EXAMINING MODERN DATA SECURITY AND PRIVACY PROTOCOLS IN AUTONOMOUS VEHICLES

Mingfu Huang, Rushit Dave, Nyle Siddiqui and Naeem Seliya

Department of Computer Science,
University of Wisconsin, Eau Claire, Eau Claire, USA

ABSTRACT

A fully automated, self-driving car can perceive its environment, determine the optimal route, and drive unaided by human intervention for the entire journey. Connected autonomous vehicles (CAVs) have the potential to drastically reduce accidents, travel time, and the environmental impact of road travel. Such technology includes the use of several sensors, various algorithms, interconnected network connections, and multiple auxiliary systems. CAVs have been subjected to attacks by malicious users to gain/deny control of one or more of its various systems. Data security and data privacy is one such area of CAVs that has been targeted via different types of attacks. The scope of this study is to present a good background knowledge of issues pertaining to different attacks in the context of data security and privacy, as well present a detailed review and analysis of eight very recent studies on the broad topic of security and privacy related attacks. Methodologies including Blockchain, Named Data Networking, Intrusion Detection System, Cognitive Engine, Adversarial Objects, and others have been investigated in the literature and problem- and context-specific models have been proposed by their respective authors.

KEYWORDS

Security & Privacy, Autonomous Vehicles, Blockchain, Connected Autonomous Vehicles.

1. INTRODUCTION

Technology has improved people's lives in many ways with the introduction of microprocessors embedded into computing systems, such as smart devices, home automation, and other similar systems. A field of embedded systems is connected autonomous vehicles (CAV), where many new and large car manufactures, who are famous for their gas-powered engines, are now spending considerable monetary and other resources into CAVs development. CAVs, when connected through vehicle to roadside infrastructures links (V2I) and vehicle to vehicle links (V2V), require less human interaction than traditional vehicles. The advantage to that not only includes liberating drivers from holding the steering wheel and focusing on the traffic, but also plays an important role in reducing human error-based traffic accidents thus improving traffic conditions [1]. A fully automated, self-driving car can perceive its environment, determine the optimal route, and drive unaided by human intervention for the entire journey [47]. Further, self-driving cars have the potential to drastically reduce accidents, travel time, and the environmental impact of road travel [48].

These technologies are attained based on using several sensors, network connections, algorithms, and other auxiliary systems. Together, they constitute the driving assist functions in CAVs, including adaptive cruise control, lanes monitoring system, etc. Despite the benefit it brings to drivers, they increase the possibility for hackers to access vehicles with malicious intent [17, 45]. For example, a hacker can perform data injection attacks on the connections between the cameras

and the electronic control unit (ECU), disrupting the vehicle from receiving accurate images. For the modern CAV, there could be more than 70 embedded ECUs. To accurately perceive the traffic conditions, an ordinary CAV should possess many different types of sensors, including, but not limited to, cameras, LiDAR (Light Detection and Ranging), and GPS (Global Positioning System) [46]. To facilitate real-time maneuvering decision, they need connection capabilities such as 4G or 5G, as well as V2V and V2I communications [2]. Each of these sensors or connected systems provides fundamental data and information for decision making in CAVs. Any failures in these systems and gadgets, could lead to shutting down of the whole autonomous system, and consequentially, causing passenger injury or death as well as property loss [3].

The focus of this paper is reviewing selected works on the topic of privacy and data security in CAVs. In the literature, considerable research has been done to ensure the robustness of the CAVs. As the research area of CAVs is quite large, reviewing all the possible solutions proposed in the literature to protect CAVs from malicious behavior is out of scope for this paper. We limit our study to the problem of privacy and data security in the context of CAVs. The following attacks could be subjected upon a CAV: attacks exploiting the vulnerabilities in various sensors of a vehicle, vehicular ad hoc network (VANET) attacks, hardware exploits and adversarial attacks. For example, an attack exploiting the vulnerabilities in various sensors of a CAV, the GPS in the vehicle can be manipulated by hackers to possible change planned directions mapped and provided by the GPS. In the case of VANET attacks, a hacker can connect to another vehicle using the V2V link and then transmit malicious data or receive sensitive information [4].

This paper will review selected works that focus on the attacks targeting data stream and user privacy among sensors and inter-vehicle networks. As mentioned previously, the importance of different systems failures causing severe consequences is critical. This paper will provide an in-depth review and elaborate upon some of the existing proposed solutions aiming to detect or mitigate the attacks on CAVs. This paper will focus on two primary topics related to CAVs: attacks exploiting the vulnerabilities in various sensors of vehicle and VANET attacks.

The data provided from the sensors are crucial for CAVs to calculate proper system routines and perform proper behavior, it helps vehicles to perceive real time road conditions such as knowing the space between cars surrounding the CAV, reading the traffic signs, and recognizing lanes directions. Thus, CAVs are susceptible to attacks performed on the various sensors. Attacks that disrupt sensors from accurately recognizing road and driving conditions can mislead the CAV causing it to make incorrect decision which could potentially create and untoward emergency. VANET is designed to be ancillary to a CAV's system by providing additional data resources through exchanging the information of identity or traffic situation. If an attacker, pretending to be a normal, establishes communication to vehicle or road infrastructure, they can broadcast malicious information or receive other users' private information. The privacy among the CAVs is thus exposed to the attackers and the VANET is then no longer credible as per its design.

The rest of the paper is structured as follows: Section 2 provides some background information related to CAVs; Section 3 provides an in-depth review of selected related papers, Section 4 provides the limitations of the current research work and pros and cons of the selected related papers, and Section 5 provides our paper's conclusion including some topics for future research.

2. BACKGROUND

Devices such as cameras, LiDAR, and GPS constitute the general cognition system on CAVs. For cameras and LiDAR, their jobs are to recognize local traffic situation such as traffic signs, distance to surrounding vehicles, lanes direction, etc. They collect these data and send it to the vehicle's computer, providing sufficient information to help the CAV's system computer to

detect and model the surrounding environment. The CAV can then implement functions that decide what behavior the vehicle should perform. GPS, being different from the previously mentioned devices, is connecting the CAV to satellites and computes the vehicle positioning and localization information, which is subsequently used to determine a proper route to the destinations. VANET is a feature that helps CAV gain information from beyond its sensors. This is done by connecting to the roadside infrastructures (V2I) and the communications between CAVs (V2V). Information from these devices is utilized to ensure the CAVs can function properly. It is thus crucial to have security methodologies to protect data from any kind of hacking which could lead to data breach in CAVs.

To protect the data in the sensors to vehicle communications, many researchers have developed methodologies that can prevent data alteration as well as mitigate the effect from an attack. Changalvala et al. [29] propose a method that inserts a binary watermark into LiDAR data using a three-dimensional quantization index modulation, which prevents attacks related to fake object insertion and target object deletion. Sun et al. [13] use a black-box spoofing attack approach to assess LiDAR's robustness and then propose the sequential view fusion (SVF) to reduce the high success rate of black-box attack to the LiDAR. Cao et al. [14] test the Baidu Apollo autonomous driving platform with their proposed black-box attack algorithms and reveal vulnerabilities of CAVs that are based on LiDAR. Shin et al. [12] reveal the vulnerability of LiDAR in that it could be completely incapacitated from sensing a certain direction of the moving vehicle.

Lim et al. [43] assess the vulnerability and impact of ultrasonic sensors in CAVs. Machine learning algorithms, for example K-NN, Random Forest, and Logistic Regression, are examined for detecting attacks in the context of CAVs [44]. The network environment associated with CAVs also provide opportunities for malicious entities to assess and attack vulnerabilities [15][16]. The authors of [27] and [38] propose a method to classify safety and security problems in CAVs including vulnerabilities of both vehicle sensors and of VANET. Their respective classification methods would be helpful for designing security-based models in CAVs research. Dutta et al. [18] propose a method based on the modified Kalman filter and a Chi-squared detector which increases the credibility of adaptive cruise control of CAVs; thereby, potentially preventing hazards during an attack. Ferdowsi et al. [37] investigated a multi-armed bandit algorithm to detect and mitigate the effect from physical attacks.

Compared to attacks on a fixed network infrastructure, CAVs present added security and privacy complexities due to the continuous movement of such vehicles during active operation. The published works of [10][41] investigate the blockchain technique in the context of CAVs, where blockchain is used to develop the tracking system of CAVs, providing a more secure storage of information as well as an improved entity detection system. In addition to providing an alternate way of data storage, blockchain is also used for implementing update schemes. Baza et al. [42] proposed a distributed firmware update scheme for autonomous vehicles' subsystem, which aims to provide a faster update delivery without any dependency on third party firmware update systems. Mahmud et al. [22] propose a software upload method using wireless communication links which require the supplier to send two or more copies of the upload file toward preventing any malicious changes in the upload file. An issue with using blockchain for implementing update schemes is that it increases the energy usage in CAVs. Sharma [11] illustrates this problem and proposes an energy-efficient model which optimally controls the number of transactions through distributed clustering in the blockchain-based update scheme.

Chowdhury et al. [20] present an internet-based architecture using named data networking (NDN) and which includes a four-level hierarchical trust model and a vehicle manufacturer related naming model for the purpose of data authentication. Qian et al. [23] provide a cognitive engine-based security algorithm for the lack of global cognitive control in traditional CAVs, where the

approach also reduces information transmission delay. Ansari et al. [39] investigate 5G in the context of VANET's privacy preservation and network security and propose a framework implementing multiple radio access technologies and a cloud radio access network. Huang et al. [24], in the context of a secure automated valet parking system, investigate a privacy-preserving reservation scheme for autonomous vehicles. Their proposed valet parking system for CAVs is modeled to prevent any of the parking provider from accessing user information while avoiding malicious behavior, such as reserving multiple parking lots for just one vehicle. In CAV networks connectivity and safety, an intrusion detection system is an important element as it assists in discriminating normal and anomalous behavior with relatively high accuracy. Most such systems are based on machine learning schemes and other schemes [26, 28, 31, 32, 34], such as the proportional overlapping scoring method [9].

3. LITERATURE REVIEW

Rathee et al. [10] investigate online cab booking services in the context of connected vehicles as a service (CVaaS). The authors contend that to ward of malicious users from malintent on the internet of vehicles, a blockchain scheme is the best approach that provides protection in real-time conditions. In online cab booking services it is possible, under a malicious attack, for a drive to extend harmful behaviors to the whole system, including altering stored information or compromise sensor scores that monitor the system. The authors state there does not exist a good tracking technology for CAVs that oversees the sensors or driver's behavior during a cab's trip. A blockchain security technique is proposed for online cab booking services. IoT devices connected to a CAV would register in the blockchain network before they can provide services, and their vehicle number and rating is stored. The blockchain network is combined with peer and miner nodes responsible for generating cryptographical keys and verify authentication. Various managers are used to secure the network and a secondary blockchain manager prevents any failures of the primary managers. When new vehicle joins the system, the IoT device sends request to the peer manager and the miner nodes will verify the authentication. Subsequently, miners generate share key for IoT which is used to connected peer nodes and IoT devices. Blockchain can be maintained with a hash and each block contains data of IoT devices attached with previous through the hash, so that any alteration in the network can be identified. Their case study is based on the network simulator version 2 (NS2) with a 700 x 700 m grid facet and having network sizes of 50 nodes. The initial rating is randomly assigned, and the intruder types include forging the identity of legitimate devices or hacking legitimate IoT sensors. Attacking nodes were added at the rate of 10% of the normal nodes to validate the authentication and the invasion of IoT indicated that 2 out of 5, 10 out of 20, and 20 out of 50 devices were compromised in a unit of time [10]. The proposed framework reduces the users' fake request, compromise of IoT devices and the alteration in the stored users' ratings, compared to the compared existing method, a 79% success rate is attained.

Figure 1 depicts the architectural framework of CAVs using the blockchain technique where all the vehicles are connected to IoT sensors or smart devices in order to control, monitor and guide the drivers on the road. The number of vehicles connected to the IoT devices or sensors depend upon their communication and transmission ranges. The vehicle number, ratings given by customers, and users' IoT devices are stored in ordinary tables as well as in the blockchain network to record each legal and illegal activity of the vehicle or IoT devices.

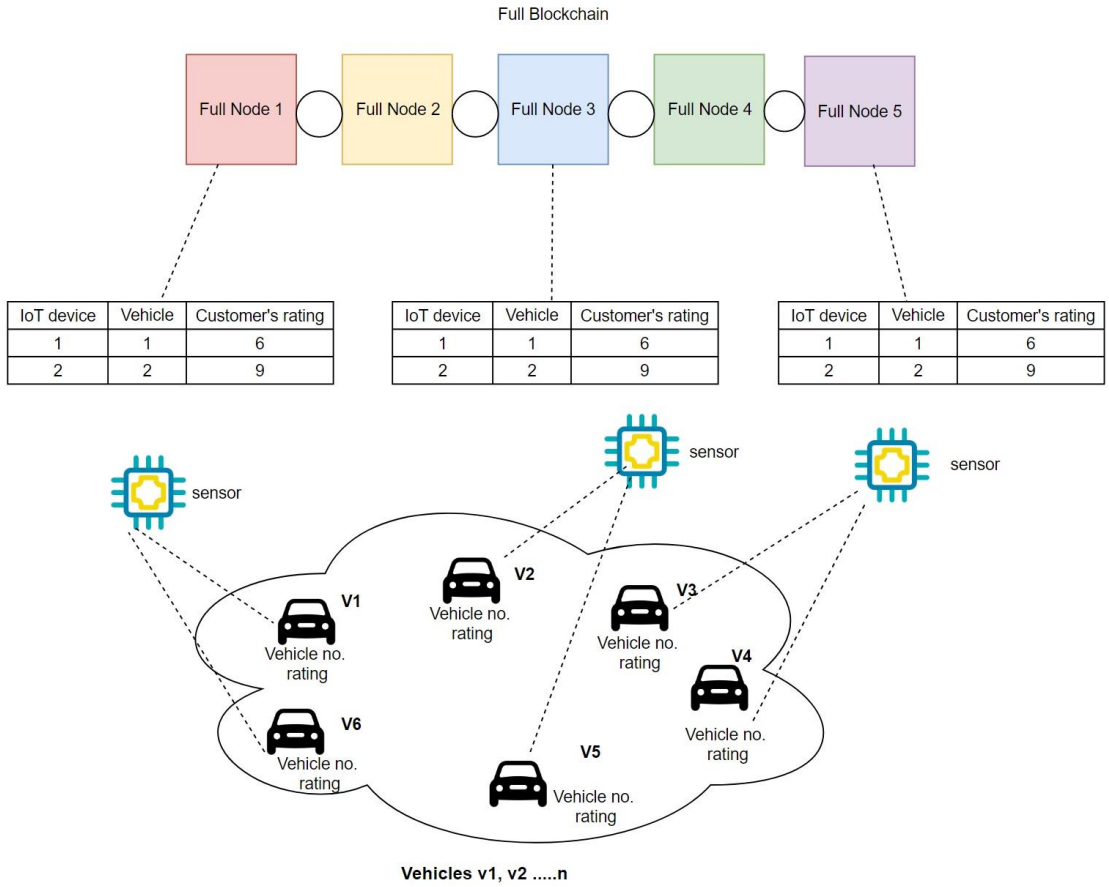

Figure 1. The architectural framework of a connected vehicle blockchain. Information is stored separately across full nodes in the network to reinfoce data security.

Sharma [11] focuses on reducing the energy consumption of a blockchain network in the VANET. As mentioned previously, the high number of transactions in a blockchain technique in CAVs require high energy consumption. In addition, security requirements for cryptography algorithms also warrant a high degree of energy consumption. Considering these issues, the author proposes adding distributed clustering into the traditional blockchain approach, which helps reduce number of transactions by finding optimal slots for updating the blockchain. The more traditional blockchain approach is compared with the proposed approach. Empirical results indicate that the proposed method helps conserve energy over 40% and reduces the number of transactions by over 82%, both as compared to traditional blockchain technology in CAVs.

Alheeti et al. [8][9] investigate ensuring driverless cars with emergency cooperative awareness messages (CAMs). Certain characteristics of VANET, such as high mobility, quick changing networks topology, and general absence of fixed security infrastructures have made the security of CAVs more exposed to unique attacks, such as black hole, gray hole [26], and DoS (Denial of Service) [9] attacks. The authors largely focus on black hole attacks and propose an intrusion detection system (IDS) targeting real time detection and isolation of the malicious user. A black hole attack is defined as a vehicle who drops all the received data from proximity vehicles. A feed-forward neural network is investigated to detect normal vs. abnormal behavior, where the data is collected using NS2 to model a VANET environment. A simulation of the Urban Mobility Model (SUMO) and Mobility Vehicle (MOVE) is used as input to the NS2 for generating the dataset. Proportional Overlapping Scores (POS) is used to increase efficiency and accuracy of the

IDS, and in addition, fuzzy set logic is incorporated to reduce classification error. The 60,000 records' dataset was divided into a 50% training set, 25% validation set, and 25% testing set. Their empirical framework consisted of two malicious vehicles representing black hole attacks, 38 normal vehicles, and nine roadside units (RSUs). The proposed method's classification accuracy ranged from 99.72% to 99.98%, compared to a fuzzy logic-based classification scheme which yielded an overall accuracy rate ranging from 85.02% to 99.12%.

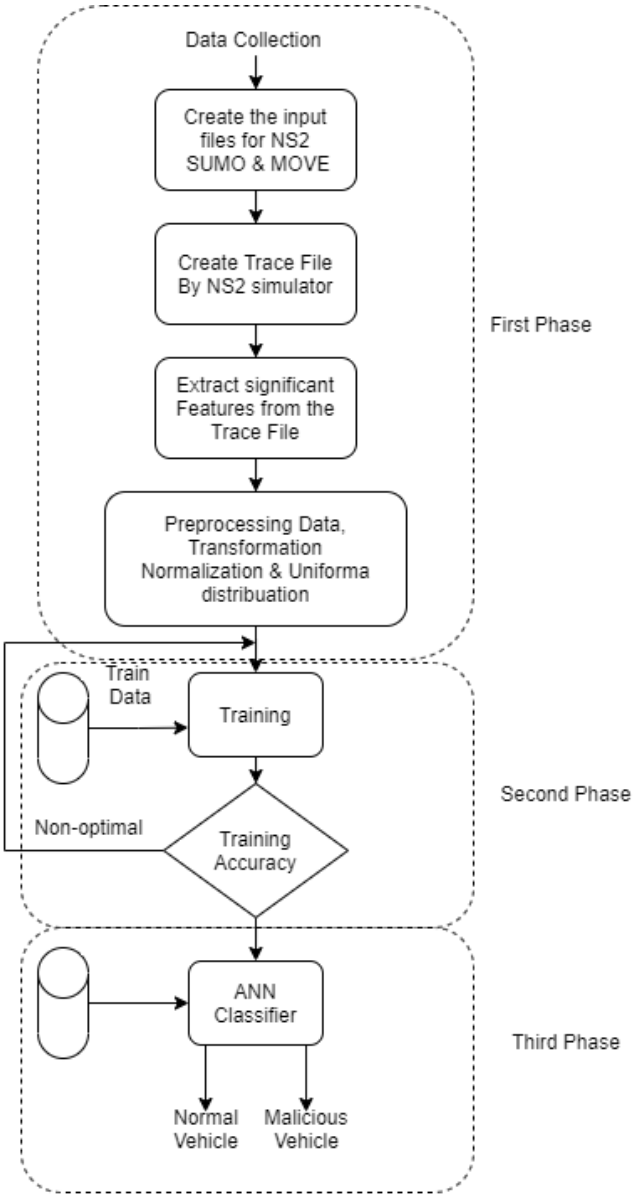

Figure 2. Overall architecture of the proposed IDS. In the first stage, the normal and malicious behavior for vehicles is built into the NS2, and a dataset is generated from the trace file [9].

Additional features are extracted from this trace file and are preprocessed using normalization, transformation and uniform distribution methods. The second stage consists of training the artificial neural network (ANN) on the extracted dataset. Lastly, the ANN is tasked with utilizing the extracted features in order to differentiate between malicious and normal behavior.

Cao et al. [14] discuss a problem in CAVs in that a small perturbation in the expected data specifications can cause well-trained prediction models to fail in detecting adversarial events. Sensors such as LiDAR and RADAR generally detect objects using laser beams, which raises the question that if texture-based differences of similar objects would affect their detection efficacy and performance. Moreover, LiDAR-based object detection systems consist of multiple non-separable steps which may limit the gradient based end-to-end attacks [14]. To counter these possible issues, the authors propose a system (LiDAR-Adv) to evaluate the impact that an adversarial object may have on the Apollo platform, an industrial real-world LiDAR-based system for CAVs. The authors are the first to exploit the impact of an adversarial object on a real-world LiDAR system. To generate an adversarial object, authors design an end-to-end attacking pipeline. An approximated differentiable renderer is implemented into the design of the object whose intention is to facilitate gradient-based algorithm. The experiment is set up using the Baidu Apollo Autonomous Driving platform, and a fully differential LiDAR simulator with predefined laser beam. Initially, a black box attack is implemented with the goal of hiding the object and to clearly indicate the LiDAR-based detection system has the specified vulnerability. Subsequently, the experiment tests the efficacy of the adversarial object with the aim of "hiding" and "changing label", the results of which shows the adversarial object yields a 71% attack success rate when the object size is 50 cm. Post these steps, the authors employ 3D printing to generate the object in the real-world and test the detection of the same with a real-world AV. Once again it is shown that the object is not detected by the LiDAR-based detection system, revealing an important vulnerability of such systems, thus, requiring a stronger detection system. Table 1 shows the attack success rates of LiDAR-Adv at different distances and different orientations under both controlled and unseen (previously unknown) settings. It is also shown that the that the generated robust adversarial object can achieve the attack goal of hiding the object with a high success rate.

Table 1: Adversarial Object Detection Performance

Controlled Setting		Unseen Setting			
Distance (cm) & Orientation (°)	Attack	Distance (cm)		Orientation (°)	
		0-50	50-100	0-5	0-10
{0, ±50} * {0, ±2.5, ±5}	41/45	96/100	91/100	10/10	9/40
{0, ±50} * {0, ±2.5, ±5}	43/45	96/100	90/100	8/10	10/10

Chowdhury et al. [20] provide a new network architecture for VANET, called Named Data Networking (NDN), which aims to help detect false data while preserving privacy of CAV users. The challenges presented by the high mobility of CAVs, and security vulnerabilities therein are targeted by the proposed solution in [20]. While existing peer-to-peer and channel-based communication cannot support an effective data distribution and high data security in the presence of high mobility vehicles, NDN does not depend on the fixed IP addresses and locations. The paper proposes a trust-model that is a four-level hierarchy including CAVs organizations, manufacturers, vehicles, and data. The organizations are responsible for certifying keys for manufacturers who in turn certify keys of its vehicles who certify their own data. This technique reduces the possibility of accepting false information. To prevent any malicious tracking, the approach requires vehicles have a set of pseudonyms, and a Certificate Issuing Proxy (CIP) system that requests certificates on a vehicle's behalf. The proposed approach prepared three vehicles equipped with different specifications of chips, one root organization, and three manufacturers. The authors are interested in the total delay between the time when a vehicle sends a specific interest and the time when it validates the received data, thus requiring evaluating Data Fetching Delays, Certificate Fetching Delay, Data Validation Delay, Data Signing Delay (RAS is used for data signing) and Certificate Sending Delay. Two vehicles operate simultaneously and ten times in total, where one is a consumer, and the other is a

producer. Empirical results indicate that lower the power of processor of the producer, the higher is the data signing delay and certification fetching delay. Figures 3a-f depict the results of [20] and indicate good performance by RPi2 and RPi3. [20] further states that since a real-world vehicle can be equipped with more powerful CPUs, the respective delays are likely to be shorter with increased computational power.

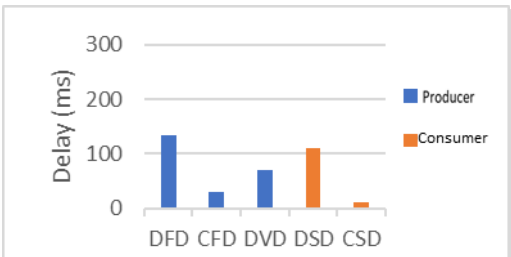

Figure 3a. Consumer (RPi1) and Producer (RPi2)

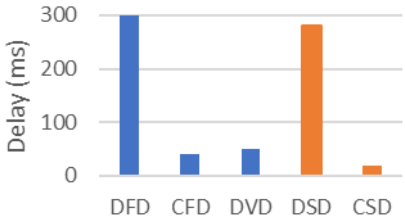

Figure 3b. Consumer (RPi2) and Producer (RPi1)

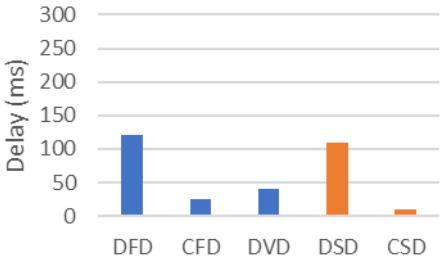

Figure 3c. Consumer (RPi3) and Producer (RPi2)

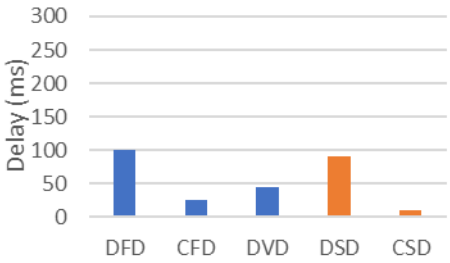

Figure 3d. Consumer (RPi2) and Producer (RPi3)

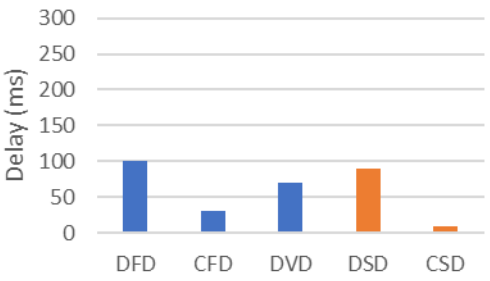

Figure 3e. Consumer (RPi1) and Producer (RPi3)

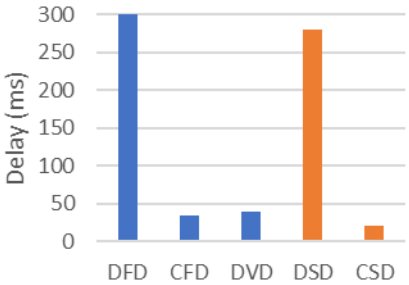

Figure 3f. Consumer (RPi3) and Producer (RPi1)

Changalvala et al. [29] focus on the authentication strategy for data security from the LiDAR system. An in-vehicle sensor communication is typically not encrypted; thus, if an attacker accesses the target network with malicious intent, it would be possible to carry out attacks such as fake object detection or target object deletion on the target CAV. Generally, data encryption and information hiding are two ways used during an integrity verification procedure [29]. Data encryption requires the system to encrypt/decrypt data lending to system process delays which has an adverse impact for an advanced driver assistance system (ADAS). Instead, the authors employ a process based on digital watermarking for integrity verification and use quantization index modulation (QIM) during their approach. Upon receiving 3D point data from the sensors, multiple quantizers are implemented to reconstruct the points for establishing interconnectivity between them. A voxel model is set up where all the points are quantized with a specific step

size. During the implementation of the QIM approach additional information can be embedded into each point via modification of the position vector of each point. The framework presented is composed of information hiding in the LiDAR sensors' unit, a point cloud verification and tampering detection method, and a localization process in the ADAS. The authors use the KITTI benchmark dataset and use it to train the object detection model as well as for evaluating the performance of their integrity verification method. The empirical work is composed of three parts: study the impact of embedding distortion on the performance of the ADAS, investigating embedding distortion analysis, and studying and analyzing the system's robustness. The proposed approach attains a 100% success rate at detecting and localizing tampering in the KITTI data set in the context when noise is within the quantization step size. The authors state that the model can be used in the other 3D point cloud data generating sensors where a dynamic message embedding technique is required.

Figure 4 summarizes the authors' proposed approach in a self-descriptive block diagram. Based on the correlation values and pattern matching between the embedded and extracted messages, the indices of the received signal where the embedded and extracted messages do not match are determined. From these indices, the corresponding LiDAR frame points are labelled as tampered, traced, and localized.

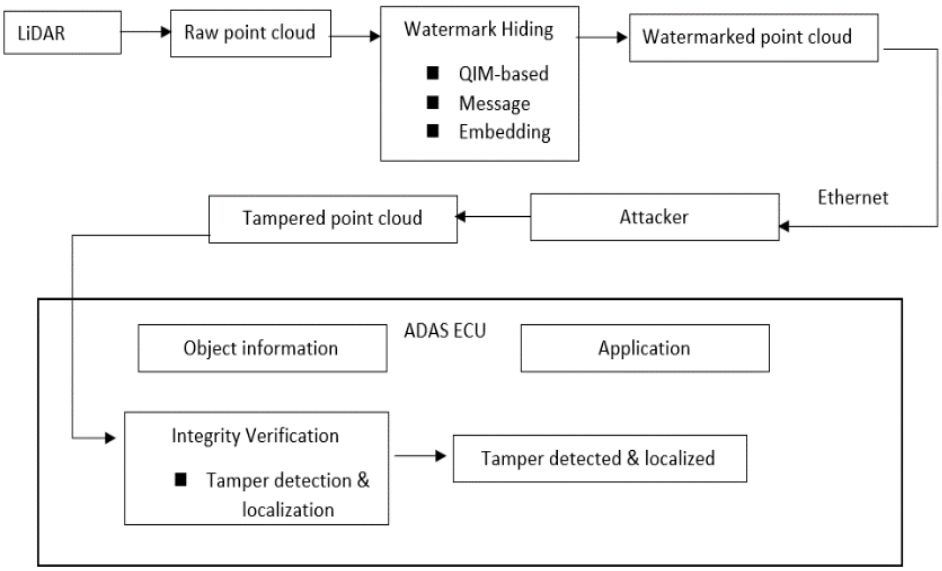

Figure 4. Autonomous vehicle general architecture

Sun et al. [13] investigate the issue of occlusion of LiDAR-based object detection, representing the area behind the target hit point from the LiDAR system's perspective. When a vehicle is in the front of a CAV, there will be relatively fewer hit points received by the sensors. However, if an external actor with malicious intent uses devices that duplicate the LiDAR laser beams to target the CAV, the latter may likely consider that false target to be a vehicle and perform unwarranted behaviors. The authors confirm this vulnerability in LiDAR-based CAVs and propose an occlusion-aware hierarchical anomaly detection solution (named, CARLO). The system is composed of two phases: free space (FS) detection, i.e., drivable area without any objects, and laser penetration detection. The former checks the ratio of FS volume to the volume of detected objects' bounding box, while the latter checks the ratio f the number of points behind the objects' detected to the total number of points. A spoof attack is identified when, if either/both of those ratios violate the physical law, i.e., not within the (0,1) limits. An empirical

case study is performed with the KITTI training, validation, and testing datasets. The CARLO model's evaluation is performed using the attack success rate (ASR), precision rate, and recall rate. The ASR metric indicates the direct performance of the model. Three types of CAV models are tested in their case study: Apollo 5.0, PointPillars, and PointRCNN [13]. The empirical results show that CARLO is effective in lowering the ASR from about 95% to about 5.5% with a recall rate of about 95% for all models. A comparison of performance of Apollo 5.0 vs. CARLO-guarded Apollo 5.0 is shown via a graphical representation in Figure 5.

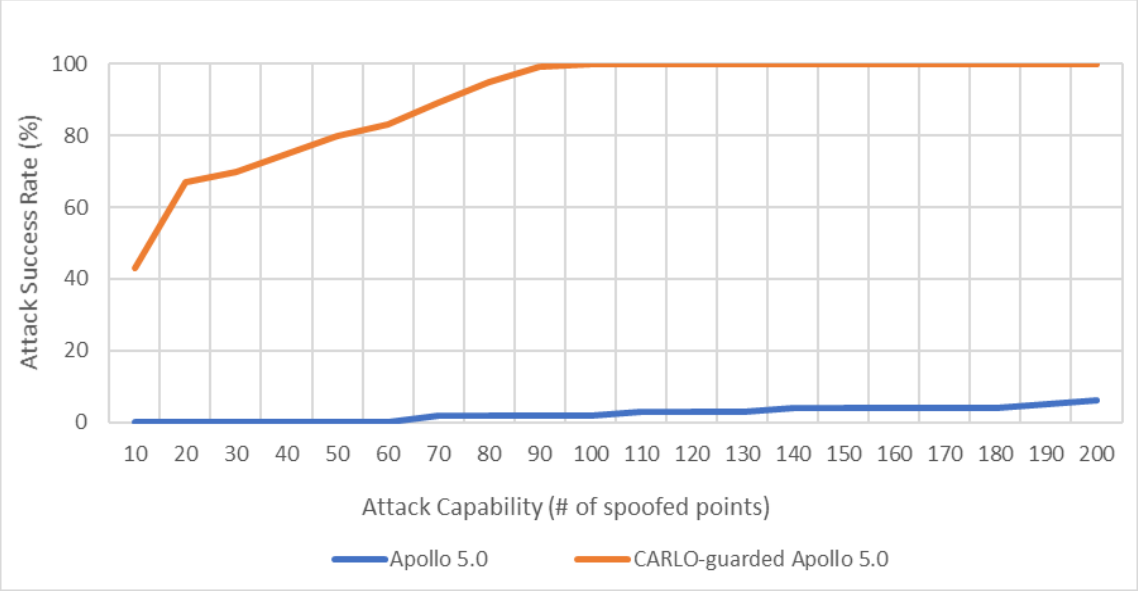

Figure 5. Attack success rates (ASRs) of Adv-LiDAR on Apollo 5.0 and CARLO-guarded model

He et al. [28] divides the CAV cyber security protocol into hardware, software, and data categories. The model of Unified Modelling Language (UML) is adapted into the CAV framework, defining the relationship between different components. The main classes in this UML-based CAV framework include Vehicle Data, Data Processor and Vehicle Functions. Several attack points are analyzed such as physical parts, software, data and communication channels. Thus, a CAV cyber security framework categorizing communication-based attacks is proposed in this paper. To simulate the network attack scenarios, [28] uses the KDD99 data set which includes Probing attacks, Denial of Service attacks, User-to-Root attacks, and Remote-to-Local attacks. The KDD99 is a data set that is commonly used as a benchmark for attack detection or online intrusion for computer and network security. Some attacks do not fit into the CAV cyber security framework or were not compatible with the CAV attack points, so before processing the dataset into the framework, these attacks are removed as well as any duplicates and other irrelevant attacks. This new data set which contains a filtered version of various attacks is called CAV-KDD. The experiment is done using the Weka library to construct and compare two classification models: Naïve Bayes and J48 (WEKA's implementation of a decision tree). Table 2 shows that while Naïve Bayes and J48 have almost the same accuracy, decision trees take less time to curate a decision despite their increased training times: a significant attribute for efficient CAV cyber security.

Table 2. Accuracy and runtime of J48 and Naive Bayes

Algorithm	Accuracy on 10-Folds Validation	Accuracy on the Testing Data Set	Time to Build Model(s)	Time on the Testing Data Set(s)
Naïve Bayes	99.42%	95.66%	0.15	3.38
J48	99.80	97.04%	2042	0.94

Baza et al. [42] proposes a distributed firmware update scheme using blockchain and smart contract technology. The architecture of this system operates on a decentralized blockchain network to verify and distribute manufacturer firmware updates to autonomous vehicles. Manufacturers release firmware updates and generate a corresponding smart contract with accompanying cryptographic keys. There are two types of AVs present in this architecture: distributors and responders. Each responder AV that receives an update can also act as a distributor of that update, ensuring the large-scale dissemination of the update quickly. The smart contract also contains the reputation of the distributor vehicles for future reference. The blockchain network executes the smart contracts in a distributed manner without relying on a central party. Attribute Based Encryption (ABE) is adopted when the manufacturers define the access policy. A rewarding phase follows after the definition of access policy, as the distributor sends a redeem transaction with multiple proofs to the smart contract, updating its reputation and the number of AVs to receive the update. The evaluation phase consists of a performance evaluation and a security analysis. In the performance evaluation, a distributor AV needs to broadcast a challenge packet encrypted by a number of attributes. After running two encryption algorithms, ABE and Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK), a proof is generated. The time to generate the proof is 6 seconds, whereas the verification is 5 milliseconds.

Figure 6 shows the architecture of its system: (1) The manufacturer creates a smart-contract for a new firmware update by including its hash code for authenticity checking by AVs. (2) The manufacturer sends the new update to top-reputation AVs (distributors). (3) A distributor exchanges an encrypted version of the update in return for proof of reception of the update by a responder AV. (4) A redeem transaction, containing multiple proofs, is sent to the smart contract to update the distributor's reputation. (5) The responder AV receives the decryption key of the firmware update from the smart contract.

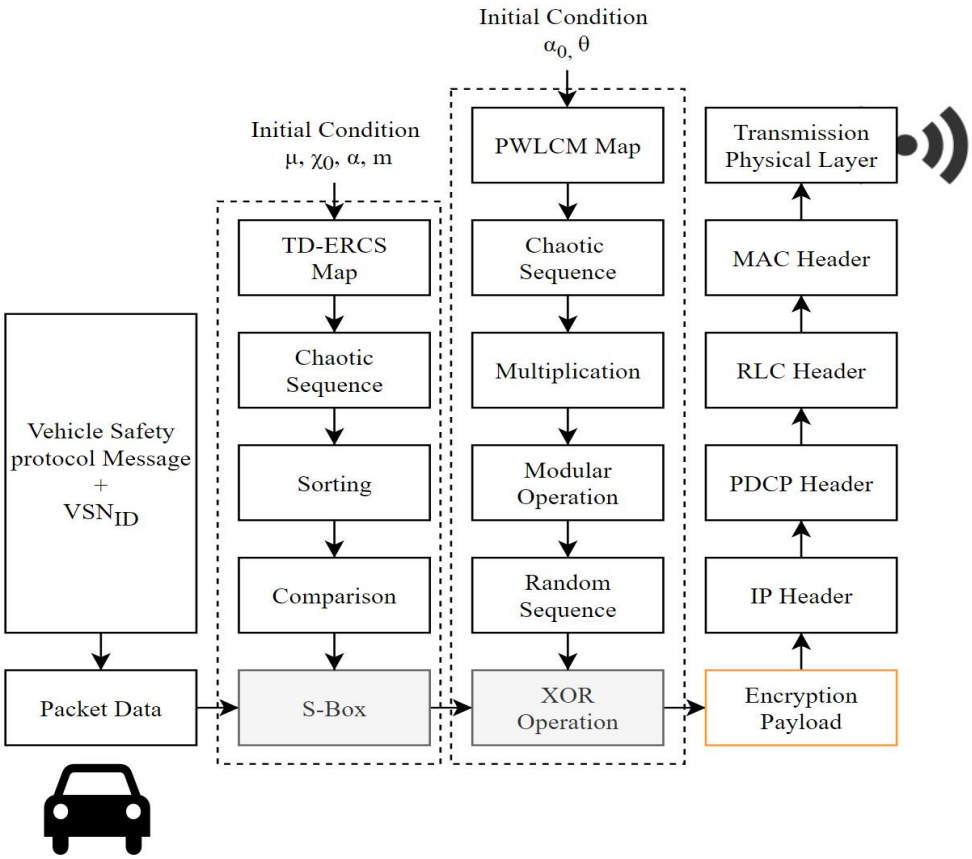

Figure 6. System architecture of blockchain-based firmware update

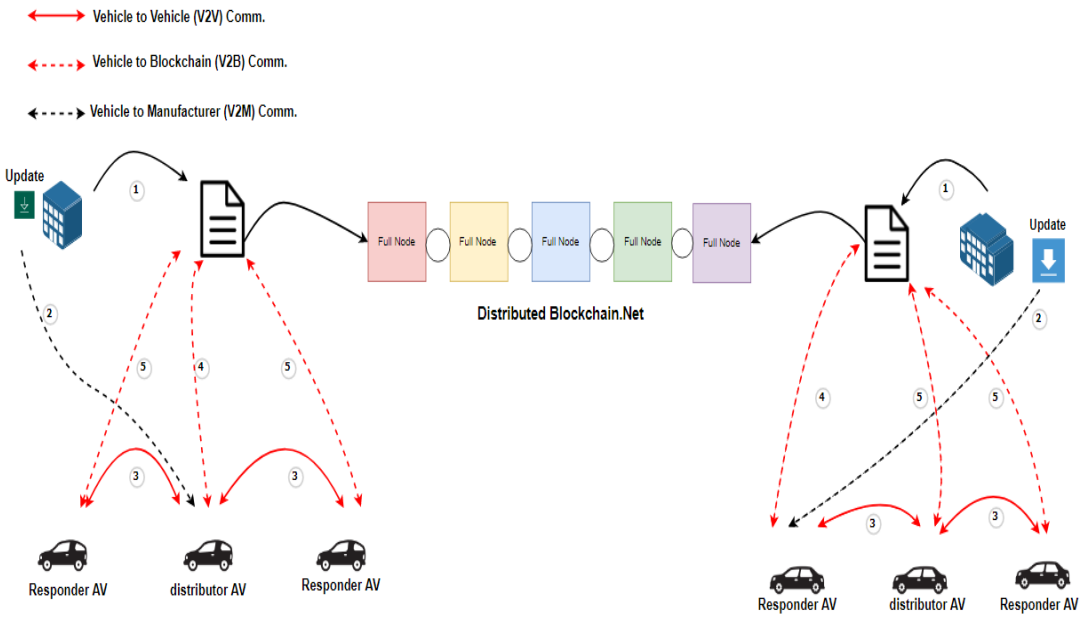

Figure 7a. Uplink flow diagram

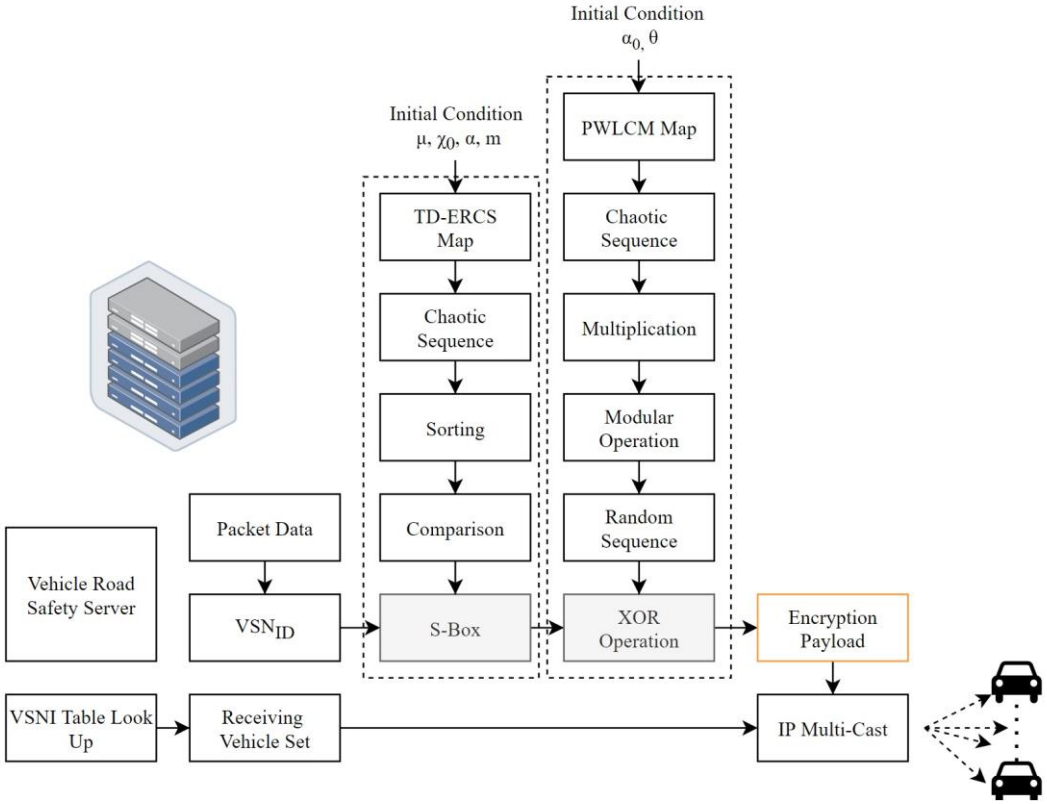

Figure 7b. Downlink flow diagram

With the increasing use of communication between CAVs and between CAVs and roadside environments, security concerns have been raised due to the potential for catastrophic attacks towards these communications. These communications include message types like Cooperative Awareness Message (CAMs) and Decentralized Environment Notification Messages (DENMs). To increase the security of the communications introduced above, Ansari et al. [39] introduces Tangent-Delay Ellipse Reflecting Cavity-Map System (TD-ERCS) - a chaos-based cryptography - into the encryption system. TD-ERCS is a 2D discrete chaotic map and compared to one dimensional chaotic maps, such as logistic and skew tent maps, 2D discrete chaotic maps are more secure and effective.

Since the safety of the CAV is of the utmost importance and relies on low latency, the multitude of applications within a CAV require the successful transmission and reception of communications to have an end-to-end delay of less than 100 milliseconds. Thus, [39] conducts an experiment focused on improving latency evaluation methods. The experiment is performed in a simulated network model of a 2×2 km^2 area of the city center located in Glasgow, Scotland. Mobility of the vehicles in the network is generated using routes mobility model, which assigns each vehicle with a route generated using Google Maps' API. With 100 vehicles transmitting one message every second, the probability of having an end-to-end delay less than or equal to 50 milliseconds is about 85%, while adding the encryption to the scenario only changes the probability by 1%.

The uplink and downlink flows implemented within the Long Term Evolution (LTE) V2X are shown in Figure 7a and 7b. Note that since Piecewise Linear Chaotic Map (PWLCM) produces a more chaotic output than the traditional logistic map, small changes in initial key parameters can drastically affect the output of the map.

4. DISCUSSION AND ANALYSIS

This study reviews and analyzes multiple works that investigate techniques that lend themselves to the different perspectives and issues observed in the protection of the communication layer in VANET, including securing sensitive data, improving security of communications, and increasing efficiency of communications in VANET. Technologies associated with CAVs, including Blockchain, Named Data Networking, Intrusion Detection System, and Cognitive Engine have been investigated in the literature and specific models have been proposed by researchers. The literature works reviewed and analyzed in this paper provide a great insight into the current state-of-the-art of those technologies associated with CAVs and are summarized in Table 3.

Blockchain technology is a popular approach as observed in the literature where many researchers like to implement it into their models. It provides secure way to store sensitive or private information for CAVs allowing for the detection of any alteration or mal-intent changes of the system data. While high energy consumption can be viewed as a disadvantage of blockchain methodology, researchers have been investigating novel methods to combat that problem associated with blockchain usage. Based on our review of articles pertaining to communications in CAVs, the NS2 (Network Simulator 2) is investigated by several of those works toward obtaining the respective dataset, and those works show that NS2-based approaches yield good performance. The LiDAR based sensor schemes are extremely popular with CAVs; however, it has some limitations and vulnerabilities, especially when comes to not recognizing an object's shape that has been tampered with by an attacker. Security and safety solutions have been proposed by some experts to improve performance of LiDAR sensors in the presence of a malicious attack. A digital watermark can be embedded in the point cloud (of the objects') for the LiDAR sensors to allow correct authentication. In addition, safety-based constraints are implemented toward improving the safety of CAV sensors during an attack. We now summarize the works we have reviewed in this paper and identify limitations in respective works which can serve as motivation for future work by researchers.

Rathee et al. [10] investigate online cab booking services in the context of connected vehicles as a service and implement a blockchain scheme in that context. The proposed technique is tested using a simulator (NS2) instead of real-world experimental scenario, and moreover, the number of network nodes in their case study, i.e., 50, is relatively small compared to a real-world environment. Sharma [11] focuses on reducing the energy consumption of a blockchain network in the VANET. However, the validation of their proposed approach is based on, and is specific to, the formulaic process presented in the paper. Alheeti et al. [8][9] investigate ensuring driverless cars with emergency cooperative awareness messages (CAMs). The authors focus on black hole attacks and propose an IDS targeting the isolation and detection of the malicious user. The proposed IDS technique is tested using a simulator (NS2) instead of real-world experimental scenario. In addition, the sizes of the training, validation and testing datasets are not varied to observe their variation commonly observed in the real-world. Chowdhury et al. [20] provide a new network architecture, Named Data Networking, toward detecting false data while preserving privacy of CAV users. Their method has an overhead of requiring that vehicles have a set of pseudonyms and a certificate issuing proxy. Moreover, demonstrating the benefits of their approach with a larger set of vehicles would have provided better validation and generalization; however, the authors only used three vehicles in the experiment. Cao et al. [14] indicate that a small change in the object's data by the LiDAR sensors, thus, creating an adversarial object, can lead to incorrect prediction by a model. However, their work is limited to experiments conducted on the Apollo platform of CAVs. Changalvala et al. [29] focus on the

Table 3: Analysis of Existing Selected Works

Title	Methodology	Novelty	Limitation
A blockchain framework for securing connected and autonomous vehicles [10]	An online cab booking system with blockchain storing the rating score.	Attacks like a fake request, alteration on user's data are reduced.	Experiment is done with small number of network nodes and using a simulator.
An energy-efficient transaction model for the blockchain-enabled internet of vehicles [11]	A mechanism that reduces the transactions required to update ledgers for blockchains in CAVs.	Conserves energy by 40% on average, reduces the ledgers transactions by 82% on average.	The experiment does not use any data set that represents real world use of CAV communication.
An intrusion detection system against black hole attacks on the communication network of self-driving cars [8]	An IDS uses an artificial neural network and fuzzified data to detect black hole attacks.	Detection rate increases compared to the IDS that does not use fuzzy set.	The performance evaluation is based on a generated data set, and the IDS is tested using only a simulator.
Secure information sharing among autonomous vehicles in NDN [20]	A NDN architecture for CAV using vehicle pseudonym scheme.	Prevents threats like false data, dissemination, and vehicle tracking.	Experiment is based only on three vehicles, involves overhead of vehicle pseudonyms and proxy certification.
Adversarial objects against LiDAR-based autonomous driving systems [14]	A robust adversarial object that evades LiDAR-based object detection system.	The adversarial object can attack the system at different position and various orientations.	The object is evaluated under only one CAV platform.
LiDAR data integrity verification for autonomous vehicle [29]	A digital water mark scheme that protects the LiDAR data from alteration using quantization index modulation.	Mechanism reaches a 100% success rate on detecting and localizing the tampering.	The evaluation does not test the mechanism for LiDAR-based CAV in real-world.
Towards robust lidar-based perception in autonomous driving. General black-box adversarial sensor attack and countermeasures [13]	Evaluation of the vulnerability of LiDAR when less points are received and when in tandem with CARLO.	CARLO accurately detects spoofing attacks and reduces the attack rate to 5.5%.	Evaluation is done with the KITTI training data set - test on a real adversarial object is not included.
Machine Learning-Based Detection for Cyber Security Attacks on Connected and Autonomous Vehicles [28]	Introduces Unified Modelling Language into the definition of attack points of AVs.	Proposes a framework that improves analysis methods of potential cyber security threats in CAV systems.	The dataset is collected from a network of computers, many of which possess attributes that may not be compatible to all CAV scenarios.
Blockchain-based firmware update scheme tailored for autonomous vehicles [42]	Utilizes blockchain and smart contract techniques for a distributed firmware update system for CAVs.	Provides a decentralized, secure update method while not affecting vehicle operation.	Experiment may not be fully representative of real-world entropy present in CAV scenarios.

Chaos-based privacy preserving vehicle safety protocol for 5G Connected Autonomous Vehicle networks [39]	Introduce Tangent-Delay Ellipse Reflecting Cavity-Map System into an encryption system for CAV communication.	Proposes a more secure and effective encryption method.	The evaluation phase does not include any test for system robustness and flexibility.

authentication strategy for data security from the LiDAR system, and employ a process based on digital watermarking for integrity verification and use quantization index modulation (QIM) during their approach. However, their work is based solely on the KITTI benchmark dataset, compared to collecting data from a real-world scenario. Sun et al. [13] investigate the issue of occlusion of LiDAR-based object detection, representing the area behind the target hit point from the LiDAR system's perspective, and propose CARLO as an occlusion-aware hierarchical anomaly detection solution. However, their work is based solely on the KITTI benchmark dataset, compared to collecting data from a real-world scenario.

5. CONCLUSION

Connected autonomous vehicles reduce human intervention in driverless vehicles, allowing for a seamless detection of objects in the environments surrounding the vehicles. Technologies associated with CAV involve numerous sensors, several algorithms working collectively, network-based interconnected nodes, and other systems that collectively assist in modern CAVs. Such environments are often subjected to intentional malicious activity, targeting various components of CAVs and their environments. Data security and data privacy is one such area of CAVs that has been targeted via different types of attacks. The scope of this study is to present a good background knowledge of issues pertaining to different attacks in the context of data security and privacy and present a detailed review and analysis of eight very recent studies providing solutions to different aspects pertaining to attacks targeting data security and privacy elements of CAVs.

Most of the mechanisms and proposed methods presented in these works are tested within simulators and not experimented in a real-world environment. Typically, data used by these works generated from algorithmic models instead of knowledge gained from studying the real application of CAVs. Our study presents a focus on the advantages and limitations of the eight studies selected for a closer review from a collection of nearly 50 recent publications in the area of CAVs and attacks performed on them. As more advanced technology is being embedded into CAV and electric vehicles are becoming ever so popular by the year, data-centric security and privacy solutions need developed effective and efficient solutions against the growing number of the types of attacks.

REFERENCES

[1] Litman, Todd. *Autonomous vehicle implementation predictions*. Victoria, Canada: Victoria Transport Policy Institute, 2017.

[2] Dey, K. C., Rayamajhi, A., Chowdhury, M., Bhavsar, P., & Martin, J. (2016). Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network–Performance evaluation. *Transportation Research Part C: Emerging Technologies*, *68*, 168-184.

[3] Othmane, L. B., Weffers, H., Mohamad, M. M., & Wolf, M. (2015). A survey of security and privacy in connected vehicles. In *Wireless sensor and mobile ad-hoc networks* (pp. 217-247). Springer, New York, NY.

[4] Kumar, Amara Dinesh, Koti Naga Renu Chebrolu, and Soman KP. "A brief survey on autonomous vehicle possible attacks, exploits and vulnerabilities." *arXiv preprint arXiv:1810.04144* (2018).

[5] Humphreys, Todd. "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing." *University of Texas at Austin (July 18, 2012)* (2012): 1-16.

[6] Petit, J., Stottelaar, B., Feiri, M., & Kargl, F. Remote attacks on automated vehicles sensors: Experiments on camera and lidar. *Black Hat Europe*, 2015.

[7] Pham, Minh, and Kaiqi Xiong. "A survey on security attacks and defense techniques for connected and autonomous vehicles." *arXiv preprint arXiv:2007.08041* (2020)

[8] Alheeti, Khattab M. Ali, Anna Gruebler, and Klaus D. McDonald-Maier. "An intrusion detection system against black hole attacks on the communication network of self-driving cars." *2015 sixth international conference on emerging security technologies (EST)*. IEEE, 2015.

[9] Alheeti, Khattab M. Ali, Anna Gruebler, and Klaus D. McDonald-Maier. "An intrusion detection system against malicious attacks on the communication network of driverless cars." *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*. IEEE, 2015.

[10] Rathee, G., Sharma, A., Iqbal, R., Aloqaily, M., Jaglan, N., & Kumar, R. (2019). A blockchain framework for securing connected and autonomous vehicles. *Sensors*, *19*(14), 3165.

[11] Sharma, Vishal. "An energy-efficient transaction model for the blockchain-enabled internet of vehicles (IoV)." *IEEE Communications Letters* 23.2 (2018): 246-249.

[12] Shin, H., Kim, D., Kwon, Y., & Kim, Y. (2017, September). Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications. In *International Conference on Cryptographic Hardware and Embedded Systems* (pp. 445-467). Springer, Cham.

[13] Sun, J., Cao, Y., Chen, Q. A., & Mao, Z. M. (2020). Towards robust lidar-based perception in autonomous driving: General black-box adversarial sensor attack and countermeasures. In *29th {USENIX} Security Symposium ({USENIX} Security 20)* (pp. 877-894).

[14] Cao, Y., Xiao, C., Yang, D., Fang, J., Yang, R., Liu, M., & Li, B. (2019). Adversarial objects against lidar-based autonomous driving systems. *arXiv preprint arXiv:1907.05418*.

[15] Feng, Y., Huang, S., Chen, Q. A., Liu, H. X., & Mao, Z. M. (2018). Vulnerability of traffic control system under cyberattacks with falsified data. *Transportation research record*, *2672*(1), 1-11.

[16] He, Qiyi, Xiaolin Meng, and Rong Qu. "Towards a severity assessment method for potential cyber-attacks to connected and autonomous vehicles." *Journal of advanced transportation* 2020 (2020)

[17] Bloom, C., Tan, J., Ramjohn, J., & Bauer, L. (2017). Self-driving cars and data collection: Privacy perceptions of networked autonomous vehicles. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)* (pp. 357-375).

[18] Dutta, R. G., Yu, F., Zhang, T., Hu, Y., & Jin, Y. Security for safety: a path toward building trusted autonomous vehicles. In *Proceedings of the International Conference on Computer-Aided Design*, 2018.

[19] Plosz, Sandor, and Pal Varga. "Security and safety risk analysis of vision guided autonomous vehicles." *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. IEEE, 2018.

[20] Chowdhury, Muktadir, Ashlesh Gawande, and Lan Wang. "Secure information sharing among autonomous vehicles in NDN." *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*. 2017

[21] Amoozadeh, M., Raghuramu, A., Chuah, C. N., Ghosal, D., Zhang, H. M., Rowe, J., & Levitt, K. (2015). Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine*, 53(6), 126-132.

[22] Mahmud, Syed Masud, Shobhit Shanker, and Irina Hossain. "Secure software upload in an intelligent vehicle via wireless communication links." *IEEE Proceedings. Intelligent Vehicles Symposium, 2005*.

[23] Qian, Y., Chen, M., Chen, J., Hossain, M. S., & Alamri, A. (2018). Secure enforcement in cognitive internet of vehicles. *IEEE Internet of Things Journal*, *5*(2), 1242-1250.

[24] Huang, C., Lu, R., Lin, X., & Shen, X. Secure automated valet parking: A privacy-preserving reservation scheme for autonomous vehicles. *IEEE Transactions on Vehicular Technology*, 67(11), 11169-11180.

[25] Tokody, D., Albini, A., Ady, L., Rajnai, Z., & Pongrácz, F. (2018). Safety and security through the design of autonomous intelligent vehicle systems and intelligent infrastructure in the smart city. *Interdisciplinary Description of Complex Systems: INDECS*, *16*(3-A), 384-396.

[26] Alheeti, Khattab M. Ali, Anna Gruebler, and Klaus D. McDonald-Maier. "On the detection of grey hole and rushing attacks in self-driving vehicular networks." *2015 7th Computer science and electronic engineering conference (CEEC)*. IEEE, 2015

[27] Cui, Jin, and Giedre Sabaliauskaite. "On the alignment of safety and security for autonomous vehicles." *Proc. IARIA CYBER* (2017): 1-6.

[28] He, Q., Meng, X., Qu, R., & Xi, R. (2020). Machine Learning-Based Detection for Cyber Security Attacks on Connected and Autonomous Vehicles. *Mathematics*, *8*(8), 1311.

[29] Changalvala, Raghu, and Hafiz Malik. "LiDAR data integrity verification for autonomous vehicle." *IEEE Access* 7 (2019): 138018-138031.

[30] Veitas, Viktoras Kabir, and Simon Delaere. "In-vehicle data recording, storage and access management in autonomous vehicles." *arXiv preprint arXiv:1806.03243* (2018).

[31] Kang, Min-Joo, and Je-Won Kang. "Intrusion detection system using deep neural network for in-vehicle network security." *PloS one* 11.6 (2016): e0155781.

[32] Kosmanos, D., Pappas, A., Aparicio-Navarro, F. J., Maglaras, L., Janicke, H., Boiten, E., & Argyriou, A. (2019, September). Intrusion detection system for platooning connected autonomous vehicles. In *2019 4th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)* (pp. 1-9). IEEE.

[33] Jameel, F., Chang, Z., Huang, J., & Ristaniemi, T. (2019). Internet of autonomous vehicles: architecture, features, and socio-technological challenges. *IEEE Wireless Communications*, *26*(4), 21-29.

[34] Ali Alheeti, Khattab M., and Klaus McDonald-Maier. "Intelligent intrusion detection in external communication systems for autonomous vehicles." *Systems Science & Control Engineering*, 6(1):48-56.

[35] Khalil, A., Al Janaideh, M., Aljanaideh, K. F., & Kundur, D. (2020, July). Fault detection, localization, and mitigation of a network of connected autonomous vehicles using transmissibility identification. In *2020 American Control Conference (ACC)* (pp. 386-391). IEEE.

[36] Raiyn, Jamal. "Data and cyber security in autonomous vehicle networks." *Transport and Telecommunication* 19.4 (2018): 325-334.

[37] Ferdowsi, A., Ali, S., Saad, W., & Mandayam, N. B. (2019). Cyber-physical security and safety of autonomous connected vehicles: Optimal control meets multi-armed bandit learning. *IEEE Transactions on Communications*, *67*(10), 7228-7244.

[38] Sheehan, B., Murphy, F., Mullins, M., & Ryan, C. (2019). Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation research part A: policy and practice*, *124*, 523-536.

[39] Ansari, S., Ahmad, J., Aziz Shah, S., Kashif Bashir, A., Boutaleb, T., & Sinanovic, S. (2020). Chaos-based privacy preserving vehicle safety protocol for 5G Connected Autonomous Vehicle networks. *Transactions on Emerging Telecommunications Technologies*, *31*(5), e3966.

[40] Dedinsky, R., Khayatian, M., Mehrabian, M., & Shrivastava, A. (2019). A dependable detection mechanism for intersection management of connected autonomous vehicles (interactive presentation). In *Workshop on Autonomous Systems Design (ASD 2019)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

[41] Narbayeva, S., Bakibayev, T., Abeshev, K., Makarova, I., Shubenkova, K., & Pashkevich, A. (2020). Blockchain technology on the way of autonomous vehicles development. *Transportation Research Procedia*, *44*, 168-175.

[42] Baza, M., Nabil, M., Lasla, N., Fidan, K., Mahmoud, M., & Abdallah, M. (2019, April). Blockchain-based firmware update scheme tailored for autonomous vehicles. In *2019 IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 1-7). IEEE.

[43] Lim, Bing Shun, Sye Loong Keoh, and Vrizlynn LL Thing. "Autonomous vehicle ultrasonic sensor vulnerability and impact assessment." *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*.

[44] Sharma, Prinkle, David Austin, and Hong Liu. "Attacks on machine learning: Adversarial examples in connected and autonomous vehicles." *2019 IEEE International Symposium on Technologies for Homeland Security (HST)*. IEEE, 2019.

[45] Jin, X., Haddad, W. M., Jiang, Z. P., Kanellopoulos, A., & Vamvoudakis, K. G. (2019). An adaptive learning and control architecture for mitigating sensor and actuator attacks in connected autonomous vehicle platoons. *International Journal of Adaptive Control and Signal Processing*, *33*(12), 1788-1802.

[46] Khadka, A., Karypidis, P., Lytos, A., & Efstathopoulos, G. (2021). A benchmarking framework for cyber-attacks on autonomous vehicles. *Transportation research procedia*, *52*, 323-330.

[47] Dave, R., Sowells Boone, E. R., and Roy, K., "Efficient Data Privacy and Security in Autonomous Cars." Journal of Computer Sciences and Applications, vol. 7, no. 1 (2019): 31-36.doi: 10.12691/jcsa-7-1-5.

[48] Patel, M., Dave, R., Rushit Dave, and Sowells Boone, E. R., "Autonomous Vehicles: Ethical Dilemmas", International Journal of Advanced Research and Publications (IJARP), http://www.ijarp.org/online-papers-publishing/August2019.html, Volume 3 - Issue 8, August 2019 Edition, #ijarporg.