Location-Based Schemes for Mitigating Cyber Threats on Connected and Automated Vehicles: A Survey and Design Framework

Dajiang Suo, John Moore, Mathew Boesch, Kyle Post, and Sanjay E. Sarma, *Member, IEEE*

***Abstract*— The increased automation and connectivity of vehicles and road infrastructure can make future transportation systems more efficient and smarter and enable new transportation business models. Connected and automated vehicles (CAVs) may form a group of autonomous fleets to transform today's shared mobility services and also play the role of mobile sensors, which share real-time traffic and road information for transportation management. However, these technological advancements also lead to new cyber and physical threats that cause safety hazards or other undesired consequences. Although there have been a large number of papers about identifying and mitigating each type of threat, the lack of design support still challenges security engineering for developing CAVs. This limits the engineering capabilities of original equipment manufacturers to prioritize among multiple system properties, including safety, security, and privacy, and dealing with ever-changing attack surfaces and the power of attackers. This paper surveys security vulnerabilities and defense mechanisms for CAVs from an engineering design perspective. We illustrate how to identify and mitigate physical threats that compromise the safety of individual vehicles and cyber threats that disrupt newly CAV-enabled transportation services in a systematic way. An integrated security engineering process and a multi-layer design framework are presented for providing traceability and guidance in threat identification and mitigation.**

***Index Terms*— Connected and automated vehicles, security, safety, intelligent transportation systems, V2V, V2I.**

I. Introduction

THE increased automation and connectivity of vehicles and road infrastructure can make future transportation systems more efficient and smarter and enable new transportation business models. Connected and automated vehicles (CAVs) can form a group of autonomous fleets to transform today's shared mobility services and also play the role of "mobile sensors" that share real-time traffic and road information for transportation management. However, these technological advancements may lead to new cyber and physical threats that cause safety hazards or other undesired consequences. For example, a CAV whose on-board sensors or Vehicle-to-Vehicle (V2V) communication modules are under spoofing attacks may initiate false warnings to the driver or conduct risky maneuvers such as unintended deceleration. Besides, when the CAV that is used for sensing for intelligent traffic management is controlled by adversaries, malicious messages that it broadcasts propagating through Vehicle-to-Infrastructure (V2I) communication can result in erroneous decisions by the transportation management center (TMC) such as unnecessary or false emergency responses.

Although there have been a large number of papers on identifying and mitigating each type of threat, the lack of design support still challenges security engineering for developing CAVs. This limits the engineering capabilities of original equipment manufacturers (OEMs) to prioritize among multiple design goals, including safety, security, and privacy, and dealing with ever-changing attack surfaces and the power of attackers.

One reason for this is that security, safety, and privacy converge when it comes to CAV development as different engineering teams need to collaborate to simultaneously achieve these three design goals. This is difficult because of ever-increasing attack surfaces. While preventing inadvertent vehicle responses and unauthorized access to on-board modules is essential to ensuring individual safety and privacy, determining the trustworthiness of V2I event reports in time is critical for CAV-based transportation management. For example, ride-hailing service providers can use vehicle and customer reported locations for route planning of their autonomous fleets. Similarly, public transportation agencies also base their traffic control on the V2I information about vehicle trajectory and real-time traffic. In the event of an incident, the TMC will send ambulance or police cars to accident sites. To deal with the ever-expanding attack surfaces, engineers may need to leverage on different security engineering principles and techniques for developing effective countermeasures [1], [2].

Another reason is the ever-changing power that an adversary has. The dynamic nature of threats can make a mitigation solution that is effective today become invalid in future CAV-based transportation due to changes in the adversary's expertise, user behaviors, or new trends in the market. This requires engineers to hold a dynamic view when prioritizing threats to tackle first. For example, the risk of an insider attacker who can spoof

Manuscript received August 1, 2019; revised May 23, 2020 and August 10, 2020; accepted September 25, 2020. Date of publication December 7, 2020; date of current version March 29, 2022. This work was supported by the Ford-MIT Alliance. The Associate Editor for this article was S. Olariu. *(Corresponding author: Dajiang Suo.)*

Dajiang Suo and Sanjay E. Sarma are with the Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, MA 02139 USA (e-mail: djsuo@mit.edu; sesarma@mit.edu).

John Moore, Mathew Boesch, and Kyle Post are with Ford Motor Company, Dearborn, MI 48126 USA (e-mail: jmoor422@ford.com; mboesch@ford.com; kpost1@ford.com).

Digital Object Identifier 10.1109/TITS.2020.3038755

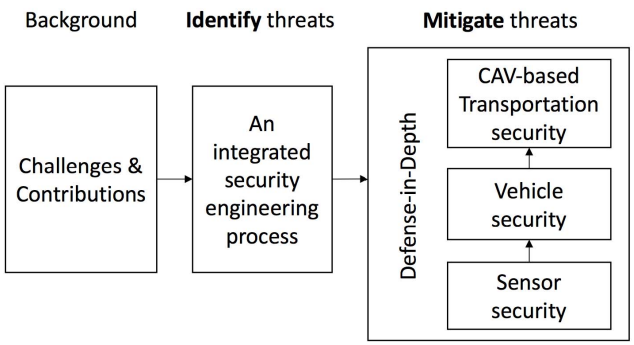


Fig. 1. Organization of this paper.

vehicle identities by using its valid credentials for Vehicle-to-Everything (V2X) communication may be low during the early stage of connected-vehicle deployment. However, the attacker may easily get access to valid vehicle credentials stored on aftermarket or stolen on-board units (OBUs) as the increasing penetration of V2X technologies. The same is true for potential attacks on on-board sensors. A robust security design must be flexible and able to adapt to changes in the power of attackers.

This paper is organized as follows, as shown in Fig. 1. In section II, we discuss current challenges in security engineering for developing CAVs and our contributions. Section III presents an integrated security engineering process that provides guidance for identifying threats. In section IV, we survey different threat mitigation solutions based on the multi-layer design framework we proposed. We discuss how to mitigate physical threats that compromise the safety of on-board sensors and vehicles and cyber threats (with a focus on V2I) which disrupt transportation management.

II. Background

A. Challenges in Designing for Security: An Industry Perspective

For automotive companies adopting new technologies and business models in CAV development, several noticeable challenges in the security engineering process reflect their urgent needs for a systematic approach to identify and mitigate threats.

1) Safety and security (including privacy) properties converge. Since driver-assistance or safety-critical functions, to a large extent, rely on external data sources from on-board sensors, V2X communication, and cloud servers, one of the main security challenges for designing automated vehicles is to protect these data from intentional manipulation and tampering [3]. In response to these security and privacy risks, OEMs often have security experts collaborate with safety and other CAV development teams from the very beginning and for the rest of the CAV development process so that security requirements can be enforced [4], [5]. The process is often guided by the industry best practices and standards, including safety-related standards such as ISO 26262 [4] and Safety of the Intended Functionality (SOTIF) [3], security-related standards such as SAE J3061 [5], ISO 21434 [6], and privacy regulations such as General Data Protection Regulation (GDPR) [7] (an European-wide privacy law that protects personal data or namely Personal Identification Information in the U.S.) in European countries but can also affect OEMs in the U.S. if a vehicle is built and sold to the EU car market. In the meantime, OEMs are left to determine how exactly the security engineering process of each individual organization is implemented.
2) New attack surfaces arise due to the increased levels of connectivity and autonomy and the evolution of car ownership. Non-automated vehicles and vehicles with lower automation levels (1-3 level defined by SAE [8]) have been enjoying enlarged sensor coverage [9], [10]. For them, protecting on-board sensors or electronic control units from malicious attacks is the top priority for the development teams. For vehicle models with enhanced autonomy (level 4-5) and connectivity (e.g., V2X or cellular networks), Since multiple OEMs have already made the announcement of developing highly automated vehicles to support ride-sharing and goods delivery [11], the need for building security into the engineering process becomes more urgent. These vehicles are designed to support information exchange among individual vehicles, cloud centers for fleet operations, and Apps for ride requests, which create rich attack surfaces for adversaries [12]. One example is the previously mentioned V2I-based incident response in which the public transportation agency makes mistakes in allocating rescuing resources if it receives false or fake V2I messages about accidents and road hazards.
3) More "insider" risks emerge. An inside adversary is someone who has privileges in accessing customer or vehicle data, holds valid credentials for communicating with nearby CAVs and road infrastructure [13], or gets the same access as a remote fleet operator such that (s)he can issue commands to control vehicles remotely. For traditional vehicle models, it is arguable that it will always be feasible for a person to get physical access to vehicles or data centers [14], [15]. However, the new CAV ecosystem makes these insider attacks feasible due to the new access points and the expertise that the adversary has. Take the CAV fleet for mobility-sharing services as an example. More third-party technicians can get physical access to in-vehicle networks for the routine maintenance of mechanical components or the software updates. This is possible as a CAV in an autonomous fleet may need maintenance in different depots within its operational regions [16]. Besides, a fleet operator can send commands to CAVs to control their maneuvers remotely in off-nominal situations [17], [18]. Another example is the increasing penetration of V2X technologies, which also gives technicians the opportunities of gaining the required expertise for manipulating communication modules from aftermarket vendors [19]. For example, during the deployment of connected vehicle (CV) pilot by Tampa-Hillsborough

Expressway Authority (THEA), the authority is discussing the possibility of hiring instructors and students from Hillsborough Community College (HCC) through a paid internship to install over 1600 OBUs in privately and publicly owned vehicles [20]. While creating more job opportunities, this also opens up more opportunities for adversaries to gain the expertise. Although there exist commercial products on the market for detecting malicious attacks on V2V messages for protecting individual vehicle safety [21], determining the trustworthiness of the reports from vehicles to infrastructure through V2I channels hasn't been fully addressed.

B. Contributions

A review of previous work surveying CAV cybersecurity provides insights into the research gaps between new threats and existing mitigation solutions. Our main contributions lie in the following aspects.

1) A systematic way of identifying threats. Most existing review papers on the cybersecurity and safety issues of CAVs are mainly focused on introducing detailed threats discovered by the ethical-hacker community and researchers in the academic field [22]–[27], as shown in Table. I. There are also surveys that focus on the security of a specific subsystem, such as machine learning security [28], in-vehicle networks [29], human factor issues [30], V2X communication [1], [31]–[37]. Admittedly, a comprehensive list of potential cyber attacks is valuable for engineers to design mitigation solutions. However, having a structured threat modeling methodology with a top-down view that maps detailed threats to the violation of design goals is crucial for dealing with the ever-changing landscape of threats that we mentioned earlier, and expand next. Here, we present a security engineering process through which safety, security, and CAV design teams can collaborate and prioritize among multiple goals when dealing with threats. Our approach developed from Attack Trees [38] can help engineers in this aspect.
2) A layered threat-mitigation framework. Existing survey papers (in Table. I) of mitigation solutions provide limited design guidance. We present redundant hardware and software solutions to form multiple layers of defenses based on the defense-in-depth [39], [40] principle. It provides guidance for engineers to determine how to add the necessary redundancy for not only protecting vehicle and passenger safety but also preventing normal or emergency transportation services from being disrupted by malicious V2X messages.
3) A multi-stakeholder approach against insider attacks. For the insider risks mentioned earlier, we summarize and present state-of-the-art mitigation solutions from existing literature from both the perspective of OEMs (for developing CAVs) and an transportation management agencies (for intelligent traffic control). Admittedly, a highly automated vehicle needs to be designed to operate itself safely without relying on external information (e.g., from V2X or cloud servers through cellular networks) [22]. This requires that the engineering teams come up with more robust sensing solutions for extreme environmental conditions. Errors due to false or malicious information in a single sensing channel can be compensated by correct information from other sensing modalities. The security awareness allows the control module to move CAVs out of dander zones under risky conditions [4]. For this reason, we first present solutions regarding robust sensor designs and sanity checks for filtering out error and malicious messages for the safety of individual vehicles. However, none of those mitigation strategies presented earlier completely eliminate malicious V2I messages sent from compromised CAVs to infrastructure or the TMC. We then discuss mechanisms to ensure the safe integration of CAVs into transportation systems by using V2I-based (traffic) event report as an example. This is important as transportation agencies and law enforcement departments can benefit from real-time traffic or collective perception information shared by every vehicle. Determining the trustworthiness of V2I messages is crucial for detecting malicious CAVs, an industry-wide "global misbehavior detection system" that the U.S. and local department of transportation (DOT) and the automotive industry have been developing [2], [41].

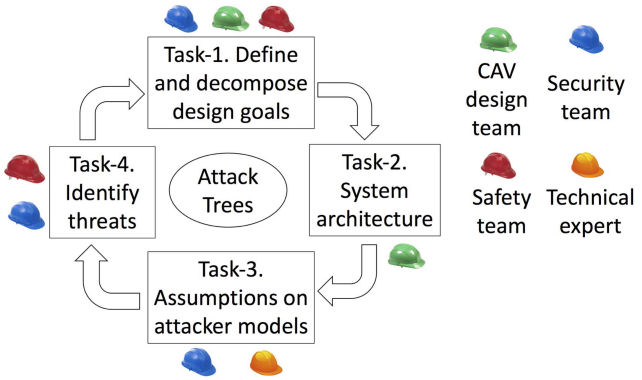


Fig. 2. The proposed security engineering process for threat identification.

III. Threat Identification for Connected and Automated Vehicles

To resolve the first challenge in CAV development, we present a security engineering process for identifying and organizing threats and adversarial behaviors, as shown in Fig. 2. The process includes 4 tasks: defining design goals, developing system architecture, documenting assumptions on attacker models, and deriving attack trees for organizing cyber and physical threats.

The framework aims to merge security (privacy) and safety analyses and is extended from the state-of-the-art work on security and safety engineering activities both in academia [47]–[50] and the automotive industry [3]–[6], [51], [52]. It enables joint work between multiple engineering teams and ensures that any undesired consequence which compromises design goals is traceable to a specific threat.

TABLE I
EXISTING SURVEYS ON THE CYBERSECURITY OF CONNECTED AND AUTOMATED VEHICLES

Authors	Focus	Design goals	Automation levels	Connectivity	System components
Parkinson et al. [22]	Knowledge gaps between known threats and existing mitigation	Security, safety, privacy	All levels	Physical and wireless access to in-vehicle networks, in-vehicle or wireless sensors, GPS, V2X, Wi-fi, cellular	CAVs, drivers, road infrastructure, cloud servers, pedestrians
Sheehan et al. [42]	Risk assesement and cyber-risk reduction by using Bayesian networks	Security, safety	Not mentioned explicitly, but vehicles with human drivers	The same as in [22], with a focus on GPS for CAV's navigation systems.	CAVs, drivers
Petit et al. [23]	A summary of cyber attacks on CAVs, their prioritization, and attack feasibility	Security, safety	Level 4-5	Physical and wireless access to in-vehicle networks, in-vehicle or wireless sensors, GPS, V2X, OBUs for digital maps	CAVs, drivers, road infrastructure, security credential management for V2X
Petit [43]	A stakeholder analysis on Avs and the ecosystem support their production and operation	Security, safety, privacy	Level 4-5	The same as in [23]	CAVs, drivers, road infrastructure, connected service providers, road contract, and fleet operators
Takahashi et al. [44]	A summary of cyber attacks in-vehicle networks, backend systems for connected services, and the communication between them	Security	Not mentioned	Physical and wireless access to in-vehicle networks, V2X, telematics	Connected vehicles, backend systems for connected services
Tokody et al. [45]	A review of security and safety co-engineering process based on industry standards	Security, safety	Level 4-5	Wireless sensors, V2X	CAVs, smart signage, smart lights, ITS traffic controller
Chattopadhyay et al. [46]	A brief summary of the use of security by design framework in designing cyber-physical systems	Security, safety, privacy	Not mentioned, but AVs without human drivers	In-vehicle wireless connection through bluetooth and smartphone, V2X, telematics	CAVs, road infrastructure
Eiza et al. [24]	A general discussion on cyber attacks through malware, OBD, or apps and mitigation solutions	Security, safety	Not mentioned	Physical access to ECUs through OBD ports, apps, or malware	Connected vehicles, backend systems for connected services
Yeh et al. [25]	A discussion on jamming, spoofing, and interference attacks on automotive radar and V2X modules	Security, safety, privacy	Not mentioned	On-board radar, V2X	CAVs and road infrastructure
Cui et al. [26]	A review of safety hazards and cyber threats	Security, safety	both CAVs with and without drivers	Physical access to in-vehicle networks through CAN, wireless sensors, V2X	CAVs and road infrastructure
Koscher et al. [29]	An experimental security analysis of ECUs and CAN bus	Security, safety	Not mentioned but vehicles with drivers	CAN, OBD-port, ECUs	regular vehicles
Qayyum et al. [28]	A review of machine learning security in the context of CAVs	Security, safety, privacy	Not mentioned	On-board wireless sensors, V2X	CAVs and road infrastructure
Linkov et al. [30]	A review of human factors issues related to cyersecurity of AVs	Security, safety, privacy	Not mentioned explicitly but Vehicles with drivers	Not the focus	AVs and human drivers
Heijden et al. [1]	A review of malicious behaviors of vehicular networks	Security, safety	Not mentioned explicitly but Vehicles without drivers	V2X modules	CAVs
Ren et al. [27]	A review of cyber threats on V2X and solutions	Security, safety, privacy	both CAVs with and without drivers	Physical and wireless access to in-vehicle networks, on-board sensors	AVs

A. Identify and Decompose Design Goals

The process starts with the agreement among three teams: safety (represented as a red hat), security (a blue hat), and CAV design (a green hat), as shown in Fig. 2. They agree on key functionalities, services, and assets, which are high-level design goals that must be achieved for the normal operation of vehicles and CAV-enabled transportation services.

The vehicle ownership and the target market segmentation determine what types of automated-driving functions and connectivity a CAV needs to support. Based on trends in the automotive domain discussed in the introduction, we assume that CAVs with lower levels of automation (level 1-3 as defined by SAE [8]) and connectivity mainly serve the market of private passenger vehicles (hereinafter referred to as "Type-1 vehicles"), while level 4-5 automated vehicles with enhanced connectivity (e.g., V2X) target mobility-sharing services (hereinafter referred to as "Type-2 vehicles").

This categorization (Type-1 vs. Type-2) is not the only way to organize the security analysis but reflects a realistic organizational structure across different departments within certain car manufactures [53]. For example, an OEM may assign a set of teams to the development of advanced driver-assistance systems (ADAS) that involve interaction with and intervention by human drivers, while a newly established division can focus on developing CAVs with fully automated-driving systems (ADS) to support ride-sharing services.

- Functionalities. For a Type-1 vehicle, it is expected to support the functions of warning human drivers about potential collision risks. On the other hand, a Type-2 vehicle must provide functions of automated braking, acceleration, or steering after a collision risk is detected. In addition, a Type-2 vehicle may also support remote control by fleet operators [17], [18].
- Services. A Type-1 CAV often provides customers with basic connected services such as remote health monitoring and roadside assistance through cellular networks. A Type-2 CAV takes the services one step further to support ride hailing or sharing and even become the enabler for intelligent traffic control and management. In the latter case, the traffic controller, public transportation agencies, law enforcement departments will rely on the information the CAV provides for allocating resources.
- Assets. We focus our discussion on digital assets (i.e., mobility data) generated by humans or vehicles. For a Type-1 vehicle, Personal Identifiable Information (PII) or location-based information stored within the vehicle or in a backend cloud server are assets and need security protection. The same holds for a Type-2 vehicle except location-based data might also be generated by new sensing or V2X modules.

The high-level goals defined are then decomposed into more detailed hazardous events (HEs) for safety or undesired events (UEs) for security activities, which is also specified in automotive safety and security standards [4].

1) Type-1 Vehicle: We define three HEs for CAV functionalities and two UEs related to customer data.

HE-1 Unintended transition to human-control mode without proper warnings

HE-2 False alarms or false notifications to drivers

HE-3 Unintended maneuvers of CAVs

UE-1 Unauthorized access to driver/vehicle generated data

UE-2 Unauthorized tracking of vehicle movement

2) Type-2 Vehicle: For a Type-2 CAV, we have different safety and security concerns and thus define different HEs and UEs. For example, a Type-2 CAV might violate traffic rules if the automated-driving system misclassifies traffic signs, which is hazardous (HE-4). In additon the UEs identified for Type-1, we can define new UEs if the CAV is used for fulfilling ride requests in ride-sharing services (UE-3) or as a sensing node providing real-time traffic and road conditions to the traffic management center for emergency responses to incidents and road hazards (UE-4).

HE-3 Unintended maneuvers of CAVs

HE-4 Violation of traffic rules/regulations

UE-1 Unauthorized access to driver/vehicle generated data

UE-2 Unauthorized tracking of vehicle movement

UE-3 CAVs do not respond to ride requests

UE-4 Transportation agencies or law enforcement does not respond to emergencies in time

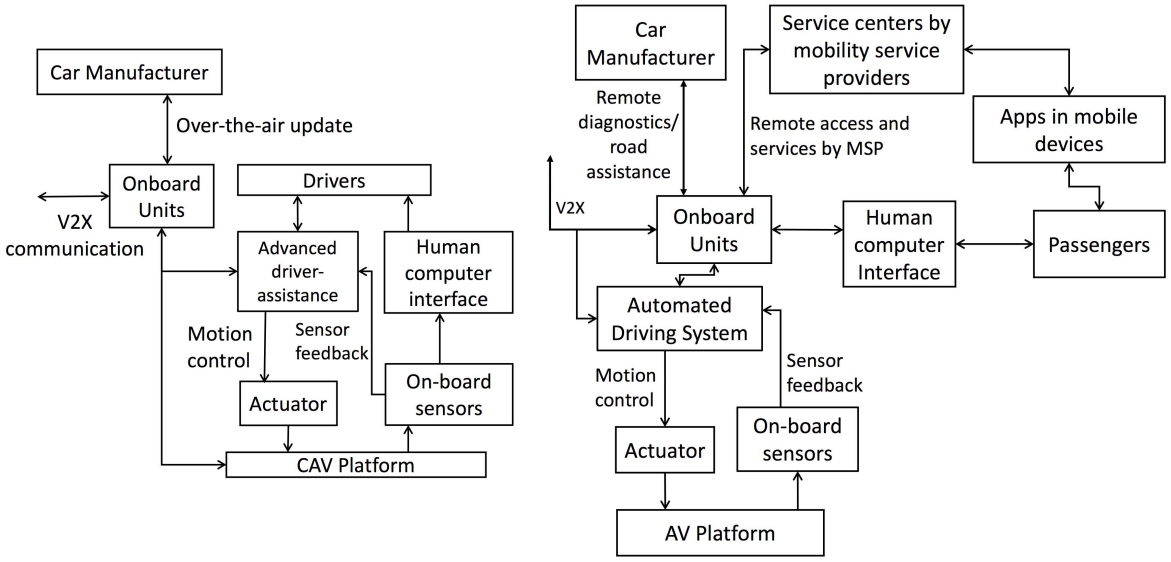
Part of these security goals and objectives are rooted in the traditional security objectives used in information systems such as the CIA (confidentiality, integrity, and availability) triad [54]. However, security goals for CAVs can have a broader scope for CAVs, including protecting digital assets such as customer and vehicle-generated data can be related to the confidentiality objective, protecting CAV key functionalities calls for message integrity, and the CAV-enable services must be protected to ensure the availability.

B. Develop System Architecture

After identifying design goals for CAVs, the second task is to derive system architectures. A CAV's security architecture often includes system components, communication channels, and principals that interact with the system. Similar to design goals, the architecture is determined by assumptions engineers make on vehicle autonomy, connectivity, and car ownership. Two candidate system architectures are presented to be consistent with the categorization of CAVs (Type-1 vs. Type-2) we made earlier, as shown in Fig. 3.

Fig. 3a represents the architecture of a Type-1 CAV, while Fig. 3b corresponds to a Type-2 CAV. We address differences between them in terms of autonomy, human-vehicle interactions, the storage of data, and physical and wireless access points by different human principals.

To begin, the most fundamental difference between Type-1 and Type-2 lies in vehicle autonomy or control authority. Both the ADAS (Fig. 3a) in auto-pilot mode and the ADS (Fig. 3b) rely on information from on-board sensors and wireless communication to determine when to brake, accelerate, or steer automatically. However, for a Type-1 CAV, the human driver is expected to monitor driving conditions and vehicle status and take over during abnormal situations, such as failures in the electronic, mechanical or power systems, when the vehicle is out of the operational design domain [4], or when the ADAS cannot determine the type of unknown objects.



(a) The architecture of Type-1 vehicle

(b) The architecture of Type-2 vehicle

Fig. 3. Architectures for Type-1 and 2 connected and automated vehicles.

Therefore, the human-vehicle interface designed for telematics, entertainment applications, and driver notifications in Type-1 needs to be re-designed for Type-2 architectures. Both human-driver and human-passenger interactions reflect this need for redesign. To design the human-vehicle interface in Type-1 architectures, engineers need to account for the possibility that drivers must take over when cyber-attacks occurs. The interface needs to provide warnings to drivers about potential risks detected by sensors or indicated by V2X messages. For Type-2, the focus of interface design is passenger authentication through on-board interfaces or user Apps [55].

Another difference lies in the physical and wireless access points that have different attack surfaces. For example, in addition to the remote diagnostics and roadside assistance services that are often provided by car manufactures for Type-1 CAVs [56], [57] based on 3G or LTE cellular network, Type-2 CAVs often introduce two new types of remote connections, as shown in Fig. 3b. The first remote connection is the communication link between CAVs and the remote control center by the mobility service provider (MSP). The controller in the cloud center, either a human or an algorithm, will dispatch CAVs after receiving ride requests according to the status of each vehicle. The second remote connection is the high-speed link that supports teleoperation of moving CAVs out of gridlock in emergency situations [17], [18].

Different types of car ownership also lead to different processes and locations for data storage. For private vehicles, the collection, storage, and sharing of PII or sensor data are governed by "terms of service" that owners sign with OEMs when they subscribe to connected-vehicle services [58]. For level 4-5 CAVs providing mobility-sharing services, it is still unclear who will own vehicle-generated or perception data if vehicle status or driving conditions are transmitted to the cloud server for fleet management and ride dispatch, as shown in Fig. 3b.

Another difference involves on-board modules or wireless links that support V2X communication. Even though both types of CAVs use V2X modules, they support different functionalities. In addition to broadcasting vehicle movement and status to support safety-critical applications in Type-1, V2X modules in Type-2 vehicles can report traffic events with high-criticality to local infrastructure or the TMC.

C. Define Attacker Model and Document Assumptions

After identifying key components, principals, and stakeholders for the system architecture, the next task for security engineers and technical experts is to jointly derive attack models. Attack models refer to the assumptions on the power of an adversary (i.e., what an adversary can do), the knowledge and expertise (s)he has about the target system, the motivation for initiating attacks, and sometimes the characteristics of a certain social group (a crime unity) to which the adversary belongs [19]. For example, an adversary can be a car owner [59] who wants to gain economic benefits from selfish behaviors, a technician installing ransomware on the victim's vehicle, or terrorists trying to sabotage CAVs or the transportation system.

To build realistic attack models, we need to consider the methods adversaries use to launch attacks. A conceptual model we developed in our previous work for security analysis in product designs [47] provides guidance in this aspect, as shown in Fig. 4. The model is based on Microsoft's STRIDE model [60] which is used in threat modeling for information systems and adapted to CAV development by merging STRIDE with control-theoretic analyses used in security [48], [50] and human performance analyses [61]. Each type of malicious behavior in the STRIDE categories, which include Spoofing, Tampering, non-Repudiation, Information Disclosure, Denial-of-Service, and Elevation privilege, influences the electronic or physical components of the CAV

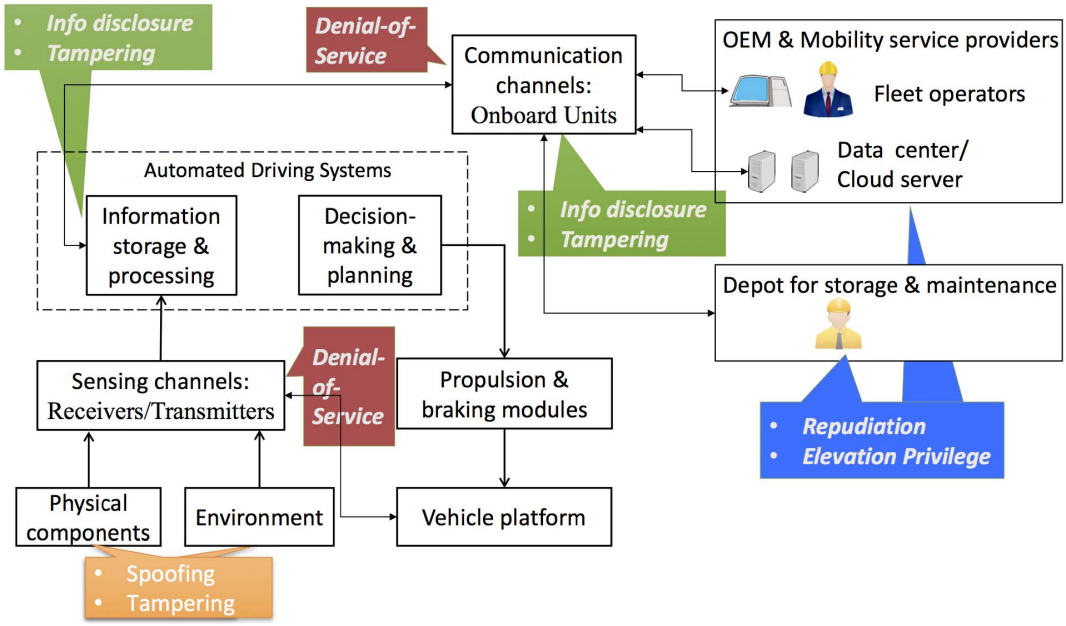


Fig. 4. A conceptual model for deriving attack behaviors extended from [47].

architecture in Fig. 4. Engineers then determine if any of these malicious behaviors would compromise CAV functionalities, disrupt services, or cause damage to assets.

To illustrate the conceptual model, we present an example of an emerging type of threats (adversarial machine learning) in the context of CAVs. This type of threat exploits the weakness of machine learning algorithms (ML), especially deep neural networks (DNNs), for perception tasks such as object detection and recognition. For example, a physical object with a small perturbation in terms of geometry shape, color, or orientation, which is imperceptible to human eyes, can fool the DNNs into misclassifying objects. In addition to causing false alarms to drivers (HE-2) and unintended maneuvers (HE-3) for Type-1 vehicles, adversarial attacks on a Type-2 CAV's perception system built from ML can also result in its violation of traffic rules and regulations (HE-4). It is demonstrated in [62] that a CAV can experience unintended acceleration and thus overspeed even if an adversary slightly perturbs the speed limit sign to fool the perception system.

In order to derive a comprehensive list of attack scenarios for adversarial attacks that cause HE-1 and HE-2, engineers can examine the path of information flow shown in Fig. 4, including signal generation and transmission in the physical environment, signal reception by receivers, information processing for generating training data for AI, data sharing and storage in the cloud. For example, three possible ways of attacking ML models in vision-based tasks based on the conceptual model include:

- Spoofing and tampering physical or digital objects in the environment.
- Spoofing sensing modules such as camera and LIDAR.
- Data poisoning of training data for DNNs through unauthorized access to cloud servers storing these data.

An adversary can spoof objects or the physical environment by creating an illusion of physical objects by projecting images of pedestrians or stop signs with equipment placed on roadside or drones [63]. The adversary can also tamper physical objects by placing paper stickers on traffic signs to fool DNNs into confusing the difference between a stop sign and a speed limit sign, which is demonstrated in both laboratory settings [64] and in the real world [62]. With small physical perturbations on traffic signs, the adversary can maximize the likelihood of classifications errors and in some cases trick ADAS to accelerate to 80 miles per hour (mph) even if the vehicle actually meets a 30 mph sign. Similar attacks are found to be effective in fooling the ADAS to misidentify lanes and cause the CAV to drive into the reverse lane [65]. In addition to camera-based perception systems, CAVs relying on LIDAR are also vulnerable to adversarial attacks [66].

Another way for an adversary to create adversarial examples is to target sensing modules directly such as LIDAR. It is demonstrated in [66] that injecting malicious signals into the reflected light pulses can create adversarial 3d point clouds that cause classification errors and thus unintended emergency braking (HE-3).

Additionally, an adversary who gets unauthorized access to training data for DNNs can conduct data poisoning [67]–[69]. Injecting false training data into the training stage of ML algorithms makes classifiers make similar classification mistakes. Since vision data for training DNNs is collected by each individual CAV but aggregated in the cloud server maintained by OEMs or MSPs, an adversary who gets access privileges (the "E" category in STRIDE) to either in-vehicle storage [23] or on-line servers [70] can initiate such attacks.

For the Type-1 CAV, a malicious driver can conduct local data poisoning by adding noise patterns to sensor data before they are uploaded to the cloud server. For example, an "evil mechanic" [19] who is responsible for vehicle-fleet maintenance has access to the unprotected CAN bus and ECUs to install malware. When it comes to the Type-2

CAV, an adversary can conduct perturbations on the collective training dataset when (s)he has sufficient privileges to access on-line cloud servers. This concern arises when companies store their data on 3rd party cloud servers for computation-intensive tasks. For example, according to the report of the data breach affecting 57 million ride-hailing riders in 2016, the adversaries used stolen login credentials owned by valid employees to gain privileged access to data servers [71].

D. Derive Attack Trees for Traceability

The final task is to document analysis results of identified threats and attack scenarios. The key is to establish traceability between high-level design goals and identified threats [47]. Here, we are interested in how a specific threat on on-board sensors, communication modules, or cloud servers can cause hazardous or undesired events previously defined.

We recommend Attack Trees [38] for this task. Threats are represented by leaves in Attack Trees while HEs and UEs are denoted by roots. This tree-based technique ensures that no high-risk threat will be omitted later in the implementation stage. The Attack Trees for organizing threats on Type-1 and Type-2 CAVs are given in Fig. 5.

Attack Trees introduce three benefits. First, the graphical forms help the three engineering teams manage design changes due to the adoption of new technologies. When an OEM uses new software and hardware modules to implement an old functionality [4], the Attack Trees visualize how these changes influence the results of the security analysis (i.e., traceability between HEs and threats). Second, the derived Attack Trees make it easier to prioritize among different design goals and thus determine which threat to deal with first. Third, the derived Attack Trees enable the estimation of the total cost of security defense mechanisms, i.e., the time and manpower allocated to dealing with identified threats.

We now give details of different types of threats based on the structure indicated by the Attack Tree in Fig. 5, which highlights the different attack surfaces between Type-1 and Type-2 CAVs.

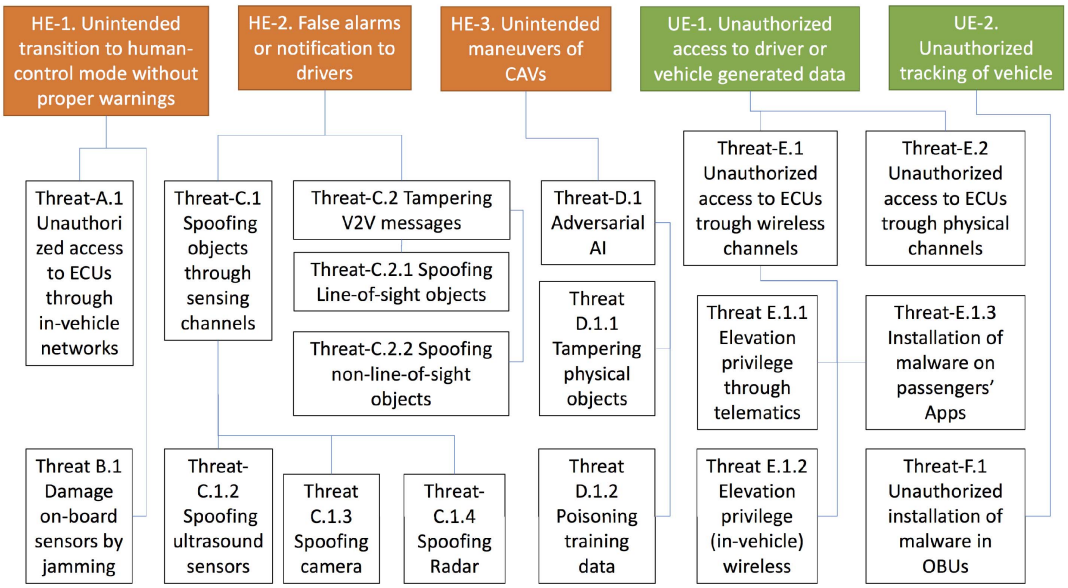
1) Attack Trees for Hazardous Events Regarding Safety: To derive the Attack Trees for a HE, the security engineering team iterates through relevant system components to identify potential threats. System components can be found in CAV architectures described in section III-B, which include in-vehicle mechatronics platforms, on-board sensors and actuators, on-board communication modules, human-computer interface (for Type-1), computer controllers within vehicles or cloud servers, and physical or wireless links. For example, HE-3 of unintended maneuvers might occur during the braking, acceleration, or steering by the automated–driving system in Fig. 3b. Any unauthorized access and tampering with on-board sensing or V2V communication can cause this HE if the related information is used by the ADS for driving maneuvers.

To use the same conceptual model in Fig. 4) to derive detailed threats for the leaf nodes of the Attack Trees for HE-3, security engineers need input from CAV design teams and technical experts for the selection of sensing modules and communication modules for ranging and object recognition. For example, range sensors that use electromagnetic or mechanical waves may be subject to signal relaying, jamming, or injection attacks [66], [72], [73]. Furthermore, perception systems based on visual clues (e.g., RGB information from photos or videos) from camera are vulnerable to adversarial attacks on the physical environment. Example Attack Tree for HE-3 and the list of physical threats on three types of on-board sensors, including LIDAR, ultrasound, and camera, are given in Fig. 5.

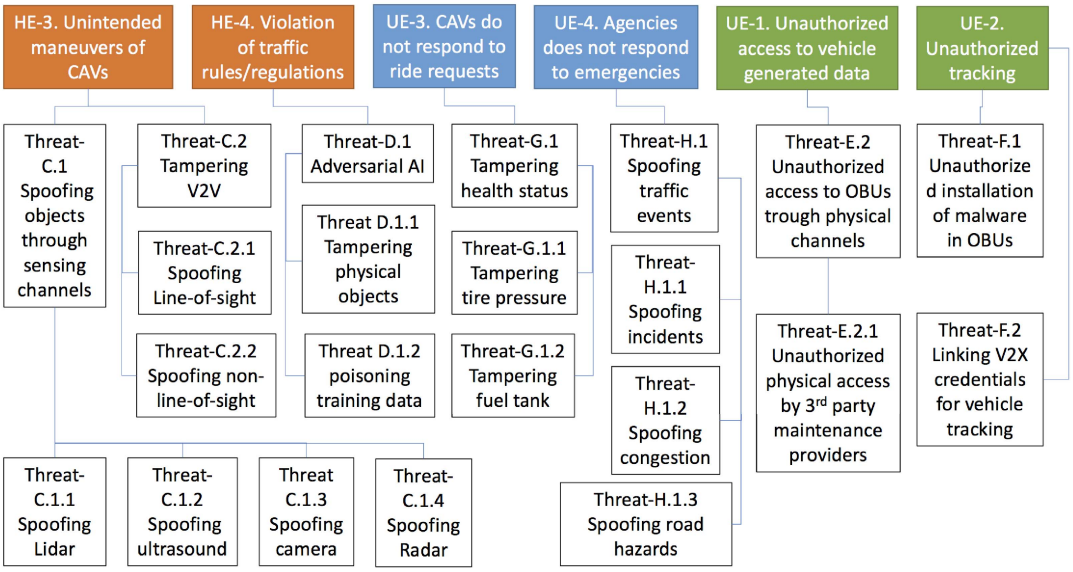
a) Cyber threats on LIDAR: LIDAR, the acronym for Light Detection and Ranging, is a method to detect the relative distance between objects. Commercial LIDAR products that are found to be vulnerable to spoofing (inject fake signals in physical channels) and jamming (denial-of-service) attacks are mostly built on the time-of-flight (ToF) principle. A LIDAR mainly consists of a laser source, a transmitter, a receiver, and a signal processing module. The laser source generates short light pulses that are directed by the transmitter towards a given object (e.g., vehicles in front). Since a proportion of light pulses will be reflected back after they hit the object and are captured by the receiver, the signal processing unit determines the distance by multiplying the one-way time-of-flight with the speed of light [74]. Often, there will be a short time window (e.g., nanoseconds scale) for the receiver module to wait for the reflected light signal after the firing of light pulses. However, if an adversary can take advantage of this short-time window to inject signals before the reflected echoes, s(he) can fool the signal processing unit into thinking that the fake echoes are real ones reflected by the object. For example, Petit *et al.* conduct jamming and spoofing attacks on a commercial product Lux 3 manufactured by ibeo to introduce fake dots that are further away from the attacker's position [75]. Shin *et al.* take one step further by injecting 10 fake dots that are closer to the target than the attacker on a VLP-16 LIDAR manufactured by Velodyne [73]. Cao *et al.* fake 60 points on a VLP-16 by an enhanced attacking platform [7]. Additionally, the possibility of unintentional interference between two LIDAR sensors has been also evaluated by researchers, raising more concerns over LIDAR security vulnerabilities [8], [9], [10], [11].

b) Cyber threats on Ultrasonic sensors: An Ultrasonic sensor used in low-speed application scenarios, such as automatic parking systems, can become the target of jamming and spoofing attacks [76], [77]. Ultrasonic sensors are also built on the ToF principle, which counts the time it takes for ultrasonic pulses generated by the transmitter to travel back to the receiver. In addition to spoofing attacks on Ultrasonic sensors targeting the same vulnerability in the transmitter and signal processing module as in LIDAR, jamming attacks exploit the resonant frequency of the membrane in the receiver of an ultrasonic sensor. Ultrasound noise at the resonance frequency can create continuous vibrations in the membrane and disable the sensor.

c) Cyber threats on Camera: Camera-based vision systems are used in object detection and recognition, tracking, and semantic segmentation tasks. This type of sensing solution is subject to denial-of-service (blinding) attacks. Just as regular



(a) The Attack Tree for Type-1 vehicle, which corresponds to the architecture of Type-1 CAVs given in Fig. 5a



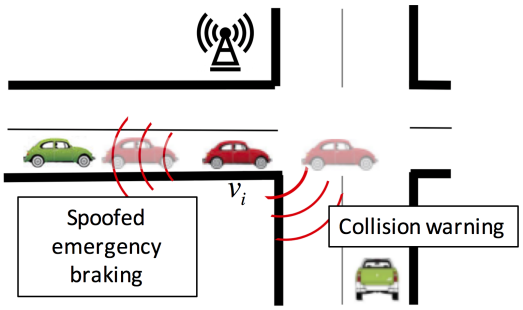
(b) The Attack Tree for Type-2 vehicle, which corresponds to the architecture of Type-2 CAVs given in Fig. 5b

Fig. 5. The Attack Trees for Type-1 and 2 connected and automated vehicles.

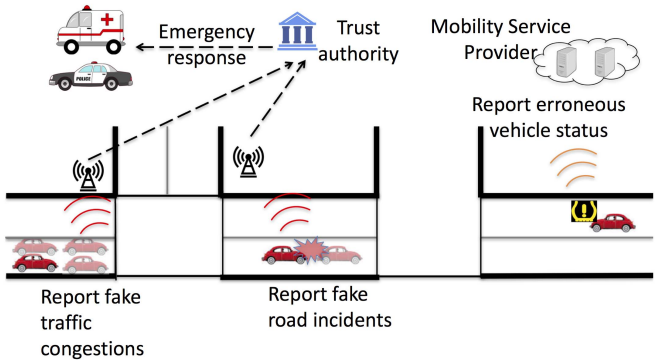
cameras can be dazzled by the glare of the sun [78], some on-board camera in CAVs can be "blinded" by aiming a light source such as laser beam or LED (with either bursts of light or a constant beam) at the receiver lens [75]. In response, the digital camera will try to adjust its exposure automatically in order to adapt to the shift in the tonal range. Besides, strong light beams can cause permanent damage to the CMOS/CCD chip on the camera used in commercial CAVs [76].

d) Cyber threats on V2V communication: An adversary who holds valid V2X credentials or has control over a vehicle can send fake messages about vehicle locations and movements, which creates unnecessary warnings or emergency braking for nearby CAVs. These "Ghost" vehicles can be located at line-of-sight or non-line-of-sight areas with respect to the target vehicle of the attack. In the line-of-sight scenario, the maneuver of the target vehicle can be influenced by emergency braking signals [13], turn signals, or even emergency signals broadcasted by police cars. The non-line-of-sight scenario often occurs when an adversary spoofs ghost vehicles approaching a non-signal intersection. One example is the stationary attacker [79] who uses a wireless device with valid credentials [80] to broadcast fake messages to other vehicles indicating a collision risk, as shown in Fig. 6a. This threat can pose dangers to CAVs who emergency braking functions rely on V2V information.

This type of threat on V2V can be mitigated by either data plausibility checking (also named local misbehavior detection) or multi-modality data fusion techniques. The former



(a) Cyber threats on V2V communication. This type of threat creates unintended maneuvers of nearby CAVs



(b) Cyber threats on V2I communication. This type of threat creates denial of service in private mobility services or public emergency responses

Fig. 6. Graphical illustrations of cyber threats on V2X.

category has been extensively studied in [81]–[84]. Sensor fusion approaches are crucial for Type-2 CAVs, which are more self-sufficient in the sense that they do not rely on information from a single channel (e.g., V2V) for decision-making. We will elaborate this mitigation strategy in section IV.

2) Attack Trees for Undesired Events Regarding Serviceability: There are more attack potentials and security concerns over serviceability for Type-2 than Type-1 vehicles, because of the additional attack surfaces below.

An adversary can initiate attacks to compromise two types of services: ride-hailing and ride-sharing services by mobility-sharing companies (UE-3) and road emergency responses (UE-4) by emergency responders, such as law enforcement and medical agencies, as shown in Fig. 6b.

a) Cyber threats on private mobility-sharing services: Ride-sharing services supported by CAVs can become the target of denial-of-service attacks [59], [85]–[87]. An inside adversary can send false information about vehicle locations and health status to the cloud server to confuse the central dispatcher. Health information may include engine status, tire pressure (Threat-G.1.1) [88], battery status, fuel level (Threat-G.1.2), or about faults in ECUs. Since the dispatching algorithm needs information to determine which CAV in the fleet should be assigned to a given ride, false information can hinder fleet scheduling. For example, spoofed alert packets that are sent to the tire-pressure monitoring system can indirectly influence fleet management.

b) Cyber threats on public emergency responders: For CAV-based transportation services, an adversary can fool the traffic control and management system by sending false reports about incidents [89] or congestion [90]. As a result, the automatic traffic controller may switch to wrong traffic signals [91], [92] or request police cars and ambulances to incorrect locations (Threat-H.1). The need for ensuring the trustworthiness of vehicle-reported information become more urgent as more connected-vehicle applications are deployed in the real world. One example is probe data enabled traffic monitoring (PDETM), an application that transmits real-time traffic data from vehicles to the traffic management system. PDETM is proposed as one of the potential applications in one of the connected vehicle pilot deployment programs by U.S. DOT [20]. The traffic controller may "use probe data information obtained from vehicles in the network to support traffic operations, including incident detection and the implementation of localized operational strategies".

3) Attack Trees for Undesired Events Regarding Privacy: Attack Trees that cause unauthorized access to customer PII data (UE-1) and tracking of vehicle movement (UE-2), as shown in Fig 5, threaten customer privacy. A Type-2 CAV has potential threats on privacy than a Type-1 CAV does, because more stakeholders have the privilege of accessing the data, such as technicians for maintenance or fleet operators as mentioned earlier. Besides, the adoption of the V2X technology for Type-2 CAVs also gives adversaries the opportunity to track the path of a vehicle's movement through V2I messages (Threat-F.2).

a) Cyber threats on access to vehicle or customer data: Unauthorized access to in-vehicle networks, one of the risks responsible for the loss of vehicle or customer data, is discussed in [93] and evaluated through experiments [15], [29]. These experiments include security analyses for attackers who gain physical access through OBD-II ports or telematics systems. The latter is demonstrated in a real-world scenario where an attacker hacks into the ECU controlling the braking function through infotainment systems [94].

For a Type-1 CAV, although it is arguable that an attacker (a person different from the driver) can easily get physical access due to its private ownership [15], the chance that a driver unintentionally installs uncertified third-party applications increases as the automotive industry develops more general-purpose operating systems to support telematics applications [24], [95]. For example, Google has collaborated with Intel and car manufactures including Audi and Volvo to develop an Android OS for vehicle infotainment systems [96].

It is also possible that an uncertified application is malware that invades customer privacy by reading data from sensors or PII data stored in the on-chip memory. Woo *et al.* demonstrate a practical attack on CAN bus through an OBD diagnostic tool. The malware OBD diagnostic tool is installed on drivers' smartphones and paired with the vehicle through Bluetooth [97]. The malicious App can give the control of ECUs to remote attackers.

For a Type-2 CAV, there exist additional modes of unauthorized access, such as when vehicle-generated and customer PII data are transmitted and stored on a cloud server. An mobility service provider can use the stored customer data for user authentication or payment when external individuals access to customer data stored in the server owned by a third-party cloud

service provider [98]. Engineers need to consider when and how to encrypt and decrypt these data during the transmission to protect the confidentiality of customer data in case of data breaches.

b) Cyber threats on tracking vehicle movement: The tracking of vehicle locations and movement results from the installation of malware in OBUs (Threat-F.1) or linking vehicle credentials included in V2X messages with location data (Threat-F.2). The latter has been demonstrated in [72] when an inside attacker deploys tracking devices on compromised RSUs to monitor a vehicle's trajectory history. The process of designing defenses to this threat illustrates how to resolve conflicts between security and privacy goals, as will be discussed further when we present mitigation solutions in section IV-C.

E. Maintaining Attack Trees for Change Management

To maintain traceability from design goals and detailed threats, to mitigation solutions throughout the security engineering process, the interdisciplinary engineering teams need tools to ensure that changes made by one team (e.g., CAV design team) can be reflected immediately and consistently in the view of other teams.

Tools developed from general modeling languages such as UML [99] or SysML [100] can help in this process. Software tools based on these formal languages help engineers visualize and manage the proposed security engineering process. Specifically, Attack Trees documenting analysis results can be serialized and stored in enterprise cloud servers. Maintaining a "single" model throughout CAV life-cycle enables multiple teams to have a consistent view of the gap between unresolved threats and existing mitigation solutions implemented.

IV. Threat Mitigation for Connected and Automated Vehicles

Designing mitigation solutions to identified threats is an interdisciplinary task. while preventing on-board sensors from physical (e.g., spoofing and jamming) attacks needs the expertise in electromagnetic theory, signal processing, and sensor designs, protecting wireless (V2X) communication requires the understanding of pros and cons for each authentication scheme in security protocols. Additionally, security engineers need to understand the role of CAVs in future mobility-sharing business and intelligent transportation applications beyond technological aspects (UE-3 and 4 in Fig. 5).

We present a design framework based on Defense-in-Depth principle [39], as shown in Fig. 7. This framework incorporates redundancies of security controls into different layers of the CAV ecosystem such that security flaws in a single vehicle node can only influence part of the whole transportation system. The color of each square box in Fig. 7 indicates which types of HEs or UEs the mitigation solution target: the orange ones are related to safety hazards, the green one related to UEs regarding privacy, and the blue one related to UEs regarding mobility or emergency services (in Fig. 5). The multi-layer framework can provide guidance to engineers on designing threat-mitigation solutions from the views of sensor suppliers, OEMs, and traffic management agencies.

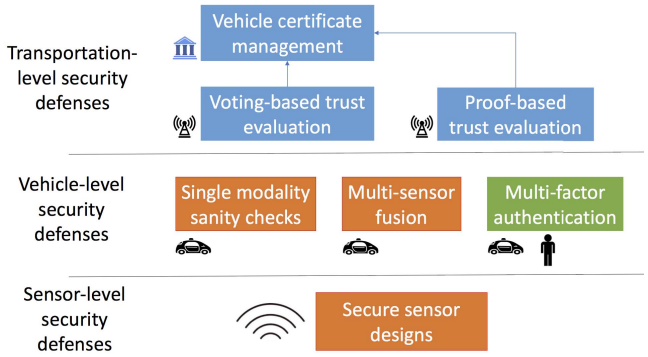


Fig. 7. The proposed framework for designing mitigation solutions based on the Defense-in-Depth principle.

A. Mitigation Solutions at the Sensor Layer

The first layer of the defense framework allows engineers to modify the mechanical or physical structure of sensors and employ sanity checks on signals from each sensing channel to defend against jamming and spoofing attacks on on-board sensors (Threat-C.1)

To mitigate spoofing and jamming attacks on LIDAR (Threat-C.1.1), engineers can reduce the receiving angle of the receiver to make it difficult for the attacker to precisely aim the laser at the optical lense of the receiver [73], [75]. An alternative approach is to employ pseudo-random modulation to manipulate the wave form from the LIDAR's transmitter such that the signal processing module on LIDAR can determine whether a received light echo is the reflection off real objects or spoofed [66], [101], [102]. Both of these two defensive approaches require engineers to prioritize between performance (i.e., sensitivity of LIDAR) and cost (because of increased complexity in the lens systems).

Another approach for detecting LIDAR spoofing is to conduct sanity checks on received optical signals based on the intrinsic property of light [103]. For example, engineers can decide if the received optical signals are faked by comparing the polarization state of the received light with the incident light [104].

For ultrasound sensors, the same anti-spoofing technique used for LIDAR can be also incorporated into the design of the transmitter and receivers for ultrasound signals [77]. However, the unique property of sound transmitters (i.e., ultrasonic transducers) give engineers more opportunities to design mitigation solutions specific for ultrasound sensors. In addition to applying a specific waveform to the transmitted signals, the transmitter can change the pattern, including frequency, phase, and amplitude, of the transmitted ultrasound signals such that the signal processing module can decide if the received signals are spoofed or tampered.

B. Mitigation Solutions at the Vehicle Layer

The second layer of the defense framework focuses on software techniques for preventing CAV safety hazards or protecting customer privacy.

1) Sanity and Consistency Checks on Sensor or V2X Data: Engineers can develop software algorithms to mitigate threats

to sensors (Threat-B.1 and C.1) or to V2V communication (Threat-C.2) based on two types of techniques: consistency check on data from a single sensing channel and multi-modality information fusion.

The former types of algorithms build on the rationale that the position, speed, and acceleration data from a given sensing module in a vehicle is unlikely to experience abrupt changes as the vehicle movement must obey physical laws, transportation regulations, and social rules. For example, sensor or V2V data received by a host vehicle must not indicate that the target vehicle (i.e., sender) is moving in an implausible region such as roadside areas [105] or at an extremely fast speed (e.g., greater than 80 mph under congestion). Solutions built on this rationale have been applied to LIDAR [73], ultrasound sensors [77], camera [63], and V2V communication modules [34], [83], [106].

The second types of algorithms rely on data fusion methods [107] to filter out false and malicious messages by cross-modality checking [26]. This implies that highly automated vehicles (Type-2) with enhanced connectivity and automation tend to (and must) be more "self-sufficient" than Type-1 CAVs and suffer less from malicious messages in V2V channels. In line-of-sight conditions, vision information from LIDAR [108] and camera [82] can be merged into sensor fusion algorithms to detect if an object indicated by V2V messages is faked by adversaries. A lot more work needs to be done in sensor fusion methods which can detect faked objects in V2V channels in non-line-of-sight scenarios. Since such non-line-of-sight objects are out of the coverage by on-board vision sensors [109], cross-modality checking become infeasible.

In general, robust mitigation algorithms must have enough redundant information channels for the automated controller to make safe transition from normal operation to degraded operation modes when one sensing channel is under cyber attacks. These redundant designs for CAV security are motivated by design concepts for CAV safety, such as minimum risk conditions and minimum risk maneuvers [4] which require that a CAV enters degraded operational mode in the event of system failures or faults.

2) Multi-Factor Authentication: Multi-factor authentication (MFA) targets unauthorized access. Three types of principals need to authenticated before getting physical and remote accesses to CAVs, including drivers and passengers, remote fleet operators, and technicians for vehicle maintenance.

- Drivers and passengers. In addition to PIN codes and passwords, the authentication module for in in-vehicle networks has more options of verifying driver and passenger identities, including digital tokens stored in physical devices such as smartphones [110], user behavior or mobility patterns [36], and biometric characteristics [111] such as fingerprint or facial features. When adopting biometric features to authenticate drivers, engineers must consider secure ways of storing these priavcy-sensitive information. Additionally, from a usability perspective, the authentication process needs to be finished within a short duration and create minimum burdens for CAV customers [36].
- Technicians and remote operators. Although similar techniques for authenticating drivers and passengers can also be applied to technicians and remote operators, the authorization process for the latter is often more strict. Security breaches caused by malicious technicians and remote operators have a much larger impact on the whole autonomous fleet. Therefore, engineers are recommended to apply a second factor authentication to verifying the identities of technicians and remote operators whenever there are changes in user contexts or login behavior [112]. For example, a remote operator or technician will be asked to provide extra certificates or confirmations from a device previously used for login if they use new devices or behave suspiciously.

C. Mitigation Solutions at the Transportation Management Layer

The security defenses discussed so far can protect individual CAVs from physical and cyber attacks targeting on-board sensors or V2V modules. Still, they cannot deal with cyber attacks (e.g., Threat-G.1 and Threat-H.1) caused by false V2I messages, which can disrupt the private mobility-sharing services (UE-3) or public emergency responses (UE-4). In particular, new methods are needed for the infrastructure components to determine the trustworthiness of V2I messages and the sender vehicles. Here, our objective is to construct new approaches to detect inside attackers who send V2I messages with tampered contents but valid credentials.

Two emerging types of approaches, proof-based and voting-based schemes, can be used for verifying V2I messages. They are built on the assumption that local digital infrastructure (e.g., RSU) has enough computing power and bandwidth to run algorithms for V2I verification. An RSU will verify the trustworthiness of a V2I message based on "proofs" that the sender vehicle presents or "votes" from other vehicles nearby. These two types of schemes are summarized in Tab. II, and expand next.

After RSUs have finished the verification process, the results regarding the trustworthiness of the message or the vehicle can be shared to the trust authority for managing vehicle credentials [41], as shown in Fig. 7. Before presenting detailed methodologies for mitigation, we describe terminologies used and assumptions we made for transportation management based on the vehicular network.

The proof-based approach rely on the RSU capabilities to directly verify the authenticity of V2I messages. These messages are location-based and sent out by each CAV along the path of its movement [123]. On the other hand, for the voting-based approach, an RSU accepts or rejects a V2I message based on votes from multiple vehicles in a local region. The idea is that each vehicle shares its opinions to form consensuses on the authenticity and correctness of a safety-critical message [124].

1) Terminologies and Assumptions: CAV nodes and surrounding road infrastructure together can form a local vehicular ad hoc network (VANET) to support non-safety or safety applications [125], [126], which is realized through the deployment of on-board and roadside units that support wireless

TABLE II
SUMMARY OF LOCATION-BASED SCHEMES ON VERIFYING V2I MESSAGES

Authors	Category	Security objectives	Assumptions on V2I message content or format
Singh et al. [113]	Proof-based	Restrict the use of the same crypt key within short-time interval	Timing information are encoded into messages
Lu et al. [114]	Proof-based	Prevent vehicles from rquesting multiple temporary keys from RSUs	Timing information are encoded into messages
Biswas et al. [115]	Proof-based	Prevent the key from being misused by colluding vehicles	Location information are encoded into messages
Chang et al. [116]	Proof-based	Detect Sybil nodes	Trajectory information are encoded into messages
Wong et al. [117]	Proof-based	Detect malicious messages with falsified vehicle movement	Trajectory information are encoded into messages
Park et al. [118]	Proof-based	Detect Sybil nodes	Trajectory information are encoded into messages
Liu et al. [119]	Hybrid: eligible to vote based on valid proofs	Detect malicious vehicles reporting fake events	Knowledge of nearby objects or environment are encoded into messages
Yu et al. [120]	Voting-based	Detect Sybil nodes	Each vote about the claimer's position contains measured signal strength
Malik et al. [121]	Voting-based	Determine event or sender trustworthiness	Each vote contains recommendation for an event or node
Yang et al. [122]	Hybrid: eligible to vote based on valid proofs	Determine event or sender trustworthiness	Each vote contains recommendation for an event or node

communication in the transportation environment. One example is dedicated short-range communication (DSRC) [127], a two way wireless communication radio service in the 5.9 GHz band. Before presenting detailed mitigation schemes, We define terminologies and list assumptions necessary for the discussion of V2I-message verification.

Claimer. A claimer is a vehicle that makes a claim about its location, movement, and observed traffic events that are within a certain region or in a position relative to other nodes in transportation systems [128]. It broadcasts messages containing the information above to surrounding vehicles, roadside infrastructure, and traffic management systems for supporting safety and non-safety applications [2].

Verifier. A verifier can be a vehicle (in voting-based schemes) or an infrastructure component (e.g., an RSU) that confirms or disproves a vehicle's claim [128]. A verifier must be capable of discriminating messages or requests between a benign vehicle or a malicious node with spoofed identity.

Trust Authority (TA). A TA is often established by public transportation agencies (e.g., local DOTs in the U.S.). It is responsible for issuing or revoking credentials assigned to a vehicle [2], [129]. One way to achieve this goal is to have the TA determine and maintain the reputation of each vehicle within a local region based on malicious behavior detection (i.e., whether a given vehicle node broadcast false and fake information about its status and traffic events) [130], [131].

OBU. An OBU is installed with credentials or certificates issued by the TA and thus can be used for uniquely identifying a CAV in vehicular networks. In the futural CAV ecosystems, an OBU can be preloaded with digital certificates for message authentication issued by the TA during the vehicle registration with transportation agencies [115]. Alternatively, this process can also be handled by aftermarket suppliers who installed them on old vehicles (vs. connected vehicles) [20].

Sybil attacks. Sybil attacks first get attention in peer-to-peer systems where a single hostile entity can present multiple valid identities [132]. In the context of CAVs, an inside adversary can initiate Sybil attacks by spoofing vehicle identities for V2X communications [105], [113], [133], [134]. An adversary may get this capability through two methods. First, if privacy-preserving schemes (e.g., group signature or short-live certificate) are used, an adversary may be capable of using one certificate to request services within a short time interval [114], [135] or use the same pseudonym to send bogus information repeatedly. Second, an adversary who gets physical access to OBUs for V2X communications can extract vehicle's credentials from stolen vehicles. If this happens, the adversary can easily impersonate vehicle identities for sending fake or bogus information [14], [89], [116].

2) Proof-Based Schemes: In the context of V2I communication, a proof refers to the context information a vehicle encodes in the V2I message it sends out. The proof can support the vehicle's claims on the locations in its trajectory and the observations the vehicle makes along the path of its movement. Since proofs about vehicle motion must conform to physical laws of movement (e.g., a vehicle moving at an implausible fast speed or being in two different locations at the same time), and proofs of a vehicle's observations must be consistent with the environmental conditions in a local region (e.g., observed traffic events or weather conditions), the verifiers (e.g., RSUs and the traffic management center) can use them to determine the authenticity and the integrity of V2I messages.

We categorize proof-based methods into two classes based on the type of content contained in proofs: spatio-temporal information as proofs and knowledge and observations about the surrounding environment as proofs. The design process of constructing proofs illustrates the prioritization balance between security and privacy.

Proof-based methods are designed to verify the authenticity and integrity of V2I messages. An adversary can fake falsified messages in two types of scenarios. The first scenario often occurs when privacy-preserved authentication techniques are adopted in V2I communication, such as group signature [135] or short-lived pseudonyms [2]. Engineers can encode location and timing information in a V2I message for verify messages. In the second scenario, an inside attacker can get physical access to OBUs storing a vehicle's credentials, which can be mitigated by encoding the complete trajectory of the vehicle.

a) Location or time-encoded proofs: We focus on encoding location and timing information in V2I messages sent out by the claimer vehicle such that the verifiers can detect insider adversaries due to the adoption of privacy-preservation schemes, such as group signature [2], [135]. The idea behind group signature is that each vehicle, as a member of a vehicle group, can generate a signature on behalf of the group and each group member can verify the signature without knowing the signer of the message. For this reason, it is possible that a malicious CAV may initiate denial-of-service attacks by sending a large quantity of fake events to nearby vehicles or infrastructure components within a short time period without being detected.

To detect falsified and faked events reported by a claimer vehicle by using time-encoded V2I messages, an RSU verifier can require the claimer to sign on the concatenation of the message and the current time rather than the raw messages, when generating digital signatures. If a verifier receives multiple V2I messages regarding the same traffic event, service request, or registration request (requesting a new session key), the verifier can check if the time interval between two consecutive requests is less than a pre-defined threshold [113], [114]. A violation of this rule indicates a potential attack.

Similarly, location-encoded V2I messages can be used to deal with insiders in anonymous message authentication. For example, rather than use group signature or short-lived pseudonyms for maintaining anonymity during V2I communication, existing authentication algorithms such as elliptic curve digital signature algorithm (ECDSA) can be enhanced such that a claimer vehicle can use a session key [115] generated by encoding its real-time locations. For a RSU, only a claimer vehicle with a session key indicating its close proximity will pass the check. This can prevent an insider who tries to achieve reputation by replaying old messages from other benign vehicles.

b) Trajectory-encoded proofs: The idea of requiring the claimer vehicle to encode timing and location information in V2I messages as proofs for identity verification can be extended to vehicle trajectory information [117]. The main use of trajectory-based verification is to defend against Sybil nodes created by insider adversaries who hold a valid vehicle credentials through physical access to OBUs, which is different from insider scenarios caused by the use of privacy-preservation schemes discussed above.

The main idea behind a trajectory-based approach is the notion of similarity testing. Each vehicle has its unique movement pattern and the possibility that two vehicles pass multiple RSUs at the exact same time points along their trajectory is extremely small [116], [118]. Therefore, V2I messages indicating that multiple vehicles have same trajectory are suspicious. To get the trajectory of a given claimer vehicle, a verifier can rely on the reports from either surrounding vehicles or infrastructure.

Any vehicles that the claimer vehicle meets along its trajectory can serve as witnesses, which receive anonymous beaconing from the claimer vehicle and report their "observations" to the verifier as proofs [14]. However, vehicle-based reports assume a high density of connected vehicles, which is difficult to achieve in early stages of connected-vehicle deployment. Infrastructure-based reports rely on RSUs deployed to road segments or intersection. The RSUs can generate location signatures to attest to the location-related claims by the claimer vehicle [116], which works for low market penetration of connected vehicles.

c) Knowledge and observations as proofs: In addition to spatio-temporal information a CAV encodes in V2X messages, an RSU verifier can also test the knowledge the CAV has about the surrounding environment such as visual clues made by on-board sensors to verify the messages reported by the CAV. For example, the verifier can pose a challenge to test a claimer vehicle's knowledge about the color, type, and size of the vehicle involved in a traffic incident when verifying the incident report from that claimer [119].

In general, proof-based schemes challenge claimer vehicles by creating burdens of spatial movements and testing claimers' knowledge. Only vehicles whose movement patterns follow physical laws of motion and pre-defined rules or who show the knowledge of the surrounding environment are authorized to participate in activities in vehicular networks such as reporting traffic events, accusing malicious vehicle nodes, and requesting for roadside assistance under emergency conditions.

3) Voting-Based Schemes: In addition to proof-based methods, voting-based schemes can also verify the authenticity and integrity of V2I-reported traffic events with high criticality, such as incidents and temporary workzone. An RSU verifier may invite nearby witness vehicles to report (i.e., vote) their observations on the same event, such as the location, the occurrence time, and the severity. The verifier determines whether to confirm and forward the event to the TMC based on the joint reports from these nearby vehicles.

The key to V2I-event voting is deciding each witness's eligibility to vote. There are three ways. The first way allows all witness vehicles in close proximity of an event to vote, and each witness has equal weight in voting [120], [136] because vehicles closer to the event location often get more precise observations than vehicles farther away. The second way is to set a group of pre-determined trusted parties as voters, rarther than determining the eligibility on the fly. Such ideas have been explored in voting-based consensus algorithms for blockchain technologies, such as the proof-of-authority [121] consensus protocols. The third way of selecting voters combines voting-based and proof-based schemes. The eligibility of a candidate voter is determined by whether this candidate can present valid proofs. A claimer vehicle presents proof for its eligibility by providing the RSU verifier with the claimer's presence in a given location at a particular time or

with the observations the claimer makes along the trajectory path [119], [122].

4) Credential Management Based on Trust: After an verifier RSU determines the trustworthiness of a V2I-reported event, the verifier can share the verification results to the TA for reputation management. Specifically, the TA can update the reputation of the claimer vehicle according to the verification results from proof and voting-based schemes [131]. It will then use the reputation score of the claimer vehicle to manage the claimer's certificates for V2X communication [41]. In case that the vehicle gets a reputation score lower than the pre-defined threshold, the TA can revoke the certificates assigned to the vehicle [2]. A detailed treatment of calculating reputation scores for claimer vehicles can be found in [131], [137]–[139]. In addition to using the TA for maintaining the reputation of every vehicle, there are also proposals for decentralized reputation management in which each vehicle will maintain a duplicate of reputations scores of all other vehicles in a local region [140] although the decentralized approach comes with a price of higher memory consumption of on-board units.

To design the trust architectures for reputation and certificate management in CAVs, engineers often need to make three tradeoff decisions. The first tradeoff is the prioritization between between security and privacy. The TA relies on trust evaluations shared by RSUs in a region to determine the reputation of a given claimer vehicle. To achieve this, the RSUs need to collectively track and interact with the vehicle to collect a certain amount of V2I messages so that the TA form opinions on the reputation of the vehicle node. However, compromised RSUs may give adversaries unauthorized accesses to edge servers that store credential or other confidential information of the vehicle, violating the requirement for location privacy [141]. The second tradeoff involves the balance between the effectiveness of threat-mitigation approaches and the cost of infrastructure deployment. Both the proof-based and voting-based methods require that a certain density level of RSUs are deployed within a local region [142], [143]. However, the high density will also incur extra cost of RSU installation and maintenance [144]. One solution is to formulate RSU deployment as an optimization problem to minimize the installation cost and delays in V2I message routing [145]. The third tradeoff is between the communication overhead and the security of communication protocols. V2I messages containing more details of the behaviors and movements of a claimer vehicle can provide the TA with more contextual information to determine the reputation of the claimer node. However, adding more contents to the V2I messages designed for evaluating vehicle trust will increase the message size and thus incur extra communication overheads, which might also hinder the normal propagation and processing of other time-sensitive V2I messages [146].

V. Conclusion

This paper discusses threat identification and mitigating in CAVs from an engineering design perspective. Specifically, we first proposed an integrated security engineering process for identifying threats to CAVs and CAV-enabled transportation. We also illustrate the use of the proposed security process in a multi-team collaboration environment by presenting two types of CAV architectures with different levels of automation and connectivity. Analysis results of threat identification stored in Attack Trees help engineering teams maintain the traceability between the design goals and the identified threats and manage design changes throughout the CAV life cycle. We then survey and present mitigation solutions on identified threats based on the proposed three-layer design framework, which includes the sensor, vehicle, and transportation layer defenses. In particular, to eliminate insider adversaries who pose threats to V2I-enabled transportation management and emergency responses, we categorize and present state-of-the-art location-based schemes to determine the trustworthiness of V2I messages. These schemes can be expanded to vehicle credential management.

References

[1] R. W. van der Heijden, S. Dietzel, T. Leinmüller, and F. Kargl, "Survey on misbehavior detection in cooperative intelligent transportation systems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 779–811, 4th Quart., 2018.

[2] T. Zhang and L. Delgrossi, *Vehicle Safety Communications: Protocols, Security, and Privacy*, vol. 103. Hoboken, NJ, USA: Wiley, 2012.

[3] *Pas 21448-Road Vehicles-Safety of the Intended Functionality*, Int. Org. Standardization, Geneva, Switzerland, 2019.

[4] *26262: Road Vehicles-Functional Safety*, International Standard ISO/FDIS 26262, 2011.

[5] J. SAE, *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. 2016*, Standard 3061, Society for Automotive Engineers, Jan. 2016.

[6] *21434-Road Vehicles–Cybersecurity Engineering*, C. SAE, ISO, London, U.K., 2019.

[7] P. Voigt and A. Von dem Bussche, "The EU general data protection regulation (GDPR)," *A Practical Guide*, 1st ed. Cham, Switzerland: Springer, 2017.

[8] SAE On-Road Automated Vehicle Standards Committee, "Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems," *SAE Standard J.*, vol. 3016, pp. 1–16, Jan. 2014.

[9] Tesla. (2019). *Future of Driving: Advanced Sensor Coverage*. [Online]. Available: https://www.tesla.com/autopilot

[10] Audi. (2019). *Experience Audi: Autonomous Driving*. [Online]. Available: https://www.audi.com/en/experience-audi/mobility-and-trends/autonomous-driving.html

[11] F. M. Company. (2018). *Ford, Walmart and Postmates Team up for Self-Driving Goods Delivery*. [Online]. Available: https://media.ford.com/content/fordmedia/fna/us/en/news/2018/11/14/ford-walmart-and-postmates-team-up-for-self-driving-goods-deliv.html

[12] Daimler. (2019). *2019 Safety First for Automated Driving*. [Online]. Available: https://www.daimler.com/documents/innovation/other/safety-first-for-automated-driving.pdf

[13] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228–255, 1st Quart., 2015.

[14] F. Malandrino, C. Borgiattino, C. Casetti, C.-F. Chiasserini, M. Fiore, and R. Sadao, "Verification and inference of positions in vehicular networks through anonymous beaconing," *IEEE Trans. Mobile Comput.*, vol. 13, no. 10, pp. 2415–2428, Oct. 2014.

[15] S. Checkoway *et al.*, "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. 20th USENIX Secur. Symp. (USENIX Secur.)*, San Francisco, CA, USA, vol. 4, 2011, pp. 447–462.

[16] T. Verge. (2018). *A Day in the Life of a Waymo Self-Driving Taxi*. [Online]. Available: https://www.theverge.com/2018/8/21/17762326/waymo-self-driving-ride-hail-fleet-management

[17] J. S. Levinson, T. D. Kentley, G. T. Sibley, R. Y. Gamara, A. G. Rege, and G. Linscott, "Teleoperation system and method for trajectory modification of autonomous vehicles," U.S. Patent 9 507 346, Nov. 29, 2016.

[18] N. Fairfield, J. S. Herbach, and V. Furman, "Remote assistance for autonomous vehicles in predetermined situations," U.S. Patent 9 720 410, Aug. 1, 2017.

[19] J. Petit, M. Feiri, and F. Kargl, "Revisiting attacker model for smart vehicles," in *Proc. IEEE 6th Int. Symp. Wireless Veh. Commun. (WiVeC)*, Sep. 2014, pp. 1–5.

[20] Tampa. (2016). *Connected Vehicle Pilot Deployment Program Phase I Comprehensive Pilot Deployment Plan*. [Online]. Available: https://www.tampa-xway.com/

[21] Qualcomm. (2019). *Aerolink Communications Security*. [Online]. Available: https://www.qualcomm.com/products/features/aerolink-security

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

[23] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. Intell. Transport. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2015.

[24] M. Hashem Eiza and Q. Ni, "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity," *IEEE Veh. Technol. Mag.*, vol. 12, no. 2, pp. 45–51, Jun. 2017.

[25] E. Yeh *et al.*, "Cybersecurity challenges and pathways in the context of connected vehicle systems," Univ. Texas Austin. Data-Supported Transp. Oper., Austin, TX, USA, Tech. Rep. 134, 2018.

[26] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles," *Ad Hoc Netw.*, vol. 90, Jul. 2019, Art. no. 101823.

[27] K. Ren, Q. Wang, C. Wang, Z. Qin, and X. Lin, "The security of autonomous driving: Threats, defenses, and future directions," *Proc. IEEE*, vol. 108, no. 2, pp. 357–372, Feb. 2020.

[28] A. Qayyum, M. Usama, J. Qadir, and A. Al-Fuqaha, "Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the way forward," 2019, *arXiv:1905.12762*. [Online]. Available: http://arxiv.org/abs/1905.12762

[29] K. Koscher *et al.*, "Experimental security analysis of a modern automobile," in *Proc. IEEE Symp. Secur. Privacy*, 2010, pp. 447–462.

[30] V. Linkov, P. Zámečník, D. Havlíčková, and C.-W. Pai, "Human factors in the cybersecurity of autonomous vehicles: Trends in current research," *Frontiers Psychol.*, vol. 10, p. 995, May 2019.

[31] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Netw.*, vol. 61, pp. 33–50, Jun. 2017.

[32] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017.

[33] M. Arshad, Z. Ullah, N. Ahmad, M. Khalid, H. Criuckshank, and Y. Cao, "A survey of local/cooperative-based malicious information detection techniques in VANETs," *EURASIP J. Wireless Commun. Netw.*, vol. 2018, no. 1, p. 62, Dec. 2018.

[34] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, "On data-centric misbehavior detection in VANETs," in *Proc. IEEE Veh. Technol. Conf. (VTC Fall)*, Sep. 2011, pp. 1–5.

[35] J. Zhang, "A survey on trust management for VANETs," in *Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl.*, Mar. 2011, pp. 105–112.

[36] A. Ometov and S. Bezzateev, "Multi-factor authentication: A survey and challenges in V2X applications," in *Proc. 9th Int. Congr. Ultra Modern Telecommun. Control Syst. Workshops (ICUMT)*, Nov. 2017, pp. 129–136.

[37] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 279–298, 2nd Quart., 2012.

[38] B. Schneier, "Attack trees," *Dr. Dobb's J.*, vol. 24, no. 12, pp. 21–29, 1999.

[39] N. S. Agency. (2010). *Defense in Depth: A Practical Strategy for Achieving Information Assurance in Today's Highly Networked Environments*. [Online]. Available: https://citadel-information.com/wp-content/uploads/2010/12/nsa-defense-in-depth.pdf

[40] A. Jalali and M. A. Hadavi, "Software security analysis based on the principle of Defense-in-Depth," in *Proc. 15th Int. ISC (Iranian Soc. Cryptol.) Conf. Inf. Secur. Cryptol. (ISCISC)*, Aug. 2018, pp. 1–6.

[41] B. Brecht and T. Hehn, "A security credential management system for V2X communications," in *Connected Vehicles*. Cham, Switzerland: Springer, 2019, pp. 83–115.

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

[43] J. Petit, "Automated vehicles cybersecurity: Summary AVS'17 and stakeholder analysis," in *Road Vehicle Automation 5*. Cham, Switzerland: Springer, 2019, pp. 171–181.

[44] J. Takahashi, "An overview of cyber security for connected vehicles," *IEICE Trans. Inf. Syst.*, vol. E101.D, no. 11, pp. 2561–2575, 2018.

[45] D. Tokody, A. Albini, L. Ady, Z. Raynai, and F. Pongrácz, "Safety and security through the design of autonomous intelligent vehicle systems and intelligent infrastructure in the smart city," *Interdiscipl. Description Complex Syst.*, vol. 16, no. 3, pp. 384–396, 2018.

[46] A. Chattopadhyay and K.-Y. Lam, "Autonomous vehicle: Security by design," 2018, *arXiv:1810.00545*. [Online]. Available: http://arxiv.org/abs/1810.00545

[47] D. Suo, J. E. Siegel, and S. E. Sarma, "Merging safety and cybersecurity analysis in product design," *IET Intell. Transp. Syst.*, vol. 12, no. 9, pp. 1103–1109, Nov. 2018.

[48] W. Young and N. G. Leveson, "An integrated approach to safety and security based on systems theory," *Commun. ACM*, vol. 57, no. 2, pp. 31–35, Feb. 2014.

[49] Microsoft. (2019). *Microsoft Security Development Lifecycle*. [Online]. Available: https://www.microsoft.com/en-us/securityengineering/sdl/

[50] N. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, MA, USA: MIT Press, 2011.

[51] K. Post and C. K. Davey, "Integrating sotif and agile systems engineering," SAE Tech. 2019-01-0141, 2019.

[52] D. Suo, S. Yako, M. Boesch, and K. Post, "Integrating stpa into iso 26262 process for requirement development," SAE Tech. Paper 2017-01-0058, 2017.

[53] F. M. Company. (2018). *A Matter of Trust: Ford's Approach to Developing Self-Driving Vehicles*. [Online]. Available: https://media.ford.com/content/dam/fordmedia/pdf/Ford-AV-LLC-FINAL-HR-2.pdf

[54] S. Samonas and D. Coss, "The cia strikes back: Redefining confidentiality, integrity and availability in security," *J. Inf. Syst. Secur.*, vol. 10, no. 3, pp. 21–45, 2014.

[55] D. T.-Z. Lu, C. K. Johnson, and R.-R. Hubert, "Unlock and authentication for autonomous vehicles," U.S. Patent 9 194 168, Nov. 24, 2015.

[56] Audi. (2016). *Audi Connect*. [Online]. Available: https://www.audiusa.com/technology/intelligence/audi-connect#

[57] OnStar. (2016). *Onstar Connected Services*. [Online]. Available: https://www.onstar.com/us/en/services/connected-services/

[58] D. Suo, J. Siegel, and A. Soley, "Driving data dissemination: The 'terms' governing connected car information (submitted)," *IEEE Intell. Transp. Syst. Mag.*, 2020, doi: 10.1109/MITS.2020.3037315.

[59] Q. Africa. (2017) *Uber Drivers in Lagos Are Using a Fake GPS APP to Inflate Rider Fares*. [Online]. Available: https://qz.com/africa/1127853/uber-drivers-in-lagos-nigeria-use-fake-lockito-app-to-boost-fares/

[60] Microsoft. (2009). *The Stride Threat Model*. [Online]. Available: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN

[61] J. Rasmussen, "Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models," *IEEE Trans. Syst., Man, Cybern.*, vol. SMC-13, no. 3, pp. 257–266, May 1983.

[62] McAfee. (2020). *Model Hacking ADAS to Pave Safer Roads for Autonomous Vehicles*. [Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/model-hacking-adas-to-pave-safer-roads-for-autonomous-vehicles/

[63] B. Nassi, D. Nassi, R. Ben-Netanel, Y. Mirsky, O. Drokin, and Y. Elovici, "Phantom of the ADAS: Phantom attacks on driver-assistance systems," IACR Cryptol. ePrint Arch., Tech. Rep., 2020, p. 85.

[64] K. Eykholt *et al.*, "Robust physical-world attacks on deep learning visual classification," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, Jun. 2018, pp. 1625–1634.

[65] Tencent. (2019). *Experimental Security Research of Tesla Autopilot*. [Online]. Available: https://keenlab.tencent.com/en/whitepapers/Experimental-Security-Research-of-Tesla-Autopilot.pdf

[66] Y. Cao *et al.*, "Adversarial sensor attack on LiDAR-based perception in autonomous driving," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2019, pp. 2267–2281.

[67] J. Steinhardt, P. W. W. Koh, and P. S. Liang, "Certified defenses for data poisoning attacks," in *Proc. Adv. Neural Inf. Process. Syst.*, 2017, pp. 3517–3529.

[68] B. Biggio, B. Nelson, and P. Laskov, "Poisoning attacks against support vector machines," 2012, *arXiv:1206.6389*. [Online]. Available: http://arxiv.org/abs/1206.6389

[69] F. Khalid, M. A. Hanif, S. Rehman, R. Ahmed, and M. Shafique, "TrISec: Training data-unaware imperceptible security attacks on deep neural networks," in *Proc. IEEE 25th Int. Symp. Line Test. Robust Syst. Design (IOLTS)*, Jul. 2019, pp. 188–193.

[70] F. Khalid, M. A. Hanif, S. Rehman, and M. Shafique, "Security for machine learning-based systems: Attacks and challenges during training and inference," in *Proc. Int. Conf. Frontiers Inf. Technol. (FIT)*, Dec. 2018, pp. 327–332.

[71] E. Newcomer. (2017). *Uber Paid Hackers to Delete Stolen Data on 57 Million People*. [Online]. Available: https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data

[72] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Self-driving and connected cars: Fooling sensors and tracking drivers," in *Proc. Black Hat Eur.*, 2015.

[73] H. Shin, D. Kim, Y. Kwon, and Y. Kim, "Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications," in *Proc. Int. Conf. Cryptograph. Hardw. Embedded Syst.* Cham, Switzerland: Springer, 2017, pp. 445–467.

[74] B. G. Stottelaar, "Practical cyber-attacks on autonomous vehicles," M.S. thesis, Dept. Elect. Eng., Math. Comput. Sci. Services, Cybersecur. Secur. Research Group, Univ. Twente, Enschede, The Netherlands, 2015.

[75] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and LiDAR," *Black Hat Eur.*, vol. 11, p. 2015, Nov. 2015.

[76] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *DEF CON*, vol. 24, p. 109, Aug. 2016.

[77] W. Xu, C. Yan, W. Jia, X. Ji, and J. Liu, "Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 5015–5029, Dec. 2018.

[78] M. Bertozzi, A. Broggi, and A. Fascioli, "Vision-based intelligent vehicles: State of the art and perspectives," *Robot. Auto. Syst.*, vol. 32, no. 1, pp. 1–16, Jul. 2000.

[79] R. K. Schmidt, T. Leinmüller, E. Schoch, A. Held, and G. Schäfer, "Vehicle behavior analysis to enhance security in vanets," in *Proc. 4th IEEE Vehicle Vehicle Commun. Workshop*, Jun. 2008, pp. 1–8.

[80] N. Bißmeyer, J. Njeukam, J. Petit, and K. M. Bayarou, "Central misbehavior evaluation for VANETs based on mobility data plausibility," in *Proc. 9th ACM Int. Workshop Veh. Inter-Netw., Syst., Appl. (VANET)*, 2012, pp. 73–82.

[81] N. Bißmeyer, "Misbehavior detection and attacker identification in vehicular ad-hoc networks," Ph.D. dissertation, Dept. Comput. Sci., Technische Univ. Darmstadt, Darmstadt, Germany, 2014.

[82] M. Obst, L. Hobert, and P. Reisdorf, "Multi-sensor data fusion for checking plausibility of V2V communications by vision-based multiple-object tracking," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2014, pp. 143–150.

[83] R. P. Barnwal and S. K. Ghosh, "Heartbeat message based misbehavior detection scheme for vehicular ad-hoc networks," in *Proc. Int. Conf. Connected Vehicles Expo (ICCVE)*, Dec. 2012, pp. 29–34.

[84] S. So, P. Sharma, and J. Petit, "Integrating plausibility checks and machine learning for misbehavior detection in VANET," in *Proc. 17th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2018, pp. 564–571.

[85] 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. Netw. Distrib. Syst. Secur. Symp.*, 2018, pp. 1–15.

[86] Ridester. (2017). *Fake GPS: Uber's Deactivation Rampage*. [Online]. Available: https://www.ridester.com/uber-fake-gps-deactivation/

[87] TMZ. (2014). *Pissed Off L.A. Homeowners WAZE is The Devil*. [Online]. Available: https://www.tmz.com/2014/11/14/waze-app-neighborhoods-pissed-la-traffic-driving-405/

[88] R. M. Ishtiaq Roufa *et al.*, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *Proc. 19th USENIX Secur. Symp.*, Washington, DC, USA, 2010, pp. 11–13.

[89] X. Feng, C.-Y. Li, D.-X. Chen, and J. Tang, "A method for defensing against multi-source Sybil attacks in VANET," *Peer Peer Netw. Appl.*, vol. 10, no. 2, pp. 305–314, Mar. 2017.

[90] J. Zacharias and S. Froschle, "Misbehavior detection system in VANETs using local traffic density," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2018, pp. 1–4.

[91] Y. Feng, S. Huang, Q. A. Chen, H. X. Liu, and Z. M. Mao, "Vulnerability of traffic control system under cyber-attacks using falsified data," in *Proc. 97th Annu. Meeting Transp. Res. Board*, 2018, pp. 1–11.

[92] B. Ghena, W. Beyer, A. Hillaker, J. Pevarnek, and J. A. Halderman, "Green lights forever: Analyzing the security of traffic infrastructure," in *Proc. 8th USENIX Workshop Offensive Technol. (WOOT)*, 2014, pp. 1–10.

[93] J. Liu, S. Zhang, W. Sun, and Y. Shi, "In-vehicle network attacks and countermeasures: Challenges and future directions," *IEEE Netw.*, vol. 31, no. 5, pp. 50–58, Sep. 2017.

[94] C. Miller, "Lessons learned from hacking a car," *IEEE Des. Test. Comput.*, vol. 36, no. 6, pp. 7–9, Dec. 2019.

[95] S. Iqbal, A. Haque, and M. Zulkernine, "Towards a security architecture for protecting connected vehicles from malware," in *Proc. IEEE 89th Veh. Technol. Conf. (VTC-Spring)*, Apr. 2019, pp. 1–5.

[96] Intel. (2018). *Developing Amazing Android Automotive in-Vehicle Infotainment Experiences*. [Online]. Available: https://www.intel.com/content/www/us/en/automotive/android-automotive-in-vehicle-infotainment-development-business-brief.html

[97] S. Woo, H. Jin Jo, and D. Hoon Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," *IEEE Trans. Intell. Transport. Syst.*, vol. 16, no. 2, pp. 993–1006, Apr. 2015.

[98] D. Khosrowshahi. (2016). *2016 Data Security Incident*. [Online]. Available: https://www.uber.com/newsroom/2016-data-incident/

[99] O. M. Group. (2017). *Unified Modeling Language*. [Online]. Available: https://www.omg.org/spec/UML/About-UML/

[100] O. M. Group. (2019). *Omg System Modeling Language*. [Online]. Available: https://www.omg.org/spec/SysML/

[101] Q. Wang *et al.*, "Pseudorandom modulation quantum secured lidar," *Optik*, vol. 126, no. 22, pp. 3344–3348, Nov. 2015.

[102] R. Matsumura, T. Sugawara, and K. Sakiyama, "A secure LiDAR with AES-based side-channel fingerprinting," in *Proc. 6th Int. Symp. Comput. Netw. Workshops (CANDARW)*, Nov. 2018, pp. 479–482.

[103] J. C. Chen, "Lidar resistant to interference and hacking," U.S. Patent App. 15 922 397, Sep. 19, 2019.

[104] Y. Yang, H. Chen, H. Chen, and Y. Shao, "Short-range detection system with polarized laser and polarization characteristics of typical targets," in *Proc. 2nd Int. Conf. Comput. Inf. Appl. (ICCIA)*, vol. 756, 2012, pp. 4640–4645.

[105] Y. Shoukry, S. Mishra, Z. Luo, and S. Diggavi, "Sybil attack resilient traffic networks: A physics-based trust propagation approach," in *Proc. ACM/IEEE 9th Int. Conf. Cyber-Phys. Syst. (ICCPS)*. Piscataway, NJ, USA: IEEE Press, Apr. 2018, pp. 43–54.

[106] Z. Huang, S. Ruj, M. A. Cavenaghi, M. Stojmenovic, and A. Nayak, "A social network approach to trust management in VANETs," *Peer Peer Netw. Appl.*, vol. 7, no. 3, pp. 229–242, Sep. 2014.

[107] N. Bismeyer, S. Mauthofer, K. M. Bayarou, and F. Kargl, "Assessment of node trustworthiness in VANETs using data plausibility checks with particle filters," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Nov. 2012, pp. 78–85.

[108] K. Lim and K. M. Tuladhar, "LIDAR: Lidar information based dynamic V2V authentication for roadside infrastructure-less vehicular networks," in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2019, pp. 1–6.

[109] O. Abumansoor and A. Boukerche, "A secure cooperative approach for Nonline-of-Sight location verification in VANET," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 275–285, Jan. 2012.

[110] A. C. Chapin, "Multifactor authentication for vehicle operation," U.S. Patent App. 16 199 101, Apr. 9, 2020.

[111] A. Ometov, V. Petrov, S. Bezzateev, S. Andreev, Y. Koucheryavy, and M. Gerla, "Challenges of multi-factor authentication for securing advanced IoT applications," *IEEE Netw.*, vol. 33, no. 2, pp. 82–88, Mar. 2019.

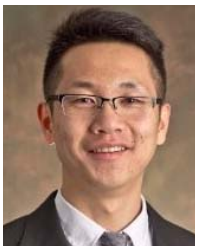
[112] T. E. Abuelsaad, V. C. Aslot, A. Bello, and G. J. Boss, "Adjusting multi-factor authentication using context and pre-registration of objects," U.S. Patent 10 057 289, Aug. 21, 2018.

[113] A. Singh and H. C. S. Fhom, "Restricted usage of anonymous credentials in vehicular ad hoc networks for misbehavior detection," *Int. J. Inf. Secur.*, vol. 16, no. 2, pp. 195–211, Apr. 2017.

[114] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Trans. Intell. Transport. Syst.*, vol. 13, no. 1, pp. 127–139, Mar. 2012.

[115] S. Biswas and J. Misic, "Location-based anonymous authentication for vehicular communications," in *Proc. IEEE 22nd Int. Symp. Pers., Indoor Mobile Radio Commun.*, Sep. 2011, pp. 1213–1217.

[116] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: Detecting sybil attacks in urban vehicular networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 6, pp. 1103–1114, Jun. 2012.
[117] W. Wong, S. Huang, Y. Feng, Q. A. Chen, Z. M. Mao, and H. X. Liu, "Trajectory-based hierarchical defense model to detect cyber-attacks on transportation infrastructure," Transp. Res. Board, Washington, DC, USA, Tech. Rep., 2019.
[118] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support," *Secur. Commun. Netw.*, vol. 6, no. 4, pp. 523–538, Apr. 2013.
[119] H. Liu, C.-W. Lin, E. Kang, S. Shiraishi, and D. M. Blough, "A byzantine-tolerant distributed consensus algorithm for connected vehicles using Proof-of-Eligibility," in *Proc. 22nd Int. ACM Conf. Modeling, Anal. Simulation Wireless Mobile Syst. (MSWIM)*, 2019, pp. 225–234.
[120] B. Yu, C.-Z. Xu, and B. Xiao, "Detecting sybil attacks in VANETs," *J. Parallel Distrib. Comput.*, vol. 73, no. 6, pp. 746–756, Jun. 2013.
[121] N. Malik, P. Nanda, X. He, and R. Liu, "Trust and reputation in vehicular networks: A smart contract-based approach," in *Proc. 18th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun., 13th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2019, pp. 34–41.
[122] Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, and C.-C. Liu, "Blockchain-based traffic event validation and trust verification for VANETs," *IEEE Access*, vol. 7, pp. 30868–30877, 2019.
[123] V. Ortega, F. Bouchmal, and J. F. Monserrat, "Trusted 5G vehicular networks: Blockchains and content-centric networking," *IEEE Veh. Technol. Mag.*, vol. 13, no. 2, pp. 121–127, Jun. 2018.
[124] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," in *Concurrency: The Works of Leslie Lamport*. New York, NY, USA: Association for Computing Machinery, 2019, pp. 203–226.
[125] A. Malhi and S. Batra, "Privacy-preserving authentication framework using Bloom filter for secure vehicular communications," *Int. J. Inf. Secur.*, vol. 15, no. 4, pp. 433–453, Aug. 2016.
[126] L. Wu, J. Fan, Y. Xie, J. Wang, and Q. Liu, "Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks," *Int. J. Distrib. Sensor Netw.*, vol. 13, no. 3, 2017, Art. no. 1550147717700899.
[127] A. Chachich *et al.*, "USDOT spectrum sharing analysis plan: Effects of unlicensed-national information infrastructure (U-NII) devices on dedicated short-range communications (DSRC)," U.S. Dept. Transp. Office Assistant Secretary Res. Technol., John A Volpe Nat. Transp. Syst. Center, Cambridge, MA, USA, Tech. Rep., 2017.
[128] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proc. ACM Workshop Wireless Secur. (WiSe)*, 2003, pp. 1–10.
[129] J. Kamel, I. Ben Jemaa, A. Kaiser, and P. Urien, "Misbehavior reporting protocol for C-ITS," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2018, pp. 1–4.
[130] N. J. Patel and R. H. Jhaveri, "Trust based approaches for secure routing in VANET: A survey," *Procedia Comput. Sci.*, vol. 45, pp. 592–601, Jan. 2015.
[131] A. Alnasser, H. Sun, and J. Jiang, "Recommendation-based trust model for vehicle-to-everything (V2X)," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 440–450, Jan. 2020.
[132] J. R. Douceur, "The sybil attack," in *Proc. Int. Workshop Peer Peer Syst.* Cham, Switzerland: Springer, 2002, pp. 251–260.
[133] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAP—Sybil attacks detection in vehicular ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 582–594, Feb. 2011.
[134] F. Boeira, M. P. Barcellos, E. P. de Freitas, A. Vinel, and M. Asplund, "Effects of colluding sybil nodes in message falsification attacks for vehicular platooning," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Nov. 2017, pp. 53–60.
[135] D. Chaum and E. Van Heyst, "Group signatures," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Cham, Switzerland: Springer, 1991, pp. 257–265.
[136] I. Khan, G. M. Hoang, and J. Harri, "Rethinking cooperative awareness for future V2X safety-critical applications," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Nov. 2017, pp. 73–76.
[137] D. Suo and S. E. Sarma, "Real-time trust-building schemes for mitigating malicious behaviors in connected and automated vehicles," in *Proc. IEEE Intell. Transp. Syst. Conf. (ITSC)*, Oct. 2019, pp. 1142–1149.
[138] H. Zhao, D. Sun, H. Yue, M. Zhao, and S. Cheng, "Dynamic trust model for vehicular cyber-physical systems," *IJ Netw. Secur.*, vol. 20, no. 1, pp. 157–167, 2018.
[139] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transport. Syst.*, vol. 17, no. 4, pp. 960–969, Apr. 2016.
[140] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, May 2018.
[141] M. Baza, M. Nabil, N. Bewermeier, K. Fidan, M. Mahmoud, and M. Abdallah, "Detecting sybil attacks using proofs of work and location in VANETs," 2019, *arXiv:1904.05845*. [Online]. Available: http://arxiv.org/abs/1904.05845
[142] B. Liu, J. T. Chiang, and Y.-C. Hu, "Limits on revocation in VANETs," in *Proc. 8th Int. Conf. Appl. Cryptogr. Netw. Secur.*, 2010, pp. 38–52.
[143] J. Kamel, A. Kaiser, I. Ben Jemaa, P. Cincilla, and P. Urien, "Feasibility study of misbehavior detection mechanisms in cooperative intelligent transport systems (C-ITS)," in *Proc. IEEE 87th Veh. Technol. Conf. (VTC Spring)*, Jun. 2018, pp. 1–5.
[144] J. Barrachina *et al.*, "Road side unit deployment: A density-based approach," *IEEE Intell. Transport. Syst. Mag.*, vol. 5, no. 3, pp. 30–39, Fall 2013.
[145] S. Mehar, S. M. Senouci, A. Kies, and M. M. Zoulikha, "An optimized roadside units (RSU) placement for delay-sensitive applications in vehicular networks," in *Proc. 12th Annu. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2015, pp. 121–127.
[146] C. Chen, S. W. Lee, T. Watson, C. Maple, and Y. Lu, "CAE-SAR: A criticality-aware ECDSA signature verification scheme with Markov model," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Nov. 2017, pp. 151–154.



Dajiang Suo received the B.S. degree in mechatronics engineering and the S.M. degree in computer science and engineering systems. He received the Ph.D. degree in mechanical engineering from MIT in 2020.

He is currently a Post-Doctoral Associate with the Auto-ID Laboratory, MIT. His research interests include the trustworthiness and privacy preservation of multimodal vehicle data. He also worked on polarization-based sensing technologies for object recognition in autonomous vehicles. Before his Ph.D. degree, he was with the Vehicle Control and Autonomous Driving Team with Ford Motor Company, Dearborn, MI, USA, working on the safety and cyber-security of automated vehicles. He also serves on the Standing Committee on Enterprise, Systems, and Cyber Resilience (AMR40) for the Transportation Research Board.

John Moore received the B.G.S. degree from the University of Michigan–Ann Arbor, in 1999, and the master's degree in computer and information science (CIS) from the University of Michigan-Dearborn, in 2003. He currently works with Ford Motor Company as a Vehicle Cyber Security Technical Specialist within the Advanced Engineering and Research Architecture and Software Team. He holds a CISSP. His current research interests include advance computation, sensing, and AI security within a vehicle ecosystem.

Mathew Boesch was born in Columbus, OH, USA. He received the B.S. degree in electrical engineering and the M.S. degrees in control systems from The Ohio State University, in 1988 and 1990, respectively.

He joined Halmar Electronics, Columbus, OH, USA, in 1986, and IBM, Research Triangle Park, NC, USA, in 1988. In 1990, he joined Ford Motor Company, Dearborn, MI, USA. He is currently a Technical Expert with Ford Autonomous Vehicles, LLC, Dearborn, MI, USA. He has authored or coauthored more than 15 technical publications and holds more than 50 U.S. and international patents. His current areas of research interests include data fusion for real-time diagnostics and prognostics, connected and autonomous vehicle communication and control, high-integrity critical systems, and functional safety.

Kyle Post received the B.S. degree in mechanical engineering from Arizona State University, Tempe, AZ, USA, in 2000, and the M.S. degree in product development from the University of Detroit Mercy, Detroit, MI, USA, in 2009.

He currently resides in Dearborn, MI, USA. He is also the Systems Safety Technical Leader of Ford Motor Company, Dearborn, MI, USA. He has more than 18 years of real-time controls and embedded software experience. He is also leading the implementation of Ford's ISO 26262-based Functional Safety Process along with leading research for the Safety of the Intended Functionality for Automated Vehicles. He has led development for projects at all stages of the product lifecycle. Prior to working at Ford, he worked in the area of controls for a number of different industries including aerospace, bio-medical, and building controls.

Sanjay E. Sarma (Member, IEEE) received the bachelor's degree from the Indian Institute of Technology, the master's degree from Carnegie Mellon University, and the Ph.D. degree from the University of California at Berkeley.

He was the Fred Fort Flowers in 1941, and the Daniel Fort Flowers in 1941, and a Professor of Mechanical Engineering with MIT. He was also the founder and the CTO of OATSystems, which was acquired by Checkpoint Systems (NYSE: CKP) in 2008. He is currently the Vide President Open Learning with MIT. He co-founded the Auto-ID Center, MIT, and developed many of the key technologies behind the EPC suite of RFID standards now used worldwide. He serves on the boards of GS1, EPCglobal, and several startup companies, including Top Flight Technologies, Hochschild Mining (HOC:LSE), and edX. He also worked with Schlumberger Oilfield Services, Aberdeen, U.K., and with the OATSystems. He has authored more than 150 academic articles in computational geometry, sensing, RFID, automation, and CAD. He was a recipient of numerous awards for teaching and research, including the MacVicar Fellowship, the Business Week eBiz Award, and the Informationweek's Innovators and Influencers Award. He advises several national governments and global companies.