# Cybersecurity on Connected and Automated Transportation Systems: A Survey

Ahmed Abdo, Hanlin ChenG, *Member, IEEE,* Xuanpeng Zhaoe, Guoyuan wue, *Senior Member, IEEE,* and Yiheng Fenge, *Member, IEEE*

*Abstract-Connected* **and automated** vehicles **(CAVs) provide various valuable and advanced services to manufacturers, owners, mobility service providers, and transportation authorities. As a result, a large number of CAV applications have been proposed to improve the** safety, **mobility, and sustainability** of **the transportation system. With the increasing** connectivity **and automation,** cy**bersecurity of** the **connected and automated transportation system (CATS) has raised attention to the transportation community in recent years. Vulnerabilities in CAVs can lead to breakdowns in the transportation system and compromise safety** (e.g., **causing** crashes), **performance** (e.g., **increasing congestion and reducing capacity),and fairness** (e.g., **vehicles fooling traffic signals). This paper presents our perspective on CATS cybersecurity via surveying recent pertinent studies focusing on the transportation system level, ranging from individual and multiple vehicles to the traffic network (including infrastructure).** It **also higWights threat analysis and risk assessment (TARA) tools and evaluation platforms, particularly for analyzing the CATS cybersecurity problem. Finally, this paper will provide valuable insights into developing** secure **CAV applications and investigating remaining open cybersecurity challenges that must be addressed.**

*Index Terms-Connected* **and automated vehicles,** cybersecurity, **risk assessment,** evaluation **platform,** cyber **attack, defense strategies.**

## I. INTRODUCTION

BY LEVERAGING advanced sensing technology, edge computing, and wireless communications, connected and automated vehicles (CAVs) will merge the capabilities of both Connected Vehicles (CVs) and Autonomous Vehicles (AVs). As a result, CAVs can not only perceive their surrounding environments with perception sensors such as cameras, radars, and LiDARs but also communicate with other equipped vehicles, roadside infrastructure, active road users (e.g., bicyclists, pedestrians), and the cloud via vehicle-to-everything (V2X) communications. This enables CAVs and other road users to cooperate more efficiently and collaboratively. Toward this end, CAVs have been regarded as a disruptive solution to many existing issues in our current transportation system, e.g., reducing trafficaccidents,improving accessibility forseniorsand disabled people, mitigating traffic congestion, and enhancing air quality.

Nevertheless, cybersecurity is a critical concern to guarantee theaforementioned benefits from CAVs. Many researchers have realized this issue and performed pertinent research over the past decade. Most existing studies on automotive cybersecurity have been focused on in-vehicle networks, such as Controller Area Network (CAN bus) [1], Electronic Control Units (ECUs) [2], Global Navigation Satellite Systems (GNSS) [3], and onboard sensors (e.g., radar, camera, LiDAR and ultrasonic) [4]. This is of particular importance for autonomous vehicles. Recent development and deployment efforts inconnected vehicle applications attract much attention to the cybersecurity problems of V2X communications. Due to connectivity, cyber-attacks may lead to breakdowns of the entire system on a much larger scale, resulting in more significant negative impacts. For example, a public report on automotive cyber incidents by *Upstream* [5] disclosed that in the years 2020 and 2021, cyber threats to vehicles' communication channels increased by 89.3%, and threats to vehicle data/code increased by 87.7%. Compared to AVs and CVs, CAVs are prone to be much more vulnerable to cyber threats from malicious attackers due to their increasing system complexity and more attack surfaces (e.g., sensing and communication systems) [6], [7], [8], [9], [10]. Therefore, reviewing the state-of-the-art cybersecurity on CAVs or, more broadly, on Connected and Automated Transportation Systems (CATS), identifying open gaps, and sketching future research paths becomes imperative and challenging.

There are several surveys on the cybersecurity of AVs, Vehicular Ad-hoc NETworks (VANETs), or CAVs [l l], [12]. For instance, Ju et al. [13] reviewed attack detection and resilience for CAVs on both intra-vehicle and inter-vehicle communications from vehicle dynamics and control perspectives. However, few provide a comprehensive review from the transportation system perspective, ranging from an individual vehicle to vehicle strings and the entire transportation system (including roadside infrastructure such as traffic signals). Furthermore, most of these surveys only emphasize vehicle-level cyber attacks (e.g., GPS spoofing, denial-of-service) and cyber defenses (such as Security Credential Management System, blockchain, and anomaly detection) but ignore risk assessment and cyber

Manuscript received 29 August 2023; revised 2 October 2023; accepted 14 October 2023. Date of publication 23 October 2023; date of current version 23 February 2024.This work wassupported by the U.S. National Science Foundation under Grant SaTC I930041. *(Corresponding author: Yiheng Feng.)*

Ahmed Abdo is with the Department of Electrical and Computer Engineering, University of California, Riverside, CA 92521 USA (e-mail: aabdo003@ucr.edu).

Hanlin Chen and Yiheng Feng are with Purdue University, West Lafayette, IN 47907 USA (e-mail: chenl 368@purdue.edu;feng333@purdue.edu).

Xuanpeng Zhao and Guoyuan Wu are with the University of California, Riverside, CA 92507 USA (e-mail: xzhao094@ucr.edu; gywu@cert.ucr.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109ffIV.2023.3326736.

Digital Object Identifier I0.1109rrIV.2023.3326736

attack/defense at the CAY application level. For example, Sun et al. [14] summarized cyber risks and safety standards. Han et al. [15] reviewed attack, defense and cyber forensics evidence reconstruction based on vehicle platforms with regard to cyber threats for modem transportation systems. However, in both papers, approaches to threat analysis and tools/platforms for resilience validation are absent. To address these gaps, we make the following contributions in this paper:

- We investigate the cybersecurity problem, not only at the single-vehicle level, but also at the multi-vehicle level as well as at the transportation system level, including infrastructure.
- We provide a comprehensive review on the threat analysis and risk assessment approaches, which are usually ignored inexisting review studies.
- We summarize useful evaluation platforms for different types (vehicle, traffic, communication)of CAT cybersecurity research.

## II. BACKGROUND

Inthis section, we first present some background information for CAVs, including communication technologies. Then, we briefly introduce the streamlined presentation of this survey.

### A. CAVs Communication Technologies

CAVs are based on different protocols that consist of information sharing, application management, security algorithms, and messaging. The main goal of these protocols is to fit the required connectivity solutions for V2X services.

Wireless Access in Vehicular Environments (WAVE) [16] isa communication protocol that is used in Dedicated Short-Range Communications (DSRC) technology. WAVE operates in the 5.9 GHz frequency band and enables communication among vehicles and between vehicles and infrastructure, such as traffic signals and signs. WAVE uses the SAE 12735 [17] standard to define the message sets, data frames, and data elements used for communication. This technology is being explored for various applications, including collision avoidance, intersection safety, and traveler information. WAVEcan potentially improve roadway safety and efficiency by providing real-time information about traffic conditions and potential hazards. However, deployment of WAVE may require further regulatory and policy development to address issues such as privacy, security, and spectrum allocation. On the other hand, LTE, or Long-Term Evolution [18], is a cellular communication technology that is beingexplored for V2X. LTE offers high data rates, low latency, and secure communication, which could benefit safety-critical applications such as collision avoidance and intersection safety. One advantage of using LTE in V2X is that it would leverage existing cellular infrastructure, potentially reducing the need for additional dedicated infrastructure investment. However, there are alsochallenges associated with using LTEin V2X, including concerns about interference and the need for standardization to ensure interoperability with other communication systems. Overall, LTE is one potential technology that could be used to enhance the capabilities of V2X for improving roadway safety and efficiency.

### B. CAV Applications

Over the past decade, numerous CAY applications have been developed toimprove transportationsystem safety, mobility, and environmental sustainability. Safety is the basis of all transportation system operations and, thus, a primary focus of the CAY applications. Safety is usually considered in the motion prediction and planning stage at the individual vehicle level with risk evaluations based on conflicting trajectories [19] and surrogate safety assessment measures [20]. Data from CAV onboard sensors are uWized to build a driving environment with static and dynamic objects as the input to the planning module. At themulti-vehicle level, vehicle-to-vehicle(V2V) and vehicle-to-infrastructure (V2I) communications become essential to information exchange and coordinate maneuvers among CAVs. Representative safety applications that rely upon V2V communications include forwardcollision warning (FCW) [21], blind spot/lane changing warning (BSW/LCW) [22], and emergency electronic brake light (EEBL). Safety applications that are based on V2I communications include red light violation warnings, curve speed warnings, and reduced speed/work zone warnings [23], etc. In addition, V2I-based safety applications also include providing advisory information to vulnerable road users (VRUs), such as pedestrian collision warning [24].

In addition to safety, efficiency is another major objective of the transportation system operation, and CAY technologies can help improve mobility significantly. A number of representative CV applications are initiated by the USDOT's Dynamic Mobility Applications **(OMA)** program [25], under which several research prototypes have been developed, such as Enable Advanced Traveler Information Systems (EnableATIS) and Multimodal Intelligent Traffic Signal System (MMITSS). Its goal is to leverage multi-sourced data from CVs and transportation infrastructure and demonstrate their performance in terms of mobility, along with associated benefits and costs. Combining V2I communication with automation, other mobility-oriented applications have been proposed, such as speed harmonization [26], spatial-temporal intersection control [27], [28], and cooperative ramp merging [29].

The third primary goalof thetransportationsystem is environmental sustainability[30], for which CAY technologies can help reduce fuel consumption and traffic-relatedemissions. Two representative applications arevehicleplatooning andeco-approach and departure (EAD). Vehicle platooning or cooperative adaptive cruise control (CACC) uWizes both onboard sensors (e.g., radar) and V2Vcommunicationstosynchronize longitudinal behaviors of astringof vehicles, which can improve stringstability and reduceheadway forhighway driving. Inaddition, platooning can significantly improve the fuel efficiency of the following vehicles (especially for trucks) due to reduced aerodynamic resistance [31] and also increase road capacity due to reduced headway [32]. On the other hand, EAD applications applied at signalized intersections use information (e.g., road map and traffic signal status) received from the infrastructure via 12V

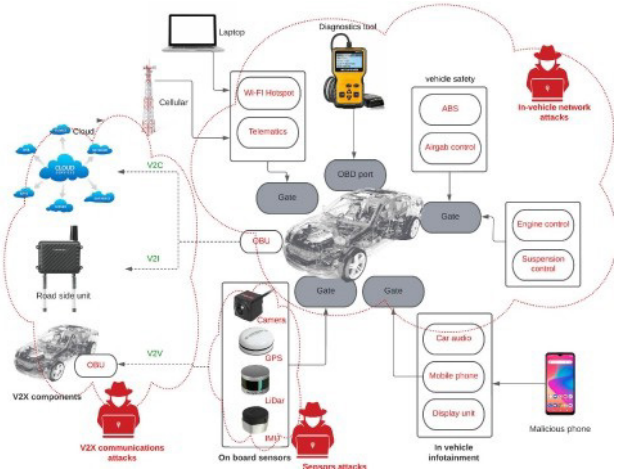



Fig. l. Overall CAY cyber vulnerabilities.

communications. Upon receiving the upcoming traffic signals' data in real time, the equipped CAV can adjust its longitudinal speed to reduce acceleration and deceleration fluctuations for energy savings. This technology has been widely tested under the GlidePath program at USDOT [33], [34] and GLOSA [35] program at EU.

### C. CAV Cyber Vulnerabilities

Modern vehicles [36] can be considered as mobile computers containing over 100 million lines of computer code in the Electronic Control Units (ECUs) that regulate vehicle maneuvers, such as brakesand steering. Moreover, connected vehicles offer a lot of conveniences and advanced intelligent features. However, as with any technology that connects to other devices and the internet, connected vehicles are vulnerable to cyber-attacks. These security vulnerabilities can lead to remote exploitation, unauthorized access to data, communication channel attacks, and physical attacks. as shown in Fig. 1.

One of the connected vehicles' most significant security vulnerabilities is the risk of remote exploitation. This is when an attacker gains unauthorized access to the vehicle's systems and can manipulate them remotely. This type of attack can be used to steal data from the vehicle, take control of it, or even cause it to crash. Remote exploitation can occur through several methods, including exploiting software vulnerabilities, using fake firmware updates,or evenexploiting unsecured Wi-Fi connections.

Another vulnerability is the potential for unauthorized access to the vehicle's data. Connected vehicles store vast amounts of data, including GPS data, driver behavior data, and vehicle diagnostics. This data is often stored in the cloud and can be accessed remotely. If an attacker gains access to this data, they can use it tostealsensitive information or eventrack thevehicle's movements. This is particularly concerning regarding location data, as it can reveal information about where the driver lives and works.

Connected vehicles also face the risk of cyber attacks that target the vehicle's communication channels. These attacks can disrupt the communication between the vehicle and other connected devices, causing traffic accidents, traffic congestion, and even vehicle crashes. For example, if an attacker manipulates traffic signals, they could cause chaos on the roads, leading to accidents and fatalities.

Furthermore, connected vehicles are also at risk of physical attacks. Adetermined attackercould breakintothe vehicle'ssystems physically, bypassing anycybersecurity measures thathave been put in place. Physical attacks can include tampering with the vehicle's sensors or devices or using devices like jarnmers or signal boosters to interfere with the vehicle's communication channels.

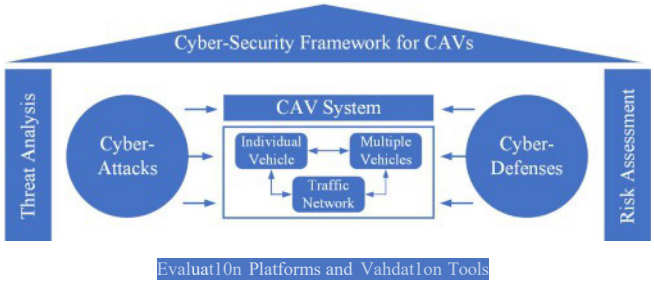



Fig. 2. Structure of this survey.

### D. Survey Structure

To streamline the presentation, as shown in Fig. 2, the survey starts with *threat analysis and risk assessment* in Section ill, which supports the existing framework for identifying cyber threats and developing countermeasures to mitigate those threats. Then specific *cyber attack* and *cyber defense* methodologies are reviewed at both individual vehicle level and CAV application level in Sections IV and V, respectively, two critical steps in the risk assessment framework in Section ill. Finally, existing CAV cybersecurity research *platforms and tools* are reviewed in Section VI, which provides environments for evaluating theimpactsofcyberattacksinSection IVand validating the effectiveness of respective cyber defense strategies in Section V. The sections can also be considered as different steps in the security analysis, which is summarized in a flowchart as shown in Fig. 3.

## III. THREAT ANALYSIS AND RISK ASSESSMENT

Threat analysis and risk assessment (TARA) evaluates the likelihood and impact of attacks and combines them to derive the system risks. To further understand the difference between TARA approaches, Fig. 4 provides a schematic representation of the systematic engineering procedures of various TARA approaches. The process commences with system definition, which lays the foundation for subsequent steps in the TARA method. Then, it is followed by a bifurcation, which leads to different types based on the path chosen. Subsequently, the process makes the transition to threat and attack modeling, which constructs potential threats and attack scenarios. Next,

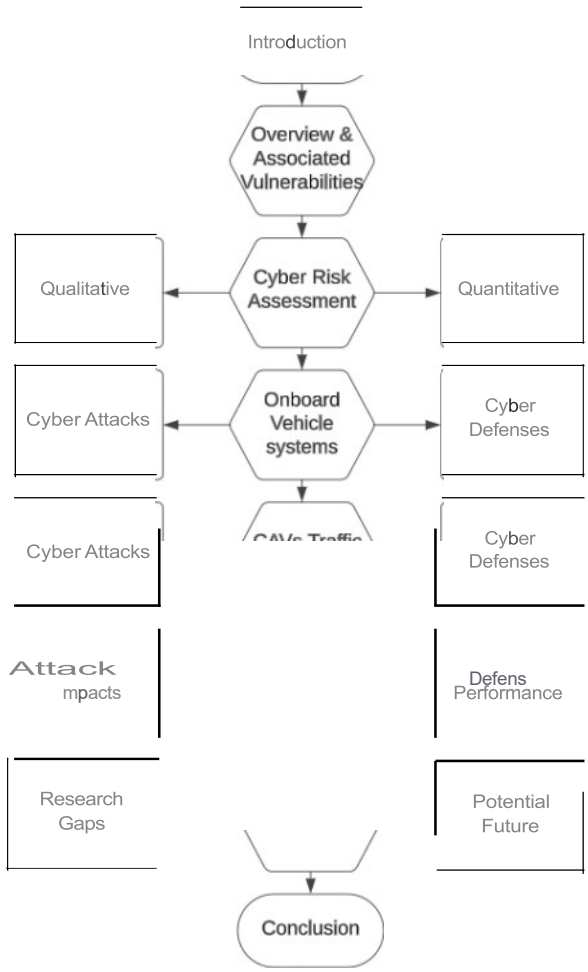



Fig. 3. Flowchart of this survey.

based on how to fonnulate the risk, TARA approaches can be further divided into two categories: qualitative approaches and quantitative approaches in therisk detennination stage, as shown in Fig. 5. Qualitative approaches take advantage of experience from experts to evaluate cyber risks and define the severity of risks at different levels: high, medium, and low, or with a risk index. These approaches provide convincing, reliable, and explainable results but cannot handle risks without prior knowledge. Quantitative approaches, instead, leverage different models to assess the threats and risks likelihood of the system based on probability theory and statistics. The results can be easily compared with other risks. However, these methods are usually quite data-demanding, which is a major challenge in the real world.

### A. Qualitative Approaches

In thequalitative approach, weclassify it from the perspective of victims and attackers based on the process after system definition. On the victim side, we assess threats and risks based on the severity of the damage inflicted on the victim. Unlike the victim-oriented approaches, the assessment method from the attacker's perspective cares more about the attacker's profile and tradeoffs between the costs and benefits to the attacker.

*I) Victim-Oriented Approaches:* Further investigation of the victim-oriented approaches results in two aspects: asset and vulnerability, both of which start with defining the system and the problem. However, they diverge in their next steps. An asset-based approach focuses on what needs to be protected in the system, such as data, software, or hardware. It prioritizes the system assets identification and then evaluates their possible threats. On the other hand, a vulnerability-based approach starts with identifying weaknesses or vulnerabilities ina system, then proceeds to analyze what failures these vulnerabilities or weaknesses could cause [37]. For more infonnation on the characteristics of the victim-oriented approaches, please refer to Table I.

*Asset-based:* Agood instance of an Asset-based method is the E-safety Vehicle Intrusion Protected Applications (EVITA) that provides a cost-effective security architecture and facilitates the design, verification, and prototyping of vehicle networks [38]. From the attacked assets perspective, security threats can be analyzed by four objectives: operational, safety, privacy, and financial. A qualitative risk level from O to 6 can be associated with three parameters: severity, attack probability, and controllability, similar to the Automotive Safety Integrity Level (ASIL). The Healing Vulnerabilities to Enhance Software Security and Safety (HEAVENS) model analyzes threats based on Microsoft's STRIDE approach [39], which is a threat modeling method that categorizes cyber threats into six types: spoofing identity, tampering with data, repudiation threats, information disclosure, denial of service, and elevation of privileges [40]. In addition, the HEAVENS method ranks the risks based on three factors: threat level, impact level, and security level, which establish a direct mapping between security attributes and threats. By investigating security guidewords, the Security Guide-word Method (SGM) can help identify possible attack scenarios, such as disclosure, disconnection, delay, deletion, and stopping. For each guide word, respective protection goals are clearly defined, such as *confidentiality, integrity,* and *availability* [41]. The Security-Aware Hazard Analysis and Risk Assessment (SAHARA) is an expansion of hazard analysis and risk assessment **(HARA),** which is an inductive analysis method and also includes the STRIDE threat model [39]. SAHARA defines various securitylevels basedonattackers' knowledge, resources, and threat criticality. The Systems-Theoretic Process Analysis forSecurity (STPA-Sec) can output a listof systematic scenarios with potential security threats [42]. TheSTPA-SafeSec analysis system is an extension of STPA-Sec, integrating with physical and infonnational safety and security analysis. The Unified Safety and Security (US2) uses a simple security level to assess safety hazards and safety threats in parallel and derives safety and security requirements effectively [43]. The NHTSA threat modeling is a hybrid method characterizing potential threats for automotive control systems [44]. It combines the benefits from STRIDE [39], Trike, and Microsoft ASF and then selects their common elements to establish the ensemble threat modeling.

*Vulnerability-based:* Asa typical vulnerability-basedmethod, the Vehicles Risk Analysis (VeRA) is suitable for evaluating the risks of attacks on AVs and CAVs [45]. When conducting a safety risk analysis, it considers human capabilities and vehicle

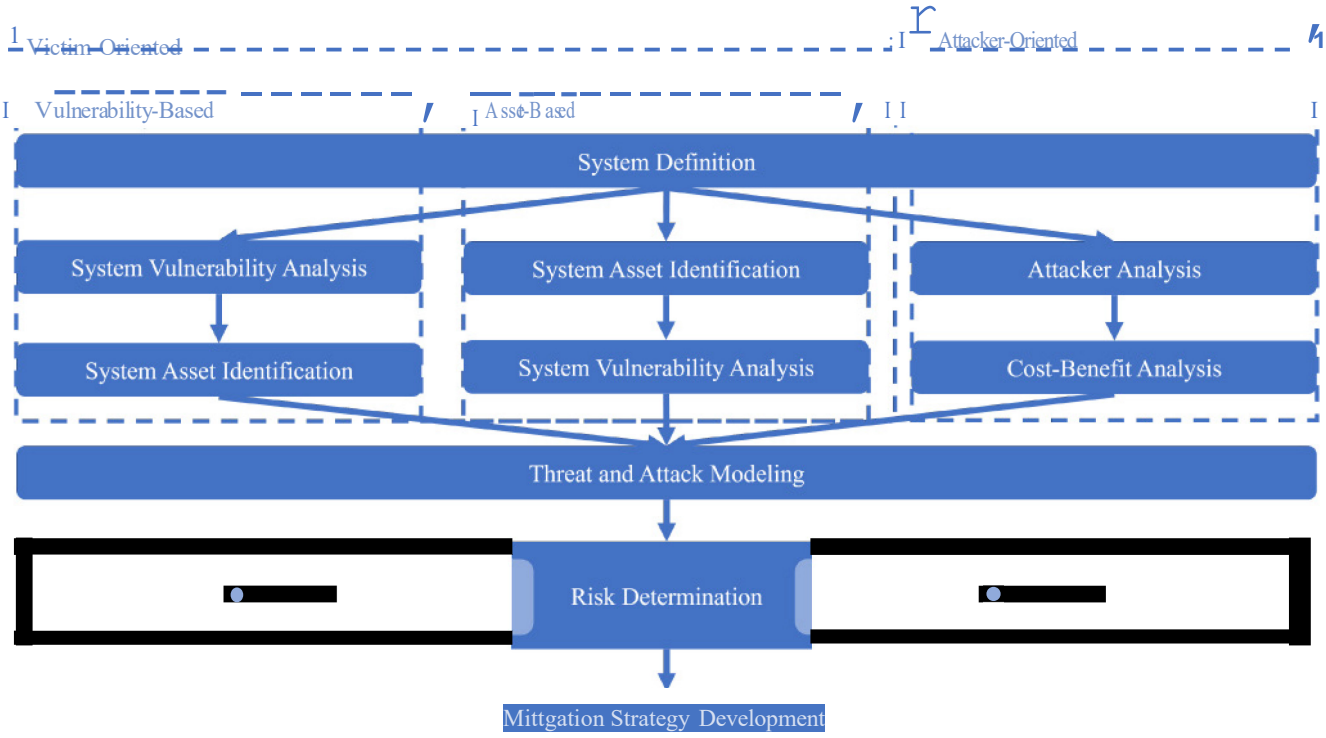



Fig. 4. Systematic engineering procedures of various TARA approaches.

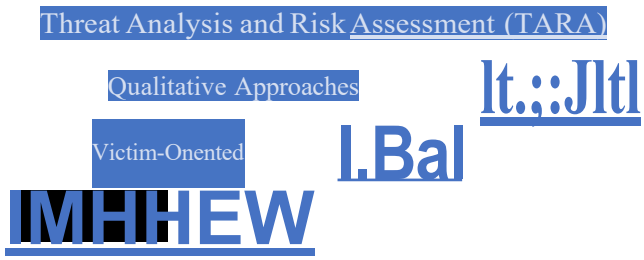



Fig. 5. Structure of threat analysis and risk assessment section.

automation levels. As a result of thesimplified analysis process, the required analysis time is significantly reduced without compromising analysis accuracy. TheFailure Mode, Vulnerabilities, and Effect Analysis (FMVEA) is an extension of the Failure Model and Effects Analysis (FMEA) with security-related threat modes [46]. It can evaluate the likelihood and severity of a system's safety and security risks.The Combined Harm Analysis of Safety and Security for Information Systems (CHASSIS) [47] is a systematic method to analyze safety and security interactively by using Hazard and Operability Study (HAZOP) guidewords. CHASSIS combines safety and security assessment and generates mitigation measures.

*2) Attacker-Oriented Approaches:* The Risk Assessment for Cooperative Automated Driving (RACAD) is an innovative application-based threat enumeration andanalysis approach that can handle different AD applications across varying levels of automation [48]. It evaluates the attack risk by the risk vector computed from weighted linear combinations of the threat matrix parameters. The likelihood of the result vector is split up into motivation and attack potential, which give a better understanding of medium likelihood threats. TheSecurity Automotive **Risk** Analysis **(SARA)** is a systematic threat analysis and risk assessment framework, including improved threat models, the latest attack method/asset map, attackers' involvement in the attack tree, and a new driving system observation index [49]. In addition, SARA offers a comprehensive threat analysiscoverage for human negligence to consider recent concerns about the trustworthiness and privacy of CAVs. The TARA+ security analysis framework for CAVs combines ISO standards and considers the levels of automation defined by SAE and the type of fault-tolerant system design [50]. The Security Abstraction Model **(SAM)** integrates security management and safety modeling as a co-engineering process with the principles of automotive software engineering [51].The Attack Tree Analysis (ATA) is similar to thesafety Fault Tree Analysis (FTA) and can adequately exploit combinations of threat patterns. However, it requires detailed information on the system design, which is inappropriate for TARA in early development phases [52]. ATA can be used forevaluating cybersecurity at different levels, depending on the scope of the specific system being analyzed. HAZOP is a well-known method that uses a list of guide-words, including fault andcybersecurity guide-words, to identify potentially hazardous situations and cybersecurity threats. HAZOP can be adapted to various ITS applications. Ref. [53]. More details of attacker-oriented approaches can be found in Table II.

### *B. Quantitative Approaches*

As aforementioned, quantitative approaches rely on the data and provide numerical results for comparison, and details of

TABLE I
SUMMARY OF QUALITXTIVE RISK ASSESSMENT APPROACHES (VICTIM-ORIENTED)

| Evaluation Approaches | | | | Risk Assessment | Risk Levels | Objectives | Suitable Systems | Ref. |
|---|---|---|---|---|---|---|---|---|
| | | | EVITA | Severity, attack probability, and controllability | 6 | Operational, safety, privacy, and financial. | IV[1], MV[2] | [38] |
| | | | HEAVENS | Threat level, impact level, and security level | 5 | Safety, tinancial, operational, and privacy and legislation | IV, MV, TN[3] | [59] |
| | | | SGM | Severity, the occurrence of operational situation and controllability | 5 | Safety | TV, MV, TN | [41] |
| | | | **SAHARA** | Reqmred resources, required know-how, and threat level | 5 | Availability, financial, privacy, safety | IV, MV, TN | [60] |
| | | | US2 | Attack potential, threat criticality, and driving automatjon levels focus | 4 | Security, safety, severity, exposure, and controllability | IV | [43] |
| | | | STPA-Sec | Attack, acc1aent, vulnerability, control, hazard | LISI 01 systemlevel scenarios | Safety and security | **TV, MV,** TN | [42] |
| | | | NHTSA method | vu1neraou1ty, a1111-culty of implementation, attack seenario, resources required, and outcome | 3 | Casualty, financial, and privacy, operator | IV | [441 |
| | | | **FMVEA** | :seventy, system susceptibility, threat properties, and probability | Risk rating | Safety and security | IV, MV, TN | [46] |
| | | | CHASSIS | users, tunctions, services, textual descriptions, sequence diagram, misuse case diagram | List risks | Safety and security | **IV,MV** | [47] |
| | | | VeRA | Attack prooaomty, severity, vehicle automation level, and human control | 3 | Safety, privacy, financial, operational | **IV,MV** | [45] |

[1] Ind1v1dual Vehicle, Multi-vehicles,[J] Traffic Network

TABLE II
SUMMARY OF QUAUD\TIVE RISK ASSESSMENT APPROACHES (ATTACKER-ORIENTED)

| Evaluation Approaches | | Risk Assessment | Risk Levels | Objectives | Suitable Systems | Ref. |
|---|---|---|---|---|---|---|
| | RACAD | Attack scenario, motivation, impact, and attack potential | Result vector | Financial, privacy, safety | **IV[1], MV[2]**, TN[3] | [48] |
| | **SARA** | Attacker profile, attack likelihood, attack goal severity, attack goal observation and controllability | Risk score | Authenticity, integrity, non-repudiation, confidentiality, authorization, unlinkability, trustworthy | IV | [49] |
| | **SAM** | Adversary, attack mouvations, attackable property, abstract failure, environment, and vehicle feature | 5 | Privacy, financial, functionality, vulnerability, security | **IV** | [51] |
| | **ATA** | Possible attacker actions and possible attack path | Tree model | Protecting vulnerable state of the system | **IV,MV, TN** | [52] |
| | TARA+ | Attack potential, attack rmpact, attack controllability, and automation level | 5 | Severity, operational, financial, and privacy | IV, MV | [50] |
| | HAWP | Attack scenario, motivation, impact, and attack potential | Keswt vector | Financial, privacy, safety | IV, MV, TN | [53] |

[1] Ind1v1dual Vehicle, Mula-vehicles.' Traffic Network

TABLE ill
SUMMARY OP QUANITIATIVE RISK ASSESSMENT APPROACHES

| Evaluation Approaches | | Risk Assessment | Risk Levels | Objectives | Suitable Systems | Ref. |
|---|---|---|---|---|---|---|
| | PASTA | Probabilistic attack analysis, regression analysis, and threat. intelligence correlation | Risk level | Identifying business objectives, identifying security and compliance requirements and impact analysis | IV[1], MV[2], TN[3] | (54] |
| | lSayes1an network-based method | tmvuonmental ractors, threat level, threat capabilities | Threat index | Safety, environment | **IV, MV, TN** | (55] |
| | **TYRA** | Attack likelihood, attack impact | Risk level | Autnentication, availability, confidentiality, and privacy | IV, **MV, TN** | (56] |
| | Bayesian Stackelberg game | Impact, likelihood, impact, at.tack resources, and TN information | Optimal actions | Probability of attacks. optimizing defense actions | IV, MV, TN | (57J |
| | PDRAFCAV | Risk profile, and user profile | Based on the selected risk assessment method | Based on needsof shareholders | **IV, MV,** TN | (58] |

[1] Indivtdual Vehicle, Multi vehicles, Traffic Network

quantitative approaches are listed in Table III. The Process for Attack Simulation and Threat Analysis **(PASTA)** is a risk-centric framework handling process for attack simulation and threat analysis [54]. Bayesian network (BN) based method is a probabilisticgraphical model thatrepresents a setof random variables and their conditional dependencies via a directed acyclic graph, which can quantitatively evaluate the risk level with analyzed parameters of the network [55]. BN can be mathematically defined by:

$$N = (G = (V,E),p), \tag{1}$$

where acyclic graph $G$ consists of a set of nodes$V$ and a set of edges $E$ between nodes, and $p$ is the set of probability distributions. Based on sufficient data, parameters can be estimated by maximizing the expectation of $Q$,

$$Q(0*10) = lEe\{logP(X10)*)1D\} \tag{2}$$

where $P$ is the density function of node $X$, $D$ is the learning data, and 8* is the updated posterior parameters. The Threat, Vulnerability,and Risk Analysis (TYRA) model analyzes assets in the system and the associated threats by modeling the likelihood of attack occurrence and the impact of attacks [56]. As a result, TYRA can generate a quantitative systematic asset risk measure to minimize system risks. The Bayesian Stackelberg game methodology is a resource-aware approach that aims to provide the optimal detection load distribution strategy for the traffic management center (TMC) used in the transportation network. This can minimize the impact of attacks and improve their detection [57]. To achieve this, the researchers defined the objective function of the attacker and TMC to maximize their expected payoffs by choosing the optimal response strategy:

$$Maximize \sum_{a\,lEA} \sum_{d;ED} L¼Jx;yJ \tag{3}$$

$$Maximize \sum_{d;ED} \sum_{qEQ} \sum_{a;EA} L\, pquix;yJ \tag{4}$$


Fig. 6. Structure of cyber attacks on CAVs section.

where $yJ$ is the probability that the attacker of type $q$ chooses action $qj$, $xi$ is the probability that the TMC chooses action $di$, ¼J and $ui$ are the payoffs of the attacker and TMC, respectively, $A$ and $D$ are action sets of the attacker and TMC, respectively. $Q$ is thesetof possible attacker types, and $pq$ is the a priori probability distribution vector containing values for all attack types $q$ in $Q$. They are both constrained by the following inequality:

$$0 :::; (aq - \sum_{d;ED} L¼)xi) :::; (1 - yJ)M \quad Vai \ E \ A \tag{5}$$

where $M$ is a predetermined maximum value used to limit the number of attack actions the attacker can choose and $aq$ represents the number of attack actions the attacker can choose. The Profile-driven Dynamic Risk Assessment Framework for Connected and Automated Vehicles (PDRAFCAV) manages data regarding CAY systems through a dynamic risk management framework. This framework provides an effective cycle of "selecting risk profiles, training and updating models and collecting data" [58].

## IV. CYBER ATTACKS ON CAVs

The structure of this section is shown in Fig. 6. In this section, we first highlight cyber attacks targeting CAVs through sensors and peripherals, including cameras, radar, Lidar, and GPS. Recentcyber attacks toward multi-sensor fusion(MSF)are also reviewed. Then, we discuss some of the applied attacks that negatively affect various CAY applications in terms of safety,

TABLEN
ATTACKS TARGETING CAV SENSORS

| Sensor | Attack Target | Attack Method | Reference |
|---|---|---|---|
| Camera | CMOS/CCD Sensors | Light Influence | [62], [63], [64] |
| | veep Learmng Model m General- CAV | Adversarial Anack | 10)], 1001, [01J |
| | 1:,na-to-ena unvmg system - CAV | | [4J, IMI |
| | Object Detection system - CAV | | [67], [69] |
| | Mult1-UOJect TracKmg System - CAV | | [IUJ |
| | Automatea Lane centenng - CAV | | Lt1j |
| Radar | Radar sensor only | Replay and spoofing | [72] |
| | bnd-to-end onvmg system with radar as only source ot perception input | :Spoonng | [1-'J |
| LiDAR | LiDAR sensor and the deep learning model | Adversarial attack and spoof-ing | [74] |
| | | 3D-printed adversarial exam-pies | [75], [76], [77] |
| | LUJAK sensor aoa me aeep learnmg moael wlm decision-level merging cooperative perception | LUJAK :spoorer aoa "'uversar-ial examples | L/ISJ |
| GPS | Message communication | Man-in-the-middle | (79] |
| | GPS Signal Overrıde | GPS spoonng | [80], [81] |
| Multi-Sensor Fusion (MSF) | Camera and LiDAR | Adversarial Anack | [82] |
| | LJUAK, Ur:S, IMU | | 1-'1 |

mobility, and environment. Note that at the vehicle level, we exclude the intra-vehicle network attacks to be more focused. Interested readers can refer to [14] for a comprehensive review.

### *A. Cyber Attacks on Vehicle Level*

Standard sensor setup in a CAY usually includes a camera, mill wave radar, Light Detection and Ranging (LiDAR), and GPS [61]. The first three types of sensors, utilized within the perception module of a CAY while the GPS is mainly used for vehicle localization, contribute to the attack surfaces. Table JV summarizes previous work targeting onboard sensors.

*1) Attack on Camera:* The camera output is image data constructed by pixels, and machine learning models are usually applied to it for information extraction. Accurate information retrieval from camera image data is vital to CAY's performance. For example, lane feature extraction is important for the localization of ego vehicles, as mentioned in [83]. **Ma**nipulation of the output of image-based perception results occurs on either the inference or the image source part. Attacks targeting the camera usually use other light sources to influencethecamera's Complementary Metal-Oxide-Semiconductor (CMOS)/Charge-Coupled Device (CCD) sensors. A study [62] showed a jamming attack targeting the camera using a laser beam, whichcanalsolead topermanent damage when a stronger beam or longer attack time is executed. Disturbances targeting the camera can affect the performance of the vision-based perception module in a CAY system, as shown in [63] and [64]. These attacks aim to maximize prediction errors of the computer vision module, which may further influence thedecision module of a CAYsystem.Moreover, the physical attackcan permanently damage the camera sensor itself. This irreversible damage can cause high replacement and fixing costs.

Attacks targeting computer-vision-based perception affect machine learning models involved in the perception module through adversarial samples focusing on object detection, classification, and tracking [67]. 1n[69], a set of adversarial attacks targeting the traffic light classification model was proposed. In this research, spatial, one-pixel, CarlirLi & Wagner (C&W), and boundary attacks were deployed to test the robustness of the traffic light classification model. Jia et al. [70] proposed an adversarial attack targeting multiple object tracking (**MOT**), which isessential in autonomous driving. This work utilizes the optimization method to generate adversarial examples that can fool **MOT** algorithms. The optimization method achieved two goals: (a) to minimize the target class probability and (b) toshift adversarial bounding boxes to desired locations. Sato et al. [71] proposed a real-world physical adversarial attack through road patches. An optimization method was used to generate a malicious patch that can be applied on the road. The proposed attack was evaluated ona production-level Automated Lane Centering (ALC) system, with a successful attack rate of over 97.5%. The successful attack led to a collision with 100% probability. Also, for end-to-end autonomous driving systems, adversarial attacks were studied to evaluate the effect on system performance. In [68], researchers generated adversarial perturbations to fool thecamera sensors and maximize steering-angle errors. Such an attack was also evaluated in the real world by[4], and the results showed that the average errors of thesteering angle could reach up to 26.44 degrees.

*2) Attack on Radar:* Compared withattack studies oncamera sensors, research targeting radar is comparatively less. This is partly because the radar information extraction process does not rely on deep learning and neural network-based classifiers, where adversarial attacks cannot be performed. There aresome studies about performing spoofing attacks on the radar sensor. Researchers in [72]executed replay attacks and spoofing attacks targeting mmWave radar. In [73], the victim vehicle was assumed to make turning decisions only based on the radar-based perception module. The attack aimed to spoof the perception module in the victim's vehicle, eventually influencing the turning decision.

*3) Attack on LiDAR:* A LiDAR utilizes lasers to measure the distance of target objects by receiving returned laser signals reflected from objects. It has been shown in [74] that directly shooting a laser beam at LiDAR does not affect its performance.

However, strategically generated adversarial examples may be able to fool machine learning models. Following this direction, Cao et al. [74] formulated the generation of spoofing attacks as an optimization problem and designed the perturbation and objective functions. Another study tried to produce 3D objects with shapes that eventually fool the deep learning model, which processed the LiDAR point cloud [75]. Similarly, Sun et al. [76] proposed aspoofing method tofindfeature mapsof the perturbed point cloud so that the target module could wrongly detect the perturbed object as a vehicle. In contrast with the goals in [75] and [76], Tu et al. [77] proposed an algorithm to generate 3D objects with the shape that makes vehicles invisible from the deep learning-based inference model. A recent work [78] considers attacking the **LiDAR** perception systems under the cooperative perception setting. This study proposes spoofing attacks, physical removal attacks, and adversarial attacks as threat models. Spoofing attacks aim to create non-existing objects in the point cloud detection with LiDAR spoofers, physical removal attacks aim to use spoofers to hide real objects from LiDAR detection results, and adversarial attacks aim to create objects in the point cloud thatDL-based inference models cannot recognize.

*4) Attack on GPS:* The most common attack type of GPS is spoofing. One form of GPS spoofing attack is from a network communication perspective. This kind of attack utilizes a man-in-the-middle attack and hijacks the global coordination for vehicle localization [79]. Most GPS spoofing attacks use a GPS spoofer to perform signal override. The GPS spoofer provides a malicious signal with a usually higher power density so that the targeted receiver chooses to lock onto the malicious signal instead of the benign one [80]. Even with the same attack vector, different works propose different attack targets and scenarios. Ref. [81] proposed a GPS spoofing attack that affects the localization first but also affects the computation of the absolute coordinate of surrounding objects. The coordination conversion from an ego-vehicle-centric to world coordinate requires the accurate localization of the ego vehicle itself.

*5) Attack on Multi Sensor Fusion (MSF):* A common belief is that multi-sensor fusion (MSF) is necessary to enhance the cybersecurity of modem CAY systems since attacking multiple sensors is much more difficult in real-world settings [82]. Different sources and information can provide cross-validationand also serve as a backup when one sensor is compromised. However, recent research showed that a multi-sensor fusion-based perception system could also be compromised [3], [82]. Io [82], researchers penetrated the MSF algorithm using an adversarial attack targeting LiDAR and the camera. Another study attacked an MSF-based localization algorithm that utilized LiDAR, GPS, and IMU information by only spoofing data in GPS signals [3]. An optimization model was developed to maximize the distance between the spoofing distance and the output of the MSF algorithm without attack. These recent studies show that there sWl exist potential attack surfaces for MSF algorithms. Therefore, MSF should not be considered an ultimate defense solution for the CAY perception module.

### *B. Cyber Attacks on CAV Applications*

Cyber attacks on CAY applications mainly focus on the system layer, which affects functionalities of a particular application such as cooperative adaptive cruise control (CACC) beaconing or message exchange in the Y2X environment [84], [85]. Io this section, we will focus on the cyber attacks that affect the overall perfonnance of CATS based on three primary performance areas; safety, mobility, and environmental impact. Some representative studies are summarized below and shown in Table Y.

*1) Safety Impact:* The safety impact concerns the potential conflict and collision between vehicles. Mani et al. [86] used radio jamming to disrupt all communications within the platoon. As a result, the space gap of the CACC vehicle stream decreased, which compromised thesafety of the whole platoon. Moreover, because there were nosecurity features implemented in vehicles, the falsified beacons were accepted and used for longitudinal control, leading to string instability; the resultant disturbance magnifies through the stream over time. Abdo et al. [6] performed a detailed analysis of CACC and used this analysis to classify the types of vulnerabilities.

Resultsshowed that their attackscould increase averagespeed difference and reduce Time-to-Collision (ITC) [87], leading to higher risks **in** car crashes for specific scenarios. **Hu** et al. [8] perfonned a security analysis to make the discovery ofDoS (Denial of Service) vulnerabilities automatically in the IEEE 1609 protocol family and CACC applications. They found that their attacks could fully eliminate the benefits of CAY applications (e.g.,Forward Collision Warning (FCW)) and increase thespeed standard by 43%, introducing instability to the upstream traffic. Koley et al. [9] created an attack that can cause collisions as well as impair performance by compromising traffic efficiency. An example from their study demonstrated a safety-violating attack scenario where the space between vehicles was reduced, resulting in a collision.

*2) Mobilty Impact:* Most studies focus on a reduction in averagespeed or a dropinroadwaycapacity in tenns of mobility. Abdo et al. [6] illustrated that their attack strategies for various CAY applications could cause speed reduction and excessive lane change maneuvers, which highly affected the system mobility performance. Chen et al. [7] and Huang et al. [88] analyzed the system design and identified data spoofing strategies that can potentially influence traffic control in the Intelligent Traffic Signal System (I-SIG). Using the data spoofing strategy and knowing the planning stage configuration, the traffic got congested, and the total delay increased by 94.0% and 38.2% on average, which completely reversed the mobility benefits of using the I-SIG system. Haydari et al. [89] proposed an attack that manipulated a traffic signal control system that relied on a Deep Reinforcement Learning (DRL) system. It turned out the proposed attacks affected the Deep Neural Network policies and degraded the performance of the traffic signal controllers in terms of average waiting time. Yen et al. [90] proposed anattack strategy targeting a back pressure-based signal controller, which could maximize the number of disrupted phases, thus increasing

TABLEV
SUMMARY OFCYBER ATTACKS ON AIJfOMATED CAYS APPLICATIONS

| Paper | Applications | Attack Type | | | | Studied Traffic Metrics | | |
|---|---|---|---|---|---|---|---|---|
| | | raJsuymg | :spoonng | Keply | LJO.) | Moornty | tmvrronmental | :Satety |
| [86] | cAcc[1] | | | | | | | |
| [6] | CACC | | | | | | | |
| [7] | ITS' | | | | | | | |
| [8] | CACC | | | | | | | |
| [9] | CACC | | | | | | | |
| [10] | CRM' | | | | | | | |

' Cooperative adapat1ve cruise control, ' Intelligent Traffic Signal System;' Cooperative Ramp Merging

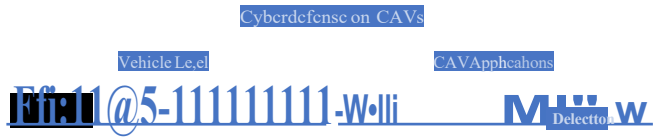



Fig. 7. Structure of cyber defense on CAVs section.

average traffic delays and disrupting fairness. Results from Zhao et al. [10] showed that mobility performance decreased by up to 55.19% for the cooperative ramp merging scenario when their spoofing attacks were implemented.

*3) Environmental Impact:* There is a minimal amount of research considering the environmental impacts due to cyber attacks. Zhao et al. [10] analyzed energy consumption and pollutant emissions impacts from the cyber attacks on both mainlineand on-rampvehicles.Inaddition, resultsdemonstrated that with the increase in theCAY penetration rate (i.e., the attack ratio), fuel consumption and CO2 emissions are significantly decreased.

## V. CYBER DEFENSE ON CAVs

Cyber defense refers to policies, practices, technologies, and infrastructure that are put in place to prevent or mitigate attacks via unauthorized access to a device, data, or network infrastructure as a whole [91]. Similar to cyber attacks, the cyber defense studies on CAVs are also reviewed at an individual vehicle level and CAY application level, as shown in Fig. 7. Cyber defense models at the vehicle level correspond tocyber attacks, in which four different sensor types are considered. We mainly focus on implementing SCMS and misbehavior detection at the CAY application level.

### *A. Defense on Vehicle Level*

Regarding cyber defense studies on CAV sensors, many studies focus on defending against adversarial attacks toward camera images. Deng et al. [92] analyzed four defense methods against adversarial attacks, including adversarial training, defensive distillation, anomaly detection, and feature squeezing. The defense methods were applied to different driving models against five different adversarial attacks. Two defense methods were proposed against the adversarial attacks on traffic light detection in [69]. The proposed defense methods were adversarial training and defensive distillation. Li and Velipasalar [93] proposed a defense method by using adversarial example detection. A new distance metric was designed to describe the differences between twoobjectdetection results.Theadversarial examples were detected by using the new evaluation metric and monitoring the variance of a temporal inconsistency. A similar method was also proposed in [94], in which a new weighted frame-wise distance metric was proposed to evaluate similarities between the detected object and ground truth. Another work proposed by [95] utilized physical constraints between stereo-images from the left and right cameras. The researchers used an optimization method to minimize the effect of the adversarial perturbation on a given stereo 3D object detector. The proposed defense method was effective against adversarial attacks.

Existing defense studies on radar and LiDAR are limited, partially due to insufficient pertinent cyber attack research.Most studies that attack radar mainly focus on interfering with wave signals. To mitigate the signal interference, Chen et al. [97] proposed to utilize Generative Adversarial Network (GAN) to recover the wave signal in the frequency domain. Such a method can address missing sensor signal problems due tospoofing and jamming attacks. A study by Sun et al. [76] showed a potential defense method against spoofing attacks targeting LiDAR. This work utilized physics-informed anomaly detection as a defense method. Laser penetration detection was used to detect abnormal point clouds and findspoofed fake vehicles. Under the cooperative perception Lidar setting, [78] also proposed several defense methods from a decision-level merging perspective. The verification and identification process is done considering the occupied area created by objects. Then, affected agents are identified with cross-validation from observation results from other agents, and suspicious points are removed. The region occupied by adversarial samples is also marked as an unsafe region and will further support the object detection process of other agents. A summary of defense work on sensors is summarized in Table VI.

### *B. Defense on CAV Applications*

To ensure that CAV technologies operate in a safe, secure, and privacy-protective manner, a proof-of-concept (POC) security system was designed and implemented to enable vehicles to trust each other and the whole system. The Security Credential Management System (SCMS) is a security solution for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. Fig. 8 gives an overview of the system architecture.

TABLE VI
SUMMARY OF DEFENSE METHODS ON SINGLE AtrrOMATED VEHICLE SENSORS

| Sensor | Defense Target | Defense Method | Reference |
|---|---|---|---|
| Camera | Adversarial Attack | Adversarial training, defensive distillation | (69] |
| | | Iterative Targeted Fast Gradient Sign Method (ITFGSM), Optimization-based method (Opt), AdvGAN, universal adversarial perturbation (Opt uni), AdvGAN universal adversarial perturbation (AdvGAN uni) | (92] |
| | | Adversarial example detection | (93]. [94] |
| | | Detection usmg physical constrams | L :>] |
| | | Modular verifical!on model | I OJ |
| Radar | Signal Interference | Generative Adversarial Network (GAN) based signal recovery | [97] |
| LiDAR | Spoofing Attack | Physics-informed anormality detection | [76] |
| | :spoonng attack and Adversarial attack | Unsafe region identification with cross-validation from other agents | (78] |
| GPS | Man-in-the-middle | Encryption and authentication | [79] |
| | GPS spoofing | Misbehavior detection | [80], [81], [98] |

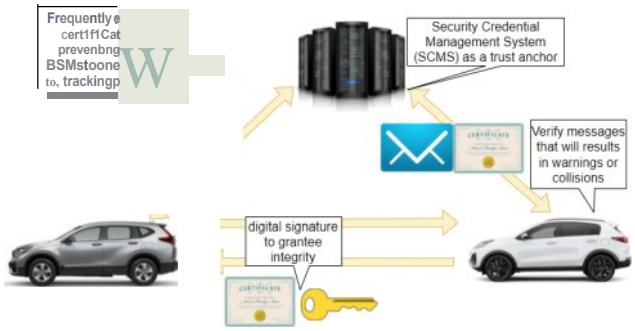



Fig. 8. SCMS ecosystem.

It relies on digital certificates and public-key cryptography to authenticate andencrypt messages, which require a trustedentity to manage the distribution and revocation of these certificates. The SCMS serves as this trusted entity, managing the digital certificates and cryptographic keys used by vehicles and infrastructure tocommunicate securely by obtaining credentials from certificate authorities (CAs) and attaching those certificates to their messages, such as basic safety messages (BSMs), as part of a digital signature. In addition, it ensures that only authorized devices are allowed to participate in the communication and that messages are protected against tampering, interception, and replay attacks. The SCMS is designed to be highly scalable, manage large numbers of certificates, and support a wide range of security policies and trust models. It has misbehavior detection as an essential feature to identify and respond to any malicious or abnormal behavior that may compromise the security and safety of the V2X network. Misbehavior can include message tampering, denial of service attacks, and false message generation. Misbehavior detection involves identifying patterns of behavior that are inconsistent with the expected behavior of a device. At thesame time, reputation-basedsystems usefeedback from otherdevices to assess thetrustworthinessofa device.Once SCMS receives misbehavior information about some devices, it will add these devices' certificates to the certificate revocation list (CRL) and distribute it to other devices so that it will no longer be considered a trusted source for sending and receiving messages.

In addition to SCMS, many other methods have been developed for misbehavior and anomaly detection over the years. For example, utilizing cross-validation with data from other sources, falsified trajectories could be identified [99], [100], [101], [102]. Other studies focused more on abnormal route detection [103], [104], where routes with excessive length were identified as outliers. Misbehavior detection is also applied to GPS spoofing attacks to determine whether the received trajectory is in accordance with the vehicle's kinematic properties and surrounding road network [98]. In [105], [106], an embedding trajectory model inspired by the word embedding model from the natural language process (NLP) is proposed to create vector representations of trajectory points. Then, a clustering model is developed to conduct a majority vote to differentiate abnormal trajectories from normal ones. In recent years, a variety of machine learning techniques have been applied to misbehavior and anomaly detection, such as clustering [107], [108], inverse reinforcement learning [109], generative adversarial network (GAN) [110], and recurrent neural network(RNN) including thelongshort term memory (LSTM) neural network [111], [112]. Table VII summarizes these emerging solutions.

There also have been some defense work against adversarial attack targeting theCAY applications. Dinget al. [113] proposed a defense method against adversarial attacks onencrypted traffic data using both passive and active defense methods. Denoising autoencoder with image reconstruction was used in the passive defense phase, and adversarial training was applied in the active defense phase. Both methods couldsignificant]y improve classification performance and were regarded as a feasible solution to adversarial attacks on encrypted traffic data. Haydar et al. [89] proposed a defense method using ensemble methods against attack targeting Deep Reinforcement Learning-based Traffic Signal Control (TSC) modules. The proposed defense method outperformed other listed methods by detection accuracy. Yen et al. [90] proposed an auction-based and hybrid-based algorithm for attack mitigation when the backpressure-based TSC module

TABLEVII
SUMMARY OF CYBER DEFENSES ON CAV APPLICATIONS

| Mitigated attacks | Solution Key | Authentication | Reference |
|---|---|---|---|
| Spooling | Semi-analytical expression | | (100], (99] |
| Sybil | Physics-based trust propagation scheme | | [101] |
| Falsification | Computing similarity | | (102] |
| Spoofing | Classification and mapping | | [104] |
| Bogus, replay, collusion | Traffic flow model | | [III] |
| Spoofing | Physical layer plausibility checks | | [IIS] |
| Falsification, sybil | Physical signal tracking and RSSJ validation | | [116] |
| Falsification, sybil | Extended Kalman Filter (EKF) | | [II7] |
| Falsification, sybil | Classifying | | [118] |
| Sybil | KNN and SVM | | [I 19] |
| Falsification | Natural language processing and hierarchical clustering | | (105], (106] |
| Falsification | Game theory | | [120] |
| Adversarial | Deep reinforcement learning | | [89] |
| Fake, replay, stealthy | Plausibility check Interacting Multiple Model **(IMM)** and reinforcement learning | | [114] |
| Falsification | Blockchain and unsupervised learning | | (121] |
| Spoofing, bad mouthing, sybil voting | Blockchain | | [122] |

TABLEVIII
SUMMARY OF EVALUATION PLATFORMS

| Evaluation Platforms | | Pros | Cons | Literature |
|---|---|---|---|---|
| Individual Vehicle Oriented | SVL | Realistic 3D scenarios, various sensors, GPU computing, various customized sensors modelling, simplified precise vehicle dynamics, open source | Hardware requirements, lack of off-road scenarios | (123] [71] |
| | CARLA | Realistic JD scenanos, vanous sensors, GPU computing, various customized sensors modelling, simplified precise vehicle dynamics, open source | Hardware requirements, lack of off-road scenarios | (126] [127] (128] [129] |
| | Gazebo | Keanst,c jLJ scenanos, extremely precise physical models and vehicle dynamics, various customized sensors modelling, open-source | '11me-consummg bu11amg 3D models, less realism environment | (131] [132] |
| | MATLAB /Simulink | Details plotting tools, clear logic boxes, precise vetucle dynamics, various customized sensors modelling | Limia:o visualizatmn, commercial | (133] [134] [88) |
| Traffic Oriented | SUMO | Built-in models, extension interface, open-source, large user community noress1ona1-graae, bmll-m models, jLJ v1sua11za11on, | No 3D visualization | (135] [137][138] |
| | VJSSJM | easy coding | Commercial | (139] [140] [7] |
| | IVIAILAH | ueta11s plothng tools, user-friendly GUI | No bmll-m mOdels | P41J I143I |
| | Aimsun | noress1ona1-grade, built-m mOdels, 1mpllc1ty m ereating network and animation, 3D visualization, extension interface, Mic/mes/macroscopic capable | Commercial, cumbersome coding | (144] [145] |
| Communication Network Simulators and Co-simulation | OMNeT++ | Modular and flexible, active community, GUI for building and visualizing simulations Scalable and efficient for large-scale simulations, | Complex to learn and use | (146] [147][148] |
| | NS-3 | wide range of networking protocols and models, simple programming interface | Limited in custornizability, no GUI | (149] [150][156] |
| | VENTOS | Integration of SUMO and OMNET++ | Only support U:SKC-enabled communication | (15t J [t52J |
| | CAKMA | Integration of :;UMO, N:'ij, andCARLA | Hardware requtrements | [157J |

had been attacked. The defense performance was evaluated by a delay of distribution, number of scheduled phases, and fairness. By using such evaluation matrices, the attack's impact was successfully mitigated by applying the proposed defense method. Abdoet al. relied on physically modeling the vehicles and their interactions using dynamics and state estimation filters as well as reinforcement learning [114]. It combined these observations with knowledge of applicable rules and guidelines to capture logic deviations. As a result, their defense could accurately and promptly detect attacks with low false positive ratesover a range of attack scenarios for different CV applications. Table VII summarizes the major studies on the cyber defense of CAV applications.

## VI. EVALUATION PLATFORMS

Emerging simulators and testbeds can provide cost-effective alternatives to quantify the impacts of cyber attacks and evaluate the performance of cyber defense on connected and automated transportation systems (CATS). This section further discusses these evaluation platforms as shown in Fig. 9.

Simulation platforms for cybersecurity can be categorized into two major types: individual vehicle-oriented and traffic-oriented. Individual vehicle-oriented platforms leverage vehicle dynamics and onboard sensing, while traffic-orientedsimulators focus on the interactions between CAVs and other road users as well as roadside infrastructure to analyze impacts on the entire


Fig. 9. Structure of evaluation platforms section.

transportationsystem. Moreover, communication network simulators that model wireless communications between CAVs may be introduced as co-simulation platforms by integrating with other platforms/modules to further exploit CATS performance in a more realistic environment.

### A. Individual Vehicle-Oriented

At the individual vehicle level, the high-fidelity simulator **SVL** takes advantage of the game engine *Unity* to model vehicle dynamics, photo-realistic 3D virtual environment, traffic simulations for vehicles and pedestrians, and multiple sensors including camera, LiDAR, GPS, IMU, and radar [123]. The simulator can create a basic dynamic vehicle model for the ego vehicle and accommodate external third-party models via a Functional Mockup Interface. A realisticenvironment, including roads, buildings, and weather conditions, can help evaluate and train vision-based perception algorithms. The simulator can provide communication bridges for messages exchanged between the Automated Driving (AD) stack and the simulator, which can be used with Autoware [124] or Baidu Apollo [125]. In addition, sensors allow intrinsic and extrinsic parameter customization. Virtual ground truth sensors are supported to provide labeled information for sensor-relatedcyber attacks and cyber defense validation. Researchers usedsoftware-in-the-loop (SiL) evaluation with SVL to evaluate the safety impact of a DNN-based Automated Lane Centering (ALC) system. They also designed a physical-world adversarial attack called Dirty Road Patch (DRP) to test thesystem's robustness.[71]. **CARLA** is an Unreal Engine-based, open-source simulator developed for autonomous driving research [126]. Similar to SVL, a variety of sensors and high-quality environments are supported. It leverages the OpenDRIVE standard to define roads and urban settings, which can automatically generate a road grid with traffic lights and signs.The simulator can support many built-in automation functions such as perception, mapping, positioning, and vehicle control, enabling end-to-end testing and training of CAV algorithms [127]. Recent work claimed that CARLA could reduce the time between digitally crafting a perturbation and testing it with realistic scenarios [128]. Additionally, the reproducibility of the CARLA simulator and the variety of environmental conditions can also enable researchers to craft new perturbations with realistic constraints so that they can have a better understanding of the efficacy of different attacks [129]. **Gazebo** is another open-source, scalable, flexible, and multi-robot 3D simulator that relies on three main libraries: physics, rendering, and communication libraries. It can provide high-precision physics for robotics-related simulation [130]. Swanson et al. created a hardware-in-the-loop **(HiL)** simulator and indicated that although ROS already included a graphical interface RViz for visualization,Gazebo was necessary because it could model much more accurate physics. Besides, ROS has a significant amount of support for stand-alone system dependency of Gazebo [131]. The listener and publisher constitute a scalable architecture that allows multiple nodes to control agents, which provides more attack surfaces for evaluation. Zhang et al. developed a Gazebo-based vehicle-to-everything (V2X) platform for the simulation of CAY environments [130]. On top of Gazebo, they extended a communication module receiving and sending information between vehicles and roadside units (RSU). They leveraged Gazebo to provide precise vehicle dynamics and construct each CAY as an independent robot model with multiple parts, such as state listener and publisher, to enable system status monitoring.

*MATI.AB/Simulink:* is suitable for model-based systems evaluation and analysis. It includes the Automated Driving Toolbox (ADT), which provides tools that can help with the design, simulation, andtesting of Advanced Driving Assistance Systems (ADAS) and automated driving systems [132]. HERE's HD live map data and OpenDRIVE road networks can be easily imported. MATLAB/Simulink allows researchers to simulate a real-time model of the target system. The model contains both continuous vehicle dynamics and discrete vehicular communication network behaviors [133]. It also allows users to use the Ground Truth Labeler app to automatically label objects. Giiven<; and Kura! used multiple-drivers-in-the-loopsimulation in adaptive cruise control tests using MATLAB and Simulink [134]. Recent work evaluated the impact of falsified data attacks on I-SIG via 20 hours MATLAB simulation [88].

### B. Traffic-Oriented

Although the 3D engines mentioned above can provide realistic vehicle dynamics and high-fidelity environments, high computational demands are required when they are used for multiple vehicles or traffic simulations. Unlike individual vehicle simulators, microscopic traffic simulation platforms treat vehicles as moving boxes, which compromises modeling accuracy in physics but significantly reduces computational loads. **Simulation of Urban Mobility (SUMO)** is an open-source microscopic traffic simulator for a variety of transportation applications, such as dynamic navigation, traffic surveillance systems evaluation, and traffic signal control algorithm development [135]. In addition, SUMO provides *Application Programming Interfaces* (APls), called *Traffic Control Interface* (TraCI), to establish the connection with external applications through a socket connection for the access of network topology, signal control, and vehiclebehavior [136].Ina recentstudy, researchers proposed a simulation-based fault injector (SUFI) that was capable of injecting faults intoADAS features using SUMO [137]. Dasgupta et al. developed a "slow poisoning" attack generation strategy foran adaptive traffic signal controller and a prediction-based "slow poisoning" attack detection strategy [138]. They modeled the attack strategy using SUMO and used the simulated data to develop the attack detection model. **VISSIM** is a commercial microscopic traffic simulator developed by PTV

Group, modeling motorway traffic as well as urban traffic operations[139].The toolcan be used to investigate private and public transportation as well as pedestrian movements. In addition, it provides a structure of one-way links, called connectors, for constructing road networks [140]. Like SUMO, VISSIM provides a component object model (COM) programming interface with user-developed algorithms and enables modeling complex control logic and V2X applications. Chen et al. deployed data spoofing attacks towards the I-SIG system, targeting both algorithm design issues and field implementation limitations in the adaptive signal control algorithm [7]. **MATLAB** is a coding-based interactive system for numerical computation [141]. It provides useful toolboxes with wide customization freedom for researchers to build various models. Besides toolboxes, MATLAB SimEvents is a discrete-event simulation software tool that is designed for modeling and simulating dynamic systems, which can provide a visual environment for building simulation models using block diagrams, similar to Simulink.. Researchers analyzed the causes of congestion using a queuing model built using MATLAB SimEvents based on observations and traffic data analysis [142]. Moreover, MATLAB has built-in functions for working with traffic data analysis, such as traffic volume, speed, and occupancy, to evaluate the impact of cyber attacks on traffic. This can involve processing and visualizing large datasets to identify patterns and trends and evaluate traffic management strategies' performance. MATLAB can be used for vehicle longitudinally microscopic behavior modeling and trajectory generation toevaluate cyber attacks' influence on the longitudinal safety of CAVs [143]. **Aimsun** is a full-featured and widely used commercial traffic simulation with the ability to simulate the detailed behavior of each individual vehicle in the traffic network ona time scale ofless than one second [144]. Aimsun is also very extendable and customizable by interfacing with external codes through various available APis. Reilly et al. constructed benchmark scenarios using Aimsun to identify the potential cyber vulnerabilities of ramp metering forfreeway traffic control [145].

### C. Communication Network Simulators and Co-Simulation

Network simulation is particularly important for cybersecurity research on CATS, as more realistic models are required to assess the impacts of connectivity-related attacks and defense strategies. There are a few state-of-the-art network simulators, as described below. **OMNeT**++ is an open-source, modular, component-based C++ simulation library and framework that can be used to simulate complex communication networks with high fidelity [146]. It can perform network attack and threat analysis in a simulation environment. For example, the data recording function in OMNeT++ can reflect the impact of different types of attacks on the network and generate datasets for learning-based cybersecurity models. For example, a previous study deployed a DDoS attack to jam the communication channel in a VANET via OMNET++ [147]. Another recent study investigated the self-reported location anomaly detection problem for CAVs with OMNeT++ [148]. **NS-3** provides support for creating virtual nodes and implementing point-to-point, wireless, or CSMA (Carrier Sense Multiple Access) connections between nodes [149]. It is suitablefor the VANET (Vehicular Ad hoc Network) environment because it supports multiple modem standards and routing protocols such as **WAVE** (Wireless Access for Vehicular environment) standards and AODV (Ad-hoc On-Demand Distance Vector) routing protocol. Acbarya et al. implemented their blackhole attack prevention scheme in the NS-3 simulator under WAVE standards with AODV routing protocol [150]. Many researchers realized that even though each simulator bas its own advantages and focused arena, more than a single simulator is needed for comprehensively modeling and evaluating cybersecurity problems as well as establishing a realistic testing environment. As a result, emerging co-simulators and integrated platforms provide more options to researchers. **VEhicular NeTwork Open Simulator** (VENTOS) is an integrated C++ simulator for modeling vehicular traffic flows, cooperative driving, and interactions among CAVs or between CAVs and infrastructure equipped with DSRC [151]. It takes advantage of the microscopic simulator SUMO and network communication simulator OMNET++ to provide realistic traffic modeling and network simulation. Kumar et al. assessed the impact of various attacks on cooperative driving use cases such as cooperative adaptive cruise control (CACC) via VENTOS [152]. Zhao et al. utilized VENTOS to reveal the cybersecurity risks of cooperative highway on-ramp merging in a mixed traffic environment [153]. Another open-source co-simulation platform **CARMA** [154] developed by the U.S. Department of Transportation integrates CARLA, SUMO, and NS-3 to establish everything-in-the-loop (XiL) simulation to evaluatecooperative automated driving.Thiscould bea potential tool forcybersecurity researchbetween the vehicle and vehicular network levels. Some early studies targeted vehicle-level cybersecurity with CARLA [68]and network-level cybersecurity with NS-3 [155].

## VII. CURRENT GAP AND FU'RuRE RESEARCH DIRECTION

In this paper, we reviewed recent cybersecurity studies on CATS from four perspectives, including risk assessment, cyber attacks, cyber defense, and evaluation platforms at both the individual vehicle and CAY application levels. Below, we discuss current gaps and challenges in the existing literature and future research directions, summarized in Table IX.

### A. Threat Analysis and Risk Assessment

Most of the analytical approaches assessing risks and threats of CAY applications are qualitative and highly dependent on subjective opinions and specific use cases. Therefore, these methods are not ready to be scaled up, and the results are hardly compared. On the other hand, quantitative approaches adapt to different risks and provide measurable results that are easily compared. With the development of more data-driven or learning-based evaluation methods, there is an increasing demand forspecialized and large-scale datasets, which iscritical to guarantee high accuracy and confidence. As a result, data-driven TARA approaches should gain more attention.

TABLE IX
CURRENT GAP AND FIJnJRE RESEARCH DIRECTION SUMMARY

| Field gap | Direction |
|---|---|
| Threat Analysis and Risk Assessment | Using specialized and large-scale datasets, i.e. data-driven TARA approaches. |
| Cyber Atlack | Limited research on attacking multi-sensor fusion (MSF) models. |
| | Inves11gatmg complex anct ume-consummg cyber attacks. |
| | Investigating vulnerabilities of ainerent CAVs applications m terms of security and safety. |
| Cyber Defense | More defenses agamst L1dar-based adversarial attacks. |
| | unexplored cyber aerense under a coopera11ve perception envrronment. |
| | Investigating more confidentiality, non-repudiation, and authentication solullons in CAVs. |
| | Invest,gatmg the system's res1hence anct m1t1gat100 solut,oos. |
| Evaluation platforms | Investigating the impact of cyber attacks and defense services. |
| | Investigating human-in-the-loop simulation. |
| | Using rea.1-world testbeds tor CAVs cybersecunty. |

### B. Cyber Attack

For deep-learning-based perception systems, current attack methods mainly focus on degrading the performance of the perception system by lowering the detection accuracy. For non-deep-leaming-based perception systems, existing research on attacks focuses on interfering with the physical signals received. It is important to investigate the impacts of the sensor attacks at the multi-vehicle and/or transportation system level since vehicles, in essence, need to interact with each other. Considering the cyber-physical nature of CATS, how to launch attacks that can cause permanent physical damage without contacting the sensor remains a question. There is also very limited research on attacking multi-sensor fusion (MSF) models. There only exist two current works addressing MSF as a target, one for localization module [3], theother for multi-sensor fusion [82].It should benoted thatmultiple types ofMSFmodelsapply toCAY deployment [158], [159], [160], and the current investigation is far from sufficient. Such models are considered one of the most common defense methods against cyber attacks on a CAY perception system. Recent research targeting attacks towards MSF only focuses on a specific CAY platform, which can not be generalized in other CATS.

At the CAY application level, the adversary uses message falsification (modification) and spoofing (masquerading) or replay attacks to affect the vehicle stream maliciously. These attacks can be easily detected using state estimation or machine learning mitigation algorithms. However, the most complex and time-consuming cyber attacks still need to be made easier to pull off.These sophisticated attacks can be adversarial adaptive attacks, stealthy attacks, frog-boiling attacks, etc. For example, in stealthy or frog-boiling attacks, the attack can be used to disrupt the whole CAY network by continuously lying to all the connected nodes without being noticed by injecting small offsets. The goal is to move some victim CAYs to arbitrary coordinates far from the rest of the traffic. The adaptive attack is specifically designed to target a given CAY mitigationscheme.It can bedone through different methodsforgenerating adversarial examples.Themostwidely adoptedapproachis gradient descent because it does not require knowledge of the machine learning model's architecture or parameters. Instead, the attack only needs to be able to query the model and compute its gradient with respect to the input data. Moreover, as the number of CAYs is expected to grow significantly, more efforts are needed to investigate vulnerabilities of differentCAY applications in terms of security andsafety. Attacks must begeneralized and not target just one or two CAY applications.

### C. Cyber Defense

Defense methods for CAY onboard sensors mainly focus on protecting against adversarial attacks (camera), signal inference (radar), and spoofing attacks (LiDAR and GPS). With the growing usage of Deep Neural Networks (DNN) in inferring Lidar point cloud data, defense againstLidar-basedadversarial attacks is an important future research topic. For non-DNN-based inference models, a possible defense method would be targeting information recovery. Given thespoofed signals from thesensor, a keyquestion is how the ground truth information can be recovered. In addition, the majority of existing studies only consider sensors of a single CAY. Although there had been work about creating cooperative perception for CAYs [161] and utilizing cooperative perception information for other applications like motion planning[162],or consideringcommunication issues undersuch assumption [163], thecyberdefense under acooperative perception environment is a largely unexplored area, as we only observe oneresearch work address the cyber-defense under such assumption [78]. Other research gaps for the defense against cyber attacks on CAY onboard sensors include the systems' resilience and mitigation solutions.

In general, most of the existing research in the transportation domain lies within the region of information integrity and availability. However, other essential factors are not yet discussed in this domain regarding cybersecurity. These factors include confidentiality, non-repudiation, and authentication. Investigation of these factors should be another critical future research direction.

Finally, revocation is a huge security concern. Given the potential damage a malicious user could causein a CATS, a mechanism that deactivates a malicious user's credentials and renders the user unable to send messages is required. Unfortunately, revocation solutions involving a central pseudonym certificate revocation list(PCRL) are not ideal because the pseudonym certificates' short lifespan necessitates a large and highly dynamic PCRL. Furthermore, thecommunication complexity required to keep all vehicles up to date on PCRL would be enormous.

### D. Evaluation Platforms

Current cybersecurity evaluation platforms focus on three types of simulation, i.e., traffic, communication, and individual

vehicle simulation. Although many emerging co-simulators are trying to integrate multiple platforms and exploit their advantages, a comprehensive simulation platform to systematically study theimpact of cyber attacks and defense servicesstill needs to be present. Besides, human-in-the-loop simulation is also worth investigating, as it is valuable to study human reactions related to reduced safety and/orcomfort caused bycyber-attacks. It should be noted that although real-world testbeds for CAV cybersecurity are costly and dangerous, they can provide a much more realistic environment.

Note that the research gaps identified above are not an exhaustive list. ln addition, as new research and deployment efforts continue, new gaps will emerge and need to be acknowledged.

## VIII. CONCLUSION

CAVshavegreat potential to transform our current transportation system into a safer, less congested, and more eco-friendly arena. But, in the meantime, there are a growing number of cybersecurity risks or even threats faced byCAVs that may introduce massive compromise from the perspective of individual vehicles, fleets, or even entire traffic flows. Many researchers have made tremendous progress investigating CATS cyber attacks and mitigation strategies. However, this review indicates that there are still gaps before claiming the current CAV applications are safe and resilient. Some questions that need to be addressed include how to prevent an attacker from obtaining a batch from SCMS and whether or not a compromised RSU would affect other neighboring RSUs. To answer these questions, innovative frameworks or approaches to vulnerability analysis and security assessment of CATS need to be further explored, and various resilient designs have to be considered.

## ACKNOWLEDGMENT

The views presented in this paper are those of the authors alone.

## REFERENCES

[I] H. Chen and B. Yang, "A performance evaluation of CAN encryption," in *Proc. IEEE!st Int.Conf.Trust, Privacy Secur. Intel/. Syst. Appl.,* 2019, pp. 140-149.

[2] D. S. Fowler, J. Bryans, S. A. Shaikh, and P. Wooderson, "Fuzz testing for automotive cyber-security," in *Proc. IEEEIIFIP 48th Atmu. Int.Conj Dependable Syst. Netw. Workshops,* 2018, pp. 239-246.

[3] J.Shen,J. Y.Won, Z. Chen, and Q. A.Chen,"Drift with devil:Security of multi-sensor fusion based localization in high-level autonomous driving under {GPS} spoofing," in *Proc. 29th USENIX Secur. Symp.,* 2020, pp. 931-948.

[4] H. Zhou et al., "Deepbillboard: Systematic physical-world testing of autonomous drivingsystems," in *Proc. IEEE/ACM 42nd Int.Conf.Softw. Eng.,* 2020, pp. 347-358.

[5] U. S. Ltd., "2022 global automotive cyber security report," 2022. [Online]. Available: https://upstream.auto/2022report/

[6] A. Abdo, S. M. B. Malek, Z. Qian, Q. Zhu, M. Barth, and N. Abu-Ghazaleh, "Application level attacks on connected vehicle protocols," in *Proc. 22nd Int. Symp. Res. Attacks, Intrusions Defenses,* 2019, pp. 459-471.

[7] Q. A. Chen, Y. Yin, Y. Feng, Z. M. Mao, and H. X. Liu, "Exposing congestion attack on emerging connected vehicle based traffic signal control," in *Proc. 25th Netw. Distrib. Syst. Secur. Symp.,* 2018, pp. 1-15.

[8] S.Hu,Q. A.Chen,J. Sun, Y. Feng,Z. **M.** Mao,andH. X.Liu,"Automated discovery of denial-of-service vulnerabilities in connected vehicle protocols," in *Proc. 30th USENIX Secur. Symp.,* 2021, pp. 3219-3236. [Online]. Available: https://www.usenix.org/conference/usenixsecurity2I/presentation/hu-shengtuo

[9] 1. Kotey, S. Adhikary, R. Rohit, and S. Dey, "A CAD framework for simulation of network levelattack onplatoons," 2022, *arXiv:2205.00769.*

[10] X. Zhao, A. Abdo, X. Liao, M. J. Barth, and G. Wu, "Evaluating cybersecurity risks of cooperative ramp merging in mixed traffic environments," *IEEE lntell. Transp. Syst. Mag.,* vol. 14, no. 6, pp. 52-65, Nov./Dec. 2022.

[11] F.Sommer, J. Dii.rrwang, and R. KriestenSun, "Survey andclassification of automotive security attacks," *lnfomiation,* vol. 10, 2019, Art. no.148.

[12] S. Parkinson, P. Ward, **K.** Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Trans. Intel/. Transp. Syst.,* vol. 18, no. 11, pp. 2898-2915, Nov. 2017.

[13] Z. Ju, H. Zhang, X. Li, X. Chen, J. Han, and **M.** Yang, "A survey on attack detection and resilience for connected and automated vehicles: From vehicledynamics and control perspective;' *IEEETrans.lnte/l.Veh.,* vol. 7, no. 4, pp. 815 37, Dec. 2022.

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

[15] J. Han, Z. Ju, X. Chen, M. Yang, H. Zhang, and R. Huai, "Secure operations of connected and autonomous vehicles," *IEEE Trans. lntell. Veh.,* to be published, doi: I0.1109/TIV.2023.3304762.

[16] S. Hamato, S. H. S. Ariffin, and **N.** Pisa!, "Overview of wireless access in vehicular environment (wave) protocols and standards," *Indian J. Sci. Teclmol.,* vol. 6, no. 7, pp. 1-8, 2013.

[17] "SAE 12735 - dedicated short range communications (DSRC) message set dictionary," 2022.[Online]. Available: https://www.standards.its.dot.gov/Factsheets/Factsheet/71

[18] **R.** Molina-Masegosa, J. Gozalvez, and **M.** Sepulcre, "Comparison of IEEE 802.1Ip and LTE-V2X: An evaluation with periodic and aperiodic messages of constant and variable size," *IEEE Access,* vol. 8, pp. 121526-121548, 2020.

[19] G. S. Aoude, B. D. Luders, J. M. Joseph, N. Roy, and J. P. How, "Probabilistically safe motion planning to avoid dynamic obstacles with uncertain motion patterns," *Auton. Robots,* vol. 35, no. I, pp. 51-76, 2013.

[20] D. Gettman and L. Head, "Surrogate safety measures from traffic simulation models," *Tra11sp. Res. Rec.,* vol. 1840, no. I, pp. 104-115, 2003.

[21] K. Leeand**H.** Peng,"Evaluation of automotiveforward collision warning and collision avoidance algorithms," *Veh. Syst. Dy11.,* vol. 43, no. 10, pp.735-751, 2005.

[22] G. Howe, G. Xu, D. Hoover, D. Elsasser, and F. Barickman, "Commercial connected vehicle test procedure development and test results--emergency electronic brake light," National Highway Traffic Safety Administration, Washington, D.C., USA, Tech. Rep. DOT HS 812 327, 2016.

[23] "Intelligent transportation systems - CV pilot deployment program," 2021, Accessed: Oct.16, 2022.[Online]. Available: https://www.its.dot.gov/pilots/cv_pilot_apps.htrn

[24] W. Liu, S. Muramatsu, and Y. Okubo,"Cooperation of V2I/P2I communication and roadside radar perception for the safety of vulnerable road users," in *Proc. 16th!flt. Conf ltltell. Transp. Syst. Telecommun.,* 2018, pp. 1-7.

[25] "Dynamic mobility applications (DMA),"2016, Accessed: Oct.16,2022. [Online]. Available: https://www.its.dot.gov/research_archives/dma/dma_faqs.htm

[26] R. E. Stem et al., "Dissipation of stop-and-go waves via control of autonomous vehicles: Field experiments," *Tra11sp. Res. Part C: Emerg. Tech11ol.,* vol. 89, pp. 205-221, 2018.

[27] Y. Feng, C. Yu, and H. X. Liu, "Spatiotemporal intersection control in a connected and automated vehicle environment," *Transp. Res. Part C: Emerg. Technol.,* vol. 89, pp. 364-383, 2018.

[28] C. Yu, Y. Feng, **H. X.** Liu, **W. Ma,** and X. Yang,"Integrated optimization of traffic signals and vehicle trajectories at isolated urban intersections," *Transp. Res. Part B: Methodological,*vol. 112, pp. 89-112, 2018.

[29] Z. Wang et al.,"Cooperative ramp merging system: Agent-based modelingand simulation usinggameengine," *SAE Int.J. CotmectedAutomated Veh.,* vol. 2, no. 2, pp. 1-14, 2019.

[30] D. Tian, G. Wu, K. Boriboonsomsin, and M. Barth, "Performance measurement evaluation framework and co-benefittradeoff analysis for connected and automated vehicles (CAY) applications: A survey," *IEEE ltltell. Transp. Syst. Mag.,* vol. 10, no. 3, pp. 110-122, Fall 2018.

[31] B. McAuliffe, M. Lammert, X.-Y.Lu,S. Shladover,M.-D.Surcel,and A. Kailas, "Influences on energy savings of heavy trucks using cooperative adaptive cruise control," SAE, Warrendale, PA, USA, Tech. Rep. No. 2018-01-1181, 2018.

[32] S. E. Shladover, D. Su, and **X.-Y.** Lu, "Impacts of cooperative adaptive cruisecontrol onfreeway traffic flow,"*Transp. Res. Rec.,*vol.2324, no. I, pp. 63-70, 2012.

[33] 0. D. Allan, G. Wu, **M. J.** Barth, K. Boriboonsomsin, and J. A. Stark, "GlidePath: Eco-friendly automated approach and departure at signalized intersections," *IEEE Trans. Intel/. Veh.,* vol. 2, no. 4, pp. 266-277, Dec. 2017.

[34] P. Hao, G. Wu, K. Boriboonsomsin, and **M.** Barth, "Eco-approach and departure (EAD) application for actuated signals in real-world traffic," *IEEE Trans. Intel/. Transp. Syst.,* vol. 20, no. I, pp. 30-40, Jan. 2019.

[35] K. Katsaros, R. Kemchen, **M.** Dianati,and D. Rieck, "Perfonnance study of a green light optimized speed advisory (GLOSA) application using an integrated cooperative its simulation platform," in *Proc. 7th I11t. Wireless CommutL Mobile Comput. Co11f,* 201I, pp. 918-923.

[36] Allot,"Connected carsattack vulnerabilities," 2018. [Online]. Available: https://www.allot.com/resources/TB_CONNECTED_CARS.pdf

[37] V. V. Vegesna,"Threat and riskassessment techniques and mitigation approaches forenhancing security in automotive domain," *Int. J.Ma11age., Tee/mo/. E11g.,* vol. 6, pp. 314-331, 2016.

[38] 0. Henniger,"EVITA: E-safety vehicle intrusion protected applications;· EVITA, Brussels, Belgium, Tech. Rep., Apr. 2011.

[39] Microsoft,"Thestridethreat model,"2009.Accessed: Nov.21, 2020.[Online]. Available: https://docs.microsoft.com/en-us/previous- versions/commerce-server/ee823878(v=es.20)?redirectedfrom=MSDN

[40] C. Schmittner, Z. Ma, C. Reyes,0. Dillinger, and P. Puschner, "Using SAE J3061 for automotive security requirement engineering," in *Proc. Int. Conf Comput. Saf, Rel., Secur.,* 2016, pp. 157-170.

[41] J. Diirrwang, **K.** Beckers, and **R.** Kriesten, "A lightweight threat analysis approach intertwining safety andsecurity for theautomotive domain," in *Proc. I11t. Conf Comput. Saf, Rel., Secur.,* 2017, pp. 305-319.

[42] **W.** Youngand R. Porada, "System-theoretic process analysis for security (STPA-SEC): Cyber security and STPA," in *Proc. STAMP Conf,* 2017, pp. t--05.

[43] G. Sabaliauskaite, J. Cui, L. S. Liew, and F. Zhou,"Integrated safety and cybersecurity risk analysis of cooperative intelligent transport systems," in *Proc. IEEE Joint 10th Int. Conf Soft Comput. Ifltell. Syst. 19th lilt. Symp. Adv. /11tell. Syst.,* 2018, pp. 723-728.

[44] C. McCarthy, K. Harnett,and A. Carter,"Characterizationof potential security threats in modem automobiles: Acomposite modeling approach," National Highway TrafficSafety Administration, Washington, DC, USA, Tech. Rep. No. DOT HS 812074, 2014.

[45] J. Cui and B. Zhang, "VeRA: A simplified security risk analysis method for autonomous vehicles," *IEEE Tra11s. Veh. Tech110/.,* vol. 69, no. 10, pp. 10494-10505, Oct 2020.

[46] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch, "Security application of failure mode and effect analysis (FMEA)," in *Proc. Int. Conf Comput. Saf, Rel., Secur.,* 2014, pp. 310-325.

[47] C. Raspotnig, P. Karpati,and V.Katta,"A combined processforelicitation and analysis of safety and security requirements," in *Proc. Enterprise, BllS.-Process Inf Syst. Model.,* 2012, pp. 347-361.

[48] D. Dominic, S. Chhawri, R. M. Eustice, D. Ma, and A. Weimerskirch, "Risk assessment for cooperative automated driving," in *Proc. 211d ACM Workshop Cyber- Phys. Syst. Secur. Privacy,* 2016, pp. 47-58.

[49] J.-P. Monteuuis, A. Boudguiga, J. Zhang, H. Labiod, A. Servel, and P. Urien, "SARA: Security automotive risk analysis method," in *Proc. 4th ACM Workshop Cyber-Phys. Syst. Secur.,* 2018, pp.3-14.

[50] A. Bolovinou, U.-1. Atmaca, A. T. Sheik, 0. Ur-Rehman, G. Wallraf, and A. Amditis, "TARA+: Controllability-aware threat analysis and risk assessment for13automated driving systems," in *Proc. IEEE Intell. Veh. Symp.,* 2019, pp. 8-13.

[51] M. Zoppelt and R. T. Kolagari, **"SAM: A** security abstraction model for automotive softwaresystems," in *Proc. /11t.Workshop Cyber Secur. Inte/1. Transp. Syst.,* 2018, pp.59-74.

[52] **H.-K.** Kong, **M. K.** Hong, and T.-S. Kim, "Security risk assessment framework forsmart car using theattack tree analysis," *J. Ambient Inte/1. Humanized Comput.,* vol. 9, no. 3, pp. 531-551, 2018.

[53] J. Dunj6, V. Fthenakis, **J.** A. Vflchez, and J. Arnaldos, "Hazard and operability (HAZOP) analysis. A literature review," *J. Hazardous Mater.,* vol. 173,no. 1-3,pp. 19-32,2010.

[54] T. UcedaVelezand **M.M.** *Morana,RiskCe11tricThreatModeling: Process for Attack Simulation a11d Threat A11alysis.* Hoboken, NJ, USA: Wiley, 2015.

[55] 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, 2019.

[56] J.E. Rossebo, S. Cadzow, and P. Sijben,"eTVRA, a threat, vulnerability and risk assessment method and tool for eEurope," in *Proc. IEEE 211d I11t. Conf Availability, Rel. Secur.,*2007, pp.925-933.

[57] T. Halabi, 0. A. Wahab, R. Al Mallah, and **M.** Zulkernine, "Protecting the internet of vehicles against advanced persistent threats: A Bayesian Stackelberg game," *IEEE Trans. Rel.,* vol. 70, no. 3, pp.970-985, Sep. 2021.

[58] A. Le, C. Maple, and T. Watson, "A Profile-Driven Dynamic Risk Assessment Framework for Connected and Autonomous Vehicles," in *Proc. livi11g Internet Things: Cybersecurity loT,* 2018, pp. 1-8.

[59] A. Lautenbach and **M.** Islam, "Heavens-healing vulnerabilities to enhance software security and safety," The HEAVENS Consortium, Stockholm, Sweden, Tech. Rep. 2012-04625, 2016.

[60] G. Macher, **H.** Sporer, R. Berlach, E. Armengaud, and C. Kreiner, "SAHARA: A security-aware hazard and risk analysis method," in *Proc. Des., Automat. Test Europe Co11f. Exhib.,* 2015, pp. 621-624.

[61] J. V.Brummelen, M. O'Brien, D.Gruyer, and H. Najjaran, "Autonomous vehicle perception: Thetechnology of todayandtomorrow," *Transp. Res. Part C: Emerg. Technol.,* vol. 89, pp. 384-406, 2018.

[62] C. Yan, W. Xu, and J. Liu,"Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *Def Con.,* vol. 24, no. 8, 2016, Art. no. 109.

[63] R. Duan et al., "Adversarial laser beam: Effective physical-world attack to DNNs in a blink," in *Proc. IEEF/CVF Conf Comput. Vis. Pattern Recog11it.,* 2021, pp. 16062--16071.

[64] A.Gnanasambandam, A. M.Sherman, and S. H.Chan,"Optical adversarial attack," in *Proc. IEEF/CVF Int.Co11f Comput.Vis.,* 2021, pp.92-101.

[65] C. Szegedy et al., "Intriguing properties of neural networks," 2013, *arXiv:I312.6199.*

[66] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," 2014, *arXiv:1412.6572.*

[67] K. Eykholt et al.,"Robust physical-world attacks ondeep learning visual classification,"in *Proc. IEEECo11f.Comput.Vis. Pattern Recog11it.,* 2018, pp. 1625-1634.

[68] N.Patel,P. Krishnamurthy,S.Garg,and F. Khorrami,"Adaptive adversarial videos on roadside billboards: Dynamically modifying trajectories of autonomous vehicles," in *Proc. IEEE/RSJ /11t. Conf /11tell. Robots Syst.,* 2019,pp.5916-5921.

[69] M. Wan, M. Han, L. Li, Z. Li, and S. He, "Effects of and defenses against adversarial attacks on a traffic light classification CNN," in *Proc. ACM Southeast Conf,*2020, pp. 94-99, doi: 10.I145/3374135.3385288.

[70] Y. Jia et al., "Fooling detection alone is not enough: Adversarial attack against multiple object tracking," in *Proc. Int. Conf Learn. Representatio11s,* 2020, pp. 1-15. [Online]. Available: https://openreview.net/forum?id=rJl31TNYPr

[71] T. Sato, J. Shen, N. Wang, Y. J. Jia, X. Lin, and Q. A. Chen, "Dirty road can attack: Security of deep learning based automated lane centering under physical-world attack," in *Proc. 30th USENIX Security Symp.,* 2021,pp.3309-3326.

[72] Z. Sun, S. Balakrishnan, L. Su, A. Bhuyan, P. Wang, and C. Qiao,"Who is in control? Practical physical layer attack and defense for mmwave basedsensing in autonomous vehicles," *IEEETrans. Inf ForensicsSecur.,* vol. 16, pp.3199-3214, 2021.

[73] R. Komissarov and A. Wool,"Spoofing attacksagainst vehicular FMCW radar," in *Proc. 5th Workshop Attacks Solutio11s Hardware Secur.,* 2021, pp. 91-97.

[74] **Y.** Cao et al., "Adversarial sensor attack on lidar-based perception in autonomous driving," in *Proc. ACM S/GSAC Conf Comput. Commllll.* Secur.,2019,pp. 2267-2281.

[75] **K.** Yang,T. Tsai, H. Yu, **M.** Panoff, T.-Y. Ho, and Y. Jin,"Robust roadside physical adversarial attack against deep learning in lidar perception modules," in *Proc. ACM Asia Co11f Comput. Cotlll1lu11. Secur.,* 2021, pp. 349-362, doi: I0.1145/3433210.3453106.

[76] J.Sun, Y.Cao,Q. A.Chen,and Z. **M.** Mao,"Towards robust LiDAR-based perception in autonomous driving: General black-box adversarial sensor attack andcountenneasures," in *Proc. 29th USENIX Secur. Symp.,* 2020, pp. 877-894.

[77] J. Tu et al., "Physically realizable adversarial examples for lidar object detection," in *Proc. IEEF/CVF Conf Comput. Vis. Pattern Recog11it.,* 2020,pp. 13716-13725.

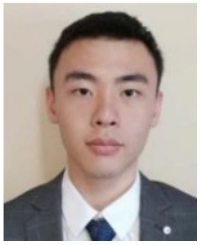
[78] H. Zhang, Z. Li, S. Cheng, and A. Clark, "Cooperative perception for safe control of autonomous vehicles under lidar spoofing attacks," 2023, *arxiv:2302.07341.*

[79] S.Tayebetal.,"Securingthepositioningsignalsofautonomousvehicles," in *Proc. IEEE Int. Conf Big Data,* 2017, pp. 4522-4528.
[80] H. Sathaye, **M.** Strohmeier, V. Lenders, and A. Ranganathan, "An experimental study of GPS spoofing and takeover attacks on UAVs," in *Proc. 31st USENIX Secur. Symp.,* 2022, pp.3503-3520. [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/sathaye
[81] Y. Li, C. Wen, F. Juefei-Xu, and C. Feng, "Fooling LiDAR perception via adversarial trajectory perturbation," in *Proc. IEEF./CVF 1111. Conf Comput. Vis.,* 2021, pp. 789&-7907.
[82] Y. Cao et al., "Invisible for both camera and lidar: Security of multi-sensor fusion based perception in autonomous driving under physical-world attacks," in *Proc. IEEE Symp. Secur. Privacy,* 2021, pp. 176-194, doi: 10.1109/SP40001.2021.00076.
[83] P. Lu, C. Cui, S. Xu, H. Peng, and F. Wang, "SUPER: A novel lane detection system," *IEEE Trans. Intel/. Ve/1.,* vol. 6, no. 3, pp. 583---593, Sep. 2021.
[84] S. Feng, Z. Song, Z. Li, Y. Zhang, and L. Li, "Robust platoon control in mixed traffic How based on tube model predictive control," *IEEE Tra11S. Intel/. Veh.,* vol. 6, no. 4, pp. 711-722, Dec. 2021.
[85] M. R. Hajidavalloo, Z. Li, D. Chen, A. Louati, S. Feng, and W. B. Qin, "Mechanical system inspired microscopic traffic model: Modeling, analysis, and validation," *IEEE Trans. Intel!. Veh,* vol. 8, no. 1, pp. 301-312, Jan. 2023.
[86] **M.** Amoozadeh et al., "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Commun. Mag.,* vol. 53, no. 6, pp. 126-132, Jun. 2015.
[87] M.M. Minderhoud and P.H. Bovy,"Extended time-to-collision measures for road traffic safety assessment," *Accident Anal. Prevention,* vol. 33, no. I, pp. 89-97, 2001. [Online]. Available: https://www.sciencedirect.com/science/art.iclelpii/S0001457500000191
[88] S. Huang, Y. Feng, W. Wong, Q. A. Chen, Z. M. Mao, and H. X. Liu, "Impact evaluation of falsified data attacks on connected vehicle based traffic signal control systems," in *Proc. NDSSWorkslwp Autonwt. Auton. Veh. Secur.,*2021.
[89] A.Haydari,M.Zhang,andC.-N.Chuah,"Adversarialattacksanddefense in deep reinforcement learning (DRL)-based traffic signal controllers," *IEEE Open J. Intel/. Transp. Syst.,* vol. 2, pp. 402-416, 2021.
[90] C.-C. Yen, D. Ghosal, M. Zhang, and C.-N. Chuah, "Security vulnerabilities and protection algorithms for backpressure-based traffic signal control at an isolated intersection," *IEEE Trans. l11tell. Transp. Syst.,* vol. 23, no. 7, pp. 6406-6417, Jul. 2022.
[91] M. E. 0. Andah, "A survey on cyber security issues of autonomous vehicles," 2021.
[92] Y.Deng, X. Zheng, T.Zhang, C.Chen,G. Lou,and M. Kim,"An analysis of adversarial attacks and defenses on autonomous driving models," in *Proc. IEEE Int.Co11f. Pervasive Comput. Commun.,* 2020, pp. 1-10.
[93] W. Chai, Y. Lu, and S. Velipasalar, "Weighted average precision: Adversarial example detection for visual perception of autonomous vehicles," in *Proc. IEEE Int. Conf Image Process.,* Anchorage, AK, USA, 2021, pp.804--808,doi: 10.1109/ICIP42928.2021.9506613.
[94] W. Chai, Y. Lu, and S. Velipasalar, "Weighted average precision: Adversarial example detection for visual perception of autonomous vehicles," in *Proc. IEEE Int. Conf Image Process.,* Anchorage, AK, USA, 2021, pp. 804--808, doi: 10.1109/ICIP42928.2021.9506613.
[95] Q. Sun, A. A. Rao, X. Yao, B. Yu, and S. Hu,"Counteracting adversarial attacks in autonomous driving," in *Proc. IEEF./ACM Int. Conf Comput. Aided Des.,* 2020, pp. 1-7.
[96] H. Xu, A. Ju,and D. Wagner,"Model-agnostic defense for lanedetection against adversarial attack," 2021, *arXiv:2103.00663.*
[97] S. Chen, W. Shangguan, J. Taghia, U. Kiihnau, and R. Martin, "Automotive radar interference mitigation based on a generative adversarial network," in *Proc. IEEE Asia-Pacific Mierow. Conf.,* 2020, pp. 72&-730.
[98] S. Dasgupta, **M.** Rahman, **M.** Islam, and **M.** Chowdhury, "A sensor fusion-based GNSS spoofing attack detection framework for autonomous vehicles," *IEEE Trans. Intel/. Transp. Syst.,* vol. 23, no. 12, pp. 23559-23572, Dec. 2022.
[99] E. S. Canepa and C. G. Claude!, "A framework for privacy and security analysis of probe-based traffic information systems," in *Proc. 2nd ACM Int. Corif. High Confidence Networked Syst.,*2013, pp. 25-32.
[100] E. S. Canepa and C. G. Claude!, "Spoofing cyber attack detection in probe-based traffic monitoring systems using mixed integer linear programming," in *Proc. 1111. Corif. Comput., Netw. Commun.,* 2013, pp. 327-333.
[IOI] Y. Shoukry, S. Mishra, Z. Luo, and S. Diggavi, "Sybil attack resilient traffic networks: A physics-based trust propagation approach," in *Proc. IEEF./ACM 9th Int. Conf Cyber- Phys. Syst.,*2018, pp. 43-54.
[102] G. Yan, S. Olariu, and **M.** C. Weigle, "Providing vanet security through active position detection," *Comput. Commun.,* vol. 31, no. 12, pp. 2883-2897, 2008.
[103] D. Zhang, N. Li,Z.-H.Zhou,C. Chen, L. Sun,and S. Li,"iBAT: Detecting anomalous taxi trajectories from GPS traces," in *Proc. 13th Int. Co11f. Ubiquitous Comput.,* 2011, pp. 99-108.
[104] C. Chen et al., "iBOAT: Isolation-based online anomalous trajectory detection," *IEEE Trans.l11tell. Transp. Syst.,* vol.14, no. 2, pp. 806-818, Jun. 2013.
[105] S. E. Huang, Y. Feng, and H. X. Liu, "A data-driven method for falsified vehicle trajectory identification byanomaly detection," *Transp. Res. Part C: Emerg. Teclmol.,* vol. 128, 2021, Art. no. 103196.
[106] Y. Feng, S. E. Huang, W. Wong, Q. A. Chen, Z. M. Mao, and H. X. Liu, "On thecybersecurity of traffic signal control system with connected vehicles,"*IEEETra11S. l11tel/.Tra11sp.Syst.,*vol.23, no.9, pp. 16267-16279, Sep. 2022.
[107] Z. Lv, J. Xu, P. Zhao, G. Liu, L. Zhao, and X. Zhou, "Outlier trajectory detection: A trajectory analytics based approach," in *Proc. Int. Co11f. Database Syst. Adv. Appl.,* 2017, pp. 231-246.
[108] J. Zhu, W. Jiang, A. Liu, G. Liu, and L. Zhao, "Time-dependent popular routes based trajectory outlierdetection,"in *Proc. Int.Co11f Web Inf Syst. Eng.,* 2015, pp. 16-30.
[109] M.-h. Oh and G. Iyengar, "Sequential anomaly detection using inverse reinforcement learning," in *Proc. 25th ACM SIGKDD Int.Co11f. Knowl. Discov. Data Mi11i11g,* 2019, pp. 1480--1490.
[110] D. Smolyak, K.Gray, S. Badirli,and G. Mohler,"Coupled IGMM-GANs with applications to anomaly detection in human mobility data," *ACM Trans. Spatial Algorithms Syst.,* vol. 6, no. 4, pp. 1-14, 2020.
[111] P. Wang, X. Wu, and X. He,"Modeling andanalyzing cyberattack effects onconnected automated vehicular platoons," *Trat1Sp. Res. Part C: Emerg. Teclmol.,* vol. 115, 2020, Art. no. 102625.
[112] D. Yao, C. Zhang, Z. Zhu, J. Huang, and J. Bi, "Trajectory clustering via deep representation learning," in *Proc. IEEE Int. joint Co11f. Neural Netw.,* 2017, pp. 3880--3887.
[113] Y. Ding, G. Zhu, D. Chen, X. Qin, M. Cao, and Z. Qin, "Adversarial sample attack and defense method for encrypted traffic data," *IEEE Trans. Intel/. Transp. Syst.,* vol. 23, no. 10, pp. 18024--18039, Oct. 2022.
[114] A. Abdo, G. Wu, Q. Zhu, and N. Abu-Ghazaleh, "CVGuard: Mitigating application attacks on connected vehicles," in *Proc. IEEE Intel/. Veh. Symp.,* 2022, pp.623---630.
[115] S. So, J. Petit, and D. Starobinski, "Physical layer plausibility checks for misbehavior detection in V2X networks," in *Proc. 12th Co11f Secur. Privacy Wireless Mobile Netw.,* 2019, pp. 84--93.
[116] V.-L. Nguyen, P.-C.Lin,and R.-H. Hwang,"Physical signal-drivenfusion for v2x misbehavior detection," in *Proc. IEEE Veh Netw. Co11f,* 2019, pp. 1-4.
[I 17] M. Sun, M. Li, and R. Gerdes, "A data trust framework for VANETs enabling false data detection and secure vehicle tracking," in *Proc. IEEE Co11f Commun. Netw. Secur.,*2017, pp. 1-9.
[118] S. Ruj, M.A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, "On data-centric misbehavior detection in VANETs," in *Proc. IEEE Veh. Tee/mo/. Co11f.,* 2011, pp. 1-5.
[119] S.So,P.Sharma,andJ.Petit,"Integratingplausibilitychecksandmachine learning for misbehavior detection in VANET;' in *Proc. IEEE 17th Int. Co11f Mach. Lean1. Appl.,* 2018, pp. 564--571.
[120] Y.Wangand N.Masoud,"Adversarial online learning with variable plays in the pursuit-evasion game: Theoretical foundations and application in connected and automated vehicle cybersecurity," *IEEE Access,* vol. 9, pp. 142475-142488, 2021.
[121] A. Abdo, G. Wu, and N. Abu-Ghazaleh, "Secure ramp merging using blockchain," in *Proc. IEEE Intel/. Veh. Symp.,* 2021, pp.401-408.
[122] X. Liu, B. Luo, A. Abdo, **N.** Abu-Ghazaleh, and Q. Zhu, "Securing connected vehicle applications with an efficient dual cyber- physical blockchain framework," in *Proc. IEEE Intel/. Veh.Symp.,* 2021, pp.393-400.
[123] G. Rong et al., "LGSVL simulator: A high fidelity simulator for autonomous driving," in *Proc. IEEE 23rd Int. Corif. lntell. Transp. Syst.,* 2020, pp. 1-6.
[124] S. Katoet al., "Autoware on board: Enabling autonomous vehicles with embedded systems," in *Proc. IEEF./ACM 9th Int. Co11f Cyber- Phys. Syst.,*2018, pp. 287-296.
[125] Baidu Apollo team, "Apollo: Open source autonomous driving," 2022. [Online]. Available: https://github.com/ApolloAuto/apollo
[126] A. Dosovitskiy,G. Ros, F.Codevilla, A. Lopez, andV.Koltun, "CARLA: An open urban driving simulator," in *Proc. Corif. Robot Learn.,* 2017, pp. 1-16.

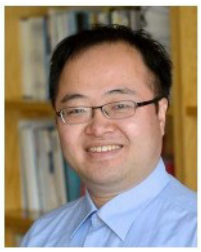
(127] S. Malik, M.A.Khan,andH.El-Sayed,"CARLA:Carlearning toact-an inside out," *Procedia Comput. Sci.,* vol. 198, pp.742-749, 2022.
(128] S.-T. Chen, C. Cornelius, J. Martin, and D. H.P. Chau, "ShapeShifter: Robust physical adversarial attack on faster R-CNN object detector," in *Proc. Joi11t Eur. Co11f Mach. Leam. Know/. Discov. Databases,* 2018, pp. 52-68.
(129] C. Cornelius, S.-T. Chen, J. Martin, and D. H. Chau, ..Talk proposal: Towards the realistic evaluation of evasion attacks using CARLA," 2019, *arXiv:1904.12622.*
(130] E. Zhang and N. Masoud, "V2XSim: A V2X simulator for connected andautomated vehicle environment simulation," in *Proc. IEEE 23rd lilt. Collf. llltell. TrallSp. Syst.,* 2020, pp. 1-6.
(131] K.S. Swanson,"Identificationof stability thresholds in time-delayed vehicleteleoperation,"M.Sc.Thesis, Dept. Mech. Nucl.Eng., Pennsylvania State Univ., pp. 1-108, 2013.
(132] **K.** Abdelgawad, M. Abdelkarim, B. Hassan, **M.** Grafe, and I. Gra81er, "A scalable framework for advanced driver assistance systems simulation," in *Proc. 6th Int. Co11f. Adv. System Simul.,* 2014, pp. 12-16.
(133] Z. A. Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Tra11s. l11tell. Transp. Syst.,* vol. 19, no. 12, pp.3893-3902, Dec. 2018.
(134] K. S. Swanson, A. A. Brown, S. N. Brennan, and C. M. LaJambe, "Extending driving simulator capabilities toward hardware-in-the-loop testbeds and remote vehicle interfaces," in *Proc. IEEE llltell. Veh. Symp. Workshops,* 2013, pp. 115-120.
(135] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, "Recent development and applications of sumo-simulation of urban mobility;' *lilt. J. Adv. Syst. Meas.,* vol.5, no. 3/4, pp. 128-138, 2012.
(136] X. Zhaoet al.,"Co-simulation platform for modeling andevaluating connected and automated vehicles and human behavior in mixedtraffic," *Int. J. Conllected Automated Veh.,* vol. 5, no. 12-05-04-0025, pp. 313-326, 2022.
(137] **M.**Maleki and B.Sangchoolie,"SUFI: Asimulation-based faultinjection tool for safety evaluation of advanced driver assistance systems modelled in sumo;' in *Proc. 17th Eur. Depelldable Comput. Coll/,* 2021, pp. 45-52.
(138] S. Dasgupta, C. Hollis, M. Rahman, and T. Atkison, "An innovative attack modelling andattack detection approach for a waiting time-based adaptive traffic signal controller," in *Proc. lilt. Coll/ TrallSp. Develop.,* 2021, pp. 72-84.
(139] M. Fellendorf and P. Vortisch, "Microscopic traffic flow simulator VISSIM," in *Fu11dame11talsof Traffic Si111ulatio11.*Berlin, Germany: Springer, 2010, pp. 63-93.
(140] M. Maciejewski, "A comparison of microscopic traffic flow simulation systems for an urban area," *Transport Problems,* vol. 5, pp. 27-38, 2010.
(141] D. J. Higham and N.J. Higham, *MATLAB Guide.*Philadelphia, PA, USA: SIAM, 2016.
(142] E. Harahap, F. Badruzzaman, Y. Permanasari, **M.** Fajar, and A. Kudus, "Traffic engineering simulation of campus area transportation using matlab simevents," */OP Co11f Ser.: Mater.* Sci. *Eng.,* vol. 830, no. 2, 2020, Art. no. 022078.
(143] Y. Li, Y. Tu, Q. Fan, C. Dong, and W. Wang, "Influence of cyber-attacks on longitudinal safety of connected and automated vehicles," *Accident Aool. Preve11tio11,* vol. 121, pp. 148-156, 2018.
(144] J. Casas, J. L. Ferrer, D. Garcia, J. Perarnau, and A. Torday, "Traffic simulation with aimsun," in *Fundamentals of Traffic Simulation.* New York, NY, USA: Springer2010, pp. 173-232, doi: to.1007/978-1-4419-6142-6_5.
(145] J. Reilly, S. Martin, M. Payer, and A. Bayen, "On cybersecurity of freewaycontrol systems: Analysisof coordinated ramp meteringattacks," *Tra11Sp. Res. Part B,* pp. 1-20, 2014.
[146] A. Varga,"OMNeT++," in *Modeling and Tools for Network Simulatioll.* Berlin, Germany: Springer, 2010, pp. 35-59.
(147] T. K. Mohd, S. Majumdar, A. Mathur, and A. Y. Javaid,"Simulation and analysis of DDoS attack onconnected autonomous vehicular network using OMNET++," in *Proc. IEEE 9thA1111u. Ubiquitous Comput., Electron. Mobile Co111111u11. Conf.,*2018, pp. 502-508.
(148] X. Wang, I. Mavromatis, A. Tassi, **R.** Santos-Rodriguez, and R. J. Piechocki, "Location anomalies detection for connected andautonomous vehicles;• in *Proc. IEEE 2nd Connected Automated Veh. Symp.,* 2019, pp. 1-5.
(149] G. Carneiro, "Ns-3: Network simulator 3," in *Proc. UTM Lab Meeting April,* 2010, pp. 4-5.
(150] A. Acharya and J. Oluoch, "A dual approach for preventing blackhole attacks in vehicular ad hoc networks using statistical techniques and supervised machine learning," in *Proc. IEEE Int. Co11f. Electro /11/ Tech110I.,* 2021, pp. 230-235.
[151] **M.** Amoozadeh, B. Ching, C.-N. Chuah, D. Ghosal, and H. M. Zhang, "VENTOS:Vehicular networkopensimulator with hardware-in-the-loop support," *Procedia Comput. Sci.,* vol. 151, pp. 61-68, 2019.
(152] P. K. Singh, G. S. Tabjul, **M.** lmran, S. **K.** Nandi, and S. Nandi,"Impact of security attacks on cooperative driving use case: CACC platooning," in *Proc. IEEE TENCON Region JO Con/,* 2018, pp.0138-0143.
(153] X. Zhao, A. Abdo, X. Liao, M. J. Barth, and G. Wu, "Evaluating cybersecurity risksof cooperative rampmerging in mixed trafficenvironments," *IEEE llltell. Trarzsp. Syst. Mag.,*2021, vol. 14, no. 6, pp. 52-65, Nov./Dec. 2022.
(154] United States Department of Transportation, "Cooperative automation research mobility applications (CARMA) overview," 2019. [Online]. Available: https://highways.dot.gov/research/research-programs/operations/CARMA
[155] 8. Zheng, C.-W. Lin, H. Yu, H. Liang, and Q. Zhu, "CONVINCE: A cross-layer modeling, exploration and validation framework for next-generation connected vehicles," in *Proc. IEEE/ACM Int.Coll/ Comput.-Aided Des.,* 2016, pp. 1-8.
(156] M. S. Alam, A. Acharya, and J. Oluoch, "A novel technique for mapping jammed areas in connected and autonomous vehicles (CAVs)," in *Proc. IEEE lilt. Coll/ Autonomic Comput. Self-Organizillg Syst. Companioll,* 2021, pp. I11-117.
(157] Y. Lou et al., "Cooperative automation research: CARMA proof-of-concept TSMO usecasetesting:CARMAcooperativeperception concept of operations," Federal Highway Administration, Washington, DC, USA, Tech. Rep. No. FHWA-HRT-22-062, 2022.
[158] C. Shuand Y.Luo,"Multi-modal featureconstraint based tightly coupled monocular visual-LiDAR odometry and mapping," *IEEE Trans. Intel/. Veh.,* vol. 8, no. 5, pp. 3384-3393, May 2023.
(159] T. Zhou, **J.** Chen, Y. Shi, K. Jiang, **M.** Yang, and D. Yang, "Bridging the view disparity between radar and camera features for multi-modal fusion 3D object detection," *IEEE Traru. lnte/1. Veh.,* vol. 8, no. 2, pp. 1523-1535,Feb.2023.
[160] Z. Zhang, J. Zhao, C. Huang, and L. Li, "Leaming visual semantic map-matching forloosely multi-sensor fusionlocalizationof autonomous vehicles," *IEEE Tratis. lntell. Veh.,*vol. 8, no. I, pp. 358-367, Jan. 2023.
(161] R. Xu et al., "The OpenCDA open-source ecosystem for cooperative driving automation research," *IEEE TrallS. Intel/. Ve/1.,* vol. 8, no. 4, pp. 2698-2711, Apr. 2023.
[162] T. Kessler, K. Esterle, and A. Knoll,"Mixed-integer motion planning on German roads within the Apollodriving stack," *IEEE Trails. Intel/. Veh.,* vol.8,no. l,pp.851-867,Jan. 2023.
[I 63] J. Li et al., "Learning for vehicle-to-vehicle cooperative perception under lossy communication," *IEEE Tra11s. Intel/. Veh.,* vol. 8, no. 4, pp. 2650-2660, Apr. 2023.

**Ahmed Abdo** received the **M.S.** degree from the Department of Electrical and Computer Engineering, California State University, Los Angeles, CA, USA, in 2015, and the Ph.D. degree in electrical engineering from the University of California, Riverside, CA, USA, 2022. He is currently a Researcher with Applied Physics Laboratory, Johns Hopkins University, Baltimore, **MD,** USA. His research interests include systems and network security. He has been focusingon thecybersecurity of theapplication layer in autonomous vehiclesand intelligent transportation.

**Hanlin Chen** (Member, IEEE) received the B.S. degree in electrical engineering and automation from the Huazhong University of Science and Technology, Wuhan, China, and the **M.S.** degree in mechanical engineering technology and the Ph.D. degree incomputer and information technology from Purdue University, West Lafayette, IN, USA. She is currently a Postdoctoral Research Assistant of civil engineering with Purdue University. Her research interests include cooperative perception, traffic-infonned perception, planning on vehicle side, cybersecurity and resilience in CDA system, and CAY in homeland security.



Xuanpeng Zhao received the B.E. degree in electrical engineering from Shanghai Maritime University, Shanghai, China, in 2019, and the M.S. degree in electrical engineering from the University of California, Riverside, CA, USA, where he is currently working toward the Ph.D. degree in electrical engineering. As a Ph.D. candidate, his research interests include connected and automated vehicle technologies, specifically focusing on cybersecurity anomaly detection to improve the security and efficiency of advanced transportationsystems.



Guoyuan Wu (Senior Member, IEEE) received the Ph.D. degree in mechanical engineering from the Universityof California, Berkeley, CA, USA, in 2010. He holds a Full Researcher and Adjunct Professor position with the Bourns College of Engineering - Center for Environmental Research & Technology (CE-CERT) and Department of Electrical & Computer Engineering, University of California at Riverside, Riverside, CA, USA.His research interests includethe development and evaluation of sustainable and intelligent transportation system (SITS) technologies, including connected and automated transportation systems (CATS), shared mobility, transportation electrification, optimization and control of vehicles, traffic simulation, and emissions measurement and modeling. His is an Associate Editorfor a few journals, including IEEE TRANSACTIONS ON INTELLIGENTTRANSPORTATIONSYSTEMS, *SAE International Journal of Connected and Automated Vehicles,* and IEEE OPEN JOURNAL OF ITS. He is also a Member of a few Standing Committees of the Transportation Research Board. He was the recipient of 2020 Vincent Bendix Automotive Electronics Engineering Award and 2021 Arch T. Colwell Merit Award.

Yiheng Feng (Member, IEEE) received the B.S. and M.E.degreesfromthe Department of Control Science and Engineering, Zhejiang University, Hangzhou, China, in 2005 and 2007, respectively, and the Ph.D. degree in systems and industrial engineering from The University of Arizona, Tucson, AZ, USA, in 2015. He is currently an Assistant Professor with the Lyles School of Civil Engineering, Purdue University, West Lafayette, IN, USA. His research interests include traffic operations and control, cybersecurity of the transportation systems and connected, and automated vehicle testing and evaluation.