technologies for V2X Communications: A Survey," *IEEE Trans Veh Technol*, vol. 65, no. 12, pp. 9457–9470, Dec. 2016, doi: 10.1109/TVT.2016.2591558.

[20] Z. Wang, H. Wei, J. Wang, X. Zeng, and Y. Chang, "Security Issues and Solutions for Connected and Autonomous Vehicles in a Sustainable City: A Survey," *Sustainability*, vol. 14, no. 19, p. 12409, Sep. 2022, doi: 10.3390/su141912409.

[21] M. Pham and K. Xiong, "A survey on security attacks and defense techniques for connected and autonomous vehicles," *Comput Secur*, vol. 109, p. 102269, Oct. 2021, doi: 10.1016/j.cose.2021.102269.

[22] B. R. Mudhivarthi, P. Thakur, and G. Singh, "Aspects of Cyber Security in Autonomous and Connected Vehicles," *Applied Sciences*, vol. 13, no. 5, p. 3014, Feb. 2023, doi: 10.3390/app13053014.

[23] B. Sheehan, F. Murphy, M. Mullins, and C. Ryan, "Connected and autonomous vehicles: A cyber-risk classification framework," *Transp Res Part A Policy Pract*, vol. 124, pp. 523–536, Jun. 2019, doi: 10.1016/j.tra.2018.06.033.

[24] A. Singandhupe and H. M. La, "A Review of SLAM Techniques and Security in Autonomous Driving," in *2019 Third IEEE International Conference on Robotic Computing (IRC)*, IEEE, Feb. 2019, pp. 602–607. doi: 10.1109/IRC.2019.00122.

[25] A. M. Wyglinski, X. Huang, T. Padir, L. Lai, T. R. Eisenbarth, and K. Venkatasubramanian, "Security of Autonomous Systems Employing Embedded Computing and Sensors," *IEEE Micro*, vol. 33, no. 1, pp. 80–86, Jan. 2013, doi: 10.1109/MM.2013.18.

[26] J. Cui and B. Zhang, "VeRA: A Simplified Security Risk Analysis Method for Autonomous Vehicles," *IEEE Trans Veh Technol*, vol. 69, no. 10, pp. 10494–10505, Oct. 2020, doi: 10.1109/TVT.2020.3009165.

[27] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 11, pp. 2898–2915, Nov. 2017, doi: 10.1109/TITS.2017.2665968.

[28] A. Nanda, D. Puthal, J. J. P. C. Rodrigues, and S. A. Kozlov, "Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions," *IEEE Wirel Commun*, vol. 26, no. 4, pp. 60–65, Aug. 2019, doi: 10.1109/MWC.2019.1800503.

[29] Q. Xiao, X. Pan, Y. Lu, M. Zhang, J. Dai, and M. Yang, "Exorcising "'Wraith"': Protecting LiDAR-based Object Detector in Automated Driving System from Appearing Attacks," *Proceedings of the 32nd USENIX Conference on Security Symposium*, pp. 2939–2956, Mar. 2023, [Online]. Available: http://arxiv.org/abs/2303.09731

[30] K. Ren, Q. Wang, C. Wang, Z. Qin, and X. Lin, "The Security of Autonomous Driving: Threats, Defenses, and Future Directions," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 357–372, Feb. 2020, doi: 10.1109/JPROC.2019.2948775.

[31] H. M. Furqan, M. S. J. Solaija, H. Turkmen, and H. Arslan, "Wireless Communication, Sensing, and REM: A Security Perspective," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 287–321, 2021, doi: 10.1109/OJCOMS.2021.3054066.

[32] S. Tout, M. Abualkibash, and P. Patil, "Emerging Research in the Security of Modern and Autonomous Vehicles," in *2018 IEEE International Conference on Electro/Information Technology (EIT)*, IEEE, May 2018, pp. 0543–0547. doi: 10.1109/EIT.2018.8500204.

[33] A. Ferdowsi, U. Challita, W. Saad, and N. B. Mandayam, "Robust Deep Reinforcement Learning for Security and Safety in Autonomous Vehicle Systems," in *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, IEEE, Nov. 2018, pp. 307–312. doi: 10.1109/ITSC.2018.8569635.

[34] L. Zhang, X. Yan, and D. Ma, "A Binarized Neural Network Approach to Accelerate in-Vehicle Network Intrusion Detection," *IEEE Access*, vol. 10, pp. 123505–123520, 2022, doi: 10.1109/ACCESS.2022.3208091.

[35] D. Uhlir, P. Sedlacek, and J. Hosek, "Practial overview of commercial connected cars systems in Europe," in *2017 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, Munich: IEEE, Nov. 2017, pp. 436–444. doi: 10.1109/ICUMT.2017.8255178.

[36] S. Zamfir and R. Drosescu, "Automotive Black Box and Development Platform Used for Traffic Risks Evaluation and Mitigation," in *The 30th SIAR International Congress of Automotive and Transport Engineering*, Cham: Springer International Publishing, 2020, pp. 426–438. doi: 10.1007/978-3-030-32564-0_50.

[37] J. Kang, D. Lin, E. Bertino, and O. Tonguz, "From Autonomous Vehicles to Vehicular Clouds: Challenges of Management, Security and Dependability," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, IEEE, Jul. 2019, pp. 1730–1741. doi: 10.1109/ICDCS.2019.00172.

[38] S. McCall, C. Yucel, and V. Katos, "Education in Cyber Physical Systems Security: The Case of Connected Autonomous Vehicles," in *2021 IEEE Global Engineering Education Conference (EDUCON)*, IEEE, Apr. 2021, pp. 1379–1385. doi: 10.1109/EDUCON46332.2021.9454086.

[39] A. A. Mehta *et al.*, "Securing the Future: A Comprehensive Review of Security Challenges and Solutions in Advanced Driver Assistance Systems," *IEEE Access*, vol. 12, pp. 643–678, 2024, doi: 10.1109/ACCESS.2023.3347200.

[40] Upstream Security Ltd, "H1'2023: AUTOMOTIVE CYBER TREND REPORT," 2023. Accessed: Dec. 08, 2023. [Online]. Available: https://upstream.auto/reports/h1-2023-automotive-cyber-trend-report/

[41] Upstream Security Ltd, "GLOBAL AUTOMOTIVE CYBERSECURITY REPORT: AUTOMOTIVE CYBER THREAT LANDSCAPE IN LIGHT OF NEW REGULATIONS," 2022. Accessed: Dec. 08, 2023. [Online]. Available: https://upstream.auto/2022report/

[42] B. G. B. Stottelaar, "PRACTICAL CYBER-ATTACKS ON AUTONOMOUS VEHICLES," University of Twente, 2015.

[43] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR," in *Black Hat Europe*, 2015, p. 995. Accessed: May 12, 2024. [Online]. Available: blackhat.com

[44] H. Shin, D. Kim, Y. Kwon, and Y. Kim, "Illusion and Dazzle: Adversarial Optical Channel Exploits Against Lidars for Automotive Applications," in *Cryptographic Hardware and Embedded Systems – CHES 2017*, W. Fischer and N. Homma, Eds., in Lecture Notes in Computer Science. , Cham: Springer International Publishing, 2017, pp. 445–467. doi: 10.1007/978-3-319-66787-4_22.

[45] Q. Wang *et al.*, "Pseudorandom modulation quantum secured lidar," *Optik (Stuttg)*, vol. 126, no. 22, pp. 3344–3348, Nov. 2015, doi: 10.1016/j.ijleo.2015.07.048.

[46] D. Davidson, H. Wu, and R. Jellinek, "Controlling UAVs with Sensor Input Spoofing Attacks," in *10th USENIX Workshop on Offensive Technologies (WOOT '16)*, Austin: USENIX, Aug. 2016, pp. 1–11.

[47] R. Matsumura, T. Sugawara, and K. Sakiyama, "A Secure LiDAR with AES-Based Side-Channel Fingerprinting," in *2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW)*, Takayama: IEEE, Nov. 2018, pp. 479–482. doi: 10.1109/CANDARW.2018.00092.

[48] Y. Cao *et al.*, "Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA: ACM, Nov. 2019, pp. 2267–2281. doi: 10.1145/3319535.3339815.

[49] K. M. A. Alheeti, A. Alzahrani, and D. Al Dosary, "LiDAR Spoofing Attack Detection in Autonomous Vehicles," in *2022 IEEE International Conference on Consumer Electronics (ICCE)*, IEEE, Jan. 2022, pp. 1–2. doi: 10.1109/ICCE53296.2022.9730540.

[50] H. Zhang, Z. Li, S. Cheng, and A. Clark, "Cooperative Perception for Safe Control of Autonomous Vehicles under LiDAR Spoofing Attacks," in *Proceedings Inaugural International Symposium on Vehicle Security & Privacy*, Reston, VA: Internet Society, 2023. doi: 10.14722/vehiclesec.2023.23066.

[51] R. Chauhan, "A Platform for False Data Injection in Frequency Modulated Continuous Wave Radar," Utah State University, 2014. [Online]. Available: https://digitalcommons.usu.edu/etd/3964

[52] R. Komissarov and A. Wool, "Spoofing Attacks Against Vehicular FMCW Radar," in *Proceedings of the 5th Workshop on Attacks and Solutions in Hardware Security*, New York, NY, USA: ACM, Nov. 2021, pp. 91–97. doi: 10.1145/3474376.3487283.

[53] A. Lazaro, A. Porcel, M. Lazaro, R. Villarino, and D. Girbau, "Spoofing Attacks on FMCW Radars with Low-Cost Backscatter Tags," *Sensors*, vol. 22, no. 6, p. 2145, Mar. 2022, doi: 10.3390/s22062145.

[54] Walter E. Buehler, Roger M. Whitson, and Michael J. Lewis, "AIRBORNE RADAR JAMMING SYSTEM," US00883 0112B1, Sep. 09, 2014

[55] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "PyCRA: Physical Challenge-Response Authentication For Active Sensors Under Spoofing Attacks," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA: ACM, Oct. 2015, pp. 1004–1015. doi: 10.1145/2810103.2813679.

[56] P. Kapoor, A. Vora, and K.-D. Kang, "Detecting and Mitigating Spoofing Attack Against an Automotive Radar," in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, Chicago: IEEE, Aug. 2018, pp. 1–6. doi: 10.1109/VTCFall.2018.8690734.

[57] S. Cohen, E. Levy, A. Shaked, T. Cohen, Y. Elovici, and A. Shabtai, "RadArnomaly: Protecting Radar Systems from Data Manipulation Attacks," *Sensors*, vol. 22, no. 11, p. 4259, Jun. 2022, doi: 10.3390/s22114259.

[58] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proceedings of the 18th ACM conference on Computer and communications security*, New York, NY, USA: ACM, Oct. 2011, pp. 75–86. doi: 10.1145/2046707.2046719.

[59] A. Helfrick, "Question: Alternate position, navigation timing, APNT? Answer: ELORAN," in *2014 IEEE/AIAA 33rd Digital Avionics Systems Conference (DASC)*, Colorado: IEEE, Oct. 2014, pp. 1–9. doi: 10.1109/DASC.2014.6979452.

[60] K. Zeng *et al.*, "All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems," in *Proceedings of the 27th USENIX Security Symposium*, Baltimore: USENIX, Aug. 2018, pp. 1527–1544. Accessed: Jan. 07, 2025. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/zeng

[61] S. Narain, A. Ranganathan, and G. Noubir, "Security of GPS/INS Based On-road Location Tracking Systems," in *2019 IEEE Symposium on Security and Privacy (SP)*, San Francisco: IEEE, May 2019, pp. 587–601. doi: 10.1109/SP.2019.00068.

[62] Q. Meng, L.-T. Hsu, B. Xu, X. Luo, and A. El-Mowafy, "A GPS Spoofing Generator Using an Open Sourced Vector Tracking-Based Receiver," *Sensors*, vol. 19, no. 18, p. 3993, Sep. 2019, doi: 10.3390/s19183993.

[63] Paul Y. Montgomery, Todd E. Humphreys, and Brent M. Ledvina, "Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-Antenna Receiver Defense against a Portable Civil GPS Spoofer," in *Proceedings of the Institute of Navigation, National Technical Meeting*, Anaheim: Institute of Navigation, Jan. 2010, pp. 124–130. doi: 10.15781/T2GB1Z038.

[64] A. Purwar, D. Joshi, and V. K. Chaubey, "GPS signal jamming and anti-jamming strategy — A theoretical analysis," in *2016 IEEE Annual India Conference (INDICON)*, Bangalore: IEEE, Dec. 2016, pp. 1–6. doi: 10.1109/INDICON.2016.7838933.

[65] B. W. O'Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Real-Time GPS Spoofing Detection via Correlation of Encrypted Signals," *Navigation*, vol. 60, no. 4, pp. 267–278, Dec. 2013, doi: 10.1002/navi.44.

[66] Y. Yang and J. Xu, "GNSS receiver autonomous integrity monitoring (RAIM) algorithm based on robust estimation," *Geod Geodyn*, vol. 7, no. 2, pp. 117–123, Mar. 2016, doi: 10.1016/j.geog.2016.04.004.

[67] Q. MENG, J. LIU, Q. ZENG, S. FENG, and R. XU, "Impact of one satellite outage on ARAIM depleted constellation configurations," *Chinese Journal of Aeronautics*, vol. 32, no. 4, pp. 967–977, Apr. 2019, doi: 10.1016/j.cja.2019.01.004.

[68] Q. Meng, J. Liu, Q. Zeng, S. Feng, and R. Xu, "Improved ARAIM fault modes determination scheme based on feedback structure with probability accumulation," *GPS Solutions*, vol. 23, no. 1, p. 16, Jan. 2019, doi: 10.1007/s10291-018-0809-8.

[69] M. Foruhandeh, A. Z. Mohammed, G. Kildow, P. Berges, and R. Gerdes, "Spotr: GPS spoofing detection via device fingerprinting," in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, New York, NY, USA: ACM, Jul. 2020, pp. 242–253. doi: 10.1145/3395351.3399353.

[70] S. Liu *et al.*, "Stars can tell: A robust method to defend against GPS spoofing attacks using off-the-shelf chipset," in *Proceedings of the 30th USENIX Security Symposium*, 2021.

[71] M. Ahmad and Y. Wang, "A Low-Cost Approach to Securing Commercial GPS Receivers Against Spoofing Attacks," in *Lecture Notes in Control and Information Sciences*, vol. 489, 2022, pp. 149–175. doi: 10.1007/978-3-030-83236-0_6.

[72] F. Wang, Y. Hong, and X. Ban, "Infrastructure-Enabled GPS Spoofing Detection and Correction," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 12, pp. 13878–13892, Dec. 2023, doi: 10.1109/TITS.2023.3298785.

[73] M. Shabbir, M. Kamal, Z. Ullah, and M. M. Khan, "Securing Autonomous Vehicles Against GPS Spoofing Attacks: A Deep Learning Approach," *IEEE Access*, vol. 11, pp. 105513–105526, 2023, doi: 10.1109/ACCESS.2023.3319514.

[74] K. S. Jasim, K. M. Ali Alheeti, and A. K. A. Najem Alaloosy, "Intelligent Detection System for Spoofing and Jamming Attacks in UAVs," 2023, pp. 97–110. doi: 10.1007/978-3-031-21101-0_8.

[75] C. Yan, W. Xu, and J. Liu, "Can You Trust Autonomous Vehicles : Contactless Attacks against Sensors of Self-driving Vehicle," *ACM SIGARCH Computer Architecture News*, pp. 1–13, 2016, doi: 10.1145/1235.

[76] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and Harnessing Adversarial Examples," *ICLR 2015*, pp. 1–11, Dec. 2014, [Online]. Available: http://arxiv.org/abs/1412.6572

[77] J. Kos, I. Fischer, and D. Song, "Adversarial Examples for Generative Models," in *2018 IEEE Security and Privacy Workshops (SPW)*, IEEE, May 2018, pp. 36–42. doi: 10.1109/SPW.2018.00014.

[78] S.-M. Moosavi-Dezfooli, A. Fawzi, O. Fawzi, and P. Frossard, "Universal Adversarial Perturbations," in *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Honolulu: IEEE, Jul. 2017, pp. 86–94. doi: 10.1109/CVPR.2017.17.

[79] C. Sitawarin, A. N. Bhagoji, A. Mosenia, M. Chiang, and P. Mittal, "DARTS: Deceiving Autonomous Cars with Toxic Signs," *ACM CCS 2018*, pp. 1–18, Feb. 2018, [Online]. Available: http://arxiv.org/abs/1802.06430

[80] T. B. Brown, D. Mané, A. Roy, M. Abadi, and J. Gilmer, "Adversarial Patch," *31st Conference on Neural Information Processing Systems (NIPS 2017)*, pp. 1–6, Dec. 2017, [Online]. Available: http://arxiv.org/abs/1712.09665

[81] K. Eykholt *et al.*, "Robust Physical-World Attacks on Deep Learning Visual Classification," in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, IEEE, Jun. 2018, pp. 1625–1634. doi: 10.1109/CVPR.2018.00175.

[82] K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip, and R. Gerdes, "Intelligent Transportation System Security: Impact-Oriented Risk Assessment of in-Vehicle Networks," *IEEE Intelligent Transportation Systems Magazine*, vol. 13, no. 2, pp. 91–104, Jun. 2021, doi: 10.1109/MITS.2018.2889714.

[83] W. Wang, Y. Yao, X. Liu, X. Li, P. Hao, and T. Zhu, "I Can See the Light: Attacks on Autonomous Vehicles Using Invisible Lights," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA: ACM, Nov. 2021, pp. 1930–1944. doi: 10.1145/3460120.3484766.

[84] [84] Sharath Yadav and A. Ansari, "Autonomous Vehicles Camera Blinding Attack Detection Using Sequence Modelling and Predictive Analytics," in *SAE Technical Paper 2020-01-0719*, Apr. 2020. doi: 10.4271/2020-01-0719.

[85] C. Guo, M. Rana, M. Cisse, and L. van der Maaten, "Countering Adversarial Images using Input Transformations," *International Conference on Learning Representations*, pp. 1–12, Oct. 2017, [Online]. Available: http://arxiv.org/abs/1711.00117

[86] V. Zantedeschi, M.-I. Nicolae, and A. Rawat, "Efficient Defenses Against Adversarial Attacks," in *Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security*, New York, NY, USA: ACM, Nov. 2017, pp. 39–49. doi: 10.1145/3128572.3140449.

[87] G. K. Dziugaite, Z. Ghahramani, and D. M. Roy, "A study of the effect of JPG compression on adversarial images," *International Society for Bayesian Analysis (ISBA 2016) World Meeting*, pp. 1–8, Aug. 2016, [Online]. Available: http://arxiv.org/abs/1608.00853

[88] W. Xu, D. Evans, and Y. Qi, "Feature Squeezing: Detecting Adversarial Examples in Deep Neural Networks," in *Proceedings 2018 Network and Distributed System Security Symposium*, Reston, VA: Internet Society, Feb. 2018, pp. 1–15. doi: 10.14722/ndss.2018.23198.

[89] W. Jiang, H. Li, S. Liu, X. Luo, and R. Lu, "Poisoning and Evasion Attacks Against Deep Learning Algorithms in Autonomous Vehicles," *IEEE Trans Veh Technol*, vol. 69, no. 4, pp. 4439–4449, Apr. 2020, doi: 10.1109/TVT.2020.2977378.

[90] C. Szegedy *et al.*, "Intriguing properties of neural networks," *ArXiv*, pp. 1–10, Dec. 2013, [Online]. Available: http://arxiv.org/abs/1312.6199

[91] T. Miyato, S. Maeda, M. Koyama, K. Nakae, and S. Ishii, "Distributional Smoothing with Virtual Adversarial Training," *International Conference on Learning Representations*, pp. 1–12, Jul. 2015, [Online]. Available: http://arxiv.org/abs/1507.00677

[92] J. Buckman, A. Roy, C. Raffel, and I. Goodfellow, "THERMOMETER ENCODING: ONE HOT WAY TO RESIST ADVERSARIAL EXAMPLES," in *International Conference on Learning Representations*, 2018, pp. 1–22.

[93] Q. He, X. Meng, and R. Qu, "Towards a Severity Assessment Method for Potential Cyber Attacks to Connected and Autonomous Vehicles," *J Adv Transp*, vol. 2020, pp. 1–15, Sep. 2020, doi: 10.1155/2020/6873273.

[94] V. L. L. Thing and J. Wu, "Autonomous Vehicle Security: A Taxonomy of Attacks and Defences," in 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, Dec. 2016, pp. 164–170. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.52.

[95] C.-W. Lin and A. Sangiovanni-Vincentelli, "Cyber-Security for the Controller Area Network (CAN) Communication Protocol," in *2012 International Conference on Cyber Security*, Washington : IEEE, Dec. 2012, pp. 1–7. doi: 10.1109/CyberSecurity.2012.7.

[96] K. Koscher *et al.*, "Experimental Security Analysis of a Modern Automobile," *2010 IEEE Symposium on Security and Privacy Experimental*, vol. 34, pp. 447–462, 2010, doi: 10.1109/SP.2010.34.

[97] S. Woo, H. J. Jo, and D. H. Lee, "A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 1–14, Apr. 2014, doi: 10.1109/TITS.2014.2351612.

[98] S. Checkoway *et al.*, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in *20th USENIX security symposium*, 2011, pp. 447–462.

[99] A. Boudguiga, J. Letailleur, R. Sirdey, and W. Klaudel, "Enhancing CAN Security by Means of Lightweight Stream-Ciphers and Protocols," in *SAFECOMP 2019 Workshops, LNCS 11699*, 2019, pp. 235–250. doi: 10.1007/978-3-030-26250-1_19.

[100] S. Nie, L. Liu, and Y. Du, "FREE-FALL : HACKING TESLA FROM WIRELESS TO CAN BUS," *Keen Security Lab of Tencent*, pp. 1–16, 2017.

[101] T. Keen Security Lab, "Experimental Security Research of Tesla Autopilot," Mar. 2019. Accessed: Jan. 28, 2024. [Online]. Available: https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Research_of_Tesla_Autopilot.pdf

[102] D. S. Fowler, J. Bryans, M. Cheah, and P. Wooderson, "A Method for Constructing Automotive Cybersecurity Tests , a CAN Fuzz Testing Example," in *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, IEEE, 2019, pp. 1–8. doi: 10.1109/QRS-C.2019.00015.

[103] M. Muter and N. Asaj, "Entropy-based anomaly detection for in-vehicle networks," in *2011 IEEE Intelligent Vehicles Symposium (IV)*, Baden-Baden: IEEE, Jun. 2011, pp. 1110–1115. doi: 10.1109/IVS.2011.5940552.

[104] T. Matsumoto, M. Hata, M. Tanabe, K. Yoshioka, and K. Oishi, "A Method of Preventing Unauthorized Data Transmission in Controller Area Network," in *2012 IEEE 75th Vehicular Technology Conference (VTC Spring)*, Yokohama: IEEE, May 2012, pp. 1–5. doi: 10.1109/VETECS.2012.6240294.

[105] M. Gmiden, M. H. Gmiden, and H. Trabelsi, "An intrusion detection method for securing in-vehicle CAN bus," in *2016 17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, Sousse,: IEEE, Dec. 2016, pp. 176–180. doi: 10.1109/STA.2016.7952095.

[106] Kyong-Tak Cho and Kang G. Shin, "Fingerprinting Electronic Control Units for Vehicle Intrusion Detection," in *25th USENIX Security Symposium*, Austin: USENIX Association, Aug. 2016, pp. 910–927.

[107] C. Valasek and Charlie Miller, "A Survey of Remote Automotive Attack Surfaces," Jul. 2014.

[108] A. S. Siddiqui, Y. Gui, J. Plusquellic, and F. Saqib, "Secure communication over CANBus," in *2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Boston: IEEE, Aug. 2017, pp. 1264–1267. doi: 10.1109/MWSCAS.2017.8053160.

[109] Z. Tyree, R. A. Bridges, F. L. Combs, and M. R. Moore, "Exploiting the Shape of CAN Data for In-Vehicle Intrusion Detection," in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, Chicago: IEEE, Aug. 2018, pp. 1–5. doi: 10.1109/VTCFall.2018.8690644.

[110] D. Basavaraj and S. Tayeb, "Towards a Lightweight Intrusion Detection Framework for In-Vehicle Networks," *Journal of Sensor and Actuator Networks*, vol. 11, no. 1, pp. 1–20, 2022, doi: 10.3390/jsan11010006.

[111] S. Adly, A. Moro, S. Hammad, and S. A. Maged, "Prevention of Controller Area Network (CAN) Attacks on Electric Autonomous Vehicles," *Applied Sciences (Switzerland)*, vol. 13, no. 16, pp. 1–23, 2023, doi: 10.3390/app13169374.

[112] F. W. Alsaade and M. H. Al-Adhaileh, "Cyber Attack Detection for Self-Driving Vehicle Networks Using Deep Autoencoder Algorithms," *Sensors*, vol. 23, no. 8, pp. 1–26, 2023, doi: 10.3390/s23084086.

[113] M. Amoozadeh *et al.*, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 126–132, Jun. 2015, doi: 10.1109/MCOM.2015.7120028.

[114] N. Ekedebe, W. Yu, H. Song, and C. Lu, "On a simulation study of cyber attacks on vehicle-to-infrastructure communication (V2I) in

Intelligent Transportation System (ITS)," in *Mobile Multimedia/Image Processing, Security, and Applications 2015*, S. S. Agaian, S. A. Jassim, and E. Y. Du, Eds., Baltimore,: SPIE, May 2015, p. 94970B. doi: 10.1117/12.2177465.

[115]J. Grover, M. S. Gaur, V. Laxmi, and N. K. Prajapati, "A sybil attack detection approach using neighboring vehicles in VANET," in *Proceedings of the 4th international conference on Security of information and networks*, New York, NY, USA: ACM, Nov. 2011, pp. 151–158. doi: 10.1145/2070425.2070450.

[116]W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A security credential management system for V2V communications," in *2013 IEEE Vehicular Networking Conference*, Boston: IEEE, Dec. 2013, pp. 1–8. doi: 10.1109/VNC.2013.6737583.

[117]M. Alimohammadi and A. A. Pouyan, "Sybil attack detection using a low cost short group signature in VANET," in *2015 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, Rasht: IEEE, Sep. 2015, pp. 23–28. doi: 10.1109/ISCISC.2015.7387893.

[118]J. Li, H. Lu, and M. Guizani, "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 938–948, Apr. 2015, doi: 10.1109/TPDS.2014.2308215.

[119]S. Taha, M. Alhassany, and X. Shen, "Lightweight Handover Authentication Scheme for 5G-Based V2X Communications," in *2018 IEEE Global Communications Conference (GLOBECOM)*, IEEE, Dec. 2018, pp. 1–6. doi: 10.1109/GLOCOM.2018.8648020.

[120]C. Xu, X. Huang, M. Ma, and H. Bao, "A Secure and Efficient Message Authentication Scheme for Vehicular Networks based on LTE-V," *KSII Transactions on Internet and Information Systems*, vol. 12, no. 6, Jun. 2018, doi: 10.3837/tiis.2018.06.022.

[121]S. Tangade, S. S. Manvi, and P. Lorenz, "Trust Management Scheme Based on Hybrid Cryptography for Secure Communications in VANETs," *IEEE Trans Veh Technol*, vol. 9545, pp. 1–12, 2020, doi: 10.1109/TVT.2020.2981127.

[122]H. Jiang, L. Hua, and L. Wahab, "SAES: A self-checking authentication scheme with higher efficiency and security for VANET," *Peer Peer Netw Appl*, vol. 14, no. 2, pp. 528–540, Mar. 2021, doi: 10.1007/s12083-020-00997-0.

[123]J. Miao, Z. Wang, X. Ning, N. Xiao, W. Cai, and R. Liu, "Practical and secure multifactor authentication protocol for autonomous vehicles in 5G," *John Wiley & Sons, Ltd*, pp. 1–18, 2022, doi: 10.1002/spe.3087.

[124]R. Ma, J. Cao, D. Feng, H. Li, X. Li, and Y. Xu, "A robust authentication scheme for remote diagnosis and maintenance in 5G V2N," *Journal of Network and Computer Applications*, vol. 198, p. 103281, Feb. 2022, doi: 10.1016/j.jnca.2021.103281.

[125]H. P. Hyunhee Park, "Edge Based Lightweight Authentication Architecture Using Deep Learning for Vehicular Networks," *Journal of Internet Technology*, vol. 23, no. 1, pp. 195–202, Jan. 2022, doi: 10.53106/160792642022012301020.

[126]Q. Li, "A V2V Identity Authentication and Key Agreement Scheme Based on Identity-Based Cryptograph," *Future Internet*, vol. 15, no. 1, p. 25, Jan. 2023, doi: 10.3390/fi15010025.

[127]J. Noh, Y. Kwon, J. Son, and S. Cho, "Blockchain-Based One-Time Authentication for Secure V2X Communication Against Insiders and Authority Compromise Attacks," *IEEE Internet Things J*, vol. 10, no. 7, pp. 6235–6248, Apr. 2023, doi: 10.1109/JIOT.2022.3224465.

[128]X. Feng, X. Wang, H. Liu, H. Yang, and L. Wang, "A Privacy-Preserving Aggregation Scheme With Continuous Authentication for Federated Learning in VANETs," *IEEE Trans Veh Technol*, vol. 73, no. 7, pp. 9465–9477, Jul. 2024, doi: 10.1109/TVT.2024.3369942.

[129]L. Zhang, "OTIBAAGKA : A New Security Tool for Cryptographic Mix-Zone Establishment in Vehicular Ad Hoc Networks," *IEEE Transactions on Information Forensics and Security*, pp. 1–13, 2017, doi: 10.1109/TIFS.2017.2730479.

[130]A. Riahi Sfar, Y. Challal, P. Moyal, and E. Natalizio, "A Game Theoretic Approach for Privacy Preserving Model in IoT-Based Transportation," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 12, pp. 4405–4414, 2019, doi: 10.1109/TITS.2018.2885054.

[131]S. A. A. Hakeem, M. A. A. El-gawad, and H. Kim, "Comparative Experiments of V2X Security Protocol Based on Hash Chain Cryptography," *MDPI Sensors*, vol. 5719, no. 20, pp. 2–23, 2020.

[132]C. Zhao, N. Guo, T. Gao, X. Deng, and J. Qi, "PEPA: Paillier cryptosystem-based efficient privacy-preserving authentication scheme for VANETs," *Journal of Systems Architecture*, vol. 138, pp. 1–10, 2023, doi: 10.1016/j.sysarc.2023.102855.

[133]U. Khan, S. Agrawal, and S. Silakari, "Detection of Malicious Nodes (DMN) in vehicular ad-hoc networks," *Procedia Comput Sci*, vol. 46, pp. 965–972, 2014, doi: 10.1016/j.procs.2015.01.006.

[134]H. Sedjelmaci and S. M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks," *Computers and Electrical Engineering*, vol. 43, pp. 33–47, 2015, doi: 10.1016/j.compeleceng.2015.02.018.

[135]M. J. Kang and J. W. Kang, "Intrusion Detection System using Deep Neural Network for In-Vehicle Network Security," *PLoS One*, vol. 11, no. 6, pp. 1–17, 2016, doi: 10.1371/journal.pone.0155781.

[136]S. M. Sangve, R. Bhati, and V. N.Gavali, "Intrusion Detection System for Detecting Rogue Nodes in Vehicular Ad-hoc Network," in *2017 International Conference on Data Management, Analytics and Innovation (ICDMAI)*, Pune, India: IEEE, 2017, pp. 127–131.

[137]A. Anwar, T. Halabi, and M. Zulkernine, "A coalitional security game against data integrity attacks in autonomous vehicle networks," *Vehicular Communications*, vol. 37, pp. 1–10, 2022, doi: 10.1016/j.vehcom.2022.100517.

[138]P. K. Singh, S. Kumar Jha, S. K. Nandi, and S. Nandi, "ML-Based Approach to Detect DDoS Attack in V2I Communication Under SDN Architecture," in *TENCON 2018 - 2018 IEEE Region 10 Conference*, Jeju: IEEE, Oct. 2018, pp. 0144–0149. doi: 10.1109/TENCON.2018.8650452.

[139]G. O. Anyanwu, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "RBF-SVM kernel-based model for detecting DDoS attacks in SDN integrated vehicular network," *Ad Hoc Networks*, vol. 140, p. 103026, Mar. 2023, doi: 10.1016/j.adhoc.2022.103026.

[140]M. Zhao, D. Qin, R. Guo, and G. Xu, "Efficient Protection Mechanism Based on Self-Adaptive Decision for Communication Networks of Autonomous Vehicles," *Mobile Information Systems*, vol. 2020, pp. 1–9, Jun. 2020, doi: 10.1155/2020/2168086.

[141]A. Al-Sabaawi, K. Al-Dulaimi, E. Foo, and M. Alazab, "Addressing Malware Attacks on Connected and Autonomous Vehicles: Recent Techniques and Challenges," in *Malware Analysis Using Artificial Intelligence and Deep Learning*, Cham: Springer International Publishing, 2021, pp. 97–119. doi: 10.1007/978-3-030-62582-5_4.

[142]A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A Survey on Homomorphic Encryption Schemes," *ACM Comput Surv*, vol. 51, no. 4, pp. 1–35, Jul. 2019, doi: 10.1145/3214303.

[143]X. Sun, F. R. Yu, P. Zhang, W. Xie, and X. Peng, "A Survey on Secure Computation Based on Homomorphic Encryption in Vehicular Ad Hoc Networks," *Sensors*, vol. 20, no. 15, p. 4253, Jul. 2020, doi: 10.3390/s20154253.

[144]F. Zhuang *et al.*, "A Comprehensive Survey on Transfer Learning," *Proceedings of the IEEE*, vol. 109, no. 1, pp. 43–76, Jan. 2021, doi: 10.1109/JPROC.2020.3004555.