IEEE ComSoc IEEE Open Journal of the Communications Society

Received XX Month, XXXX; revised XX Month, XXXX; accepted XX Month, XXXX; Date of publication XX Month, XXXX; date of current version XX Month, XXXX.

Digital Object Identifier 10.1109/OJCOMS.2022.1234567

A Comprehensive Survey of V2X Cybersecurity Mechanisms and Future Research Paths

Roshan Sedar[1,2], Charalampos Kalalas[1], Francisco Vázquez-Gallego[3], Luis Alonso[2], and Jesus Alonso-Zarate[3]

[1]Centre Tecnològic de Telecomunicacions de Catalunya (CTTC/CERCA), Barcelona, Spain
[2]Universitat Politècnica de Catalunya, Barcelona, Spain
[3]i2CAT Foundation, Barcelona, Spain

CORRESPONDING AUTHOR: Roshan Sedar (e-mail: roshan.sedar@ cttc.es).

This work is supported by the H2020-INSPIRE-5Gplus project (under Grant agreement No. 871808), the "Ministerio de Asuntos Económicos y Transformación Digital" and the European Union-NextGenerationEU in the frameworks of the "Plan de Recuperación, Transformación y Resiliencia" and of the "Mecanismo de Recuperación y Resiliencia" under references TSI-063000-2021-39/40/41, and the CHIST-ERA-17-BDSI-003 FIREMAN project funded by the Spanish National Foundation (Grant PCI2019-103780).

ABSTRACT Recent advancements in vehicle-to-everything (V2X) communication have notably improved existing transport systems by enabling increased connectivity and driving autonomy levels. The remarkable benefits of V2X connectivity come inadvertently with challenges which involve security vulnerabilities and breaches. Addressing security concerns is essential for seamless and safe operation of mission-critical V2X use cases. This paper surveys current literature on V2X security and provides a systematic and comprehensive review of the most relevant security enhancements to date. An in-depth classification of V2X attacks is first performed according to key security and privacy requirements. Our methodology resumes with a taxonomy of security mechanisms based on their proactive/reactive defensive approach, which helps identify strengths and limitations of state-of-the-art countermeasures for V2X attacks. In addition, this paper delves into the potential of emerging security approaches leveraging artificial intelligence tools to meet security objectives. Promising data-driven solutions tailored to tackle security, privacy and trust issues are thoroughly discussed along with new threat vectors introduced inevitably by these enablers. The lessons learned from the detailed review of existing works are also compiled and highlighted. We conclude this survey with a structured synthesis of open challenges and future research directions to foster contributions in this prominent field.

INDEX TERMS Artificial intelligence, Attack classification, Cybersecurity solutions, Machine learning, Misbehavior detection, Privacy preservation, Proactive/reactive security, Security threats, Trust management, V2X communication

I. INTRODUCTION

MODERN vehicles are progressively transforming into sophisticated computing units able to gather, process, and exchange information with each other and with relevant entities. The deployment of ultra-high-definition cameras, radars, LiDARs, ultrasonic range finders and positioning sensors allow vehicles to become increasingly aware of their local surroundings. In addition, vehicles are gradually equipped with an on-board unit (OBU), which includes a vehicle-to-everything (V2X) communication stack and allows on-board sensor data interactions with neighboring vehicles, roadside units (RSUs) and cloud applications, over wireless connectivity [1], [2]. V2X involves various connectivity modes, e.g., vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrians (V2P) and vehicle-to-network (V2N) communication.

In principle, the exchange of information facilitated by V2X connectivity allows extending the perception range of a vehicle beyond the limits of its on-board sensors and enables the realization of connected and automated mobility (CAM) services. Such services aim at improving traffic efficiency and road safety for intelligent transport

systems (ITS). However, despite the multitude of benefits offered by V2X communication, vulnerabilities and security breaches are not uncommon in vehicular networks [3]. The peculiar characteristics of V2X systems, in conjunction with the increased levels of connectivity and driving autonomy, introduce entirely new security concerns and issues that have not been addressed in a similar context before. As a result, evolving security requirements are expected to be more stringent as services and applications for the automotive sector will be often mission-critical [4]. Emerging CAM use cases, such as cooperative collision avoidance, advanced vehicle platooning and dynamic map sharing, exhibit idiosyncrasies in terms of functionalities and deployment scenarios, with several security threats lurking.

This complex V2X connectivity landscape renders the attack surface sufficiently large with expanded threat vectors, which an adversary may maliciously exploit to intrude into the system. For example, a vehicle platoon disruption attack can be realized by simply replaying certain critical information in a short time-period, without any need for message alteration [5]. While V2X accommodates multiple relevant entities in a multi-domain cooperative ITS environment, there exist various security threats which may destabilize system operation and degrade network performance [6]–[10]. As safety and security are tightly coupled in V2X, security attacks may compromise the safety of road users and lead to serious accidents. Novel security and privacy-aware mechanisms are thus essential to address vulnerabilities in safety-critical vehicular scenarios and reduce the extent of their detrimental effects.

A. Scope and Target Audience

The flourishing field of vehicular communication currently calls for an increasing attention to the prominent area of V2X cybersecurity research. Therefore, this paper is motivated by the anticipated growing importance of cybersecurity in V2X technology and the ever-evolving threat landscape in the emerging Internet-of-Vehicles (IoV) paradigm. Recent advancements in V2X communication and the introduction of unprecedented vehicular use cases need a continuous threat assessment and call for a diverse set of novel security solutions to address vulnerabilities. In recent years, a plethora of research contributions have attempted to cope with the new V2X security demands and deliver actionable results for a safer and smarter V2X ecosystem. However, addressing V2X security concerns is still far from being completely resolved. The ubiquitous vehicular connectivity in conjunction with the increased levels of driving autonomy give rise to finely targeted, stealthier, and scalable attacks which exploit the inherent vulnerabilities of IoV systems. In addition, the progressive penetration of artificial intelligence and machine learning (AI/ML) tools in various aspects of V2X communication may also detrimentally affect the operation of vehicular systems. In this context, the primary goal of this paper is to familiarize the reader with key V2X security aspects, offering a systematic and comprehensive review of existing works to date in the field. The identification of strengths and weaknesses of proposed mechanisms helps determine their feasibility in preserving fundamental V2X security and privacy requirements against various attacks.

The contents of this paper can be useful to a variety of relevant target groups. Researchers may use the conducted literature review as a basis for gap analysis and a source for innovative enablers tailored to the foreseen V2X security evolution. Industry experts working in the telecommunication sector, such as mobile network operators, vendors and service providers, may capitalize on the performed threat analysis to carry out detailed risk assessments and V2X infrastructure protection plans, in accordance to their needs. V2X stakeholders not directly involved in the design and development of communication technologies (e.g., road authorities, municipalities or policy-makers) may gain meaningful insights on emerging V2X threats and respective mitigation practices and measures to trigger potential policy actions. Finally, the assessed vulnerabilities and granular review of V2X security countermeasures may be a valuable resource for relevant standardization bodies to verify the completeness of already performed assessments.

B. Existing Surveys

Table 1 highlights the principal aspects covered in this paper compared to several recent surveys dealing with security in vehicular communication. We particularly pinpoint key limitations of existing works, in an effort to motivate the need for a comprehensive survey in the area of vehicular communication security. Additionally, we highlight the type of vehicular network (i.e., scope in Table 1) considered in each survey. The differentiating aspects of our methodology are summarized in Table 2, where the coverage of relevant security topics is compared to existing surveys. It is worth noting that a holistic and in-depth discussion of proactive, reactive, and AI/ML-based defense mechanisms in V2X cybersecurity is still missing [8], [12], [14], [15].

In this work, motivated by the identified shortcomings of existing surveys, we have followed a systematic approach to determine the relevance of a taxonomy for proactive, reactive, and AI/ML-based defense mechanisms in V2X cybersecurity. Towards this end, we performed a thorough search in the Scopus database to identify relevant research works published in the course of recent years. In particular, keywords-based search queries were carried out to fetch pertinent publications dealing with proactive, reactive, and AI/ML-based defense approaches in vehicular communications security. The Scopus search results in terms of number of research publications over the recent years are depicted in Figure 1.

It can be observed that there is a notable escalation in the number of published works every year for proactive (Figure 1a) and reactive (Figure 1b) defense mechanisms. Similarly, there is a remarkable proliferation of recently pub-

TABLE 1: Comparison of existing surveys on V2X cybersecurity.

Year	Paper	Scope	Key contributions	Limitations
2014	[10]	VANET	Classification of attacks for VANET. Common cryptographic tools for VANET security.	An early study focusing on traditional VANET communication. A categorization of countermeasures is not included. Lacks approaches for attacks against safety-critical applications.
2014	[6]	VANET	Attacks description for VANET. Security and privacy issues for VANET applications.	An early study focusing on traditional VANET security. A categorization of countermeasures is not included. Lacks approaches for attacks against safety-critical applications.
2017	[11]	VANET	A taxonomy of VANET authentication schemes. Cryptography-based authentication schemes.	Study is limited to authentication issues and corresponding countermeasures.
2017	[9]	VANET	Attacks classification. Countermeasures against attacks based on cryptographic techniques.	A categorization of countermeasures based on analyzed cryptographic techniques is not included. Lacks approaches for attacks against safety-critical applications.
2018	[3]	V2X	Attacks description. Security issues and requirements in C-V2X.	The study is limited to authentication issues in LTE-V2X systems.
2019	[12]	V2X	Threat analysis of IEEE 802.11p and LTE-V2X communication technologies. Countermeasures categorization based on cryptography, behavioral and identity-based techniques.	Lacks discussion on other cryptographic techniques, such as symmetric and asymmetric based solutions. Discusses primarily V2V security issues and countermeasures. Lacks approaches for attacks against safety-critical applications.
2020	[8]	V2X	Attacks classification. Security solutions classification based on symmetric cryptography, privacy preservation and message authentication.	Solution analysis is limited to symmetric cryptography. Lacks discussion on other techniques such as asymmetric and identity-based cryptography. Lacks approaches for attacks against safety-critical applications.
2020	[13]	VANET	In-vehicle network attacks classification and potential countermeasures. Discussion on threats and solutions for VANET security.	The focus is largely on in-vehicle security issues and countermeasures. A categorization of countermeasures for the listed attacks at V2V and V2I level is not presented. Lacks approaches for attacks against safety-critical applications.
2020	[14]	V2X	Standardization efforts for V2X security. Countermeasures against DoS, Sybil and false data attacks categories. A taxonomy of misbehavior detection techniques is presented.	Discussion of security aspects is limited to LTE-V2X technology. No categorization for discussed countermeasures. Attacks classification is limited to a small set. Lacks approaches for attacks against safety-critical applications.
2020	[15]	V2X	Discussion on security and privacy issues in V2X. Attacks classification. Countermeasures categorization based on cryptography and trust-based techniques. Review of C-V2X security architectures, i.e., LTE-V2X and 5G V2X.	Lacks security aspects for IEEE 802.11p technology. Lacks discussion on other cryptographic techniques such as asymmetric and symmetric. Lacks approaches for attacks against safety-critical applications.
2020	[16]	VANET	Cryptography-based authentication and privacy-preserving methods.	No attacks classification. The study is limited to authentication and privacy issues.
2021	[17]	Vehicular networks	Classification of ML-based techniques for security in vehicular networks. Attacks classification.	The study is limited to ML-based techniques.
2022	[18]	C-ITS	Security issues and recent advancements on vehicular public-key infrastructure.	The study is limited to security and privacy aspects of public-key infrastructure.
2022	[19]	IoV	Security and privacy aspects in beyond 5G and 6G for IoV.	The main focus is on beyond 5G and 6G technological enablers for IoV.

lished papers, pertaining to AI/ML techniques (Figure 1c) for vehicular communications security. The outcome of this systematic analysis reinforces the importance of a comprehensive and timely review of the literature on proactive, reactive, and AI/ML-based security schemes in V2X.

Several prior surveys ([3], [6], [8]–[10], and [12]–[19]) have reviewed security and privacy issues concerning vehicular communication. In particular, the authors in [12] review the security capabilities of IEEE 802.11p and LTE technologies for V2X, including an overview of potential threats and a coarse-grained classification of solutions into cryptography-based, behavior-based and identity-based. The survey in [8] performs a comparative study of V2X attacks, classifying them into commonly known categories, such as hardware/software, behavioral, infrastructure, privacy and trust-based. Security approaches are also grouped in three categories, i.e., cryptography-based, privacy-preserving and message authentication. A similar categorization is proposed in [15], where the authors review security and privacy issues and discuss standard cellular V2X (i.e., LTE-V2X and 5G V2X) security architectures. In contrast, our fine-grained classification relies on a detailed taxonomy of existing mechanisms based on their proactive/reactive defensive approach. In addition, we incorporate in our review a broader set of security solutions, including physical layer defense techniques, misbehavior detection methodologies, and mechanisms empowered by emerging paradigms (AI/ML), which are recently gaining momentum by the research community.

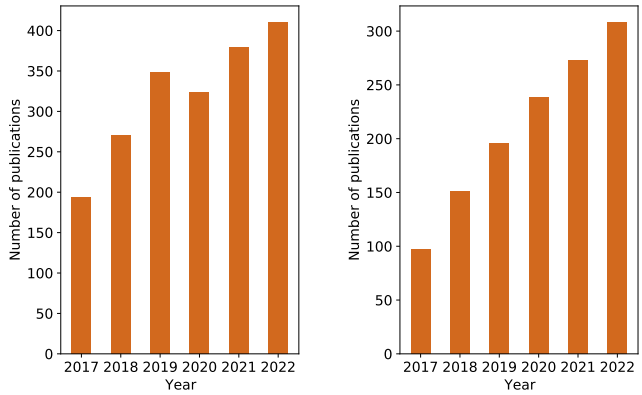
In [13], the authors discuss in detail intra-vehicular security, focusing mainly on the automotive bus system and in-vehicle network threats. A classification of attacks based on inter-vehicle V2V and V2I communications is also proposed, and pointers for the applicability of ML techniques are provided. The authors of [17] discuss vehicular network security

TABLE 2: Comparative overview with existing survey papers in terms of security topics covered and respective enhancements.

Paper	Key V2X enabling technologies						Security issues	Attacks classification with practicability and operational principles	Countermeasures							Defense mechanisms taxonomy	Emerging security with AI/ML
	IEEE 802.11p	LTE V2X	5G V2X	Mobile edge computing	Network slicing	Blockchain			Asymmetric cryptography (PKI)	Symmetric cryptography	Identity-based cryptography	Attribute-based encryption	Physical layer security	Privacy preservation	Misbehavior detection		
[3]	✓✗	✓✓	✓✗	×	×	×	✔	×	×	×	×	×	×	×	×	×	×
[6]	×	×	×	×	×	×	✔	×	×	×	×	×	×	✔	×	×	×
[8]	✓✗	✓✗	✓✗	×	×	×	✔	×	×	✔	×	×	×	✔	×	×	×
[9]	×	×	×	×	×	×	✔	×	×	×	×	×	×	×	×	×	×
[10]	✓✗	×	×	×	×	×	✔	×	×	×	×	×	×	×	×	×	×
[11]	✓✗	×	×	×	×	×	✔	×	✔	✔	✔	×	×	×	×	×	×
[12]	✓✓	✓✓	×	×	×	×	✔	×	×	×	✔	×	×	×	×	×	×
[13]	✓✗	✓✗	×	×	×	×	✔	×	×	×	×	×	×	×	×	×	×
[14]	✓✗	✓✗	×	×	×	×	✔	×	×	×	×	×	×	×	✔	×	×
[15]	✓✗	✓✓	✓✓	×	×	×	✔	×	×	×	✔	×	×	✔	×	×	×
[16]	×	×	×	×	×	×	✔	×	×	×	×	×	×	×	×	×	×
[17]	×	×	×	×	×	×	✔	×	×	×	×	×	×	✔	✔	×	✔
[18]	×	×	×	×	×	×	✔	×	×	×	×	×	×	×	×	×	×
[19]	×	×	✓✗	✓✓	✓✓	✓✓	✔	×	×	×	×	×	✔	✔	×	×	×
Our paper	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Related sections in our paper	Sec. II-B1	Sec. II-B2	Sec. II-B2	Sec. II-C	Sec. II-C	Sec. II-C	Sec. II-B, II-C, III, IV, V, VI	Sec. III	Sec. IV-A	Sec. IV-A	Sec. IV-A	Sec. IV-A	Sec. IV-B	Sec. IV-C	Sec. V-B	Sec. IV, V, VI	Sec. VI

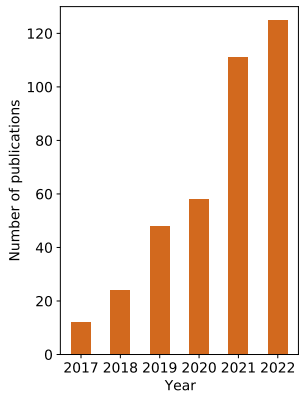
✔ Covers the topic × Does not cover the topic ✓✓ Covers the topic including operational principles and security aspects
✓✗ Covers the topic without security aspects

only from the perspective of ML-based approaches. Another survey in [18] focuses solely on security and privacy aspects of public-key infrastructure regarding vehicular communication. The authors of [19] present an overview of security and privacy aspects of beyond-5G and 6G technologies for IoV. Their focus is generally on the role of new technological developments towards 5G and beyond technologies for IoV. A complementary state-of-the-art review on security aspects of V2X communication platforms is presented in [14], with a particular focus on standardization activities for V2X security. The authors are essentially oriented in discussing three major attack types, i.e., denial-of-service (DoS), Sybil and false data injection, and review existing solutions against those attacks. On the contrary, we provide a classification of various types of attacks while describing the *practical feasibility* and deployment mechanics for each attack type. We further extend the considered V2X attack surface to cover the entire cybersecurity spectrum, while our conducted review primarily aims to determine the *extent* to which existing mechanisms comply with key security and privacy



(a) Proactive

(b) Reactive



(c) AI/ML

FIGURE 1: Number of publications per year for (a) proactive, (b) reactive, and (c) AI/ML defense mechanisms pertaining to vehicular communications security [Scopus data, Access month: December 2022].

requirements. In this context, we highlight the important role of AI/ML in enabling self-managing security functionalities, empowering key privacy functions and delivering trust enhancements. An elaborate discussion on the applicability of data-driven techniques against sophisticated attacks in emerging V2X applications is provided, without overlooking the introduced risks pertaining to the malevolent use of AI.

C. Contributions and Organization

In short, the contributions of this survey paper can be summarized as follows:

- We describe fundamental principles and building blocks of V2X communication, including enabling technologies, emerging V2X applications and associated challenges which introduce stringent security/privacy requirements.
- We present an in-depth classification of V2X attack variants, including the practical feasibility and severity of each attack type, which may hinder the secure and safe operation of V2X systems.
- We perform an exhaustive and systematic review of existing V2X security mechanisms that can be found in the literature to date. We rely on a taxonomy of state-of-the-art approaches according to their proactive/reactive defensive attitude, which helps identify the limitations of relevant classes of countermeasures for V2X attacks.
- We shed light on advanced capabilities offered by AI for V2X security, and we compile existing AI/ML-based solutions aimed to address identified security gaps and privacy/trust limitations.
- We provide guidelines and promising lines of research in the field of V2X security, in an effort to advance security vision and steer future research contributions towards novel enablers for secure V2X systems.

Figure 2 illustrates the organization of this survey. Section II provides an overview of V2X communication fundamentals, including core entities with their roles, enabling technologies and emerging applications, as well as associated security and privacy requirements. In Section III, the complex V2X threat landscape is unveiled with a classification of attacks which violate security and privacy in V2X systems. Proactive V2X security mechanisms are reviewed in-depth in Section IV, by classifying existing solutions into cryptography-based, physical-layer-based and privacy-preserving methods. Section V elaborates reactive V2X security mechanisms, focusing on entity-centric and data-centric approaches. Promising AI/ML techniques tailored to address limitations of existing V2X security/privacy solutions are thoroughly discussed in Section VI. Section VII outlines key open challenges and identifies future research directions, aiming to foster contributions in the area of V2X security. Finally, our concluding remarks are presented in Section VIII. The acronyms included in this survey are summarized in Table 3.

II. V2X Communication: An Overview

In this section, we present an overview of the core entities in a V2X ecosystem with their associated roles (Section II-A), and two promising and future-proof communication technologies for V2X (Section II-B). Key enabling technologies pertaining to the evolution of vehicular systems are discussed in Section II-C. In addition, we list challenges naturally posed by emerging V2X applications with stringent quality-of-service (QoS) constraints in Section II-D. Finally, we elaborate on fundamental V2X security and privacy requirements that should be in place to thwart potential cyber threats and attacks (Section II-E).

A. V2X Ecosystem

The integration of advanced wireless communication technologies into vehicles paves the way for V2X communication, enabling real-time connectivity and information sharing among vehicles (V2V) and between vehicles and other connected entities, e.g., communication networks (V2N) or RSUs (V2I). Ubiquitous V2X connectivity is contributing to the realization of IoV paradigm, a concept which has recently emerged from the Internet of Things (IoT) [20].

TABLE 3: List of acronyms and their definitions.

Acronym	Definition
3GPP	3rd Generation Partnership Project
5G	Fifth Generation
ABE	Attribute-based Encryption
AI	Artificial Intelligence
ARPF	Authentication credential Repository and Processing Function
AUSF	Authentication Server Function
AV	Autonomous Vehicle
BSM	Basic Safety Message
CA	Certificate Authority
CAM	Cooperative Awareness Message
CCAM	Cooperative, Connected and Automated Mobility
C-ITS	Cooperative Intelligent Transport Systems
CRL	Certificate Revocation List
C-V2X	Cellular Vehicle-to-Everything
DSRC	Dedicated Short-Range Communication
DL	Deep Learning
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
DENM	Decentralized Environmental Notification Message
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ETSI	European Telecommunications Standards Institute
FL	Federated Learning
HSM	Hardware Security Module
IBC	Identity-Based Cryptography
IoV	Internet-of-Vehicles
ITS	Intelligent Transport Systems
LBS	Location-based Services
LTE	Long Term Evolution
MEC	Mobile Edge Computing
ML	Machine Learning
MitM	Man-in-the-Middle
NFV	Network Functions Virtualization
OBU	On-board Unit
PKI	Public Key Infrastructure
PLS	Physical Layer Security
QoS	Quality-of-Service
RAN	Radio Access Network
RSSI	Received-Signal-Strength Indicator
RL	Reinforcement Learning
RSU	Roadside Unit
SAE	Society of Automotive Engineers
SCMS	Security Credential Management System
SDN	Software-Defined Networking
SDR	Software-Defined Radio
SEAF	Security Anchor Function
TA	Trusted Authority
UAV	Unmanned Aerial Vehicle
UDM	Unified Data Management
UE	User Equipment
V2I	Vehicle-to-Infrastructure
V2N	Vehicle-to-Network
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VCF	Vehicle-to-Everything Control Function
VNF	Virtual Network Function
VANET	Vehicular *ad hoc* Networks
VRU	Vulnerable Road User
WAVE	Wireless Access in Vehicular Environments

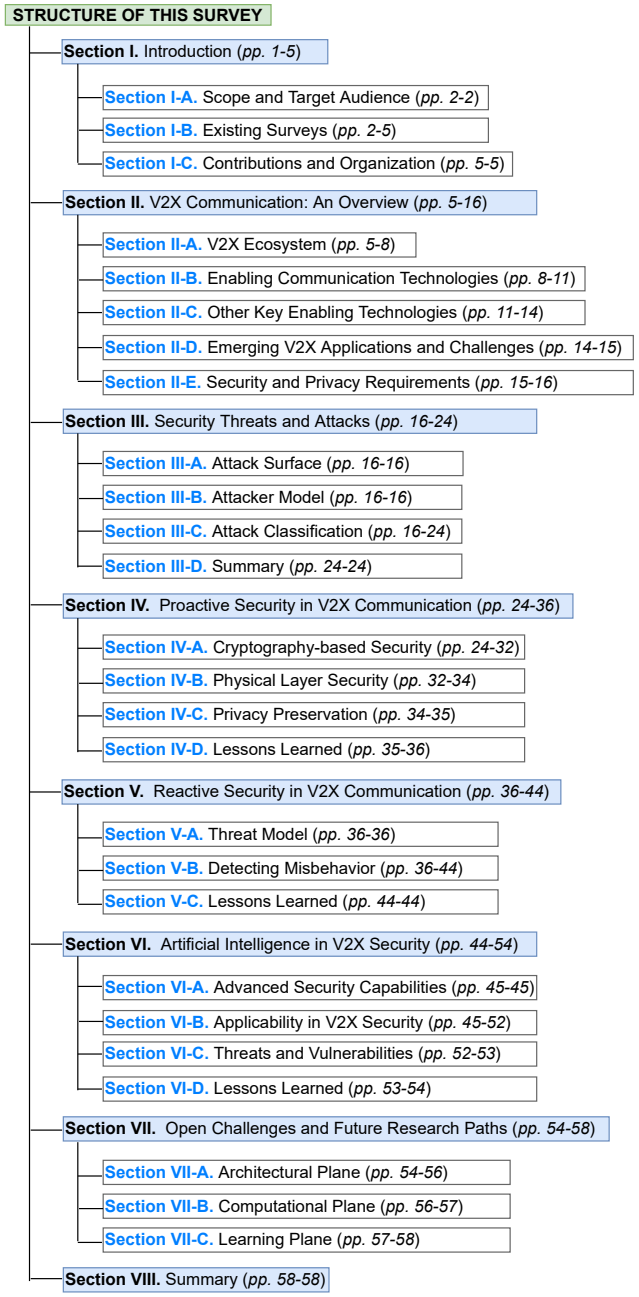


FIGURE 2: Organization of the survey.

IoV has recently evolved from the conventional vehicular *ad hoc* networks (VANETs) towards a new direction of intelligence and networking. The conventional VANETs have been seen as an ITS subsystem, mainly with V2V and V2I connectivity modes using IEEE 802.11p- and cellular-based technologies [21]. Internet access is usually not fully available within VANETs while limiting its support mainly to safety and traffic efficiency applications. This new IoV paradigm consists of intelligent vehicles with on-board sensing, computing and storage platforms, being able to interact

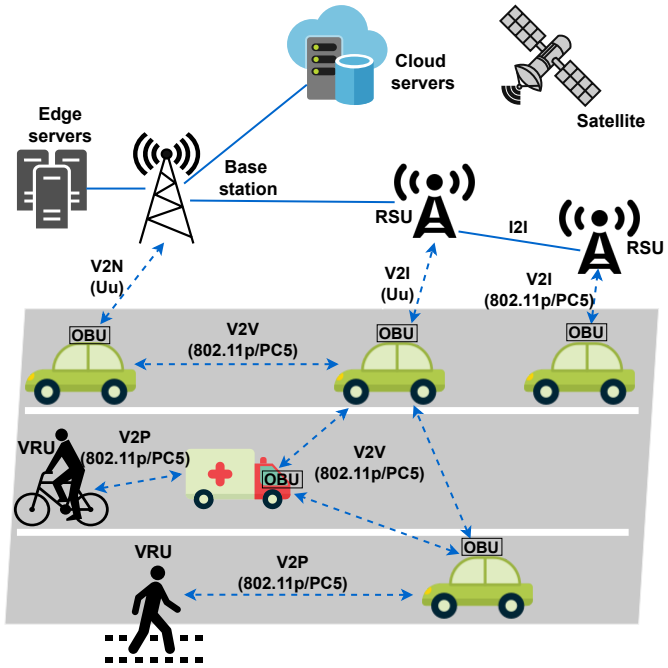


FIGURE 3: V2X connectivity modes composing Internet-of-Vehicle (IoV) paradigm.

with any entity via multiple V2X connectivity modes [22]. In principle, IoV constitutes an integrated network of three domains, i.e., intelligent devices, communication network and service platform, for the support of ITS applications and Internet services of diverse QoS requirements, via radio technologies, e.g., ETSI ITS-G5, Dedicated Short-Range Communication (DSRC), 4G/LTE and 5G [2], [23]. As shown in Figure 3, IoV comprises vehicles and surrounding entities in which inter-vehicle, vehicle-infrastructure and infrastructure-to-infrastructure communications occur. The following entities can be identified across the three IoV domains:

- **OBU** is the integral part of ITS. An OBU of a modern vehicle is equipped with computational power for processing collected data, and it is capable of interacting with other vehicles' OBUs and RSUs. Each OBU includes a networking protocol stack for V2X communication that enables to effectively exchange information with neighboring vehicles and infrastructure located in their vicinity. OBUs use 802.11p/PC5 (described in Section II-B) interfaces for direct communication in V2V, V2I, and V2P connectivity modes. The Uu interface is used for network-based communication in V2N connectivity mode. In V2N, OBUs can communicate with any connected entity (e.g., traffic management systems, map servers) over the network, while in V2I, OBUs communicate directly with road infrastructure (e.g., RSUs). Moreover, an OBU is equipped with a hardware security module (HSM) to safeguard and manage cryptographic keys. An HSM is a physical computing device that can facilitate security operations such as authentication, authorization, data confidentiality, and data integrity.
- **RSUs** constitute part of the transport infrastructure. They are typically stationary and are deployed at the roadside as well as at specific locations such as parking areas or intersections [21]. RSUs are mainly acting as gateways between OBUs and the communication infrastructure whilst extending the short-range communication capabilities (e.g., ETSI ITS-G5, DSRC). Additionally, RSUs contribute in V2X ecosystem by offering various services, such as Internet access, security keys distribution and real-time traffic data distribution. To extend such services, RSUs are deployed in IoV while being interconnected with each other and with the Internet. The direct communication between RSUs is often referred to as infrastructure-to-infrastructure (I2I) communication. Moreover, in LTE- or 5G-V2X systems, an RSU can be implemented either as a stationary UE or as part of a cellular base station (eNodeB/gNodeB) [24]. OBUs and the RSU exchange messages via the PC5 sidelink interface in the former case, and via the Uu interface in the latter case.
- **Roadside users** are typically pedestrians, cyclists and motorcyclists. These users are considered vulnerable road users (VRU), as they are at high risk of injury in the event of vehicular collision. VRU can participate via V2P communication using intelligent personnel devices (e.g., mobile terminal systems, apps). In VRU safety situations, a vehicle can transmit its position and kinematic parameters to VRUs over the PC5 interface to avoid accidents.
- **Base station** constitutes part of the cellular infrastructure and facilitates V2N connectivity for V2X terminals. V2X terminals transmit service data using their cellular interface (Uu) to the base station (eNodeB/gNodeB) on the uplink. The base station then broadcasts received data from several V2X terminals using the Uu interface on the downlink. The Uu interface provides a large dissemination range for V2X data through the cellular core network. User traffic in the Uu interface is predominantly unicast communication [25]; however, ongoing efforts are oriented towards multicast and broadcast support for V2X services in the future [26].
- **Edge/central cloud servers** are used to fuse information from multiple sources at a central location [27], [28]. They are able to obtain a holistic view on all connected entities, traffic information, roads and infrastructure.

B. Enabling Communication Technologies

Over the last two decades, several radio technologies have been proposed to cover all different aspects of vehicular communication and support the demanding requirements imposed by diverse V2X use cases. As the design targets of future V2X services continue to evolve, standardization

efforts aim at novel and innovative approaches to overcome the bottlenecks in terms of performance over the radio interface. In this context, two dominant radio technologies can be identified for V2X connectivity: *i*) IEEE 802.11p-based communication [29] and *ii*) 3GPP cellular-based communication [30]. In what follows, an overview of these two communication technologies is presented, together with associated security aspects.

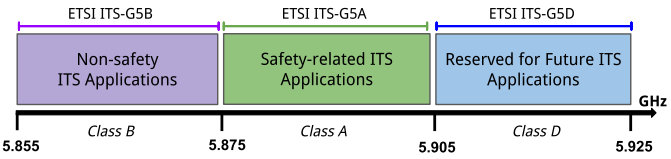


FIGURE 4: Sub-bands of the original European variant ITS-G5.

1) IEEE 802.11p-based V2X Communication

The IEEE has been working since 2004 on amendments of their well-established 802.11 family of standards to support wireless access for V2X communication in rapidly-changing mobile environments. In this context, the IEEE 802.11p standard defines the data exchange between high-speed vehicles, and between high-speed vehicles and roadside infrastructure. It operates in the 5.9 GHz frequency band, which has reserved for ITS services in Europe and the US, with a special focus on safety applications. The IEEE 802.11p constitutes the underlying radio communication basis for two matured standards: *i*) DSRC in the US [31], [32] and *ii*) original radio access technology of ETSI C-ITS in Europe [33], [34].

Both DSRC and ETSI C-ITS operate in the 5.9 GHz frequency band, and the PHY and MAC layers rely on the IEEE 802.11p standard [35] and ITS-G5 standard [36], respectively. The operating range of DSRC is from 5.85 GHz to 5.925 GHz, and wireless channels are separated into control and service channels. Switching between channels is instructed by the IEEE 1609.4 standard. The PHY layer of IEEE 802.11p uses OFDM and, compared to WiFi, it reduces the 20 MHz channel bandwidth to 10 MHz and doubles the time parameters of the PHY, to cope with the rapidly varying channels of vehicular environments. The original European variant of IEEE 802.11p is sub-divided into three bands as shown in Figure 4: class A (5.875 GHz to 5.905 GHz) for safety-related applications, class B (5.855 GHz to 5.875 GHz) for non-safety applications and class D (5.905 GHz to 5.925 GHz) is reserved for future applications. In addition, ITS-G5 introduces features for decentralized congestion control, as specified in [37], aiming at maintaining network stability, throughput efficiency and fair resource allocation to ITS stations. Recently, ETSI has officially standardized the use of C-V2X as an access layer technology for ETSI C-ITS, and it can be operated at the 5.9 GHz frequency band allocated in Europe [38].

The standards at the application layer of DSRC and ETSI C-ITS specify a set of requirements and functionalities to implement V2X applications. These standards include V2X messaging protocols, position management and data fusion in local dynamic map, among others. In DSRC, the society of automotive engineers (SAE) J2735 [39] standard defines the syntax and semantics of V2X messages, i.e., basic safety messages (BSMs) which are sent periodically at a maximum rate of 10 Hz, and convey state information of the vehicle, including position, dynamics, status and size. In ETSI C-ITS, the cooperative awareness messages (CAMs) are specified in [40], as equivalent to BSMs in DSRC. CAMs are periodic messages that provide status information to neighboring vehicles and RSUs. The rate of CAMs may vary between 1-10 Hz, depending on vehicle dynamics and the congestion status of the wireless channel. In addition, the distributed environmental notification messages (DENMs), specified in [41], are event-triggered messages controlled by the application (e.g., for collision avoidance).

Security aspects of IEEE 802.11p: Both DSRC [42] and ETSI C-ITS [43] standards rely on cryptographic standards for establishing trust and preserving confidentiality between communicating parties. The use of cryptographic procedures helps secure communication by reducing security threats such as malicious spoofing and eavesdropping. The security layer of DSRC and ETSI C-ITS protocols is based on the IEEE 1609.2 security standard [42] and provides message authentication and encryption based on digital signatures and certificates. Figure 5 shows the structure of a secured protocol data unit (SPDU) within a frame. The SPDU encapsulates a digitally-signed (BSM/CAM) message with the security information required for verification. Safety messages (BSMs and CAMs) are transmitted in a standardized format to support safety applications; thus, they are non-encrypted. This allows all other participating vehicles in the network to read these messages. On the other hand, the content is encrypted in messages that contain security information (e.g., certificates) [43], [44]. Such certificates exchanging messages are thus trusted and contents are encrypted. Figure 6 illustrates a broadcast of an SPDU via V2X communication. At the reception, the receiver verifies the sender's signature for authenticity. Moreover, there is a provision for restricting the sender's certificate to an identified geographical region. The implementation of such a feature is optional and left to the appropriate authority for the region where the certificate is being used. For example, SAE J2945/1 specifies three countries (US, Canada, and Mexico) as identified regions for transmitting signed messages with certificate, which may enable the feasibility of realizing V2X use cases in cross-border/cross-country scenarios [45].

For cryptographic algorithms, strong elliptic curve cryptographic (ECC) mechanisms, such as elliptic curve digital signature algorithm (ECDSA) for signing and elliptic curve integrated encryption scheme (ECIES) for encryption, are used. To minimize security overhead, the certificate of the

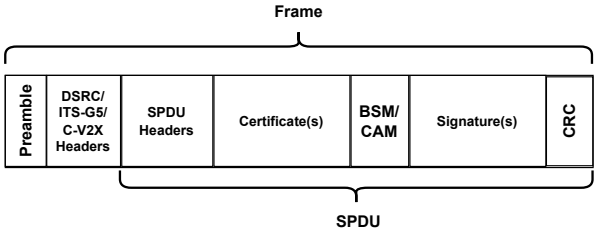


FIGURE 5: Structure of a signed message.

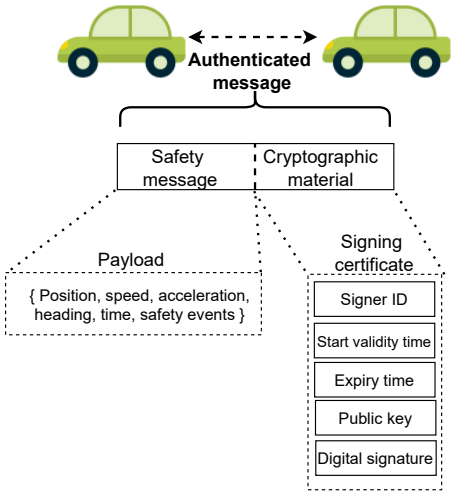


FIGURE 6: Signed messages for authentication between vehicles.

sender is embedded in the security header of secured messages as a specialized certificate format for V2X. Specifically, the IEEE 1609.2 certificate format is advantageous since it is smaller in size compared to the size of conventional X.509 certificates [46], but still capable of leveraging strong ECC algorithms (ECDSA and elliptic curve Diffie-Hellman). Regarding privacy protection, certificates are pseudonymized (i.e., pseudonym certificates) in order not to include the identity information of the user or the vehicle, and only the certificate authority (CA) can link the certificate to the real user/vehicle identity. In addition, each vehicle can change its certificate frequently, after using it for a limited time period, to avoid being tracked by malicious entities [42], [43]. However, DSRC/WAVE protocols are vulnerable to various critical attacks, such as malware, black hole, GPS spoofing and DoS [47]. Furthermore, the limited bandwidth and channel capacity constraints of existing 802.11p-based standards hinder the applicability of matured security solutions derived from other communication systems [48].

2) Cellular-based V2X Communication

The 3GPP developed the first set of cellular standards in Release 14 [49] for V2X communication based on LTE technology, which has been recently evolved into the 5G New Radio V2X (5G NR-V2X) standardized in Release 16 [25]. C-V2X is gaining support from leaders of the automotive and telecom industries, which has, in turn, led to worldwide C-V2X trials (e.g., [50], [51]). It has already been claimed that C-V2X offers superior performance with larger coverage compared to IEEE 802.11p-based DSRC/ETSI C-ITS radio technologies [52].

The lower layers of C-V2X protocol are specified by the 3GPP for radio access, whereas the upper layers (i.e., applications, facilities, networking, transport and security) are reused from DSRC and ETSI C-ITS standards. This allows an one-to-one mapping of existing applications already developed on DSRC or ETSI C-ITS, and ensures interoperability with the emerging C-V2X ITS use cases. C-V2X standard specified in the 3GPP Release 14 [53] and Release 15 [54] provides two radio interfaces (i.e., the Uu interface and the PC5 interface) to support all types of vehicular use cases.

In general, C-V2X radio supports both infrastructure-based solutions over the Uu interface and sidelink-based solutions over the PC5 interface. The Uu interface leverages the conventional cellular link between the vehicular UE (V-UE) and the base station (eNodeB/gNodeB) while operating in commercial licensed cellular spectrum. The Uu interface is used for V2I and V2N communication. The Uu-based communication requires the V-UE to reside within the coverage area of the base station, and the base station is responsible for the radio resource management [55]. The main advantage of the Uu interface is the long-range dissemination of V2X messages through the cellular core network. However, due to the inherent network delays, the Uu interface is expected to be used for latency-tolerant use cases, such as dynamic high-definition (HD) maps, software updates, infotainment, traffic information, and informational safety.

The PC5 interface supports direct communication between V-UEs, between V-UEs and RSUs, and between V-UEs and other road users without routing every message through the base station. Therefore, the PC5 interface becomes ideal for time-critical safety use cases that require low latency communication with enhanced range, reliability and non line-of-sight performance. The PC5-based communication entails V2V, V2I and V2P communication [49]. The PC5 interface specified in 3GPP Release 14 and Release 15 evolves from the device-to-device (D2D) framework standardized in the previous Release 12 and Release 13 for proximity services (ProSe) [56], e.g., emergency communication in case of natural disaster. Ideally, V-UEs can use the PC5 interface to operate both in the presence and absence of a base station (i.e., with or without cellular coverage). When a V-UE is in cellular coverage, the base station manages resource allocation, which is referred to as centralized scheduling mode (sidelink Mode 3) of the PC5 interface. In case of out-of-coverage, decentralized scheduling mode (sidelink Mode

4) occurs, and the V-UE itself manages radio resources for the PC5 interface in an autonomous manner.

The sidelink Mode 4 of PC5 interface is capable of operating without provisioning of a subscriber identity module (SIM); thus, subscription to a mobile network operator (MNO) is not required. As a result, the PC5-based communication can support mission-critical vehicular safety services when cellular coverage is not available or when the vehicle does not have cellular subscription [57]. In order to support SIM-less operation, automotive original equipment manufacturers will have to configure the on-board UE in each vehicle with the required parameters to autonomously reserve radio resources.

The enhancements introduced in C-V2X were primarily aimed at handling high relative vehicle speeds and improving reliability, throughput and latency. In 3GPP Releases 14 and 15, C-V2X provides the support for a basic set of vehicular use cases that require the exchange of safety messages ranging from 1-10 Hz periodicity and 50-100 ms end-to-end latency. However, with the continuous evolvement of C-V2X, 3GPP 5G NR-V2X specification in Release 16 [58] provides further enhancements to improve short-range sidelink-based (NR-PC5) direct communication mode for critical vehicular use cases. In particular, NR-PC5 sidelink will provide ultra-reliability, lower latency, higher throughput and improved positioning. These new features are expected to support advanced V2X use cases (e.g., remote driving, vehicle platooning) that could enhance advanced and autonomous driving without relying on cellular network [59]. In addition, NR-PC5 sidelink provides sidelink time synchronization feature which allows robust V2X operation even without GPS coverage.

Security aspects of C-V2X: In what follows, we elaborate key security aspects of LTE V2X and 5G V2X technologies.

1) LTE V2X: Related security aspects for LTE support of V2X are described in [60] for both PC5- and Uu-based communications. The 3GPP LTE-V2X architecture introduces two new dedicated network entities $i)$ V2X control function (VCF), and $ii)$ V2X application server (V2X AS) to manage V-UEs. The VCF is mainly responsible for configuring V-UEs to enable both Uu and PC5 interfaces prior to V2X communication. In addition, the VCF is involved in facilitating security operations such as authentication, authorization and revocation of V-UEs. The authorization of V-UEs by VCF allows the PC5 interface to directly communicate with other V-UEs and the Uu interface for conventional communication with the eNodeB. The authentication and authorization of V-UEs are handled by the VCF through home subscriber server in the core network. The V2X AS acts as a group communication system using the 3GPP cellular-based communication to disseminate application data to a group of V-UEs. However, there is no normative solution for the security of V2X application data [60]. Therefore, security requirements (e.g., authentication, authorization, integrity protection, replay protection, and confidentiality) that apply to V2X communications will have to rely on the application-layer security protocols defined by other standards-developing organizations [42], [43].

Mutual authentication between the V-UE and the core network should be established prior to PC5- and Uu-based communications. LTE-V2X leverages the existing authentication and key agreement protocol (EPS-AKA) for mutual authentication, and supports various functions, such as user identification and key derivation. Security features of ProSe defined in [61] provision a secure cryptographic channel for one-to-many ProSe direct communication over PC5 interface. In ProSe direct communication, a group of V-UEs shares a secret (i.e., ProSe encryption key) which is derived from the group security key (i.e., ProSe group key). The derived ProSe encryption key encrypts all data for that group. Although security requirements for LTE-V2X are specified in 3GPP Release 17 [60], the specifications do not impose any mechanisms for PC5 privacy, leaving it to the regional regulators and operators. The 3GPP suggests pseudonyms in the PC5-based communication as privacy procedures. This is achieved by changing and randomizing the V-UE's layer-2 ID (i.e., member ID) and source IP address. On the other hand, the existing evolved packet system (EPS) security solution is applied for Uu-based communication. Apparently, there are no specific enhancements on security and privacy aspects in the LTE-Uu interface within 3GPP Release 17 [60].

2) 5G V2X: Ideally, 5G-V2X can utilize equivalent security functionalities that have already been defined in the LTE-V2X counterpart for NR-PC5 and Uu interfaces. The functionalities of PCF are equivalent to the VCF in LTE-V2X. Similarly to VCF, the PCF can use the general principle to authorize and provision both NR-PC5 and Uu interfaces for V2X communication in 5G-V2X architecture. 3GPP describes related security aspects in [62] for the 5G system to support V2X communication. While no additional security procedures for Uu interface are proposed in [62] beyond those given in [60], security considerations are expected for V2X over NR-PC5 due to unicast, groupcast, and broadcast communications support. According to [62], the V-UE establishes a security context for each NR-PC5 unicast link using hierarchical layers of cryptographic keys. They constitute a shared key (K_{NRP}) between two communicating V-UEs derived from long-term credentials of V-UEs, a session key ($K_{NRP-sess}$) per unicast link derived from K_{NRP}, an encryption key ($NRPEK$), and an integrity key ($NRPIK$). The keys $NRPEK$ and $NRPIK$ derived from $K_{NRP-sess}$ are used in confidentiality and integrity protection algorithms respectively for protecting signalling (PC5-S and PC5-RRC) and user-plane data carried over NR-PC5 interface. There are no any specific security requirements defined in [62] for groupcast and broadcast modes over NR-PC5. For privacy protection, a similar approach to LTE-V2X privacy (i.e., a

periodic change of the layer-2 ID and source IP address) can be applied in NR-PC5 based communication modes.

5G networks do not aim to replace or change the existing communication architecture (i.e., LTE) but rather underpin a unified platform that offers diverse services by leveraging all existing and envisioned techniques [63]. However, the integration of key enabling technologies such as software-defined networking (SDN) and network functions virtualization (NFV) into 5G introduces new security challenges for the application of V2X connectivity [64]. Hence, new application layer security protocols can be introduced to enhance security and privacy of V2X users. The 3GPP has recently standardized new measures to enhance security and privacy in several domains that can benefit V2X communication [65]. For example, *i*) increased home control, *ii*) security in radio access network (RAN) and network slicing, *iii*) enhanced privacy for international mobile subscriber identity (IMSI) and *iv*) authentication and authorization, among others. Yet, security and performance at large are considered to persist as issues for the successful deployment of 5G-V2X systems. Characteristics such as centralized architecture, different authentication types for distinct scenarios (V2V/V2I), V2X UE privacy, and broadcast message security in one-to-many communication affect security and performance in 5G-V2X [66]. Furthermore, frequent control signaling traffic when authenticating a large number of V-UEs and handover/roaming authentication for V2V/V2P systems in heterogeneous 5G scenarios can lead to security and performance issues.

C. Other Key Enabling Technologies

The widespread deployment of V2X systems notably relies on high performance computing and storage closer to the end users, resource isolation at multiple levels, and enhanced security, privacy and trust in message dissemination and data management [67], among others. In this context, *i*) mobile edge computing, *ii*) network slicing and *iii*) blockchain technologies can be identified as key enablers to satisfy stringent requirements in emerging V2X use cases, such as autonomous and assisted-driving vehicles. In what follows, we briefly describe the aforementioned key technologies and associated security aspects.

1) Mobile edge computing: In emerging V2X use cases, there is a gradual inclination towards deploying high performance computing and storage devices on board of a vehicle; autonomous driving is expected to transform vehicles into powerful computing and networking hubs for increased safety. Besides semi/fully autonomous driving, other use cases in this category include in-vehicle infotainment and over-the-air vehicular maintenance. However, such resource-hungry applications pose a serious challenge on the limited computation and storing capabilities of vehicle OBUs. It has been highlighted that *a single autonomous test vehicle produces about 30 TB per day, which is 3,000 times the scope of Twitter's daily data [68].*

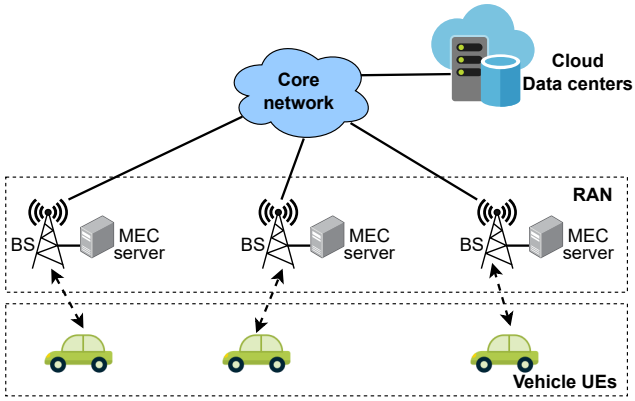


FIGURE 7: MEC support for connected vehicles.

Cloud-based mobile edge computing (MEC) has recently been considered as an innovative computing paradigm to cope with the explosive demands for efficient computation of large amounts of on-board generated data by vehicles [69]. Particularly, the combination of 5G and MEC technologies are considered to be the key to drive the widespread adoption of autonomous vehicles (AVs) by enabling constant, near-instantaneous uploading, processing and downloading of massive amounts of data [70]. An example of a real-world deployment of 5G MEC can be found in [71] for testing vehicular C-V2X and extended reality use cases. It is apparent that MEC is a key technological enabler for connected vehicles by deploying computation and geographically distributed V2X services at roadside base stations.

MEC is seen as a promising approach to effectively push cloud services to the edge of the RAN and provide cloud-based resources in the vicinity of the vehicles. Figure 7 illustrates an example of MEC support for connected vehicles. MEC servers usually are small-scale data centers that can be co-located with wireless access points, e.g., base stations [72]. The communication between MEC servers and vehicle UEs is established via the wireless interface with the possibility of direct D2D communications. The placement of MEC servers within RAN allows vehicles to offload certain computation-heavy tasks to a selected MEC server [73]. The co-location of MEC servers with base stations helps achieve end-to-end low-latency in safety-critical scenarios [74]. Moreover, stringent performance requirements of mission-critical V2X applications can be achieved using an optimal application placement strategy based on available resources on MEC servers [75]. By deploying cloud-based infrastructure in close proximity of vehicles, efficient content (e.g., HD maps) caching can be achieved, reducing the data streams infused to the network while a short response delay can be provided.

Security aspects of mobile edge computing: MEC environments typically encompass a multi-vendor, multi-supplier, and multi-stakeholder ecosystem of hardware and software

components. In such complex distributed systems, one cannot assume that a centralized entity is able to provide system-wide security; instead, multi-party security mechanisms are needed to assess the trust of each other. In this context, ETSI has been involved in standardizing MEC security (ETSI ISG MEC [76]) with various security proposals for MEC applications (e.g., MEC service application programming interfaces (APIs) over HTTPS with encrypted traffic, application level authentication and authorization, use of trusted computing modules). Furthermore, mature security techniques, such as firewalls to control data traffic and intrusion detection systems (IDS) to mitigate distributed denial-of-service (DDoS) attacks, can be used on the MEC to protect V2X applications [77]. Zero-trust security concept can be further leveraged to mitigate security risks, particularly when 5G-based V2X systems are deployed with untrusted infrastructure [78]. Zero-trust provides protection for data and services, including assets (devices, infrastructure components, applications, virtual and cloud components), end users and applications. Specifically, zero-trust protection minimizes access to resources and continuously authenticates, authorizes and validates the identity and security posture of each request [79]. Moreover, computation offloading from vehicles to MEC servers can be securely performed using AL/ML techniques; such approaches help minimize the risk of eavesdropping [80].

2) Network Slicing: 5G systems offer dedicated resource management through network slicing. Network slicing allows MNOs to split their monolithic network into independent slices and support dedicated use cases with different network resource capacities [81]. Figure 8 illustrates a high-level overview of the network slicing concept in 5G systems, a key enabler to flexibly isolate network connections. As it can be observed, each slice consists of its own logically isolated network with management and security to support a specific use case. A set of core network functions are responsible for access and mobility management (AMF), session management (SMF), and policy control (PCF). The user plane function (UPF) forwards V2X traffic between RAN and Internet (where the V2X AS is deployed). Furthermore, a network slice may span across several domains including RAN (data plane), core network (control plane), and service platform on distributed cloud infrastructure. SDN and NFV are two key technologies that enable the slicing concept. NFV enables dynamic computing and storing management among different MEC servers, leading to a scalable architecture. Since SDN control modules in MEC servers can separate the control plane from the data plane, multiple RANs can interwork to support the increased traffic data in IoV scenarios, while various radio resources can be abstracted and reallocated to base stations [82].

Provisioning of V2X services entails diverse requirements for latency, data rate and reliability from vehicular networks. For example, autonomous driving requires an order of few

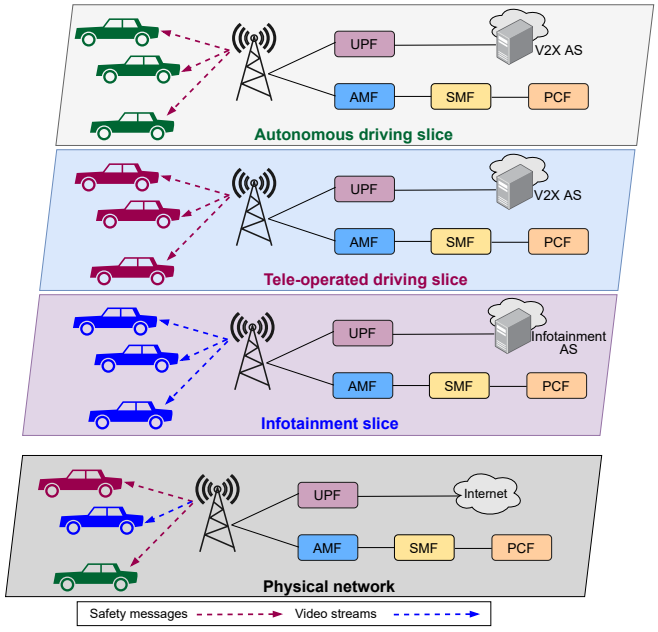


FIGURE 8: Network slicing support for V2X services.

milliseconds of latency, higher data rates, and close to 100% reliability (details in Section II-D). However, infotainment services can tolerate longer delays and low reliability given higher data rates. Although LTE technology has enhanced the support of V2X services [24], existing LTE networks cannot satisfy such stringent and dynamic requirements. Network slicing emerges as an effective solution for this challenge, since diverse V2X applications are supported by logically separated networks. This helps isolating, for instance, mission-critical V2X traffic whilst achieving stringent performance requirements. Moreover, the complexity of service provisioning with network slicing can be minimized using advanced AL/ML techniques. AL/ML models help implement intelligent slicing mechanisms for V2X service provisioning while optimizing QoS performance of each V2X service request [83].

Security aspects of network slicing: In the slicing context, isolation is a prerequisite for end-to-end security. End-to-end security is a natural approach as network slices are end-to-end logical networks. Slicing constitutes one of the 5G enabling technologies, thus a secondary authentication at slice level is necessary to prevent unauthorized access to slices by intruders. The 3GPP suggests a secondary authentication mechanism to implement NSSAA (network slice-specific authentication and authorization) procedure [65]. The NSSAA procedure authorizes a UE to gain access to a certain network slice, which is identified by an S-NSSAI (Network Slice Selection Assistance Information). The NSSAA procedure is triggered between UEs and the AAA-S (authentication, authorization, and accounting server) by the AMF. The AAA-S may be owned by the home network operator or

a third-party enterprise. As described in [65], the extensible authentication protocol (EAP) is used for NSSAA between a UE and the AAA-S using the UE's ID and credentials which are different from the 3GPP ones. Once the EAP-based NSSAA procedure is completed, the AMF sends updates to update the UE's subscription database for the requested S-NSSAIs.

Slice-level security is discussed in [84] at a fine-grained level under life-cycle, intra-slice, and inter-slice security categories. The authors highlight that the use of cryptographic primitives at all those levels is important to fulfill fundamental security requirements such as confidentiality, integrity, authenticity of data and mutual authentication between peers within a slice. It is further suggested to provide secure access to slice APIs using state-of-the-art TLS or O-Auth techniques [84]. An application of dedicated security policies with secure API access is presented in [85] to protect safety-critical V2X data traffic in an end-to-end fashion. A secure and privacy-preserving authentication framework is proposed in [86] to support secure access to service data in slice selection.

Although 3GPP suggests NSSAA procedure at the slice level, security and privacy aspects of network slicing still constitute open issues [66]. Network slices serve different services that may require contrasting security and privacy requirements. The realization of differentiated security policies for contradictory requirements among slices becomes complex in multi-tenant and multi-domain environments. Security support for group authentication and group security management is key to avoiding potential issues when UEs can access several network slices. The use of external entities (e.g., a third-party AAA-S) may have trust implications. In the context of V2X, security in network slicing is a critical problem to be solved when the majority of V2X traffic is mission-critical. Lightweight security protection mechanisms at the slice level are crucial for V2X services to address low latency, high mobility, frequent authentication and re-authentication, and ephemeral connectivity requirements.

3) Blockchain: Blockchain is considered a disruptive technology offering transfer ownership, record of transactions, asset tracking and security/trust in open environments. It serves as a decentralized database which stores all transactions encoded, while cryptography applied for each update in transactions, ensures its immutability [87]. A blockchain consists of a chain of data packages (i.e., blocks) where each block comprises multiple transactions, and it is extended with additional blocks resulting in a complete ledger of the transaction history. Figure 9 depicts an example of a blockchain, where each block points to the immediately previous one through a hash value. The hash value is generated from the data that was in the previous block, which essentially links all blocks together in the blockchain. Blockchain technology is widely adopted in cryptography and cybersecurity, ranging from cryptocurrency systems to smart contracts

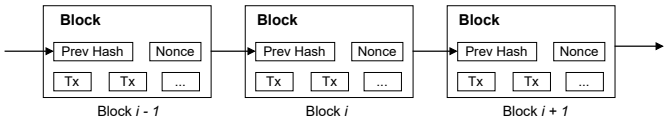


FIGURE 9: Structure of a blockchain with a chain of continuous blocks.

and smart grids over IoT. Novel paradigms such as IoT data collection, AVs, unmanned aerial vehicles (UAVs) and federated learning (FL) entail new security requirements (e.g., immutability, decentralization and transparency) for their successful roll-out in beyond-5G networks [88]. In an IoV context, several blockchain-based use cases, including vehicular data security, on-demand transport services and vehicle management, are discussed in [89].

In emerging V2X use cases, vehicles largely rely on edge nodes (RSUs, MEC servers) for offloading computation, utilization of shared data and for storing on-board generated data. In such scenarios, vehicular data protection and management are of utmost importance to ensure security, privacy and trust. Cooperative resource sharing in IoV supports spare computational and spectrum resources sharing between nearby entities, latency-sensitive services deployment, and AI/ML applications. Smart parking and emerging vehicle platooning are well-known example use cases in vehicle management. All aforementioned use cases are distributed in nature with inherent security, privacy and trust challenges. Blockchain-based systems have been recently adopted to address such issues in IoV networks [90].

Security aspects of blockchain: From a security perspective, the blockchain is constructed to ensure security attributes such as integrity protection, privacy, anonymity, trust and resistance to DDoS attacks. Each block of the blockchain is secured through intelligent and decentralized utilization of cryptography with crowd computing. A consensus mechanism is used to validate all transactions within the blocks, and ensures that each transaction is true and correct.

In the context of V2X, authentication is an integral part of security and thwarts most security attacks that originate from intruders. Some works have applied well-known authentication mechanisms in V2X security using blockchain technology [90]. Techniques such as mutual authentication between vehicles and access points (e.g., RSUs), privacy-preserving anonymous authentication, and certificate-based authentication are few examples. V2X edge nodes in MEC networks are usually operated by multiple service providers [91]; thus, it is often difficult to ensure interoperability among different actors, by imposing regulations and trust among them while guaranteeing service continuity. They are also inherently vulnerable to security and privacy related attacks by being geographically distributed. Blockchain can be adopted in V2X data management to address such security and privacy issues, and for trust management among edge nodes. The

adoption of blockchain and smart contracts technologies for secure and distributed data management in vehicular edge networks is introduced in [92]. Smart contracts ensure secure data sharing and storage within vehicles and edge nodes, as well as prevent unauthorized data sharing. In a collaborative V2X environment, trust establishment among multi-operator and distributed infrastructure nodes (RSUs) can be achieved using a blockchain-based system [93]. Proof-of-work and proof-of-stake consensus mechanisms are utilized in [93] to stimulate RSUs to become the miner that can add a trust block to the blockchain. However, there are still security concerns, e.g., 51% attack, threats/attacks in dynamic vehicular networks, associated with blockchain that need further investigations [94].

D. Emerging V2X Applications and Challenges

V2X systems present certain peculiarities in terms of deployment options and data traffic characteristics with respect to traditional network applications. Covering a wide range of network scenarios, V2X systems accommodate vehicular services with diverse QoS requirements. There are four prevalent classes of emerging V2X applications that can be identified within ITS domain, namely, road safety, traffic management, comfort and infotainment and autonomous driving, as defined in [95]. Table 4 presents the main V2X application categories and a set of example use cases per category with their service-level requirements. Essentially, latency, data rate and message transmission reliability are considered as key performance indicators (KPIs) in the realm of road safety and mobility applications. Latency refers to the maximum tolerable end-to-end packet delay across all processing layers involved, while reliability is defined as the percentage of expected rate of successful packet deliveries. The data rate is defined per vehicle on the uplink and downlink.

Cooperative road safety use cases are based on periodic message broadcast by vehicles with a typical transmission rate between 1 and 10 Hz [96]. The payload of each of these messages ranges from 60 to 1500 Bytes, while data rate is not a concern due to the dynamic characteristics of such applications. As shown in Table 4, maximum delay ranges from 50 ms to 100 ms in this category. The acceptable service-level reliability value is in the range of 90–95% without re-transmission of a single CAM; this is compatible with the ETSI requirement of $<5\%$ probability that two consecutive CAM transmissions fail [97]. Traffic management use cases offer various infrastructure-assisted services (e.g., speed limits and/or traffic flow control via RSUs) that can enhance traffic efficiency. Both delay and reliability KPIs are not as critical as in the safety use cases [98]. Vehicular Internet and infotainment use cases do not usually impose strict KPIs; thus, latency in the order of 100 ms for Web surfing and up to 15 Mbps data rate for high-definition video streaming have been identified as potential requirements [99].

A set of advanced V2X use cases within autonomous driving ITS application is also listed in Table 4. Such use cases entail stringent service-level requirements with ultra-reliable and ultra-low latency connectivity constraints. The maximum delay varies from 3 ms to 100 ms in advanced driving, while reliability is in the range of 90–99.999% to enable semi or fully automated driving. For vehicle platooning, the maximum latency is 10 ms with 99.999% reliability requirement in the case of a high degree of automation. Remote/tele-operated driving introduces a 5 ms maximum delay budget with nearly 100% reliability [95]. In remote driving, a remote driver or a V2X application (via V2N) takes over the operations of a remote vehicle located in a crash mitigation situation (e.g., icy roads, bad weather conditions). In such scenario, a large amount of raw data (25 Mbps) should be transmitted in the uplink within 5 ms with very high reliability [95]. For instance, data rate of 25 Mbps is necessary in the case when LiDAR and sensor data are transmitted. It is worth noting that as QoS and security guarantees are tightly coupled, security enhancements should not be incorporated at the expense of such critical performance requirements. Achieving optimal trade-off between QoS and security levels becomes therefore essential for V2X communication systems.

Regarding V2X deployment options, a key consideration is the highly dense vehicle connectivity in urban areas, which may require small cell sizes while vehicles move at high velocity. This, in turn, results in dynamic network topologies with different mobility patterns, unbounded scalability, intermittent connections, heterogeneous networking infrastructure, frequent handovers due to network entries/re-entries, and data priority in case of safety requirements. Such distinct characteristics of V2X systems provide an ideal playing field for malicious actors while imposing severe challenges on security. Furthermore, V2X messages are transmitted either periodically or in an event-driven manner by vehicles and/or by other V2X network entities (i.e., RSUs, VRUs). Exchanged messages are typically small in size [3], [10]; thus, the addition of security-related payloads (e.g., digital certificates, pseudonyms, keys) into V2X messages inherently introduces extra overhead and increased processing times. In this context, it is important to ensure that security architectures and solutions are interoperable with the existing V2X platforms as well as adaptable for upcoming future V2X technologies. The prevention of adversarial attacks and the preservation of users' trust in heterogeneous V2X environments are also major challenges to overcome. Such diversified characteristics and challenging V2X features render the fulfillment of security and privacy requirements a non-trivial task [8].

E. Security and Privacy Requirements

The foremost purpose of V2X communication systems is to increase road safety and traffic efficiency through information exchange between vehicles and between vehi-

TABLE 4: V2X application categories and associated QoS requirements.

Application	Use cases	Connectivity mode(s)	Maximum Delay (ms)	Data rate (Mbps)	Reliability (%)	Reference
Road safety	• Collision warning • Vehicle status warning • Vehicle type warning	V2V, V2I	50 100 100	Not a concern	90–95	[96][98]
Traffic management	• Speed limit notification • Vehicle tracking • Traffic flow control	V2I, V2N	500∼1000	Not a concern	< 90	[96][98]
Comfort and infotainment	• In-vehicle Internet access • Point of interest alerts • Parking booking	V2I, V2N	100 $>$1000 $>$1000	0.5–15 0.01–2 0.01–2	Not a concern	[98][99]
Autonomous driving	• Advanced driving • Remote driving • Vehicle platooning	V2V, V2I V2N V2V, V2I	3∼100 5 10∼500	10–50 UL:25/DL:1 50–65	90–99.999 $>$ 99.999 90–99.999	[95]

cles and road infrastructure. For instance, when a safety-critical situation occurs, event-based warning messages (e.g., DENMs/BSMs) are initially triggered to notify the driver, and subsequently the authorized users should not be prevented from accessing such warning messages. In the next step, the receiving vehicle needs to accept the message content whilst trusting that it was originated from a legitimate entity in the V2X system. These steps directly convey three fundamental security aspects of V2X information, i.e., availability, message integrity and message authenticity [44].

There can be situations where a compromised vehicle triggers false alarms for non-existent road hazards, such as a traffic jam or an accident. The messages sent by legitimate entities can also be fabricated by an attacker to mislead other V2X participants. Such security threats can severely affect the overall functionality of the communication system. It is clear that security attacks and threats come to the fore largely from V2X use cases in the domain of C-ITS. They are unique to V2X systems due to the characteristics of V2X use cases (e.g., vehicle platooning, cooperative collision avoidance, dynamic map sharing, and remote driving). Similarly, security attacks and threats specific to V2X communication technologies (i.e., IEEE 802.11p and C-V2X) are becoming highly effective against V2X systems [12], [14], [100]. Therefore, it is of utmost importance to satisfy fundamental security/privacy requirements and guarantee a safe ITS environment by avoiding/mitigating potential cybersecurity attacks. It is noted that these requirements can vary depending on the level of security/privacy sensitivity required for an ITS application [101], as well as on the adopted approaches to avoid different threats.

In what follows, we provide a concise description of V2X security and privacy requirements.

Authentication: It implies that legitimate entities are differentiated from malicious ones involved in V2X communication and, at the same time, message recipients are ensured that receiving messages are originated from a genuine sender. Authentication can be considered as one of the most significant security features in V2X systems, being able to uniquely distinguish and verify each participating entity [102]. Within V2X services, the authentication entails: *i*) user authentication, where the legitimacy of a device is ensured; *ii*) message authentication, which ensures that messages are authenticated such that each recipient can verify whether they are originated from a legitimate entity and that message contents are not tampered.

Authorization: It serves to control access to V2X services while ensuring the right accessibility to solely legitimate V2X entities. Authorization is based on a predefined set of rules and policies, allowing rightful access to V2X services or denying the rights to use certain V2X services.

Availability: It implies that authorized users are not prevented from accessing the information (i.e., V2X messages). Availability requirement ensures that V2X services and protocols remain functional in the presence of attacks, e.g., service deniability in DoS attacks. Hence, the V2X system ensures that authorized V2X entities are able to access the network at anytime and from anywhere.

Confidentiality: It provides the assurance for non-disclosure of V2X message contents, allowing them only to be accessed by the intended recipients. Data confidentiality prevents accessing the content of messages by adversarial nodes or unauthorized parties. It can usually be achieved by employing an encryption mechanism based on shared keys between communicating parties. There are no specific requirements for data confidentiality in V2X communication as the information exchanged (e.g., periodic beacons or event-triggered messages) is mostly public [43]. However, it is necessary to ensure that the data cannot be linked to infer and reveal private information of vehicle users and their locations.

Integrity and data trust: It ensures that shared information among V2X entities is accurate and consistent, and should be able to be verified in a timely manner. V2X systems are required to introduce integrity-preservation mechanisms in

order to detect any tampering or manipulation of data by malicious users or devices.

Privacy: It is necessary to preserve the identity of V2X users, making it hard (or impossible) to track locations of vehicles and sensitive information of users. The disclosure of private information may lead to system-wide attacks on V2X entities and manipulate personal assets of users. Anonymization and/or information hiding can be employed as a way of preserving one's privacy [16]. As such, vehicles are assigned pseudo-identities, known as pseudonyms, to keep real identities hidden within the scope of the V2X service. Similarly, other key privacy-related requirements (i.e., anonymity, unlinkability, and unobservability) should be preserved through necessary security mechanisms and policies [103].

III. Security Threats and Attacks

In this section, we describe in detail the security threats and attacks that may hinder the proper operation of V2X networks. A thorough classification of various malicious attacks identified in existing literature is also provided.

A. Attack Surface

The attack surface encompasses all possible vulnerable entry points that undermine a V2X system's security, and constitute the source of adversarial attacks and malicious incidents. For example, in-vehicle user devices (e.g., USB, WiFi, Bluetooth) of the infotainment system or vehicle's sensors can potentially covert to attack surfaces. As the level of driving automation in vehicles increases, the available electronics of in-vehicle networks also escalate whilst expanding the attack surface for in-vehicle components such as electronic control units (ECUs) and the control area network [13]. The work in [104] presents a systematic analysis of different threat vectors in the vehicle (e.g., Bluetooth, Cellular, WiFi, RFIDs) by experimentally demonstrating that in-vehicle ECUs can be compromised using remote attacks. Moreover, the introduction of C-ITS enables the interconnection with the surrounding environment (e.g., other vehicles, RSUs, and pedestrians) via V2X technologies. As a result, the in-vehicle network components are exposed to the outside world even more.

In IoV environments, attack surfaces can emerge in three different domains [105], namely *i*) in-vehicle, *ii*) V2X access and *iii*) infrastructure. Some attack types, e.g., DoS and flooding, may be common across all three domains, while others target a single domain, e.g., tampering or physical damage to in-vehicle units. V2X communication has become the main target of IoV security attacks, e.g., eavesdropping, communication hijacking, spoofing, data injection, impersonation, etc. Therefore, in this paper, we focus specifically on the V2X access domain that comprises all V2X connectivity modes such as V2V, V2I, and V2N.

B. Attacker Model

Attack detectors are often designed to detect certain attacks and then evaluate the detection performance. Hence, it is necessary to have an understanding of the behavior/profile of attackers and associated attack types to implement resilient defense mechanisms. Apparently, there is no universally adopted model for classifying V2X attack variants; therefore, we resort to the attacker's model proposed in [106], which consistently defines the capabilities and methods available for an attacker to access the target asset (e.g., vehicle, RSU and communication channel). According to [106], the attacker becomes an *insider* when possessing valid credentials to communicate with other legitimate members and/or obtain system-wide access. These authenticated attackers usually behave according to the underlying system protocol, but can send false or fabricated information. On the other hand, when the attacker does not possess valid credentials or does not have system access, it is ranked as *outsider*. The outsider, also referred to as intruder, has limited capabilities to launch attacks, but is capable of eavesdropping on the communication link and inferring sensitive information (e.g., security keys, user information).

Furthermore, attackers can be classified as either *malicious* or *rational* based on their moral behavior. A malicious attacker usually seeks no personal benefits but to disrupt or cause harm to the benign users and destabilize the functionality of the system (e.g., cause an accident, DoS, traffic congestion). Such an attacker, therefore, may disregard any costs and consequences on achieving their objectives. On the other hand, a rational attacker typically operates on personal benefits (e.g., financial incentives, insurance fraud); thus, this type of attacker can be predictable in terms of methods to launch an attack and target assets. Regarding their execution mode, V2X attacks can be further distinguished as *active* or *passive*. In case of active attacks, attackers are actively engaging with the system and can transmit malicious packets or signals in V2X channels. DoS, message replay, false data injection, man-in-the-middle (MitM) and Sybil attacks can be reported as representative active attacks. Such attacks executed over V2X channels are generally considered as the most frequent and effective attacks against vehicular networks [6]–[11]. On the contrary, passive attackers are likely to eavesdrop on the communication to infer critical information (e.g., certificates, private keys, user information) without directly interacting with the system.

C. Attack Classification

A variety of existing works have investigated security threats in the context of V2X communication [8], [14], [107]. Those studies provide different classes of attacks (e.g., attacks to wireless interface, attacks based on the scope of communication, attacks based on behavior) which are useful for understanding and developing robust security solutions for vehicular services. In the following, we elaborate on security threats and attacks that are common and effective against

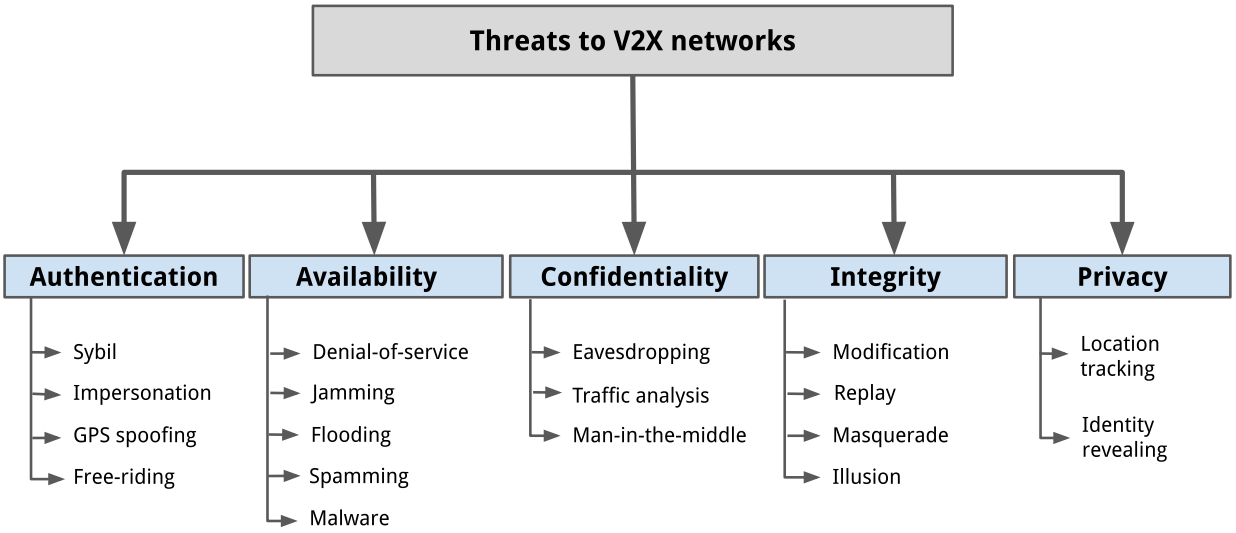


FIGURE 10: Classification of V2X cybersecurity threats based on the affected security and privacy requirements.

V2X networks. A classification (summarized in Figure 10) is further performed, based on the following key requirements under impact (described in Section II-E): authentication, availability, confidentiality, data integrity and privacy. Although the classification of attacks is performed under a single security requirement, it is worth noting that certain attacks (e.g., malware) may compromise multiple security requirements at a time. This is clearly reflected in Table 5, which summarizes the key characteristics of various attacks in V2X networks. Table 5 further presents the level of feasibility (i.e., whether it is difficult or not to practically launch a particular attack) as well as information related to the severity of an attack, considering the safety-critical aspect of V2X scenarios. The impact on the operational performance of the V2X system or private information leakage can have severe security implications in safety-critical V2X scenarios. The level of severity for an attack is categorized as low, moderate, or high [108]. If an attack impacts heavily on the operational performance of the V2X system or breaches privacy, the severity of the attack is inferred as high. Relevant references are also provided to highlight which communication technologies are susceptible to the corresponding attacks/threats. Such examples reinforce that many existing attacks/threats for conventional communication systems are highly effective against V2X systems.

Attacks on authentication: Attacks of this category can affect the process of authentication/identification while inflicting serious damage to the V2X network (e.g., expose identities). In what follows, a set of example attacks are described.

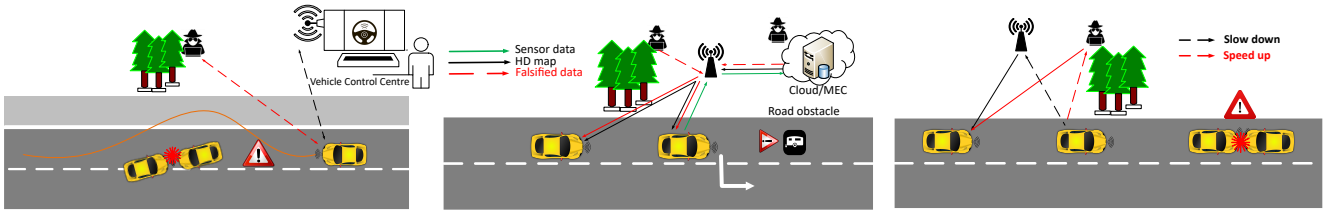
1) Sybil: An attacker forges multiple identities to achieve personal goals whilst disrupting normal system operation [148]. Such multiple fake identities could appear as real unique identities to the outside observers. For example, a Sybil node can use multiple pseudonym certificates of compromised vehicles to fake a congestion or a traffic jam by sending warnings as if several vehicles are located on the road. Similarly, a Sybil attacker can use multiple identities to boost its own reputation/trust score or reduce the reputation/trust of benign vehicles [149]. Furthermore, joint Sybil and DoS attacks may be launched to destabilize the overall network, rendering services unavailable for legitimate users. The pseudonymization of vehicles inadvertently enables a new threat vector, through which an adversary may execute Sybil attacks by pretending as though multiple vehicles are simultaneously on the road [109]. As shown in Table 5, it is apparent that malicious actors may exploit such vulnerabilities that exist in V2X communication technologies, e.g., DSRC [109] [110], ITS-G5 [111], and LTE-V2X [112], to launch Sybil attacks.

Sybil attack has been identified as a severe security threat for V2X networks, and can be launched at multiple layers of the protocol stack (e.g., application, transport, network, or data link). Its detection becomes challenging in distributed V2X environments [150]. The lack of CA or digital signatures' implementation in many V2X networks, and/or the absence of tamper-proof devices in vehicles makes the feasibility of a Sybil attack high [13]. The work in [113] presents a practical Sybil attack implementation at the network layer protocol in VANETs. In this demonstration, the normal behavior of a greedy perimeter coordinator routing protocol used for V2V is disrupted, by deploying Sybil vehicles on the packet forwarding paths in the network. In such a way, Sybil vehicles mislead other legitimate vehicles by modifying or truncating data packets before forwarding them.

2) Impersonation: This attack occurs when an attacker usurps the identity of a legitimate node/user to execute malicious actions [6]. An impersonation attack takes place

TABLE 5: Key characteristics of V2X attacks.

Attack type	Attacker model	Level of practical feasibility	Compromised security requirement(s)	Level of severity	Connectivity mode(s)	Communication technology	Layer(s)	Practical examples
Sybil	Active, Insider	High	Authentication	High	V2V	DSRC [109][110], ITS-G5 [111], LTE-V2X [112]	Application, Transport, Network, Data link	[113]
Impersonation	Active, Insider, Outsider	Low	Authentication, Integrity	High	V2V, V2I, V2N	LTE-V2X [112][114]	Application, Transport, Network, Data link, Physical	[115]
GPS spoofing	Active, Outsider	High	Authentication	Moderate	V2V	IEEE 802.11p, C-V2X [116]	Physical	[117]–[120]
Free-riding	Active, Passive, Insider	Low	Authentication	Low	V2V	N/A	Application, Transport	N/A
DoS	Active, Insider	High	Availability	High	V2V, V2I	ITS-G5 [111][121], DSRC [122], C-V2X [123][124]	Application, Transport, Network, Data link, Physical	[111] [121]–[124]
Jamming	Active, Outsider	High	Availability	High	V2V, V2I, V2N	DSRC [125][126], ITS-G5 [121], LTE-V2X [3]	Physical	[127][128]
Flooding	Active, Insider	Low	Availability	Moderate	V2V	ITS-G5 [129], LTE-V2X [12]	Application, Transport, Network	[129]
Spamming	Active, Insider	High	Availability	High	V2V, V2I	DSRC [47]	Application	N/A
Malware	Active, Insider	High	Availability, Authentication, Confidentiality, Integrity	High	V2V, V2I	DSRC [47]	Application	[130][131]
Eavesdropping	Passive, Insider	High	Confidentiality, Privacy	High	V2V	DSRC, C-V2X [132], [133]	Physical	[134][135] [136]
Traffic analysis	Passive, Insider, Outsider	Moderate	Confidentiality	Low	V2V, V2I	N/A	Data link	N/A
MitM	Active, Insider	Moderate	Confidentiality, Integrity, Authentication	High	V2V, V2I, V2N	C-V2X [137], DSRC [138]	Application, Transport, Network, Data link, Physical	[137][138]
Message modification	Active, Insider	Moderate	Integrity	Moderate	V2V	DSRC [110], ITS-G5 [121]	Application, Transport, Network, Data link, Physical	[139][140] [141]
Replay	Active, Insider	High	Integrity	Moderate	V2V, V2I	DSRC [109][110], ITS-G5 [121]	Application, Transport, Network, Data link	[142][143]
Masquerade	Active, Insider, Outsider	Moderate	Authentication, Integrity	Moderate	V2V, V2I	DSRC [47], C-V2X [3][144]	Application, Transport, Network, Data link	[144]
Illusion	Active, Insider, Outsider	Low	Integrity	Moderate	V2V, V2I	N/A	Application, Data link	[145]
Location tracking	Passive, Insider	High	Privacy	High	V2V, V2I, V2N	DSRC [47], LTE-V2X [3][114]	Network	[146][147]
Identity revealing	Passive, Insider	High	Privacy	High	V2V, V2I	DSRC [47], LTE-V2X [3][114]	Transport, Network	[146][147]



(a) False command to remote-driving function. (b) Map poisoning with falsified information. (c) Hazard data modification.

FIGURE 11: False data injection attacks in safety-critical V2X scenarios.

as a single-hop, and it usually targets a particular node. Each vehicle in the network has a unique identity, which is used to communicate with others and to verify the sender. Impersonation is a highly severe attack with the possibility of expanding to multiple layers in the protocol stack. For instance, a malicious vehicle may impersonate to make use of a V2X communication session without authentication, resulting in IP address spoof or TCP session hijack [151]. In V2V communication, a vehicle may broadcast safety-critical messages with malicious/selfish intentions to cause an accident or create a traffic jam, and then deny involvement in the incident before authorities by changing its identity. Such types of attack may thus be difficult to detect [150]. Moreover, impersonation can be identified as a realization of a Sybil attack if a malicious vehicle secretly changes its identity using the identities of compromised vehicles and causes an accident [100]. Adversarial V2X entities can threaten the authenticity of the system by impersonating vehicles, RSUs or base stations. The authors of [115] demonstrate a practical example of impersonation attack, by setting up a fake LTE eNodeB. The fake eNodeB pretends to be a real MNO, and forces UEs to attach to it. Nonetheless, the feasibility of launching this type of attack in V2X is low. Similarly, works in [112] and [114] demonstrate impersonation attacks through malicious vehicles by exploiting vulnerabilities that exist in the authentication process in LTE-V2X technology. The attacker uses the identification and certificate of the compromised genuine vehicle to launch an impersonation attack. The feasibility of such impersonation attacks caused by malicious vehicles in V2X is moderate.

3) GPS spoofing: In this attack, the attacker tries to drag victim vehicles off to incorrect positions through fabricated spurious signals. For instance, an attacker may generate false geolocation information without revealing the actual position and cause hidden-vehicle attacks [9]. GPS spoofing is also known as the tunneling attack in which an attacker injects fake position information using GPS simulators with stronger signals than weak signals from long-distance satellites. Such GPS signals may end up being accepted by victim vehicles with detrimental effects [117], [152]. A GPS spoofing attack is illustrated in Figure 11a where an attacker may influence the trajectory of a remotely operated automated vehicle to create a dangerous situation. Reported incidents (e.g, [117]–[120], [153]) manifest that this type of attack is practical with high feasibility. The lack of encryption and authentication in ordinary GPS signals enables an adversary to generate malicious GPS signals readily via software-defined radio platforms. Such malicious GPS signals can be verified via the location information retrieved from the base station [154]. However, security vulnerabilities that exist in IEEE 802.11p and C-V2X technologies can lead to geolocation data poisoning attacks in cases of verifying valid GPS satellite information via RSUs or base stations. [116], [154].

The severity of GPS spoofing attack is generally moderate, but it can be particularly critical for high-level AVs. The work in [118] demonstrates GPS spoofing in multi-sensor fusion algorithms used in AVs' context, materializing AV-specific "off-road" and "wrong-way" attacks; such attacks can cause the AV to drive off road or onto a wrong way, respectively. In a similar line, the authors in [120] inject selected fake GPS signals to drag the victim vehicle off to an incorrect pre-defined location, manipulating victim's road navigation system (e.g., Google Maps); such attack becomes more effective and serious against driver-less AVs. In [119], cybersecurity researchers experimentally demonstrate a GPS spoofing attack against Navigate-on-Autopilot (NOA) system of Tesla's Model 3 car, forcing the vehicle to exit the highway at the wrong location or comply with incorrect speed limit.

4) Free-riding: This type of attack is common in cooperative message authentication schemes, where a selfish user may exploit other user's authentication contributions without having its authentication. This type of attacker generally tries to benefit from the system without contributing its fair share, and the severity level of the attack is low. Such selfish behavior is called free-riding, and it is typically initiated by an active malicious user with fake authentication efforts [155]. In the case of passive attack, the attacker is not making any attempt of authentication; instead passively listens to the information sent by other nearby vehicles. Message authentication is the standard tool for ensuring information reliability, which includes data integrity and authenticity. However, an individual-based authentication service becomes inefficient when a vehicle receives numerous

messages in a short time period and subsequently performs verification per-message [155], [156].

Attacks on availability: Availability ensures that the network is functional and the services/information are available at any time for users. A set of example attacks of this category are given as follows.

1) DoS: In this attack, an attacker tries to prevent legitimate users from accessing the network and services [150]. DoS is a well-known attack that can exploit both vehicle OBUs and RSUs to jam and compromise the V2X network. DoS attackers send requests in higher frequency than the system can handle, resulting in extensive periods of network unavailability where legitimate users cannot be served. If DoS attacks are launched from spatially different physical locations, this results in the distributed DoS (DDoS) variant. DoS and DDoS attacks are considered severe threats as they could shut down or destabilize the whole network, causing harm for the safety of V2X users [9], [100].

Existing incidents (e.g., [111], [121]–[124]) demonstrate that DoS attacks can lead to real-world exploits with high feasibility. The study in [111] exhibits a wide range of DoS attack variants within an ITS-G5 network by combining various malicious attacks, e.g., DoS Sybil, DoS replay, and DoS disruptive. All DoS attacks are executed as active insider attacks, by generating excessive amounts of periodic beacon messages at a frequency higher than the limit set by the ETSI ITS standard. Another DoS attack implementation for ITS-G5 technology is presented in [121]. In this analysis, the attack is performed as an external jamming attack on a vehicle platoon resulting in a vehicle platoon disruption attack. Also, intelligent protocol-aware jamming attacks may carry out DoS attacks by targeting specific types of messages. The work in [123] presents protocol-aware stealthy DoS attacks against C-V2X communication technology. Two novel protocol-aware DoS attacks (i.e., targeted sidelink jamming and sidelink resource exhaustion) are demonstrated and validated by exploiting vulnerabilities of C-V2X slot-based PHY and MAC layer protocols. In a similar direction, [124] presents a novel set of DoS attacks against PC5-based (sidelink Mode 4) C-V2X communication. Three types of DoS attacks (i.e., oblivious, smart and cooperative) are introduced, exploiting the existing vulnerabilities in autonomous resource block selection process.

2) Jamming: In this attack, the attacker interferes with the communication channel using a strong radio frequency signal with an identical frequency, while occupying the channel with illegitimate traffic [157]. Jamming attacks are a special type of DoS attacks where an attacker attempts to disrupt the availability of the communication channel. For example, the strength of GPS signals from long-distance satellites is weak; hence, launching a jamming attack on GPS is easy, using stronger signals in the same frequency [117]. This attack, although common to any wireless communication system, can significantly delay mission-critical V2X traffic and degrade the network's reliability [14]. A jamming attack is typically limited by the communication range of the attacker's wireless device. Several existing works ([3], [121], [125], [126]) demonstrate jamming attacks that exploit security issues in DSRC, ITS-G5, and LTE-V2X communication technologies. The findings in [3] state that current LTE systems lack defense mechanisms to protect from radio frequency spoofing (also known as protocol-aware jamming) attacks. This attack can be realized by transmitting control signals and higher layer messages via a rogue LTE eNodeB ([115]) with relatively higher power levels than the legitimate eNodeB. Another jamming case is discussed in [121], where the attack deliberately disrupts a platoon of vehicles that communicate over ITS-G5 technology. In a similar direction, the work in [125] demonstrates testbed-driven experimentation of jamming attacks, exploiting PHY layer vulnerabilities of IEEE 802.11p-based DSRC technology. The work in [126] introduces a novel intelligent jamming attack, coined targeted discreditation attack, against vehicular misbehavior detection systems that rely on the IEEE 1609.2 security protocol. In this attack, the attacker aims to discredit the victim by corrupting its pseudonym certificates exchanged in periodic BSM messages in DSRC-based V2V communication, which results in message verification failures. Consequently, the victim's certificate may eventually be revoked from the network due to the degraded reputation.

Intentional jamming attacks against on-board sensors may lead to severe safety-critical road incidents. The Tesla Model S crash against a tractor trailer raises the concern that existing on-board sensors cannot yet reliably detect neighboring vehicles [158]. Successful jamming attacks against three essential sensors of AVs (i.e., ultrasonic, millimeter-wave radars (MMW) and cameras) are shown in [128]. They use ultrasound against ultrasonic sensors, radio against MMW radars, and laser against cameras to jam and compromise the vehicle. In [128], the Tesla Model S's self-parking and summon function are jammed by continuously emitting ultrasound at the parking sensor using off-the-shelf 40kHz transducers; this causes the sensor to lower its signal-to-noise ratio level and makes objects undetectable. The ultrasonic noises generated in jamming attacks cause continuous vibration on the sensor membrane, rendering distance measurements impossible. A similar type of jamming attack is launched in [127] using off-the-shelf 40kHz transducers. They validated jamming attacks on 11 standalone ultrasonic sensors in the laboratory, and on the on-board sensors of 7 vehicles, including the self-parking and summon features of the Tesla Model S.

3) Flooding: In this attack, an attacker generates bogus messages to drain network resources, e.g., bandwidth, power and CPU, out from legitimate users. Although bogus messages are not considered part of the actual network traffic, they could be received by V2X nodes (OBUs and RSUs), rendering them unable to handle a large volume of incoming data [8], [100]. A flooding attack can be launched at multiple

layers of the V2X protocol stack. Flooding attacks on the control and data planes of 5G SDN networks may create a large set of forwarding rule requirements and overflow the limited flow tables of SDN switches, respectively [159]. The work in [129] demonstrates a practical network layer flooding attack exploiting vulnerabilities in ITS-G5 communication technology. Forwarding parameters of keep-alive forwarding mechanism are manipulated to flood the network with malicious DENM messages, triggering neighboring vehicles to forward DENMs as well. Moreover, the IEEE 802.11p MAC layer is vulnerable to flooding attacks where an attacker may exploit the binary exponential back-off scheme to send data constantly to flood the channel [12]. Similarly, LTE-V2X systems are vulnerable to flooding attacks. Flooding attacks can be launched by targeting the victim UE in two ways [12]: *i*) the attacker may use resource scheduling information to transmit uplink control signals when the victim UE uses the channel to cause conflicts at the eNodeB; *ii*) the attacker may inject packets when the victim UE is in active mode while the transceiver turned off to save power. Such incidents may force genuine UEs to detach from the eNodeB without sufficient network resources.

4) Spamming: In this attack, numerous spam messages are injected by an attacker into the network, which eventually becomes prone to resource collisions due to bandwidth consumption [160]. As an example, spamming messages (i.e., advertisements) by marketers may inject into the network with the objective of gaining lucrative benefits [47]. For this purpose, the marketers who are insiders may acquire RSUs or OBUs to distribute such content while unnecessarily consuming bandwidth and causing transmission delays for the genuine messages. There is particularly a risk of increasing the transmission latency of mission-critical V2X traffic, and the severity level of spamming attacks is high. Spamming attacks can be often difficult to contain due to the distributed nature of V2X networks.

5) Malware: An attacker injects malicious software components, such as viruses or worms, into OBUs and RSUs. Such an injection may occur during periodic software and firmware updates [47]. Malware attacks are more likely to originate from rogue insiders who may gain access to software and firmware. A malware attack could lead to malfunctioning components of the V2X network, inflicting serious damage to the normal system operation. The objective of this type of attack is to impede accessing a device, by compromising the availability security feature. Ransomware is a type of malware attack that hinders access to the device or the data stored in the device. For instance, massive distribution of ransomware can take place by injecting malware in multimedia and Internet traffic [161].

Malware attacks have been identified as serious threats to V2X security and safety of V2X users. Such attacks are usually launched at the application layer and are shown to be practical. In [130], cybersecurity researchers demonstrate a remote malware injection attack, coined “TBONE”, in the Tesla S, 3, X and Y models. They exploit the vulnerabilities of the Internet connection manager in Tesla cars to load new Wi-Fi firmware. The attacker becomes capable of controlling in-vehicle infotainment system, including modifying steering and acceleration modes, among others. The work in [131] shows that the boot security of Nvidia system on chip, used in Tesla’s autopilot and Mercedes-Benz’s infotainment system, can be circumvented using voltage fault injection attack. Such an attack can inject and execute malicious software components and cause safety-threatening situations.

Attacks on confidentiality: Any violation involving disclosure of confidential information to unauthorized entities can lead to such malicious attacks. A set of attacks falling under this category are discussed below.

1) Eavesdropping: This attack aims at extracting or inferring sensitive information (e.g., security keys, user identity, vehicle location) from protected data [10], [162]. Eavesdropping represents a usual threat to wireless communication technologies, and it constitutes a simple attack to launch since the attacker is passively listening to the communication link between legitimate users. An eavesdropping attack could compromise privacy in addition to confidentiality. The attacker could exploit periodic broadcast safety-related messages [132] or the control signals exchanged between base stations or RSUs to vehicles via V2N/V2I links [133]. Eavesdropping is difficult to detect, as the victim may not be aware of the underlying threat. Moreover, passive eavesdropping may be the initial step towards other more sophisticated attacks, e.g., black hole and DoS, with severe impact on the network performance [100].

The realization of eavesdropping attacks reveals serious vulnerabilities, affecting millions of connected and automated vehicles worldwide [134]. The authors in [135] present eavesdropping attacks on the wireless remote keyless entry (RKE) system used in Volkswagen (VW) Group, affecting 100 million vehicles. By reverse-engineering the firmware of the ECUs used in RKE, they show that cryptographic algorithms and keys can be recovered from the ECUs. Using a clone of VW Group remote control, the attacker is able to infiltrate a vehicle by eavesdropping a single signal sent by the original remote of the RKE system. The study in [136] demonstrates eavesdropping attacks on a moving car from a 40m distance. They have captured and analysed raw signal data between sensors and the ECUs of tire pressure monitoring system (TPMS) using GNU radio together with a commercial universal software radio peripheral unit. The performed eavesdropping attacks reveal that *i*) the TPMS protocols do not use cryptographic mechanisms; and *ii*) TPMS transmits a fixed 32-bit sensor identifier in each packet that can potentially lead to privacy attacks (e.g., vehicle tracking). These practical examples manifest that eavesdropping attacks can lead to severe real-world exploitation.

2) Traffic analysis: In this attack, the attacker passively listens to the transmission of messages and then performs traffic analysis to infer useful information about vehicles and communication patterns [162]. This sophisticated attack, also known as stealth attack, is considered a dangerous threat that can violate confidentiality requirement [163]. The severity of this type of passive attack can be considered low in safety-critical situations.

3) MitM: This attack occurs when a malicious node listens to the communication between two vehicles (V2V) or between vehicles and infrastructure (V2I/V2N). The active attacker may inject false information into the channel, drop and/or delay messages [138]. In the case of passive attacker, the attacker may eavesdrop on the communication channel between legitimate vehicles (e.g., ambulances, police vehicles). As the name suggests, the attacker sets up in the middle and can gain control of the communication link; however, communicating vehicles would still assume that their communication remains private [9]. For example, an attacker may attempt map poisoning, as shown in Figure 11b, by injecting false content (e.g., alter/remove road signs) into the map database resulting in unavailability of the necessary information and/or wrong maneuvers.

In [137], two cybersecurity researchers demonstrate MitM attacks on the Jeep Cherokee. This attack was realized by exploiting the cellular network interface of the Jeep, and was able to seize control of the vehicle (e.g., kill Jeep's engine) through the infotainment system. Another set of MitM attacks are presented in [138] with several active attack scenarios in VANET. The study demonstrates that MitM attacks bring severe risks in VANET by intercepting or tampering messages exchanged between legitimate nodes. MitM attacks are multi-layer and can target all layers of the V2X protocol stack. This type of attack is considered to be moderately feasible, but can cause severe safety-threatening situations. These examples exhibit that the vulnerabilities present in DSRC and C-V2X-based communication technologies may lead to MitM attacks.

Attacks on integrity and data trust: There are several types of attacks in this category that aim to manipulate the exchanged information. Representative attack examples are described in the following.

1) Message modification: This attack is also known as message fabrication or tampering attack, where an attacker either tries to modify or alter a part of the original message to be transmitted [8]. Traffic safety applications are based on V2X messages (e.g., BSM, CAM) broadcast by vehicles. These messages are usually in standardized format (with no encryption) to allow being read by all participating vehicles. Hence, such V2X applications can easily be a target for modification attacks based on self-interest or malicious objectives. For example, an attacker may modify the congestion data of a clear road to indicate that the road is heavily congested (i.e., hazard warning), causing other vehicles to change their driving paths. In other cases, a rogue insider may attempt to inject false traffic information into warning messages, or a MitM attacker may inject false traffic-safety messages into the network [47]. Another example of a modification attack is illustrated in Figure 11c, where an attacker modifies the message content of a legitimate vehicle (i.e., "slow-down") with misleading information (i.e., "speed up"). In a similar direction, the works in [110], [121] demonstrate message fabrication attacks for the IEEE 802.11p-based DSRC and ITS-G5 technologies, respectively. In [121], the attacker modifies the acceleration parameter similar to the scenario presented in Figure 11c.

The work in [139] demonstrates bogus information attacks based on false or fabricated data injection. In this type of attack, the attacker possesses multiple malicious nodes spread across multiple wireless hops. The attacker sends several wrong packets with small errors to go undetected over the security checks, and then, executes the bogus information attack with the overall accumulation of errors. Falsified BSM data injection attacks using a traffic signal control (TSC) system are introduced in [140]. In this type of attack, the attacker exploits the control logic of the TSC system (with broadcast BSMs and signal timing messages of RSUs) to broadcast falsified BSMs via a compromised OBU. Through GPS spoofing, an attacker can inject fabricated position information using GPS simulators, causing the victim vehicles to accept bogus information [117]. All aforementioned examples show that message modifications are practical attacks and can cause safety-critical issues in V2X.

2) Replay: As the name suggests, an attacker re-transmits or replays already transmitted valid data and tries to exploit the conditions that existed at the time of the original message transmission [100], [162]. Thus, the attacker's objective remains realistic as long as the original data remains valid. Replay attacks can be either location-based or time-based [14]. In particular, an attacker stores an authentication message at location l_1 and replays it immediately to a neighboring location l_2; similarly, an attacker captures a valid message at time t_1 and replays it to the same location at time t_2. To execute such replay attacks, an attacker needs to be located in the communication range of other vehicles. Furthermore, excessive message replays could also lead to DoS attacks [164]. Existing works (e.g., [109], [110], [121]) highlight security issues in V2X communication technologies that can exploit to execute replay attacks. The work in [109] presents data replay attacks launched by rogue insiders in a DSRC-based V2V communication setup. It further demonstrates that replay attacks can be executed in Sybil mode while frequently changing the attacker's identity. Another work in [121] discusses an implementation of a replay attack on a vehicle platoon for ITS-G5 communication technology. In this attack, the attacker tries to disrupt a platoon of vehicles by re-transmitting captured data from the platoon communication.

The work in [142] demonstrates replay attacks against a Mitsubishi Outlander PHEV, exploiting the unsecured Wi-Fi access point on the vehicle to extract keys. The attacker then remotely performs various actions (e.g., drain battery, switch off theft alarm) by replaying various messages from the mobile app of the vehicle. Replay attacks could be launched in conjunction with other attacks, such as eavesdropping, MitM and jamming. For example, the attacker in [143] performs a replay attack jointly with a jamming attack. In particular, the attacker jams radio frequency signals from the wireless keyfob, and records the latest valid code to replay and unlock the car. However, this type of attack is not effective against modern vehicles due to the adoption of rolling codes for the wireless keyfob. In principle, replay attacks may target multiple layers in the protocol stack. The severity of replay attacks is generally moderate, but it can be safety critical for high-level AVs (e.g., in vehicle platooning).

3) Masquerade: An attacker uses a valid ID of another vehicle to pretend and get unauthorized access to the resources [162]. For example, an attacker may pretend to be an emergency vehicle and force other vehicles in front to change their lanes or reduce their speed. This kind of attack may be triggered either by an insider or an outsider [8]. In masquerade attacks, message fabrication, alteration and replay may also be involved, affecting V2X communication at multiple layers. An outsider may disguise as a legitimate node (e.g., an OBU) using a valid ID and launch various other attacks such as black holes or false data injection [47]. Similarly, a rogue insider may masquerade as another OBU or RSU, and inject fabricated messages to render another entity responsible. As shown in Table 5, existing studies (e.g., [3], [47]) reveal that security vulnerabilities that exist in V2X communication technologies, e.g., DSRC and C-V2X, may enable real-world exploits to instigate masquerading attacks. In [144], a successful masquerading attack is launched on Jeep Cherokee, by controlling the collision prevention system in the vehicle. These examples show that masquerading attacks can be practical and cause safety-critical issues.

4) Illusion: In this attack, a vehicle adversary could directly control and trick its own sensors to broadcast information of a non-existent event, based on self-interest or malicious objectives. Illusion attacks may harm V2X applications through malicious behaviors, such as injecting fake information or fabricating exchanged messages, replaying messages to pretend located at a fake position, or spoofing IDs of legitimate nodes [165]. Such illusions can lead to dangerous vehicle collisions, traffic congestion, and also degrade the actual network performance by consuming unnecessary radio resources.

The study in [145] presents an illusion attack against VANET. In this attack, the adversary targets traffic-safety applications to create favorable traffic conditions for its own benefits. In the realization of the attack, the adversarial vehicle first achieves the prerequisite traffic situation (e.g., rush hour or mass traffic in the front). It then broadcasts fraud messages to convince other vehicles to react to a non-existent road incident (e.g., accident or dead end) causing an illusion. Nonetheless, the authors do not provide an implementation of this attack in a simulator. Illusion attacks may target multiple layers (e.g., application and data link) in the V2X protocol stack. This kind of attack may cause safety-threatening issues in autonomous driving scenarios.

Attacks on privacy: These attacks comprise any violation or threat exposing the privacy of drivers and other V2X users. In what follows, two widely identified privacy attacks are described.

1) Location tracking: This attack aims at tracking the location of a vehicle and its driving path over a period of time [166]. Location-based services (e.g., locating the closest gas station or a restaurant recommendation) offer valuable information for vehicle users as long as their locations are shared. Current location-based services (LBS) require users to continuously send their location information to an edge server offering a service at a specific area, which, in turn, may lead to critical issues for users, e.g., physical harm, if the server is compromised [167]. Furthermore, the works in [3], [47], and [114] reveal that continuous broadcast messages from OBUs in cases of safety situations or LBS services offered over V2X communication (e.g., DSRC, LTE-V2X) may enable attackers to extract location information. The work in [146] present privacy attacks by injecting a malware payload through a Trojan-horse app onto an Android-based vehicle infotainment system. Using the malicious app, the attacker is able to connect to the in-vehicle network, granting access to smart devices (e.g., smartphones) connected to the infotainment radio system. This, in turn, allows the adversary access activities of the driver (e.g, sending messages, emails, surfing the Web) as well as retrieve voice recordings and the GPS coordinates. Such software vulnerabilities could lead to real-world exploitation.

In [147], a software vulnerability in Hyundai Motor's Blue Link mobile app (compatible also with newer Hyundai vehicles) is reported. The app is used for remote access of the vehicle. Security researchers argue that an attacker could exploit a vulnerability in the Blue Link application software over an insecure Wi-Fi connection, or via a MitM attack. Once the exploitation is realized, a remote adversary could gain access to insecurely transmitted privacy-sensitive information, and then remotely locate the vehicle. These examples show that the feasibility of launching adversarial privacy attacks appears to be high, potentially causing high security and safety issues.

2) Identity revealing: In this attack, an attacker tries to disclose the ID information (e.g., name, address, license number and public-key certificate) which can be linked to the owner of a vehicle [166]. For example, an IMSI catching attack can be launched by an eavesdropper requesting the long-term subscriber ID of a mobile device in

the 5G network [168]. As mentioned before, attackers may exploit location information gathered over time to extract the identities of certain individuals ([3], [47], [114]). Furthermore, previously described attacks in [146], [147] allow an adversary to extract private information of the driver. For example, an adversary may access emails, messages and voice recordings of the driver using a malicious app connected to the infotainment system, and disclose sensitive information for additional attacks [146]. Similarly, an adversary in [147] could capture private information (e.g., usernames, passwords and PIN numbers) by exploiting the Blue Link mobile of the Hyundai vehicle. These practical examples demonstrate that software vulnerabilities can become easy-to-exploit interfaces for malicious attacks.

D. Summary

As thoroughly discussed in previous sections, each attack variant behaves differently while potentially compromising several security/privacy requirements simultaneously. As an example, GPS spoofing can be executed in different forms across different sites in conjunction with jamming or message modification attacks [169]. Similarly, DoS and replay attacks can be executed in Sybil mode resulting in DoS Sybil and replay Sybil attack variants, respectively [109]. The attack model variability and the non-deterministic nature of attacks' execution result in an unprecedented evolving threat landscape for V2X systems. Multiple layers of security are thus necessary for the detection and prevention of V2X attacks, since one-size-fits-all security approaches are rendered insufficient.

IV. Proactive Security in V2X Communication

In the context of V2X communication, existing security solutions can be classified into two categories, i.e., *proactive* and *reactive* defense mechanisms. Proactive approaches tend to preemptively identify V2X security weaknesses and provision security measures to identify threats before they occur. On the other hand, reactive approaches involve responding to V2X security incidents after their occurrence. Figure 12 illustrates a fine-grained taxonomy of proactive and reactive defense mechanisms for secure V2X communication presented in Sections IV and V, respectively. By individually discussing proactive and reactive defensive schemes, we aim to reveal the advantages and pitfalls of each approach, as well as identify limitations which give rise to emerging security enhancements relying on AI/ML paradigm (Section VI).

This section compiles proactive security solutions from related literature, which aim at avoiding attacks from outsiders. V2X applications rely on data exchange between vehicles, and between vehicles and other road side entities. Besides the confidentiality of shared information [43], it is also imperative to provide data integrity, sender authenticity and non-repudiation, for which standardization bodies (i.e., ETSI and IEEE) mandate proactive security mechanisms, e.g., public-key infrastructure (PKI) [42], [43]. Proactive approaches usually enforce security policies, such as authenticity and integrity checks, using digital signatures and authorization for services through access control [200]. Therefore, any security mechanism using PKI, digital signatures/certificates, proprietary (non-public) protocols with customized hardware, or tamper-proof hardware modules can be classified as proactive mechanisms.

We hereinafter provide an extensive overview of proactive defense mechanisms, by fine-grouping them into three main classes according to the taxonomy shown in Figure 12: *i*) cryptography-based (Section IV-A), *ii*) physical layer security (Section IV-B), and *iii*) privacy preservation (Section IV-C). Table 6 provides a comprehensive summary of the key characteristics of proactive solutions.

A. Cryptography-based Security

Authentication of network participants and messages is considered as the first line of defense against various malicious attacks (e.g., DoS, Sybil, impersonation) which can cause traffic disruptions and even destabilize the V2X communication system. Relevant works (e.g., [3], [11], [16]) suggest that many adversarial attacks (e.g., DoS, impersonation, MitM, message replay, and Sybil) can be thwarted using cryptography-based authentication and integrity protection schemes. A recent survey in [14] reviews key security issues concerning V2X communication platforms in the scope of insider and outsider attacker models. Pertinent to other works [3], [10], [11], the authors of [14] underline that the majority of authentication schemes for outsider attacks mitigation are cryptography-based, and these schemes ensure authenticity, availability, confidentiality, and message integrity security requirements. It is worth noting that authentication is an integral part of V2X security and thwarts most security attacks (Section III-C) that originate from outsiders.

In what follows, we elaborate on the use of different cryptographic techniques mainly focusing on authentication and integrity protection, highlighting their characteristics along with limitations and performance-related issues. The categorization is performed according to three widely used types of cryptographic primitives: asymmetric (PKI-based), symmetric and identity-based cryptography [8], [9], [15].

PKI-based asymmetric cryptography. A PKI is a security service acting as a trusted third-party for managing public keys and binding users while guaranteeing C-ITS security. Typically, a PKI consists of computer systems, policies and people that create, manage and revoke public-key certificates [201]. Both ETSI ITS (Europe) [43] and IEEE 1609.2 (US) [42] standards recommend the PKI-based approach to provide security for all V2X safety applications. In particular, both standards mandate the use of ECDSA for digital signatures to achieve fast authentication and non-repudiation at the cost of computationally expensive operations [202].

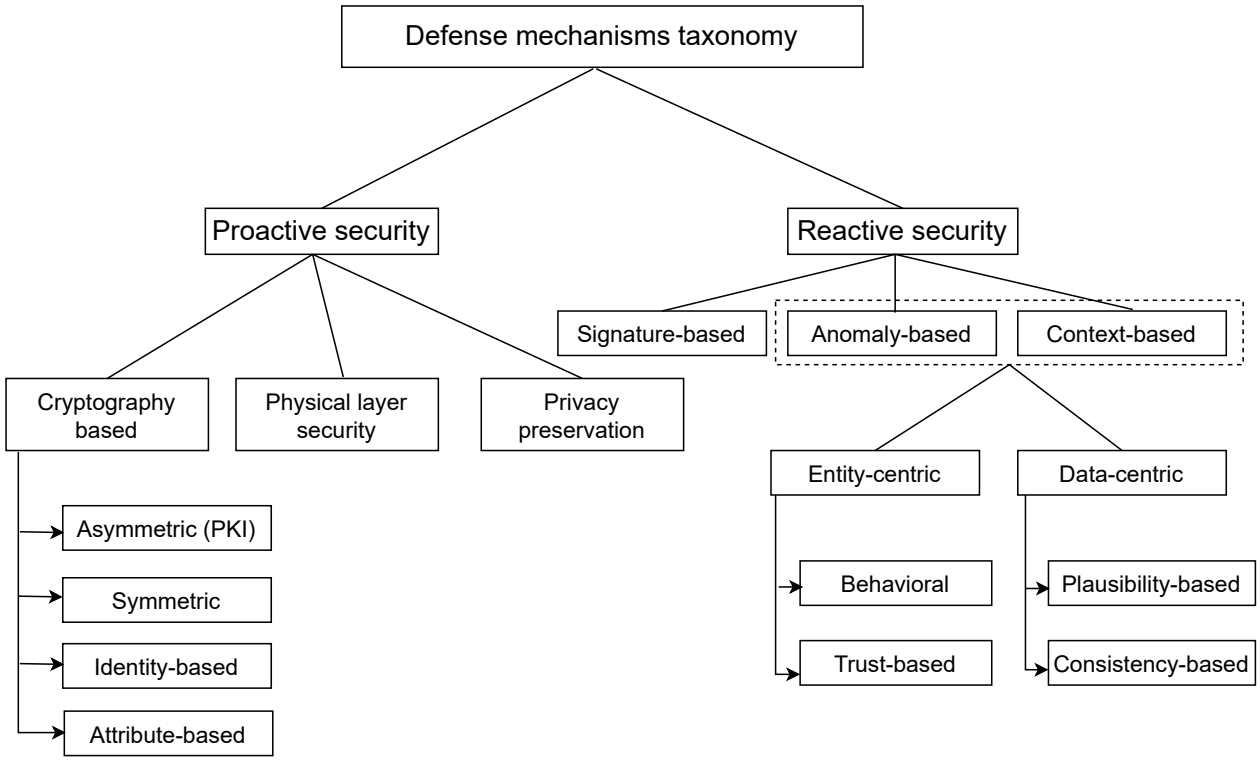


FIGURE 12: A taxonomy of defense mechanisms for state-of-the-art security approaches in V2X communication.

The major standards developing organizations, such as IEEE, SAE and ETSI, have converged to the use of V2X security architectures based on PKI for credential and identity management [43], [203].

The general PKI architecture comprises the following key elements: *i)* root CA (RCA), *ii)* Pseudonym CA (PCA), *iii)* Long-Term CA (LTCA) and *iv)* hardware security module (HSM). An RCA is the root at top of the certificate chain, hence, a trust anchor that verifies the identity of V2X entities (i.e., vehicles, RSUs). The certificate of the RCA is self-signed and is distributed to users. It contains user's public key and additional information such as validity and permissions. Additionally, the RCA issues certificates for PCA and LTCA entities. The PCA is responsible for issuing pseudonym certificates to V2X entities. These short-term certificates do not contain any user identifiable information, and are reduced to a minimum size to be efficient. The LTCA is entrusted to manage long-term certificates of V2X entities, including user identifiable information. An HSM is used for in-vehicle certificate storage, and manages the life-cycle of cryptographic keys while securing the issued certificates and private keys.

Figure 13 illustrates a high-level vehicular PKI implemented for secure V2X communication within the European project *PRESERVE* [204]. V2X nodes (i.e., vehicles and RSUs) request certificates from the PKI, and are equipped with a unique key and a corresponding long-term certificate. Short-lived pseudonym certificates are used to sign messages by vehicles. When a vehicle is involved in an accident or misbehavior, certificate revocation lists (CRLs) are updated by PCA and LTCA with the status of revoked certificates (pseudonym and long-term), and CRLs are made publicly available for V2X entities. The security architecture of *PRESERVE* is ECDSA digital signatures-based PKI. The OpenSSL [205] library is used to implement cryptographic operations such as ECDSA and transport layer security (TLS) tunnels. The former are used to secure V2I and I2I communication, while CAs are implemented utilizing OpenCA framework [206]. In-vehicle HSM storage is realized using physical unclonable functions [207]. In a similar direction, the works in [44], [208], [209] implement and evaluate PKI-based approaches for secure vehicular communication. Furthermore, the authors of [18] present an extensive review of vehicular PKI schemes, including different architectures adopted (e.g., ETSI ITS and IEEE 1609.2) and evaluation metrics (e.g., trust, security, privacy, and availability). Also, the study provides classifications for existing vehicular PKI schemes (e.g., SCMS [44], *PRESERVE* [204], VeSPA [208], SEROSA [209]) based on credentials management mechanism and the credential revocation mechanisms based on different data structures, i.e., CRL-based, online

TABLE 6: Summary of proactive security mechanisms with their key characteristics

Paper	Methodology	Attack/Threat type	Connectivity mode(s)	Communication technology	Validation technique(s)	Major limitation(s)
[44]	PKI with butterfly keys cryptography for signing and encryption.	False message injection, Identity revealing, Location tracking	V2V, V2I	IEEE 802.11p (DSRC)	Field trials	Overhead of large certificate revocation lists. Lacks misbehavior detection mechanisms. Storage issues on OBUs due to large number of pseudonym certificates.
[170]	PKI with ECDSA and ECIES cryptographic algorithms.	False position, Replay, DoS	V2V, V2I	IEEE 802.11p (ITS-G5)	Testbed evaluation	Latency overhead at scale in pseudonym issuance and certificate revocation list distribution. Latency overhead due to per-message-verification by recipients.
[171]	PKI with ECC-based DAA cryptography and trusted computing on OBUs.	Identity revealing, Location tracking	V2V, V2I	IEEE 802.11p (ITS-G5)	Design framework	Trusted computing usage on OBUs creates a trust issue.
[172]	PKI with Bayesian game theory and learning automata.	Replay, Mis-authentication, DoS	V2V, V2I	IEEE 802.11p (DSRC)	Theory, Simulation (NS-2 [173])	Performance bottleneck in dense V2X scenarios. Trust value exploitation of group members.
[174]	Symmetric cryptography (MAC algorithms) with ECDSA signatures and *TESLA++* protocol.	Computation and memory-based DoS	V2V	IEEE 802.11p (DSRC)	Simulation (NS-2 [173])	Packet losses and packet reception delays affect message authentication and lead to safety issues.
[175]	Symmetric cryptography with Bloom filters and TESLA protocol.	DoS, Masquerade, Sybil, Message modification	V2V	IEEE 802.11p (DSRC)	Simulation (NS-3 [176] and SUMO [177])	Performance limitation in grouping of neighboring vehicles (for k-anonymity privacy) at moderately high vehicle speeds with short time periods.
[178]	Identity-based cryptography with batch messages verification using Cuckoo filter and binary search.	Identity revealing, Impersonation, Replay	V2V, V2I	IEEE 802.11p (DSRC)	Theory, Simulation (C++ based simulation)	Batch verification overhead at the RSU at high vehicle density. Vulnerable to attacks such as DoS and Sybil.
[179]	Identity-based cryptography with anonymous dynamic identities' generation via on-board smart cards.	Impersonation, Identity revealing	V2V	IEEE 802.11p (DSRC), C-V2X	Simulation (VanetMobiSim [180])	Vulnerable to side channel attacks on smart cards. Communication and computation overhead at high vehicle density.
[181]	Identity-based cryptography with RSU-assisted message verification and broadcast.	Fabrication, MitM, Replay, Sybil	V2I	IEEE 802.11p	Simulation (N/A)	RSU-based message verification and broadcast incur delays in safety scenarios.
[182]	Identity-based cryptography with computation and verification offload to RSUs.	Impersonation, Identity revealing	V2V, V2I	N/A	Theory (Empirical evaluation on OBUs)	Bilinear pairing computation delays affect real-time safety situations.
[183]	Identity-based cryptography with Paillier and ECIES encryption and ECDSA signature.	Replay, Modification, Identity revealing	V2V, V2I	IEEE 802.11p (DSRC)	Simulation (Veins [184])	Vulnerable to vehicle tracking when same pseudonyms are used over fixed lifetime.
[185]	Identity-based cryptography with biological-password-based two-factor authentication.	Modification, Replay, DoS, Identity revealing	V2V, V2I	IEEE 802.11p (DSRC)	Formal analysis (ProVerif [186]), Simulation (ONE DTN [187])	Relies on ideal tamper-proof devices on OBUs. Batch verification of multiple signatures is not considered.

Continued on next page.

certificate status protocol-based, tree-based, activation code-based, and distributed ledger-based.

PKI-based solutions yield strong security while providing message authentication, data integrity, non-repudiation, and group-based communication, albeit exhibiting performance drawbacks. According to ETSI ITS specifications [43], almost every single message is verified by recipients for sender identification at the expense of communication and computation overhead. Although not ideal for mission-critical V2X applications, message verification provides additional

Paper	Methodology	Attack/Threat type	Connectivity mode(s)	Communication technology	Validation technique(s)	Major limitation(s)
[188]	Identity-based message authentication with ECC (batch verification).	MitM, Replay, Modification, Impersonation	V2V, V2I	LTE-V2X	Cryptographic analysis (MIR-ACL [189]), Simulation (NS-3 [176])	Lacks mutual authentication. Increased message delays at high vehicle density scenarios.
[190]	Study effectiveness of changing pseudonyms based on cryptographic mix-zones.	Eavesdropping, Location tracking	V2V	N/A	Simulation (SUMO [177])	Changing pseudonyms at higher frequencies induces overhead through cryptographic operations.
[191]	Random change of pseudonyms at predetermined locations of cryptographic mix-zones.	Impersonation, Location tracking, Replay	V2V, V2I	IEEE 802.11p	Simulation (MATLAB)	Unlinkability between the vehicle and its pseudonyms is low in individual mix-zones. Vulnerable to misbehavior attacks from insiders.
[192]	Pseudonyms change within cryptographic mix-zones, together with fictive chaff messages broadcast.	Identity revealing, Location tracking, False data injection, Replay	V2V, V2I	IEEE 802.11p (ITS-G5)	Simulation (Veins [184] and SUMO [177])	Longer chaff traces and active chaff pseudonyms outside mix-zones introduce increased overhead.
[193]	Random silent period between pseudonyms change and creating groups.	Impersonation, False data injection, Location tracking	V2V, V2I	IEEE 802.11p (DSRC)	Analytical evaluation, Simulation (N/A)	Silent periods negatively impact periodically broadcast messages in safety applications.
[194]	Anonymous group message authentication using MAC and group signature.	Vehicle trajectory tracking	V2V	LTE-V2X	Cryptographic analysis (MIR-ACL [189]) and Simulation (N/A)	Lacks an evaluation to determine the feasibility of the approach. Vehicles share the common MAC group key to generate MAC codes within the same group.
[195]	Anonymous batch authentication and integrity preservation protocol.	Password-guessing, MitM, Privileged-insider, Impersonation, Replay	V2V, V2I	IEEE 802.11p (DSRC)	Analytical evaluation, Simulation (N/A)	Vehicles receive their private keys offline, which complicates revocation. Vulnerability to forgery attacks. Pseudo-IDs are not part of the signature verification.
[196]	Differential privacy in location-based services deployed on the edge node.	Location tracking	V2I	IEEE 802.11p (DSRC), LTE-V2X	Theory, Application development (custom Java application)	Susceptible to edge node vulnerabilities or eavesdropping attacks.
[197]	ABE scheme using techniques including binary tree structure, key embedding and signature of knowledge.	Replay, Forging, Tampering	VANET	N/A	Simulation (CHARM [198])	Computation and communication costs are high due to more bi-linear pairing and ECC operations. Vulnerability to MitM and Sybil attacks.
[199]	ABE-based scheme considering various road situations as attributes, used as encryption keys to secure the transmitted data.	False data injection, Impersonation, Replay	V2V, V2I	IEEE 802.11p (DSRC)	Simulation (N/A)	The scheme may suffer from DoS attacks. Collusion resistance under strong security requirements, misbehavior detection and revocation need to be further explored.

security. In this context, *PRESERVE* proposed the deployment of a PKI-based V2X security system based on ETSI ITS architecture and evaluated its performance [170]. The *PRESERVE* implementation is compatible with IEEE 1609 and ETSI certificate formats, and both infrastructure and vehicle certificates are based on ECC-256 keys. The evaluation is focused on pseudonym requests by vehicles, pseudonym issuance by the CA and CRL distribution. Yet, security vulnerabilities exist in ETSI ITS security framework [164]; message replay attacks, which can turn into DoS attacks, may target the initial communication between a vehicle and the roadside infrastructure. On the other hand, IEEE 1609.2 standard verifies messages on-demand and only when a warning is generated [210], as most of the periodic messages will not result in warnings. However, on-demand verification may not entirely alleviate overhead since the relevance of a message is only revealed at the application layer.

Similar to ETSI ITS framework, the security credential management system (SCMS) has been recently developed in the US as a proof-of-concept for secure V2X commu-

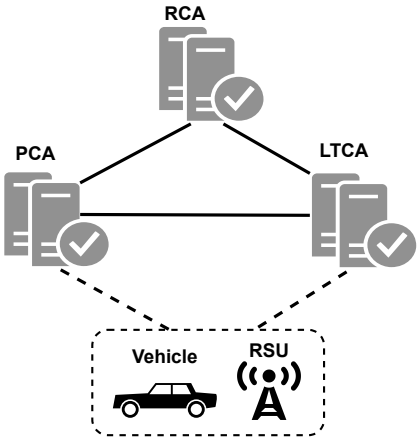


FIGURE 13: Schematic of a generic vehicular PKI (source [204]).

nications [44]. SCMS aims at supporting the establishment of a nationwide system by adopting a PKI-based approach, which is designed to be scalable with the number of vehicles. It provides security solutions for V2V and V2I communications while protecting the content of safety messages through authentication and encryption mechanisms. In particular, SCMS is able to issue approximately 300 billion certificates yearly for 300 million vehicles at its full capacity. The SAE J2945/1 standard [45] adopts the PKI-based SCMS. One of the drawbacks of SCMS is that the revocation mechanism may lead to large CRLs; as a result, it impacts the bandwidth usage and processing latency. Overall, SCMS lacks a performance balancing policy, as well as mechanisms for detecting misbehaving vehicles.

Although the security performance of a PKI system is strong, its scalability is rather limited due to the inherent centralized architecture. The existence of interoperability issues that usually arise in large-scale multi-domain automotive environments further exacerbates the scalability potential. To alleviate the limitations of the centralized setup, the authors in [171] propose a decentralized PKI-based approach by shifting the trust of PKI systems to the edge of the network and, at the same time, freeing the need for a dedicated centralized trust anchor entity. Furthermore, they propose a trusted computing technology within vehicles as trust enabler, leveraging direct anonymous attestation (DAA) cryptographic primitives. In this way, vehicles can become trusted entities and generate their own pseudonym certificates independently of a central authority. However, trust on the edge is still in its early stages; thus, the efficiency and practical feasibility of such distributed frameworks remain to be fully validated.

In a similar direction, the work in [172] proposes an efficient decentralized PKI to handle security in vehicular networks, leveraging the Bayesian coalition game and learning automata concepts. The coalition between vehicles is formed based on the trust value and duration of the stay of the vehicles in the coalition. If the trust value of a vehicle goes beyond a predefined threshold, then the certificate may be revoked by the CA. The proposed scheme provides authentication and message integrity while protecting from replay and internal/external revocation-DoS attacks. Based on simulation results, the authors demonstrate that their scheme exhibits superior performances in terms of verification, communication cost and packet delivery ratio, compared to benchmark schemes in its category. Nevertheless, the scheme may suffer from performance bottlenecks due to the high density of vehicles in urban areas. In addition, privacy issues could arise causing the certificate owner to be tracked, while a set of rogue insider attackers may abuse the trust value scheme by forming a coalition.

V2X communication entails certain authentication requirements that need to be satisfied:

- Low computation and communication overhead;
- Strong and scalable authentication;
- Provisions for re-authentication and revocation in the event of security breaches.

Although PKI systems exhibit robust security performance, complex cryptographic operations impose additional overhead on communication and computation, degrading network performance [209], [211]. Hence, lightweight authentication schemes have been identified as efficient countermeasures to alleviate computational and communication complexities [162]. Striking a balance between network performance and effectiveness of security solutions is particularly important. In this context, the work in [101] performs an analysis of the trade-offs among security, safety and network performance. The results reveal an increased message delay and throughput reduction with the introduction of an authentication scheme. It is noted that not all V2X messages possess the same level of sensitivity to security and privacy; therefore, adaptive security models would be needed to configure different parameters of the security policies based on the sensitivity of supported V2X services.

Symmetric cryptography. Symmetric cryptographic algorithms are commonly used for data encryption and message integrity checks. In particular, symmetric algorithms exhibit performance advantages over asymmetric ones since they often require fewer memory resources and incur less communication and computation overhead [3]. In addition, symmetric schemes are, in principle, decentralized and do not depend on the underlying infrastructure. However, they do not provide equivalent security levels as asymmetric solutions, while being limited only to pairwise communication (e.g., V2V/V2I). If the secret key is revealed, the symmetric cryptosystem becomes compromised due to its complete reliance on the same shared secret key between communicating parties.

The 3GPP networks adopt the symmetric-key based MILENAGE cryptographic algorithm set (detailed in TS 35.205 [212]) to generate message authentication codes (MAC) and session keys during the subscriber authentication

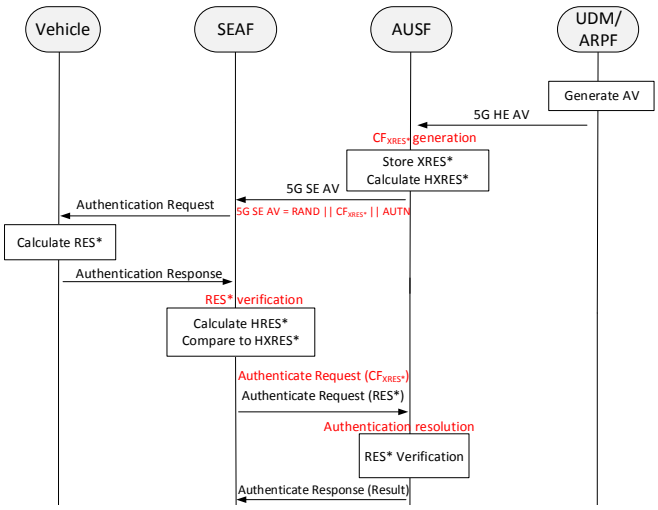


FIGURE 14: Signalling flow in standardized 5G-AKA procedure and proposed extensions (highlighted in red) in [214].

phase. In particular, the 5G authentication and key agreement (5G-AKA) protocol employs the MILENAGE algorithm set to mutually authenticate subscribers to the network and the network to subscribers [213]. The 5G-AKA protocol is based on a symmetric cryptography scheme, where the secure communication is realized between subscribers and providers using a long-term pre-shared secret key.

As shown in Figure 14, the key 5G functional elements involved in the signalling between the vehicle and the network are the following:

1) Security anchor function (SEAF), which performs authentication at the serving network level, and one of its roles is to generate a unified anchor key that can be used by the vehicle and the serving network to protect the subsequent message exchange.
2) Authentication server function (AUSF), which handles authentication requests in the home network and implicitly performs serving network authorization via interaction with the SEAF. It provides authentication functionalities through message exchange with the unified data management (UDM), e.g., it notifies UDM for successful/unsuccessful authentication of a vehicle.
3) Authentication credential repository and processing function (ARPF), which stores long-term credentials, e.g., the vehicle's subscriber key, used to uniquely identify a subscription and mutually authenticate the vehicle and the 5G core network.

However, the use of MILENAGE procedure on V2X terminals, e.g., involving frequent authentication and re-authentication during handovers, often results in excessive computation and communication overhead. The authors in [214] propose a lightweight vehicular authentication mechanism to extend the 5G-AKA procedure and address highly dense V2X connectivity scenarios. The proposed approach exploits the space-efficient Cuckoo filter properties to minimize the control signalling traffic required for security context establishment between home and serving networks. The performance analysis in [214], [215] reveals that a properly designed Cuckoo filter can significantly improve the authentication efficiency of the standardized 5G-AKA scheme. Gains in terms of end-to-end latency and protocol overhead can also be attained, while the introduced space cost remains close to the information-theoretic lower bound, even for stringent false positive rate requirements.

Another work in [174] proposes an efficient broadcast authentication mechanism, named *VAST*, targeting various V2X application types. The *VAST* approach relies on a modified version of the symmetric key *TESLA* protocol (i.e., *TESLA++*). In *TESLA* and *TESLA++*, the sender attaches a MAC to each broadcast packet computed with a private key k, and after a short delay, the sender discloses the key k. A single MAC is consequently sufficient to provide broadcast authentication having the receiver synchronized its clock with the sender ahead of time [216]. Compared to *TESLA*, the *TESLA++* version offers equivalent authentication performance in terms of computational efficiency, but achieves reduced memory usage. The joint use of *TESLA++* and ECDSA signatures in *VAST* offers non-repudiation and multi-hop authentication features, whilst preventing computation- and memory-related DoS attacks. The authors conclude via simulations that *VAST* is able to authenticate 100% of the received messages while maintaining acceptable delays. However, *TESLA++* relies on successful reception of packets with original MAC and keys; thus, in case of packet losses, the receiver will not obtain the complete data while the delay of exchanged packets for *VAST*'s authentication can be negatively affected.

A scheme based on *TESLA* symmetric key authentication protocol and Bloom filter probabilistic data structure is proposed in [175]. The authors make use of Bloom filter instead of ECDSA to achieve better performance in verifying and broadcasting communication keys. The Bloom filter implementation allows a trusted authority (TA) to efficiently generate CRLs in terms of space and computation. To achieve privacy protection, the scheme leverages the k-anonymity method to create a set of k neighboring vehicles in close vicinity, and performs pseudonym change while synchronizing via the RSU. In turn, the scheme achieves both anonymity and unlinkability features. Simulation results indicate that a superior level of anonymity is achieved with increasing size of the expected anonymity set. The scheme is shown to prevent a number of attacks, such as DoS, masquerade, modification and Sybil. However, it is often difficult to group/cluster vehicles with similar dynamics (e.g., in terms of heading angle and speed) in real-world vehicular scenarios. False positive rate is also shown to gradually increase with the number of vehicles, revealing scalability issues in highly dense vehicular scenarios. The non-negligible delay between message arrival and message

authentication in *TESLA*-based protocols needs also to be taken into consideration.

Identity-based cryptography. Identity-based cryptography (IBC) constitutes a type of asymmetric cryptography scheme that uses device/user identities instead of digital certificates for linking public keys [217].

> Unlike PKI approaches, IBC schemes are decentralized, infrastructure-less and with no certificates involved, since only trusted entities are issued private keys.

These characteristics simplify the key management process; however, such techniques do not yield strong security levels as PKI-based solutions, and are limited to pairwise communication [3], [8], [11], [15]. The identities are self-constructed, and are then used as unique identifiers for vehicles to authenticate them with the network. IBC schemes generate less cryptographic overhead on communication since certificates (i.e., credentials) are not sent at the time of authentication. This, in turn, results in smaller message sizes and improved transmission efficiency. In particular, IBC authentication schemes leverage pseudonyms for concealing the actual identity of vehicles, ensuring that the private information of participants is preserved throughout the authentication [218]. Such solutions help prevent several attacks such as impersonation, modification, fake location and replay.

A software-based authentication scheme, coined *SPACF*, is proposed in [178] where the Cuckoo filter data structure and the binary search method are exploited. *SPACF* alleviates heavy dependency on a tamper-proof device (TPD) installed in each vehicle. The adopted system model follows the typical vehicular network architecture shown in Figure 15. The TA acts as a registration center and communicates with RSUs to distribute shared secrets including pseudo-identities and passwords for vehicles; vehicles authenticate with RSUs, and the TA through RSUs. RSUs perform batch verification when a group of vehicles communicate with each other using a group key. In batch verification, *SPACF* leverages Cuckoo filter properties to verify hash values of the signature and the message without the need of bilinear pairings. For signature validation, *SPACF* employs two filters (i.e., negative and positive) in an effort to reduce false positive rate. If signatures are valid, they are stored in the positive filter; otherwise, signatures are inserted in the negative filter. Message overhead is thus reduced, and only valid messages are extracted from a batch without discarding it entirely. An elaborate assessment reveals that *SPACF* attains low communication and computation overhead in generating pseudonyms and verifying message signatures. Furthermore, *SPACF* achieves important security objectives, such as integrity, authenticity, traceability and revocability, and also thwarts collusion attacks from a group of colluded vehicles and message replay attacks. Nevertheless,

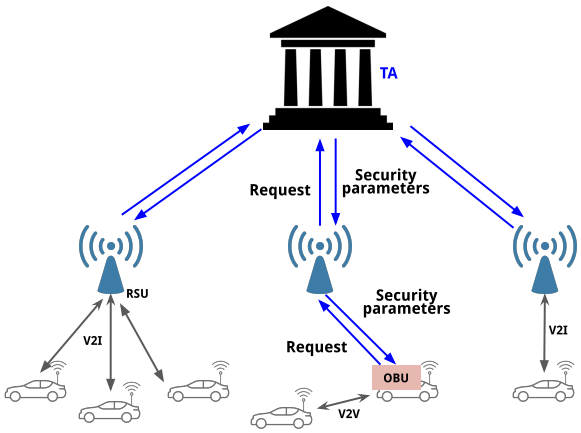


FIGURE 15: Typical architecture of vehicular networks.

the approach makes strong assumptions; for example, TA and RSUs are never compromised. *SPACF* is also prone to several other attacks, such as DoS, false information and Sybil.

An anonymous and lightweight authentication protocol based on smart card is presented in [179], where low-cost cryptographic operations are employed for authentication and validation of messages. In the proposed approach, vehicles communicate with each other or with RSUs, and RSUs communicate with the TA, which is responsible for provisioning anonymous certificates and keys to all vehicles. Smart cards generate anonymous credentials for vehicles and are capable of changing passwords offline without having to contact the TA. A formal security analysis proves that unlinkability and anonymity properties can be satisfied while withstanding several attacks, such as offline password guessing, impersonation and RSUs' compromise. In terms of performance, the communication and computation overhead of the protocol increases with the number of vehicles; however, a low packet loss ratio is maintained with increasing number of vehicles and communication range.

The work in [181] proposes an infrastructure-assisted efficient authentication scheme relying on RSUs, which are used to distribute security keys and pseudonyms for OBUs. RSUs communicate over wired or wireless links with the TA which issues vehicle certificates (Figure 15). Each RSU uses a group key to encrypt and send messages to vehicles in a specific area, while vehicles send messages to the RSU for dissemination. In turn, RSUs verify the authenticity and integrity of receiving messages and avoid propagating redundant messages. Overall, the scheme prevents a number of attacks, including Sybil, replay, message modification and rogue RSU, while reducing computation overhead from OBUs. Despite the security benefits, relying on RSUs for multiple operations tends to add extra load on them, which naturally leads to higher processing delays. In an effort to relieve the computational load in RSUs, the authors in [195] introduce a batch authentication scheme where RSUs can

simultaneously authenticate a group of vehicle users in a coverage region.

In a similar line, the authors in [182] propose two lightweight anonymous authentication schemes for V2X communication, utilizing a dynamic accumulator to manage membership proofs. The first scheme is tailored to V2V and employs a computation-outsourcing mechanism to prevent resource bottleneck on OBUs during credential verification. The second scheme is applicable to V2I and offloads the verification process to the RSU. In both schemes, the limitations in V2X communication, such as the stringent latency requirements and resource-constraint features of vehicle OBUs, were considered. The authors provide analytical and experimental assessment and argue that computation and verification outsourcing incurs less overhead to communication. However, both proposed schemes do not eliminate computation- and communication-expensive bilinear pairing cryptographic operations.

In [183], the authors introduce a hierarchical pseudonym structure for V2V and V2I communications without having to maintain inefficient CRLs. The hierarchical pseudonym structure comprises primary and secondary pseudonyms. In particular, Paillier non-deterministic encryption is specifically used by RSUs and the CA, while the rest of network entities use ECC tools (i.e., ECIES for encryption and ECDSA for the signature). The primary pseudonyms are provided by a CA and then used by RSUs for vehicle authentication. The secondary pseudonyms are issued by RSUs upon request by a vehicle. Vehicles broadcast messages using the secondary pseudonyms, and receiving vehicles verify incoming messages by checking the RSU's signature in the sender's secondary pseudonym. If a vehicle is found to behave maliciously, then its true identity is revealed to the revocation authority (RA) to revoke it from the network. However, this approach does not ensure unlinkability and requires the involvement of an RSU or CA to generate a valid pseudonym. Additionally, since most of the processing is offloaded to CA, a single-point-of-failure problem may occur.

Related to [183], the work in [185] introduces a two-factor lightweight privacy-preserving authentication scheme, named *2FLIP*. The *2FLIP* scheme decentralizes the functions of a CA to a local security center to reduce associated workload. It first requires the driver's biological password and passes this information to a TPD embedded in the OBU. Once authentication is completed, vehicles can use the TPD to communicate with each other. The TPD performs access revocation upon receiving commands from the CA on malicious activity, and subsequently stops the communication by rendering the vehicle unable to send messages. Although *2FLIP* satisfies most of the security requirements, its heavy reliance on an ideal TPD hardware requires further verification for its practical feasibility in real deployments. The scheme also relies on a single system key from the CA, which weakens the overall security if the CA is compromised. Both TPD and CA may potentially result in single-point-of-failure problems.

Finally, the authors in [188] propose an efficient message authentication scheme for LTE vehicular networks, which relies on identity and ECC. The proposed scheme, named *ESMAV*, achieves message authentication between a massive number of OBUs and the RSU, while providing single message verification, batch messages verification, non-repudiation and reduced signalling cost. *ESMAV* is able to preserve privacy, and remains robust against various LTE-based attacks, including impersonation, MitM, modification, replay and redirection. The authors analytically demonstrate that the security objectives of *ESMAV* are guaranteed, while both communication and computation overhead, related to batch verification, are kept in lower levels compared to similar schemes. The overall latency performance of *ESMAV* is also evaluated and shown to achieve low values in real environments. However, *ESMAV* lacks mutual authentication and incurs significant storage cost.

Attribute-based encryption. Attribute-based encryption (ABE) constitutes an extended concept of IBC, where public keys are defined in terms of attributes. In ABE, a user's keys and ciphertexts are labeled with sets of descriptive attributes and a particular key can decrypt a particular ciphertext only if there is a match between the attributes of the ciphertext and the user's key. This type of public-key encryption has recently gained research interest in the field of V2X security due to its characteristics of fine-grained access control, expressive access policy and one-to-many encryption [219]. However, decryption in ABE involves extensive computing overhead, which increases linearly with the number of considered attributes of the access policy.

A VANET framework based on attribute-based signature is presented in [197] to ameliorate the overhead caused by pseudonym/private key change or update in existing solutions based on symmetric/asymmetric key and IBC primitives. Their proposed scheme enables access control over attributes and supports vehicle traceability and revocation by a TA. To alleviate computational load in the vehicular edge, the authors in [219] propose a parallel outsourced decryption method for ABE, which can significantly improve the speed of decryption. The total decryption time can be reduced while the security level remains equivalent to the original ABE scheme. An RSU-assisted ABE scheme using blockchain is proposed in [220], aiming to reduce the computational load at vehicles and achieve fine-grained access control. A detailed security proof shows that the proposed outsourced encryption scheme is secure, while transactions recorded on the blockchain maintained between RSUs can be used for traceability and auditing. The combination of ABE with blockchain for IoV is also presented in [221] to strike a balance between privacy preservation and availability of information. Finally, an ABE-based security policy enforcement method for VANETs is presented in [199] which

TABLE 7: Overview of physical layer security techniques applied in V2X

Paper	Methodology	Attack/Threat type	Connectivity mode(s)	Key remarks and limitations
[222]	Moving relay concept, Non-orthogonal spectrum sharing	Eavesdropping, Jamming	V2X	Moving relay in conjunction with non-orthogonal spectrum sharing improve the ergodic sum secrecy capacity. The signal-to-noise-ratio of eavesdroppers is deteriorated due to vehicle penetration loss. Security|reliability tradeoff needs to be carefully optimized.
[223]	Adaptive resource allocation, Artificial noise injection with multi-antenna approaches, interference alignment	Eavesdropping, Jamming, Spoofing	V2X	The proposed proactive framework chooses adaptively the most-suited security mechanism by utilizing radio environment, user condition and V2X application requirements information. Sensitivity to channel reciprocity and estimation mismatch errors.
[224]	Maximal ratio combining	Eavesdropping	V2I	The joint impact of antenna correlation and imperfect channel information on the outage and secrecy outage probability reveals that it is advantageous to have exponentially correlated branches at the legitimate receiver side and uniformly correlated branches at the eavesdropper side. Secrecy performance is affected by high velocity values.
[225]	Cooperative relaying	Eavesdropping	V2N, V2V	Joint impact of fading parameters and relay positions on the secrecy outage probability is investigated. Secrecy outage probability performance is shown to degrade with increasing vehicle speed.
[226]	Secrecy capacity performance analysis with unknown exact distance for the eavesdropper link	Eavesdropping	V2V	Average secrecy capacity is evaluated taking into account the effects of fading, path loss and eavesdropper location uncertainty. The study highlights the importance of considering the location uncertainty of an eavesdropper while designing secure V2V systems.
[227]	Cooperative relaying	Eavesdropping	V2I	Better secrecy outage probability is achieved when the predefined secrecy rate threshold is low. A shorter relay-eavesdropper link degrades the system secrecy performance.
[228], [229]	IRS-based relay, IRS-based access point	Eavesdropping	VANET, V2V	Secrecy capacity performance is improved with the use of IRS. Average secrecy outage probability decreases with increased transmit power or increased number of IRS elements. Results further show the impact of the IRS location and size on the relay-based VANET. Doubling the number of RIS cells results in less impact on the average secrecy capacity, as compared to the influence of the source power.
[230]	Angle-of-arrival estimation to verify the message originator location	Location spoofing, Position falsification	V2X	The scheme makes use of the information contained in beacon messages to validate the claimed GPS location information with the angle-of-arrival information obtained at the physical layer. The RSU should accept beacon messages that are received only when the moving vehicle is within a threshold from the expected angle-of-arrival. Calibration of the angular signature matrix based on real measurements is needed to achieve accurate estimation under dynamic vehicular conditions.

considers various road situations as attributes for access control and secure group data transmission. Their scheme is shown to be adaptable to highly dynamic environments and ephemeral vehicular connectivity, by properly changing encryption keys with a dynamic attribute set.

B. Physical Layer Security

The management and maintenance of key-based cryptographic primitives are challenging, particularly in highly dynamic, decentralized and heterogeneous environments like those encountered in V2X communication. In addition, computation/communication overhead and the increasing demand to use longer security keys constitute key concerns in cryptographic approaches [222]. While security has traditionally been implemented at the higher, logical layers of communication networks, physical layer security (PLS) leverages the innate physical properties of radio propagation to provide certain types of security. In particular, diffusion and superposition of transmitted signals can be exploited to provide data confidentiality through several mechanisms that degrade the ability of potential eavesdroppers to gain information about confidential messages. In this context, PLS schemes have been identified as non-cryptographic security solutions that can complement cryptographic primitives.

> The fundamental hallmark of PLS constitutes the ability to exchange confidential V2X information over the shared wireless medium in the presence of unauthorized eavesdroppers, without relying on higher-layer message encryption.

PLS can be either achieved by properly designing transmit coding strategies without the need for an encryption key (*key-less* PLS) or via the generation of symmetric secret keys at the physical layer without the overhead of public key encryption (*key-based* PLS). Key-less PLS is based on information theory principles and the pioneering works of Shannon [231] and Wyner [232]. It leverages the secrecy

capacity concept, which characterizes the maximum secure transmission rate between legitimate nodes without leakage of information to an eavesdropper. On the other hand, key-based PLS [233], [234] extracts keys from a common source of randomness (i.e., the wireless channel) which varies in time, space and frequency. Key-based PLS relies on channel reciprocity assumption and a common approach to accomplish it, is by processing the received-signal-strength indicator (RSSI) [235].

In related literature, PLS mechanisms emerge as an effective approach that can exploit the dynamic features of wireless communication to secure V2X links between legitimate nodes [236]. The inherent random characteristics of the propagation channel, i.e., interference, multi-path fading and noise, in conjunction with advanced signal processing techniques can be exploited to limit the amount of information inferred by a malicious receiver. Various approaches for achieving PLS have been proposed, including cooperative relaying [237], artificial noise (AN)-aided beamforming [238] and cooperative jamming [239]. An overview of PLS schemes applied in V2X security is presented in Table 7. It is worth noting that a common consideration of these mechanisms is the reliance on accurate channel modeling, which may be challenging to achieve in practical V2X setups.

The authors in [223] introduce a proactive V2X security framework which utilizes information about the radio environment and application requirements to provide diversified PLS solutions via a software-defined platform. The framework employs AN injection with multi-antenna-based schemes at the transmitter to protect information from eavesdropping, and interference-alignment techniques at the receiver to combat jamming. Considering a legitimate V2I communication link under the presence of a passive mobile eavesdropper, the authors in [224] derive analytical expressions for the secrecy outage rate and reveal useful insights on the joint effect of vehicle mobility and antenna correlation on the secrecy performance. A detailed assessment of the impact of mobility on PLS is conducted in [240] where the authors devise a general analytical framework to evaluate the secrecy capacity and propose two types of secrecy-improvement strategies.

A relevant study is performed in [225] for a relay-based highway scenario. Assuming a fading channel specifically tailored to a V2X environment, the authors study the joint impact of fading parameters and relay positions on the secrecy outage probability. In an effort to highlight the importance of the eavesdropper's location uncertainty in the design of secure V2V systems, the authors in [226] derive closed-form expressions for the average secrecy capacity when the exact location of the eavesdropper vehicle is unknown due to mobility and eavesdropper's intention to hide its exact position. The detrimental effect of a mobile passive eavesdropper vehicle in the PLS performance is evaluated in [227] for a cooperative vehicular network where a mobile amplify-and-forward relay vehicle assists the V2I legitimate link.

The emerging paradigm of intelligent reflecting surfaces (IRSs) has recently attracted significant research attention as a means to achieve PLS through the control of the signal characteristics [241]. By leveraging the tuning capabilities of IRS elements (e.g., phase shifts), the reflected signal by IRSs can be added constructively or destructively with the non-reflected signal at the legitimate vehicle or eavesdropper for signal enhancement or cancellation, respectively. Compared to other PLS techniques, such as jamming with AN and multi-antenna beamforming [236], [242], [243], IRS-aided secure communication has been shown to achieve superior secrecy rate performance when the channel of the legitimate link and that of the eavesdropping link are spatially highly correlated [244], [245]. The authors in [228], [229] consider two different IRS-enabled vehicular scenarios to demonstrate the applicability of IRS technology: *i*) a VANET scenario with an IRS-based relay deployed on a building; and *ii*) a V2V network model where the source employs an IRS-based access point (for transmission). Their analysis reveals the gains in terms of secrecy capacity performance when employing IRSs as well as the impact of IRSs' location and size.

Recent works on IRS-enabled PLS have focused on the joint optimization of IRSs and conventional approaches, e.g., transmit beamforming and AN injection at the BS, to enhance the secrecy performance [241], [246]–[249]. In [250], the authors investigate the joint transmit beamforming with AN and IRS reflect beamforming in an IRS-assisted secrecy communication system. Simulation results reveal that incorporating jamming or AN can be an effective means to enhance the secrecy rate performance, especially when the transmit power is high and/or the number of eavesdroppers increases.

Since PLS techniques essentially operate independently of the higher layers, they can be used in conjunction with already existing security methods to enhance security performance. In certain cases, cryptographic primitives are still required together with PLS schemes to provide important security properties like traceability, unlinkability and unobservability. In [235], the authors introduce two channel-assisted authentication schemes based on RSSI values which can complement cryptographic mechanisms, e.g., hash-based MAC. Both schemes exploit the spatial diversity and channel reciprocity to identify non-legitimate users. The work in [230] proposes a physical layer-assisted message authentication scheme which complements the conventional PKI authentication procedure in V2X. The proposed scheme utilizes the receiving signal's angle-of-arrival (AoA) information to cross-verify the reported location information and mitigate the risk of location spoofing and falsifying attacks. Experimental results show that security gains come with no extra communication, bandwidth or transmit power overhead as opposed to upper-layer security solutions. However, the

consistency check for location verification at the receiver could add extra computation overhead in highly dense V2X scenarios.

C. Privacy Preservation

Ubiquitous vehicle connectivity increases the chances of compromising privacy and leaking sensitive private information to the outsiders. There exist various adversarial attacks, such as eavesdropping, traffic analysis and location tracking, which may try to extract the owner's identity and track the trajectory of a vehicle [7], [251]. In the scope of V2X applications, vehicles broadcast safety messages periodically (typically every 100 ms to 500 ms [33]), including information about location, speed and direction. A potential information leakage can thus lead to severe privacy issues, e.g., location information of a vehicle can be linked to its driver/owner [252].

> Privacy preservation resides in protecting both identity and location information of vehicles.

To preserve privacy, untraceability and unlinkability properties need to be satisfied by privacy solutions; untraceability implies that a vehicle's actions should not be traced and unlinkability suggests that linking a vehicle's identity with that of its driver/owner should be impossible for an unauthorized entity. However, linkability should only be allowed to authorized parties in case of liability issues.

For privacy protection, the 3GPP TS 33.501 [65], ETSI ITS [43] and IEEE 1609.2-2016 [42] standards propose to employ pseudonyms to relate vehicles, i.e., a vehicle is assigned a base identity while hiding its true identity for service access. Such pseudo-identities can be self-constructed or chosen by a central entity, such as the V2X service provider or the TA. Pseudonyms are usually short-lived and often changed by vehicles to prevent being tracked [43], [44]. A vehicle's true or permanent identity should only be observable by properly authorized parties. In addition, it should not be possible to infer a vehicle's true identity from its network traffic. Many V2X security solutions, e.g., anonymous authentication schemes [178], [179], [182], have utilized pseudonyms to preserve privacy of vehicles. The use of anonymous credentials at the time of authentication helps withhold any identifying information from the observer, e.g., a service provider or an attacker. That, in turn, achieves unlinkability since different uses of the same credential cannot be easily linked or distinguished by the observer or attacker [181].

ETSI ITS and IEEE 1609.2 standards recommend PKI-based security solutions which employ pseudonyms for privacy protection. At the time of registration, the PKI system issues several pseudonym certificates for a vehicle to achieve a reasonable level of privacy. For example, a registered vehicle in the SCMS [44] receives a batch of 20 (at minimum) pseudonym certificates at once from the CA with a validity of a week per certificate. Vehicles often change certificates within the batch, to avoid tracking while communicating. However, the allocation of a batch of pseudonym certificates per vehicle has become one of the key challenges for efficient certificate revocation of malicious vehicles whilst preserving privacy from internal attackers. The rate at which pseudonym certificates should change is also questionable. In this context, the work in [190] studies the effectiveness of changing pseudonyms based on the mix-zone concept [253]. The authors demonstrate through simulations that frequent change of pseudonyms results in increased privacy, but a higher frequency of change adds extra cost to the system through cryptographic operations.

Although the change of pseudonyms addresses location-tracking threats, it is still possible to link old and new pseudonyms of a vehicle. This allows an attacker to trace the entire trajectory of the vehicle between two locations [254]. On this basis, two solutions can be identified in [191], [193] which aim at mitigating such movement-tracking attacks. In particular, [191] proposes a *cryptographic mix-zone* (CMIX) protocol to achieve location privacy. All legitimate vehicles share the same secret key in a mix-zone, but public keys are changed only when a vehicle switches between zones. The vehicles obtain the secret key from the RSU of a mix-zone, and encrypt their messages with this key while located within the zone. In this way, location privacy can be preserved. Moreover, the authors show through simulations that unlinkability of mix-networks is generally high, but becomes relatively low within individual mix-zones.

In [192], a *chaff*-based CMIX scheme is introduced to improve privacy under varying traffic conditions and during low traffic periods. The *chaff*-based CMIX introduces fictive CAMs that are generated and signed with the private keys of *chaff* pseudonyms, minimizing the chances of compromising a legitimate vehicle by linking its old and new pseudonyms. RSUs are deployed at road intersections to create encrypted mix-zones for private pseudonym change, and Cuckoo filter is utilized to preserve the functionality of safety applications and correctly identify *chaff* messages. Compared to original CMIX [191], the authors demonstrate through simulations that privacy protection can be enhanced up to 76% under realistic traffic conditions. Even though encryption may conceal the content of CAMs within CMIX, the physical layer properties of radio signals cannot be obfuscated using encryption, and may potentially lead to external eavesdropping attacks [255].

The authors in [193] propose a solution for location privacy, where vehicles use a random silent period between pseudonym update. The vehicle's anonymity can be further enhanced by creating groups and applying extended random silent period. A vehicle in a group is not allowed to listen to pseudonyms from another group; thus, location privacy can be preserved with unlinkability. Nevertheless, silent periods are undesirable for safety applications which rely on periodically broadcast messages. A relevant work in [194] presents an anonymous group message authen-

tication protocol to achieve trajectory privacy of vehicles in LTE-based group communication. The incorporation of batch verification minimizes the overhead on vehicles, with no need to perform verification for every single message. In addition, the protocol uses ECC, zero-knowledge and bilinear pairing cryptographic operations to guarantee the trajectory privacy of a vehicle. The authors conduct a theoretical analysis of security objectives and show that the protocol satisfies confidentiality, integrity, accountability and trajectory-privacy properties. Higher gains in terms of computational performance are attained using the batch verification compared to single verification. However, the protocol lacks mutual authentication, incurs non-negligible computational overhead through cryptographic operations, and poses burdens on managing vehicle groups.

Recent surveys in [15], [107], [256] review the current advances in privacy-preserving techniques for V2X communication and highlight that anonymous authentication with anonymous credentials can be widely accepted for use by V2X actors when accessing V2X services. Anonymous credentials are initially assigned to vehicles by V2X service providers at the time of registration. Subsequently, credentials are checked for ownership at the time of access to services. Existing surveys further discuss that group signatures [257] or pseudonyms can be used as anonymous credentials during the authentication stage. In group signature-based schemes, a group of vehicles can sign messages using their group private-keys while keeping anonymous in the group. The recipient can then verify the validity of a group signature using the group public key, but the receiver cannot trace back to the sender. However, the signature can be revealed by the group head if necessary. Such anonymous schemes have been applied to achieve conditional privacy in V2X; a vehicle's privacy is protected as long as no malicious activity is executed by that vehicle. In such case, the real identity of a vehicle shall be revealed by the authority.

Although identity privacy can be realized by employing pseudonyms, pseudonyms alone are not sufficient to entirely preserve location privacy [15]. As a solution, differential-privacy techniques have been used to effectively achieve location privacy in location-based services (LBSs). Differential privacy can be regarded as a method that does not reveal whether an individual's record is present or not over an aggregate dataset. This can be achieved by adding a random noise into the dataset. The work in [196] propose a privacy-preserving LBS framework based on differential privacy, which protects vehicle's location privacy while still being able to access V2X services from edge servers. Nevertheless, offloading data filtering to the edge server can result in security issues if the server is compromised or eavesdropped by attackers. Diverse V2X applications also require different levels of privacy and service quality; thus, the effectiveness and efficiency of such schemes cannot be entirely guaranteed. In this setting, k-anonymity, spatial cloaking, caching, and dummy locations, have been identified as ways to preserve location privacy at the expense of location accuracy [15]. This, in turn, further confirms that there is always a trade-off between the accepted level of privacy and achieved service quality.

D. Lessons Learned

As described in Sections IV-A and IV-C, the use of predefined authentication, integrity protection and timestamps renders V2X technology robust, to efficiently mitigate the severity of Sybil, spoofing (e.g., replay or MitM) and DoS attacks. The baseline requirements of V2X information security, e.g., availability, authenticity and integrity, can be achieved using cryptography-based approaches. Although the major standards developing organizations (e.g., IEEE, SAE and ETSI) have converged to the use of digital signatures and PKI, there is a lack of practical evaluations and benchmarking for V2X applications [18]. We note in related literature several works [44], [170], [208], [209] on experimental assessment (e.g., prototype/testbed, simulation) of vehicular PKI; however, such evaluations have been performed under limited operating conditions. Particularly, large-scale and real-world effects cannot sufficiently be modelled on prototype/testbed or simulation environments.

> Fundamental trade-offs among various aspects, such as per-message-based verification, on-demand verification and complexity, as well as computation-heavy operations render PKI vulnerable to threats and/or not ideal for mission-critical V2X applications.

Decentralized PKI architectures [171], [172] have been proposed to address scalability and interoperability issues; however, such approaches often suffer from trust issues. Symmetric key protocols have also been introduced to alleviate heavy computation operations and infrastructure dependence through broadcast authentication protocols [174], [175]. Nonetheless, high delays between message arrival and message authentication limit their applicability in safety-critical V2X scenarios. The distribution of large CRLs and pseudonym changing strategies are still open issues that deserve further investigation [43], [44]. The applicability of PLS as a complementary solution to cryptographic primitives constitutes an active area of research. As discussed in Section IV-C, frequent or random pseudonyms changing strategies may not be sufficient to prevent entirely location tracking, since the attacker may correlate pseudonyms and location information [192]. Most of the existing proactive security solutions studied in Section IV are also prone to high computation and delay overheads. In addition, cryptography-based techniques are ineffective against adversarial attacks from rogue insiders.

An analysis of the energy consumption and computation cost required by cryptographic solutions constitutes an important topic for consideration. Deriving qualitative relationships between cryptographic algorithms and energy

requirements would offer design guidelines for greener configurations and optimization of resulting tradeoffs. However, energy consumption models and computational cost analyses are scarce in available literature pertaining to V2X cryptographic countermeasures. Our thorough review of the available works reveals that aspects related to the energy requirements of encryption and hashing algorithms are often overlooked or neglected, even if the emerging trend is to explicitly consider their impact as well. Instead, the primary focus lies on the detection performance of the proposed methods/models/algorithms, as well as on their impact on V2X network performance (e.g., latency). On the other hand, there may be intrinsic difficulties in measuring power drains in a non-invasive manner and deriving mathematically tractable models. Achieving precise understanding of how the different hardware and software components contribute to energy drains remains an open research problem, especially due to heterogeneity of V2X implementations.

V. Reactive Security in V2X Communication

Proactive security solutions may fall short in effectively protecting V2X communication from rogue insiders. Therefore, reactive approaches are considered an essential second layer of security that can compensate for the shortcomings of proactive approaches. Reactive security approaches include *signature-based*, *anomaly-based* and *context-based* methods [200]. Their common underlying characteristic is that they verify whether the received information conforms to normal system/protocol operation. Key characteristics for each of these reactive methods are briefly described in the following.

Signature-based approaches detect attacks by comparing network traffic to known signatures of attacks [258]. Such detection requires an attack database with a predefined set of signatures or rules to scan the network traffic and update signatures/rules if signatures are modified or new attacks appear. Thus, signature-based schemes are typically limited to known attacks and are unable to detect zero-day attacks. As the name implies, zero-day attacks exploit vulnerabilities that are unknown to the public community [259]. These attacks are difficult to analyze as information is not available until an attack is uncovered.

Anomaly-based detection relies on the comparison of received information with normal system behavior; any deviation from normal behavior is recognized as an attack [260]–[262]. Importantly, this type of detection requires the definition of normal operational behavior. For example, statistics-based anomaly detection performs a statistical analysis on the received information to check whether it reaches any predefined threshold level. If a threshold level is reached, the detection system triggers a warning signal for an ongoing attack. Anomaly-based techniques can detect previously unknown (i.e., zero-day) attacks; however, the drawback of such approaches resides in the complexity of defining normal system behavior. In addition, anomaly-based attack detection usually tends to generate false alarms (false positives).

Context-based techniques leverage intrinsic properties of V2X communication and safety applications. In these methods, each vehicle collects information from available sources in its vicinity and creates an independent view of the current system status and its local environment [263], [264]. In this way, a vehicle can autonomously evaluate the content (e.g., speed, origin and position) of a received message. Three context verification types, i.e., position information, timing information and application context-dependent, are defined in [200]. Such verification checks allow a fast analysis of exchanged messages based on their rudimentary and simple-to-execute principles. However, the lack of a *global view* may limit the identification of sophisticated attacks while autonomous decisions may often be imprecise.

In what follows, we describe the threat model for reactive security concepts (Section V-A) and we elaborate on the use of reactive security mechanisms for detecting misbehavior in V2X communication (Section V-B). An in-depth review of misbehavior detection methodologies is also provided. We highlight that even though anomaly-based and context-based approaches are primarily orthogonal, the combination of both can be used for misbehavior detection, as shown in Figure 12.

A. Threat Model

With the wide deployment of V2X systems in the form of C-ITS or VANETs, an attacker may exploit system vulnerabilities and get physical access to a legitimate vehicle. In other cases, the attacker acquires credentials to interact with other legitimate entities in the network. Such attackers are identified as insiders (as defined in Section III-B) and are capable of launching safety-critical attacks such as false data injection, DoS, replay and Sybil [145], [265]. For instance, if the attacker is able to access the key material kept in a regular storage unit of a vehicle, then the compromised content can be easily distributed to other devices to generate arbitrary messages (e.g., false alarms) with valid signatures.

B. Detecting Misbehavior

The widely used definition for misbehavior in the literature [100], [106], [266], [267] refers to the case when an entity transmits incorrect or erroneous data while both hardware and software are functioning as expected. If a node deviates from the expected behavior and transmits false information with malicious intent, it is identified as a malicious node or an attacker. On the other hand, any node that generates incorrect or erroneous data with no malicious intent is considered a faulty node [200], [268], [269]. Faulty behaviors are usually related to sensor malfunction that could be either attributed to bugs in the software module or physical damage. For example, a node may transmit -50 degrees of Celsius as the current temperature due to an

erroneous temperature sensor [266], or a vehicle may share incorrect location information because of a malfunctioning GPS device. However, these definitions have not been consistently used across all works in related literature; thus, in this paper, we resort to the definition of misbehavior detection as identifying V2X entities with malicious intent.

This section focuses on security approaches that can effectively detect behavior of rogue insiders and possible attacks that may originate from them.

> Those approaches are collectively referred to as *misbehavior detection* in V2X, and can complement proactive V2X approaches as an essential second layer of security.

For example, an authenticated legitimate vehicle can act selfishly or maliciously to achieve personal objectives (e.g., send false messages to create a non-existent traffic jam). Selfish or malicious behaviors are difficult to detect and contain, since those nodes may change their behavior intelligently in an on-off fashion [266]. Widely used cryptographic security techniques are, in principle, unable to detect rogue behavior of an insider [270]. In particular, PKI-based proactive solutions usually provide authentication, integrity and non-repudiation, which reduce attack surfaces by restricting outsider attackers. However, such solutions cannot distinguish dishonest vehicles from honest ones; thus, the trustworthiness of exchanged information cannot be guaranteed [271]. In addition, current ETSI ITS and IEEE 1609.2 standards do not support misbehavior detection and reporting [272].

A taxonomy of misbehavior detection mechanisms into two main classes, i.e., *entity-centric* and *data-centric*, is shown in Figure 12. Entity-centric mechanisms primarily focus on identifying misbehaving nodes and typically employ *monitoring* over *time* (e.g., past behavior and interactions with other participants) in order to ascertain its trustworthiness. The trustworthiness of a node can be measured by analyzing its forwarding behavior, including checks for packet transmission rates (e.g., CAM/BSM), checks for correctly formatted messages (e.g., DENM/BSM warnings), and checks for send/receive packet ratios. Instead, data-centric mechanisms specifically focus on verifying the *correctness* of received information regardless of the sender and its associated trustworthiness. Although both entity-centric and data-centric detection mechanisms are primarily orthogonal, many researchers often propose the use of a combination of both. Meanwhile, Table 8 summarizes the key characteristics of the existing solutions for misbehavior detection.

1) Entity-centric Detection

Entity-centric mechanisms for misbehavior detection can be further classified into two categories: i) *behavioral* and ii) *trust-based*.

Behavioral schemes, as the name suggests, analyze patterns in the *behavior* of specific nodes at a protocol level. These mechanisms specifically focus on node-related aspects, including message volumes, send/receive packet ratios, or correct message formats, among others. For example, the concept of a watchdog system for intrusion detection in self-organizing ad-hoc networks has been used in [297], where each node monitors information at the routing level to verify whether neighbor nodes forward the messages correctly.

On the other hand, trust-based schemes employ *trust-score assessment* to evaluate a node's trustworthiness, assuming that the majority of network nodes are honest. Trust-based mechanisms often use an infrastructure-based CA to remove malicious nodes, which simplifies the revocation process. Behavioral schemes generally operate locally on a vehicle, whereas trust-based schemes operate in a distributed and collaborative fashion among vehicles and RSUs [298].

In what follows, a literature review on entity-centric detection mechanisms is presented per category.

a) Behavioral: The work in [273] evaluates the usefulness of a traditional watchdog mechanism for detecting selfish nodes and malicious attackers in V2X. Watchdog mechanisms are, in principle, capable of coping with the detection of routing disruption attacks, such as DoS, black hole and gray hole. The black hole attack causes packet drops by distributing forged routing information. The gray hole is a special case of the black hole attack, in which the attacker selectively drops packets. The gray hole attacker forwards control packets but selectively drops only the data packets of a selected application [10]. The proposed watchdog mechanism assumes that V2X routing is standardized, and a vehicle's behavior is predictable by another neighboring vehicle. Each vehicle uses a trust level towards a neighbor to determine malicious behavior. The trust level measures the ratio between the packets sent to the neighbor and the packets effectively forwarded by the neighbor. Packets may be dropped due to a collision and/or an attack; therefore, a tolerance threshold is used to measure acceptable packet loss levels. If a vehicle drops packets frequently and exceeds the watchdog threshold, it is considered malicious. Evaluation of detection performance reveals that finding a global threshold for misbehavior detection can be difficult.

Another work presented in [275] aims to detect malicious vehicles that drop or duplicate packets at application level. The detection approach uses a cluster-based monitoring where a set of trusted vehicles in the cluster, called verifiers, monitor the behavior of every vehicle joining the cluster. All verifiers monitoring a node reside within the communication range of the cluster head (the most trusted node within the cluster) and send monitoring reports. If a vehicle drops or duplicates packets, its distrust value (trust indicator) increases. The vehicle is reported to CA by the cluster head as malicious if its distrust value becomes higher than a tolerable threshold. Consequently, malicious vehicles are blocked by CA and remain isolated from other vehicles.

TABLE 8: Summary of reactive security mechanisms with their key characteristics

Paper	Methodology	Attack/Threat type	Connectivity mode(s)	Communication technology	Validation technique(s)	Major limitation(s)
[273]	An IDS monitoring all network traffic of neighbors at routing protocol level (network layer) in promiscuous mode (Entity-centric).	Routing disruptions (DoS, Black hole, Gray hole)	V2V	IEEE 802.11p	Testbed emulation (Castadiva testbed [274])	Difficulty in finding a global threshold for detecting misbehaving vehicles. False positives due to high mobility of nodes and collisions.
[275]	Application-level packet monitoring algorithm via a set of trusted nodes (verifiers) in a cluster of vehicles (Entity-centric).	MitM (packet drops, packet duplicates)	V2V, V2I	N/A	Theory, Simulation (N/A)	Vulnerable to colluding Sybil attacks. Lacks trust evaluation under high mobility and high density.
[276]	Physical layer radio inference model based on computing correlation between the reception error and correct reception times (Entity-centric).	Jamming, DoS	V2V, V2I	IEEE 802.11p	Theory, Simulation (NS-2 [173], SUMO [177])	Evaluation limited to low-speed vehicular scenarios. Detection accuracy decreases at high vehicle density.
[157]	Study of the impact of radio frequency jamming through implementations of different jamming patterns under IEEE 802.11p with an SDR platform (Entity-centric).	Jamming	V2V	IEEE 802.11p (WAVE)	Field trials	Evaluation is under the assumption that the jamming attacker's presence is detectable.
[277]	Statistical network traffic analysis with window-based discrete sequences mining (Entity-centric).	Jamming, DoS	V2V	IEEE 802.11p (ITS-G5)	Simulation (MATLAB)	Simulation does not involve realistic traffic conditions. Detection accuracy decreases when platoon expands.
[278]	Trust evaluation fusing multiple evidence using theory of belief functions. Recommendation trust using collaborative filtering (Entity-centric and Data-centric).	MitM, false data injection	V2V, V2I	IEEE 802.11p	Simulation (GloMoSim [279])	Prone to trust manipulation by colluding attacks. Communication overhead increases with increasing number of vehicles.
[280]	Reputation update using weighted sum. ECC cryptography for secure message authentication and batch verification (Entity-centric).	Impersonation, Identity revealing, Modification, Replay	V2V, V2N	5G V2X	Simulation (N/A)	Difficulty in finding a threshold value for reputation score. Reputation update is exploitable by colluding attackers.
[281]	Multi-source information filtering for event detection with a threshold curve and certainty of event curve (Entity-centric and Data-centric).	False data injection, MitM, Sybil	V2V	IEEE 802.11p (DSRC)	Theory, Simulation (NS-2 [173])	Difficulty in finding a balance to minimize false positives and false negatives. Extra delays from filtering.
[282]	Trust establishment through direct trust and indirect trust calculation by each vehicle (Entity-centric).	DoS/DDoS	V2V	IEEE 802.11p	Simulation (NS-2 [173], VanetMobiSim [180])	Stealthy attackers may bypass the detection and remain undetected by manipulating trust values.
[283]	Trust evaluation of messages with extended Kalman filter and Chi-square test (Entity-centric and Data-centric).	False data injection	V2V	IEEE 802.11p (DSRC/WAVE)	Theory, Simulation (MATLAB)	Privacy is not addressed. Applicability is limited to highway scenarios.
[284]	Mobility data verification with Kalman filter (Entity-centric and Data-centric).	False data injection	V2V	IEEE 802.11p (ITS-G5)	Field trials (sim^{TD}[285])	Allows tracking vehicle movements. Vulnerable to tracking pseudonyms.
[286]	Similarity measure of (Z-score normalized) RSSI time-series using dynamic time warping distance (Data-centric).	Sybil	V2V	IEEE 802.11p (DSRC)	Field trials, Simulation (NS-2 [173])	Attacker may bypass the detection utilizing more than one radio, or modifying transmission power.

Continued on next page.

Paper	Methodology	Attack/Threat type	Connectivity mode(s)	Communication technology	Validation technique(s)	Major limitation(s)
[287]	Position plausibility checks using RSSI information in BSMs (Data-centric).	Position falsification	V2V	IEEE 802.11p (DSRC)	Simulation (VeReMi)	Advanced attacker may bypass plausibility checks by obfuscating physical layer properties. Real-time access to RSSI distributions may not always be feasible.
[288]	Sensor-based position verification by calculating a trust value with weights per observation towards neighbors (Entity-centric and Data-centric).	Position falsification	V2V	IEEE 802.11p	Simulation (NS-2 [173])	Autonomous standalone detection cannot fully detect falsified location information.
[289]	Physical position verification using on-board radar and GPS measurements. Virtual position-based cells to cluster vehicles with a leader to verify positions (Data-centric).	Position falsification, Sybil	V2V	IEEE 802.11p (DSRC)	Simulation (N/A)	Privacy issues in clustering vehicles. High vehicle density and transmission range impact detection latency.
[145]	Traffic warning messages verification based on plausibility validation network with pre-defined set of rules (Data-centric).	Illusion	V2V, V2I	N/A	Model validation (PVN)	Lacks network assessment to analyze effectiveness. Limited attack detection with a pre-defined rule set.
[290]	Behavioral analysis with plausibility checks with positive/negative ratings and trust evaluation. Exponentially weighted moving average is used for categorization (Data-centric).	False data injection, Sybil	V2V	N/A	Conceptual framework	Lacks network performance assessment. Relies on an honest majority.
[291]	Mobility verification based on plausibility checks with Kalman filter and collective perception messages (Data-centric).	False data injection	V2V	IEEE 802.11p (ITS-G5)	Simulation (Veins [184], SUMO [177])	Vulnerable to collective perception fabrication and Sybil attacks. Feasibility is limited due to collective perception messages.
[292]	Cooperative position verification by exchanging information with neighbors, including extra verification such as map-based and maximum vehicle threshold (Entity-centric and Data-centric).	Position falsification	V2V	IEEE 802.11p	Simulation (NS-2 [173])	Relies on an honest majority.
[264]	Cooperative position verification with local sensors and exchanged position information with neighbors (Entity-centric and Data-centric).	Position falsification	V2V	IEEE 802.11p	Simulation (NS-2 [173], Daimler-Chrysler FARSI [293])	Fixed thresholds vulnerable to spoofed location attacks. Spoofed beacons by colluding attackers can reduce trust values of legitimate vehicles. Relies on an honest majority.
[294]	Consistency-based information verification constructing neighbors' location data table based on time intervals (Data-centric).	Replay, False data injection, Sybil	V2V	IEEE 802.11p	Simulation (MMTS [295])	Difficulty in finding a threshold duration for detection decision. Sybil attacks with short duration may bypass the detection.
[296]	Behavior analysis of neighbors using rule-based data mining with *Itemset-tree* structure and association rules (Data-centric).	False data injection	V2V	N/A	Simulation (N/A)	Execution time and memory consumption increase at high vehicle density. Lacks an evaluation on detection rate and latency.

Moreover, the warning messages from the cluster head to CA are encrypted using hash-based MAC and the symmetric cluster key. However, the detection approach is susceptible to colluding Sybil attacks, while its feasibility is limited in high-mobility and high-density V2X scenarios.

The authors in [276] propose a behavioral mechanism for the detection of jamming-based DoS attacks. The approach considers that the attacker selectively transmits jamming signals to avoid being detected. The proposed model is based on analyzing patterns in radio interference and statistically calculating the correlation between the reception error and correct reception times of transmission. If the resulting correlation coefficient is unusually high, the wireless medium can be considered jammed. Simulation results confirm that the correlation coefficient is higher in the presence of jamming than when regular signal reception occurs. However, the correlation coefficient gradually decreases in high-density scenarios, and the evaluation is based on low-speed vehicles; thus, applicability is limited only to specific V2X scenarios (e.g., urban areas).

The work in [157] discusses various jamming attack types and evaluates their impact under different scenarios, such as an open-space road and a crossroad in dense buildings. The authors implement various jamming attack patterns (e.g., constant, random, reactive and pilot) against IEEE 802.11p-based V2V communications on an SDR platform, and conduct a field measurements campaign. Evaluation demonstrates that certain jamming attacks may entirely hinder communication and cause excessive packet drops. Nonetheless, the assessment is under the assumption of the jamming attacker being detectable. In a similar direction, the authors in [277] combine statistical network traffic analysis with data mining methods to detect random and intelligent on-off jamming attacks. A platooning C-ITS application is considered for the evaluation, and vehicles exchange CAM messages in the platoon. In an on-off jamming attack, CAMs are not jammed in *off* state, while a sequence of CAMs are attacked in *on* state. Subsequently, the attacker switches back to *off* state. Simulation results reveal that an acceptable level of detection performance can be achieved using the proposed approach. However, the detection accuracy decreases when the platoon expands.

b) Trust-based: An attack-resistant trust management scheme, called *ART*, is introduced in [278] to model and evaluate the trustworthiness of vehicular data and nodes. The proposed scheme leverages the theory of belief functions (Dempster–Shafer framework) to fuse local evidence of a vehicle and external evidence shared by other vehicles. A vehicle's trust is divided into functional trust and recommendation trust:

- Functional trust directly reflects the trustworthiness of a vehicle;
- Recommendation trust indicates the trustworthiness of a vehicle towards neighboring vehicles.

Recommendation trust is built using user-based collaborative filtering by computing the similarities between vehicles. Simulation results reveal that *ART* is able to mitigate active attacks such as false data injection, bad mouthing and MitM, originated from an outsider or a rogue insider. It further achieves superior performance compared to a conventional weighted-voting method in trust management. However, *ART* scheme may not work well in the case of platooning attack, where a platoon of attackers collaborates to generate positive recommendations for each other. The communication overhead is also shown to increase when the total number of vehicles increases. Also, false positive rate increases when the percentage of malicious vehicles becomes high.

In [280], a reputation system-based lightweight message authentication (*RSMA*) scheme for 5G-enabled vehicular networks is presented. *RSMA* integrates the trust management with ECC to achieve secure message authentication with low computational overhead. Trust management in *RSMA* is especially used as a complementary tool to cryptography, aiming to provide a robust vehicular system. A multi-weighted reputation method is adopted to update the vehicle's reputation score; the TA issues a credit reference only if a vehicle's reputation score exceeds a threshold value. The credit reference is only valid for a certain time period, and it is used to sign and verify messages. The authors provide formal security analysis on the protocol and evaluate message authentication, identity privacy-preservation, traceability and unlinkability requirements. The selection of a proper threshold value for reputation score remains an open issue to be further explored for network performance maximization.

The authors in [281] propose a multi-source message filtering mechanism to verify the validity of received messages. Message validity is determined by comparing the content against local sensor data, messages from other vehicles, source location, sender reputation, and infrastructure validation. The combined information is evaluated based on a threshold curve and a certainty of event (CoE). The threshold curve defines the importance of an event to a driver, and the CoE evaluates whether a message report is a critical event or not. As a result, only relevant and valid events are presented to the driver. The authors suggest that a vehicle may prioritize sources of information depending on the application requirements (e.g., avoid cryptographic authentication to reduce computation and communication overhead). However, simulation results show that it is difficult to strike a balance between minimizing false positive and false negative rates in the alerts. Furthermore, the filtering process adds extra delay with increasing distance between the driver and the event. The requirement for pre-determined event locations also limits the applicability of the scheme only to specific V2X scenarios.

A security framework for evaluating vehicles' trust based on behavior analysis is proposed in [299]. The framework uses a hybrid (direct and indirect) trust model to evaluate vehicles' behaviors and estimate the corresponding trust metric values. Each vehicle computes direct and indirect trust values of other vehicles and transmits all values to a backend system, i.e., misbehavior authority (MA). Based on locally received trust values, a vehicle can limit the number of accepted messages from neighbor vehicles. In case of mis-

behavior and ensuing violation of a certain trust threshold, a report is sent to MA to deactivate malicious vehicles. The lack of implementation details and performance evaluation of the approach yet limit its feasibility. The framework may also underperform in case of multiple Sybil attacks, where attackers collaborate and increase their trustworthiness.

In a similar direction, the authors in [282] introduce a hybrid trust establishment scheme, called *TFDD*, to prevent DoS/DDoS attacks and eliminate misbehaving vehicles in a distributed manner. In *TFDD*, each vehicle calculates both direct and indirect trust values; the direct trust evaluates the sender (or forwarder) and the indirect trust reflects the opinion of the last forwarder about the message. Each vehicle maintains a local blacklist to add neighboring misbehaving vehicles, and sends this information to the global blacklist maintained by the TA. If the trust score of a vehicle is lower than the minimum threshold due to a DoS attack, the vehicle's identity is included in the global blacklist and the TA suspends the vehicle from network operations. The authors demonstrate that TFDD yields highly accurate detection under DoS/DDoS attacks with a high ratio of dishonest vehicles. However, a malicious stealthy attacker may bypass the proposed detection scheme by manipulating trust values, and remain undetected.

2) Data-centric Detection

As shown in Figure 12, data-centric mechanisms can be classified in two categories: (a) *plausibility-based* and (b) *consistency-based*. The operating principle of data-centric approaches is similar to conventional intrusion detection systems used in legacy networked systems [300]: received network traffic is compared against already known historical information or behavior accumulated over time.

a) Plausibility: Plausibility-based misbehavior detection exploits real-world data models to validate whether received information is consistent with the underlying model. Such plausibility models can vary from a narrowly defined set of rules to complex models with a wide range of rules capturing different variations, e.g., driver behavior prediction [266]. Narrowly defined rules can be exploited to check for physically infeasible content and discard it directly. Speed of 300 km/h for a passenger vehicle, identical position coordinates shared by two vehicles and reception of messages beyond the communication range are such physically inconsistent examples.

> Plausibility-based detectors are considered rudimentary as they use packets from individual vehicle senders, which may often result in imprecise decisions.

Moreover, plausibility checks are typically *local* and may fall short of identifying sophisticated attacks due to a lack of global view. Nonetheless, they allow *rapid* analysis of received packets and their outputs can be used as input feature vectors in ML models for further verification [301].

A data trust framework is proposed in [283] for tracking misbehaving vehicles and detecting false data in received V2X messages. The proposed scheme employs the extended Kalman filter (EKF) to estimate the behavior of sending vehicles while leveraging AoA and Doppler speed (DS) measurements from the received signal. This information is combined with position data of each received message to evaluate whether received messages can be trusted or not. The authors apply the Chi-square test on their own measurements and the predicted measurements from the EKF to detect false reported data. However, privacy is not addressed in this scheme, and its applicability is limited to highway scenarios. Another relevant work is presented in [284] for mobility data (CAMs) verification by exploiting the Kalman filter to analyze the consistency of a vehicle's movement. The approach can reliably track movements of a vehicle in the presence of pseudonym changes, which may raise privacy issues. It appears that both [283], [284] can be exploited to track pseudonyms.

A Sybil attack detection method based on RSSI is presented in [286]. The proposed method evaluates the similarity of RSSI time series between the malicious node and its Sybil nodes over time. The authors argue that acquiring two RSSI series of equal time length is not always possible due to frequent packet losses in V2X. Thus, their proposed method exploits the dynamic time warping (DTW) distance to measure the similarity of RSSI time series. Moreover, Z-score normalization is applied to all RSSI time series to prevent an attacker from using different transmission power levels for each Sybil node. The detection method uses linear discriminant analysis to determine the threshold for DTW and correctly distinguish Sybil nodes from normal ones. Nonetheless, the detection method may not work well when an attacker utilizes more than one radio or when an attacker modifies its transmission power for Sybil attacks.

In a relevant path, the work in [287] proposes physical layer plausibility checks based on RSSI information from BSMs. The authors analyze RSSI distributions of several location-falsification attacks, considering the distance between receiver and attacker pairs. The detection mechanism assumes that when a vehicle enters a new area, it should be aware of the local RSSI distribution from a trusted RSU or have it predefined. At the reception of BSMs, each vehicle classifies the messages as normal or anomalous by comparing the computed RSSI with its local RSSI distribution. Misbehavior detection classifies BSMs as anomalous based on three plausibility checks (i.e., confidence interval, majority rule and weighted moving average). Yet, the proposed plausibility checks may not work well for the case of intelligent and advanced attacker models. For instance, advanced attackers may try to obfuscate physical layer properties and penetrate plausibility checks. In addition, real-time access to local RSSI distributions may not be always feasible.

The authors in [288] propose a trust-based position verification approach that can operate without the support of infrastructure or dedicated hardware. The verification system uses vehicle sensors autonomously to detect false position claims of neighboring vehicles. Based on sensors' observations, each vehicle calculates a trust value by assigning a weight to each observation, and decides the trustworthiness of neighboring vehicles. The receiving vehicle discards beacon messages if the claimed position information falls beyond a maximum-range threshold. In this approach, the sender's trust level can be affected by abnormal observations of the recipient. In the case of position falsification detection, a malicious vehicle is required to send several correct beacon messages to recover its trust level. This type of standalone verification cannot entirely prevent malicious vehicles from using false location information. To this end, the authors propose *cooperative* consistency-based approaches in [264], [292] to improve position verification.

The joint use of on-board radar and GPS vehicle measurements is suggested in [289] to detect and verify the physical presence of other neighboring vehicles. In the proposed approach, vehicles are clustered into position-based cells, where each cell contains a group of vehicles with a cell leader. The cell leader verifies GPS positions of all other vehicles in its cell and informs them. In turn, each vehicle locally verifies neighbor positions by comparing the received GPS and on-board radar measurements. In the case of Sybil attacks, such local verification may not be successful; thus, the authors perform cosine similarity computation on a vehicle's on-board radar data, incoming traffic data and neighbors' reports to detect Sybil attacks. Simulation results reveal that the proposed cell-based message exchange performs better than message flooding; however, detection time increases when both the number of vehicles and transmission range increase. Local verification may also be limited when the radar signal gets blocked by obstacles, while privacy issues related to vehicle clustering may inevitably occur.

In an effort to resolve illusion attacks in traffic-safety applications, [145] introduces a plausibility validation network (PVN) model which compares incoming traffic warning messages based on a predefined set of rules stored in a database. Traffic comparison includes a series of validation procedures to determine whether a specific field in a message is reasonable or not. If all elements in a message are successfully verified, the message is considered trustworthy to the application; otherwise, the message is dropped. The PVN model is interoperable with existing authentication methods and cryptography mechanisms. Nevertheless, the approach is limited to a specific attack type with a predefined set of plausibility rules. A larger rule set needed to detect additional attack variants often results in performance degradation due to extra delay and computational overhead for rigorous message analysis. However, the authors do not provide network assessment to evaluate holistically the effectiveness of their approach.

In [290], the authors introduce a vehicle behavior analysis and evaluation scheme (*VEBAS*) which entails behavioral, plausibility and trust-based mechanisms. The combination of multiple behavior-analysis modules in *VEBAS* allows the detection of unusual vehicle behavior. Plausibility checks in *VEBAS* help analyze the content of received messages (e.g., positive/negative rating if the information is correct/incorrect). For example, when a vehicle exceeds the maximum beacon frequency threshold, its behavior is considered as potential attack (i.e., negative rating). The scheme uses an exponentially weighted moving average (EWMA) calculation on the ratings derived from plausibility-based checks to find a continuous average. During the integration of ratings for EWMA, older information is assigned less weight than fresh information. Once a vehicle has aggregated all information about surrounding vehicles' behavior, it broadcasts the local trust rating results to its single-hop vicinity. The lack of network performance assessment as well as the assumption of honest majority limit the feasibility of *VEBAS*. Since the validity of information in received messages is not verified, vulnerabilities due to data manipulation attacks may also remain unresolved.

A mechanism to verify the plausibility of mobility data inside CAMs is proposed in [291]. The authors leverage collective perception messages (CPM) of ETSI standard and Kalman filter to validate the content of CAMs. In the proposed approach, the vehicles maintain a local dynamic map to fuse the content of receiving CAMs and a Kalman filter per sender to verify the plausibility of CAMs. In the case of a CAM reception from a known vehicle, the CAM is accepted into the map when position and velocity data are not deviating from the output of the Kalman filter associated with the corresponding sender. If the CAM is receiving from a new vehicle outside the communication range, CPM data is leveraged from surrounding vehicles to verify CAMs sent by new vehicles. Simulation results show that CPM-based verification reduces the false positive rate to yield similar detection performance compared to methods that use only CAMs. The detection method is, however, vulnerable to attacks such as CPM falsification and Sybil. The feasibility of this approach is also limited as CPMs may not be widely available.

b) Consistency: Consistency-based misbehavior detection aggregates packets from multiple sending vehicles to determine the trustworthiness of new data. Alternatively, pairwise comparison of messages from different vehicles has also been considered as a way of checking consistency [266]. In this context, raw data comparison can be the simplest type of consistency-based detection, where message contents are directly compared for potential conflicts, e.g., position verification. In addition, a vehicle may use the (previously calculated) average speed of its neighboring vehicles to identify speed consistency/deviation in new beacon messages (CAM/BSM). Consistency-based detection schemes

typically operate in a distributed or collaborative manner among vehicles and RSUs [302].

> The drawback of such cooperative consistency schemes is that they often require an *honest majority* to draw reliable conclusions; otherwise, they may not effectively detect malicious information of sophisticated colluding attacks.

A cooperative consistency-based approach is proposed in [292], where position information is exchanged among neighbors. Upon reception, beacons are checked against received neighbor tables for consistency between the claimed position in the beacon and the table. The authors combine previously discussed autonomous [288] and cooperative approaches to improve position verification. The proposed mechanism performs additional checking using: *i*) maximum vehicle density threshold, to limit beacons from an area and minimize possible Sybil attacks; *ii*) map-based verification, to compare the claimed location in the beacon against the road map; *iii*) position claim overhearing, to compare different overheard packets and their intended destinations and verify false position indications [264]. However, the consistency checks have limited detection capabilities while such cooperative schemes still rely on an honest majority.

The authors in [294] propose a consistency-based approach to detect Sybil attacks in a distributed way by comparing neighboring information from multiple vehicles over time. In this approach, each vehicle maintains a neighbor table which includes vehicles located in its transmission range. The table contains a record of neighboring vehicles at discrete time intervals, and this information is monitored over time to detect Sybil nodes. If a set of vehicles persist in the neighbor table for a substantial duration of time, those vehicles are classified as Sybil group category. The proposed approach assumes that Sybil attacks remain active for a significant amount of time, and consequently leverages this observation for detection. The authors demonstrate that the number of neighbors of legitimate nodes increases due to Sybil-identity creation by an attacker. Moreover, a narrower monitoring threshold duration improves detection accuracy for a different number of Sybil attackers at the cost of higher false positive rates. Evaluation outcomes show equivalent computation performance compared to benchmark schemes. However, it is noted that the selection of a threshold duration is non-trivial due to the dynamic characteristics of V2X networks. The detection mechanism may also underperform in the case of Sybil attacks with short duration.

Data mining techniques have been used to extract useful information from safety messages (e.g., CAM/BSM) and check the consistency of exchanged information by vehicles. Such an approach is presented in [296], where the authors resort to data mining techniques to detect misbehavior. The proposed method, coined VARM, exploits association rules to correlate vehicles and communication events; in turn, the behavior of surrounding vehicles is analyzed to detect malicious ones. VARM dynamically generates association rules from data received from neighbors using a tree-based data structure, called *Itemset-tree*. By applying association rules, a vehicle can extract relevant information from received messages to estimate the expected behavior of senders. The authors suggest that the representation of correlated information via association rules renders the method interpretable, and such knowledge may help extract other useful information, e.g., local road conditions. Simulation results show that *Itemset-tree* produces compact storage compared to relevant schemes. Nevertheless, the resulting execution time and memory consumption considerably increase with the number of neighboring vehicles. Besides, the study lacks the evaluation of key performance indicators such as detection latency and rate.

3) Standardization and Regulation

Ongoing efforts by standard organizations and regulators aim at developing specifications and regulations to secure vehicles against misbehavior attacks. In particular, ETSI is currently leading activities for specifying a cybersecurity system against V2X misbehaviors, with a standard under development that defines misbehavior detection and reporting activities for CAM and DENM message types [303]. The standard is based on the supporting technical report [272] which defined a V2X misbehavior detection and reporting system with a basic set of detectors. Future releases of [303] are expected to include an updated list of detectors for each new and existing V2X message type. The document also specifies the structure of the misbehavior report sent by the vehicle to the MA, following the basic format elements, data structure and certificate profiles prescribed in [304]. In addition, the United Nations Economic Commission for Europe has recently imposed new regulations to vehicle manufacturers to implement measures for security risk management, remediation of incidents, and software updates without compromising the vehicle's safety and security [305], [306]. Finally, [307] specifies a framework to assess the security risk of misbehavior attacks on V2X systems.

A fair feasibility assessment of the available misbehavior detectors requires the adoption of a common validation methodology and a common consideration for the attack model. The extension of the misbehavior report format to all V2X message types also remains an open standardization challenge. The misbehavior report design should be scalable and extendible for future functionality. Finally, standardization efforts should focus on potential local reactions to an ITS after detecting a misbehavior attack to allow early mitigation, while the minimal set of evidence needed by the MA to detect an attack needs to be properly prescribed. Establishing well-documented use cases and performance metrics for the assessment of a set of misbehavior detectors

could be a starting point for addressing the aforementioned technical specifications.

C. Lessons Learned

Reactive security mechanisms are considered an essential second layer of defense to compensate the shortcomings of proactive mechanisms (i.e., validate exchanged information and detect misbehavior from malicious insiders). For this reason, it is worth stressing the need for applying V2X security solutions using the defense-in-depth principle [308], which provides multiple layers (i.e., prevention, detection and deflection) of independent security controls. Several entity-centric and data-centric security mechanisms are reviewed, some of which are statistical and data mining based techniques.

As discussed in Section V-B1, entity-centric mechanisms involve behavioral analyses and trustworthiness evaluation. Behavioral schemes accumulate behavior patterns of specific nodes over a period of time, focusing on their actions at a protocol level. These techniques generally operate individually and locally on a vehicle. Such characteristics pose challenges and reliability issues due to ephemeral connectivity, high-density and high-mobility in V2X systems. For example, the mechanisms used in [273], [275] for detecting packet drops/duplicate attacks may potentially lead to additional attacks, while significantly deteriorating the underlying network performance. Trust-based schemes often rely on the infrastructure assistance (i.e., RSUs) while resorting to the assumption that the majority of network nodes are honest. Although trust evaluation mechanisms monitor nodes over a period of time, this becomes challenging due to the short-lived connections and mobility patterns.

> Trade-offs among false positive rates, threshold levels for detection, RSUs availability, trust issues of RSUs and CRL size need to be further investigated.

Data-centric mechanisms (i.e., plausibility and consistency) presented in Section V-B2 behave similarly to conventional intrusion detection mechanisms. Plausibility-based detection is autonomous and may often result in imprecise decisions due to the lack of global view. Although such detectors provide fast responses, the rudimentary rule-based checks may easily be penetrated by an adversary. Consistency-based detection fuses data from more than one source to compute the trustworthiness of new data. While cooperative consistency schemes are more robust than rudimentary plausibility checks, there is a drawback of requiring an honest majority in the network to derive reliable conclusions. This type of cooperative detection typically operates in a distributed manner among vehicles and RSUs. Solutions relying on RSUs often assume that RSUs are trusted and not vulnerable to attacks [14]. RSUs may also be limited to specific places (e.g., intersections) causing availability issues. We note that even though data-centric schemes are not robust enough to defend against sophisticated attacks, the resulting outputs can be utilized as inputs to robust AI/ML models for further verification [301]. Similar to entity-centric approaches, trade-offs among false positives, detection threshold, trust and availability of RSUs, deserve further research attention. Most of the existing reactive security solutions reviewed in Section V are complementary tools to cryptographic techniques, resulting in additional execution and verification delays with memory consumption.

Given the increasing catalog of available V2X misbehavior detectors, ongoing standardization efforts aim at prescribing updated security regulations and specifications. Misbehavior detection and reporting are already considered by the standardization bodies from the early stages of the design of V2X systems. Since local detection only provides limited information in time and space, which may be insufficient to identify an attack reliably, global detection that relies on the backend systems/backbone infrastructure (i.e., the MA) may be necessary. Misbehavior detection also raises privacy issues that need to be properly addressed. First, the privacy of the misbehavior reporter and the reported vehicle should be preserved. Second, the MA requires means to either link pseudonym certificates with their real long-term certificate, or use another mechanism for both investigation and revocation purposes. Finally, it is expected that a promising standard-related direction would be the incorporation of data-driven AI techniques for the detection of novel/unknown attack variants.

VI. Artificial Intelligence in V2X Security

As thoroughly discussed in previous sections, V2X systems are inherently complex with rapidly evolving dynamics, introducing peculiar security requirements compared to other wireless systems. Key open issues in existing security approaches underscore the need for advanced data-driven techniques for effective protection of V2X communication links. In this context, the emerging field of AI is foreseen as a promising paradigm, with wide applicability fueled by advanced computational methods and tools [309]. Security approaches based on AI have been lately identified as key enablers for many safety-critical applications in next-generation wireless networks [310]. Recent breakthroughs in AI-based security are continuously gaining momentum, delivering actionable results for safer and smarter V2X cybersecurity systems [67], [311], [312].

Data-driven ML approaches provide a fertile ground towards:

- Learning attack patterns and signatures from experience and generalizing to future threats (supervised learning);
- Automatically identifying traffic patterns deviating from normal system behavior (unsupervised learning);
- Learning from interactions how to perform detection and dynamically improve with the detection experience (reinforcement learning).

Each of these categories corresponds to different workflows and data types fed into the learning algorithms. In particular, supervised learning infers a function from labelled training data consisting of a set of training examples. On the other hand, unsupervised learning learns patterns from unlabelled data, and discovers hidden patterns or data groupings without the need for human intervention. Finally, reinforcement learning (RL) enables the learner to infer optimal sequential decisions in an interactive environment based on rewards/penalties received as a result of previous actions and experiences.

Recent evolution of deep learning (DL) techniques has gained widespread attention due to their feasibility and superior performance over traditional ML [313], [314]. DL relies on a multi-layered representation of the input data via linear or nonlinear operations, and can perform feature selection autonomously through a process called representation learning. By leveraging their ability to learn high-level features from data in an incremental manner, DL variants are pervasively used in cyber-threat detection due to their improved accuracy compared to conventional ML [315]. The rapid emergence of DL is also dictated by the fact that classical learning-based classification and intrusion detection methods often become inadequate to handle large data volumes induced by the high number of connected vehicles in IoV [316]. DL is also preferred over traditional ML when there is lack of domain understanding for feature introspection due to unforseen changes in vehicular scenarios, caused by either naturally drifting traffic mobility patterns or non-anticipated variability in malicious behavior of attackers [317].

In the following subsections, the advanced capabilities introduced by AI are first highlighted, aiming at addressing limitations of existing V2X security approaches. We further shed light on the current applicability of AI-based techniques in V2X security. Finally, the perils introduced by the integration of AI/ML in V2X systems are pointed out.

A. Advanced Security Capabilities

One of the key elements for secure V2X communication is cryptography, which is essential to ensure information security (i.e., authenticity and integrity) for in-vehicle, inter-vehicle and vehicle-infrastructure communications. However, the implementation of cryptography mechanisms on low computing devices, such as vehicle OBUs and RSUs, is non-trivial. The computation and communication overhead of cryptographic operations is typically high; thus, authentication, authorization, access control and privacy-preserving services become challenging in highly dynamic V2X environments. On the other hand, the growing data volume and real-time nature of V2X applications impose the need for on-the-fly detection of threats on security and privacy [262]. Several existing misbehavior detection techniques lack the capability of identifying threats in real-time, and they are not efficient and robust enough to exploit the staggering amount of V2X data. Therefore, future V2X deployments would highly benefit from:

- Data-driven schemes offering intelligent security enforcement with real-time threats' prevention/identification/mitigation;
- Automation of security services with zero-touch workflows and self-managing capabilities (e.g., self-protection, self-healing and self-optimization);
- Efficient decision-making for security and privacy countermeasures.

In this context, AI/ML-empowered methods introduce key assets that can be effectively exploited in V2X security. Such techniques rely on large-scale datasets for model training and subsequent knowledge extraction.

> With the increasing avalanche of available data generated by vehicles and V2X infrastructure, AI/ML models can be trained to derive relationships between data points and detect threats not previously identified by traditional approaches.

Specifically, data-driven AI techniques can be used for traffic classification (e.g., encrypted data [318]) and detection of novel/unknown attacks by differentiating legitimate from misbehaving traffic. The analysis of behavioral patterns of vehicles and other V2X entities can also be facilitated by AI to determine trustworthiness levels. In principle, data-driven AI techniques are able to:

- Support automated selection of data features for improving the detection performance;
- Provide agile decision-making and automated response for adaptation to a dynamic threat landscape;
- Support attack detection and prevention of system-evasion strategies;
- Manage efficiently alarms (e.g., reducing false positives and false negatives).

Such capabilities can thus compensate the limitations of existing security solutions, conforming to V2X characteristics and providing effective means to achieve stringent security requirements.

B. Applicability in V2X Security

In this subsection, we elaborate on the applicability of AI/ML in V2X security, while summary tables synopsize key aspects of the proposed mechanisms in related literature. As illustrated in Figure 16, we have classified existing security enhancements in four different thematic areas, namely intrusion detection (Table 9), authentication and access control (Table 10), privacy preservation (Table 11), and trust management (Table 12). We provide the details in the following.

1) Intrusion detection

A key application of AI in V2X security is intrusion detection in heterogeneous environments involving entities

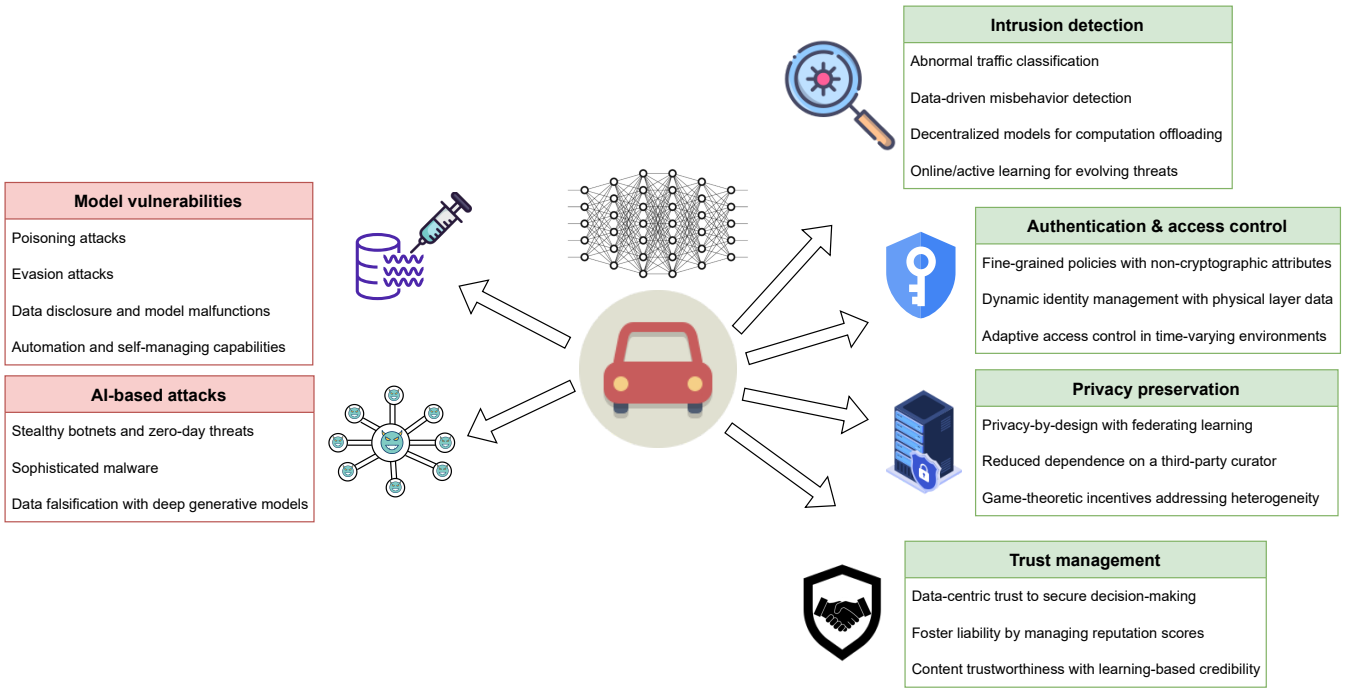


FIGURE 16: Benefits and threats introduced by AI/ML in V2X security. While data-driven techniques hold the promise of addressing highly sophisticated attacks, their application may expand V2X attack surface giving rise to new threats of escalating severity and complexity.

(i.e., vehicles, RSUs and edge/cloud servers) with asymmetric computational capabilities [319]. Existing V2X threat and attack detection approaches mainly depend on reactive mechanisms in order to balance communication cost and security overhead. The majority of those techniques employ supervised ML for known attacks using labelled V2X datasets [320], [322]–[325]. The work in [320] employs supervised learning algorithms selected in the WEKA toolset [338] to detect and classify misbehaving vehicles (e.g., position and identity spoofing and replay attacks) based on physical properties and message content. Attributes such as position, range, speed and RSSI, are exploited for detecting Sybil attacks; other features (i.e., number of packets transmitted, received, dropped and captured) are used to detect temporal attacks. Performance evaluation shows that random forest and J-48 algorithms yield significantly high classification performance. In [326], an ensemble-based ML approach is introduced to improve the detection accuracy of their earlier work [320]. The ensemble method combines the results of individual classifiers into a single output, and a majority-voting scheme is then used to decide whether a behavior is legitimate or malevolent.

The authors in [322] apply supervised learning to detect false-position information from safety messages sent by vehicles. In particular, the open-source VeReMi dataset [339] is used, which simulates several misbehavior attacks (e.g., position falsification, sudden stop and traffic congestion). The study applies support vector machine (SVM) and logistic regression (LR) algorithms to classify vehicles as attackers or non-attackers. Evaluation results show that LR yields higher detection accuracy with a normalized feature set than without normalization. Overall, SVM with normalization provides better accuracy than LR with or without normalization. A related work in [323] applies ML techniques on the same dataset to detect location-spoofing misbehavior. The proposed approach exploits plausibility checks (i.e., location and movement) to extract feature vectors from the dataset, and feeds them into two supervised ML models: K-Nearest Neighbors (KNN) and SVM. Results show that ML models produce higher accuracy than using a single plausibility check metric. The authors argue that adding better and more advanced plausibility checks to feature vectors would further increase the detection rate of applied ML models.

Supervised ML techniques (e.g., KNN, decision trees and LR) are also considered in [132] and [328] to quickly detect vehicles transmitting false alerts and position falsification. Using an augmented feature set which combines information from successive BSMs in VeReMi, the authors in [325] achieve improved detection performance for position falsification attacks compared to existing ML-based approaches. Position-related features are also used in [327] to extend VeReMi for a decentralized detection of position falsification attacks. Finally, a supervised learning classifier is introduced in [329] to extract mobility features and distinguish three types of Sybil attackers from benign vehicles by analyzing their mobility behavior.

With the continuous advancements of next-generation networks (e.g., beyond 5G), V2X security solutions are

TABLE 9: Overview of AI/ML applicability for intrusion detection in V2X

Paper	Methodology	Attack/Threat type	Connectivity mode(s)	Data/Simulator	Key remarks and limitations
[319]	Artificial neural network, Online support vector machine	Impersonation, Physical vulnerability	VANET	GloMoSim 2.03 simulator [279]	Multi-level intrusion detection from malicious RSUs and vehicles. Accuracy and attack detection rate gains over benchmark ML-based detectors. Local intrusion detection relies on packet dropping scanning which may not be always attributed to a security vulnerability.
[320]	Feature extraction, ML-based classifiers	Packet suppression/replay/detention, Identity spoofing, Position falsification	VANET	NCTUns-5.0 simulator [321]	Binary and multi-class misbehavior classification. Random forest and J-48 classifiers perform better compared to benchmark classifiers. Detection may fall short in identifying temporal attacks because of unavailability of packet transmit/receive information.
[322]	Support vector machine, Logistic regression	Position falsification	VANET	VeReMi	Support vector machine is shown to outperform logistic regression in terms of misbehavior detection performance. Multiple misbehavior detection remains an open issue.
[323]	K-nearest neighbor, Support vector machine, Plausibility checks	Position falsification	VANET	VeReMi	Detection precision improves by over 20%, while detection rate heavily depends on the plausibility check performance. Advanced plausibility checks are needed to increase recall and precision performance. Detection of Sybil attacks remains an open issue.
[324]	Support vector machine, K-nearest neighbor, Naïve Bayes, Random forest, Ensemble-boosting, Ensemble-voting, Plausibility checks	Position falsification	V2V	VeReMi	Ensemble learning algorithms outperform all other techniques. The addition of plausibility checks improves precision and recall values. Attackers can still foul play and manipulate the data without getting detected due to the high similarity between normal and abnormal data.
[325]	K-Nearest Neighbour, Random Forest, Naïve Bayes, Decision Tree with augmented feature set	Position falsification	VANET	VeReMi	An augmented feature set by combining information from successive BSMs allows more accurate attack detection compared to existing approaches using the same dataset and ML algorithms. Need for robust models capable of detecting inconsistencies in other BSM parameters (e.g., speed, acceleration, heading).
[326]	Ensemble method with ML-based classifiers	Packet suppression/replay/detention, Identity spoofing, Position falsification	VANET	NCTUns-5.0 simulator [321]	Ensemble method achieves classification gains over individual classifiers. A voting scheme performed by all individual classifiers enhances detection accuracy. True positive rate outcomes reveal that the accuracy of misbehavior detection can be further improved.
[327]	Ensemble learning, K-Nearest Neighbour, Random Forest	Position falsification	VANET	VeReMi	Decentralized position falsification attack detection using an augmented set of features related to the sender position. Evaluation for different traffic densities and attacker rates. Location-related features may not always be available, while multiple misbehavior detection remains an open issue.
[132]	K-nearest neighbor, Decision tree, Logistic regression, Bagging, Random forest	False alert, Position falsification	V2X	VeReMi	Improved detection compared to rule- and threshold-based detectors. Local misbehavior detection relies on neighboring information being available in the detector of each vehicle. Recall performance for constant offset attack needs to be improved.

Continued on next page.

expected to benefit from proactive exploration-based techniques for enhanced security levels [340]. For example, the authors of [341] propose a proactive anomaly detection approach to prevent cyberattacks on connected vehicles. In addition, supervised ML approaches may be impractical in real-time V2X scenarios, as the training and detection of labelled data do not work well when attacks change dynamically. In this context, RL and imitative learning methods can be further exploited in proactive and context-aware V2X security, e.g., for enhancement of threat-detection performance [331], [342]. Detection mechanisms can be dynamically improved with the accumulation of experience, and learn new V2X threats and attacks in rapidly changing environments.

Paper	Methodology	Attack/Threat type	Connectivity mode(s)	Data/Simulator	Key remarks and limitations
[328]	Feature extraction, Support vector machine, Decision tree, Random forest, K-nearest neighbor, Naïve Bayes, Logistic regression	Position falsification	V2V, V2I	VeReMi	Binary and multi-class misbehavior classification. The method provides accurate and real-time detection, leveraging only position features. VeReMi dataset inconsistencies affect the accuracy of the multi-class classifier.
[329]	Feature extraction, Naïve Bayes, Decision tree, Support vector machine	Sybil, Position falsification, Collusion	V2N	GAIA Open Dataset [330]	Learning-based classification together with location certificates and community-detection algorithms are able to effectively mitigate three levels of Sybil attackers. Sybil attack detection depends on the resolution of GPS data, while the trust value threshold affects detection performance.
[331]	Q-learning, Game theory	Eavesdropping, Jamming	Not specified	Customized simulator	Enhancement of PLS. The proposed scheme efficiently suppresses the attack rate and improves network secrecy performance. Location change of attacker not considered. Learning time is long and the convergence speed is slow.
[332]	RL-based detector	Position falsification, Speed falsification, DoS, Sybil, Replay	V2N, V2I	VeReMi	Detection of multiple misbehaving attacks variants from insiders. High accuracy using streaming vehicular mobility data. The characteristics of few attacks tend to resemble the genuine behavior, and mislead the RL model to trigger false positives.
[333]	Double deep Q-network, Q-learning	DDoS	V2X	Shenzhen taxicab dataset [334]	A feature-adaption reinforcement learning approach is proposed, taking into account the traffic space-time regularities to address unknown DDoS attacks with unlabeled data and less prior knowledge. Time and memory consumption of the proposed method needs to be controlled.
[335]	Deep Q-learning	Eavesdropping	V2X	Customized simulator	Enhancement of PLS. A deep Q-learning power allocation strategy is proposed to limit the decoding capabilities of eavesdroppers and improve secrecy performance. Cooperation among vehicles may further enhance secrecy performance.
[336]	Deep multilayer perceptron, Recurrent neural network architecture with a long short-term memory hidden layer	DoS, Command injection, Malware	In-vehicle network	Robotic vehicle testbed	Prototype implementation of DL-based intrusion detection for in-vehicle network. Enhanced detection accuracy against standard ML classifiers. Security of wireless medium not taken into consideration, rendering the approach vulnerable to physical availability threats.
[316]	Convolutional neural network, Long short-term memory	DoS, Data replay, Disruptive, Random, Sybil, Traffic congestion	V2V, V2I	VeReMi	A fine-grained classification is able to detect faults, attacks and normal behavior more accurate than a coarse-grained method.
[337]	Convolutional neural network, Long short-term memory, 4-layer multilayer perceptron	Disruptive, Data replay, DoS, Sybil	V2N, V2I	VeReMi	Time-sequence-based and sequence-image-based classification methods are implemented on a real-environment edge device. Sequence-image-based classification using convolutional neural networks is shown to outperform all models considered. Discrimination among security attacks, sensor malfunctioning and faulty data transmission remains an open issue.

In [343], the authors claim that most of the existing anomaly detection algorithms become less effective in the presence of high-dimensional data. In principle, V2X mobility data exhibit high dimensionality with multiple features, such as speed, location and heading angle, which are temporally and spatially co-evolving. RL-based detection mechanisms are identified as highly effective in dealing with such evolving data, even if labelled anomalous data samples are scarce [333], [344]. More importantly, RL-based detection can learn new threats and attacks from interactions with unknown environments while improving detection experience and performance [345]. Such approaches can practically be applied to V2X misbehavior detection, which may otherwise be hindered due to the lack of labelled data and/or the dependence on security threshold values. For example, an RL-empowered mechanism is proposed in [332]

for the detection of multiple misbehavior attack variants in VeReMi dataset. Misbehaving vehicles are shown to be effectively detected by sequentially analyzing their mobility patterns (i.e., real-time position coordinates and speed vectors). A deep Q-learning-based power allocation strategy is introduced in [335] to ensure optimal secrecy performance under the presence of eavesdroppers while guaranteeing the QoS requirements.

Given the real-time nature of vehicular applications, inference methods should be agile enough to perform anomaly detection and/or incident response in real-time. A centralized configuration, albeit leveraging the entire set of data fused from different geographical locations to reduce the risk of false positives, comes at the cost of higher computational complexity and extra communication delay. A centralized intrusion detection method for vehicles using DL is proposed in [336]. In an effort to enhance detection accuracy against standard ML classifiers, the authors in [336] resort to cloud-based computation which, in turn, introduces challenges related to the availability, cost, and security of the remote infrastructure used for offloading [346]. This cogently justifies the use of distributed and decentralized V2X setups for rapid attack detection with localized training and learning.

Two DL-based approaches relying on edge computing are introduced in [316] for identifying and classifying misbehaving vehicles. In a similar context, a MEC-based intrusion detection architecture is proposed in [337], which comprises DL engines for handling malicious vehicular traffic. Nevertheless, computation offloading at the edge poses significant challenges in dynamic multi-vehicle environments, which pose perils to system stability due to uncertain decision-making [347]. Further, a distributed learning model may not accurately detect certain attacks due to the lack of global view. Overall, the advantages of both approaches can be exploited in hybrid methods which can locally train the model in a distributed manner, and detect centrally [348]. Anomaly detection can thus be performed at different levels depending on the available information and computing capabilities, e.g., spatial deployment of MEC/cloud servers [349].

Online learning can also be leveraged for abnormal traffic detection in time-series V2X mobility data, especially in cases when training samples are not available all at once (e.g., in batches) and/or training over the entire dataset is infeasible, e.g., due to limited computational resources of vehicle OBUs. For example, an online learning technique is exploited in [350], to incrementally train a neural network for in-node anomaly detection with resource-constrained devices. Similarly, an online anomaly detection approach is presented in [351], where the model is sequentially updated while detecting anomalous data not conforming to normal behavior. However, normal behavior often tends to change across different geographical sites in V2X environments, while attacks may in parallel evolve. Hence, V2X threat-detection algorithms need to evolve accordingly. Active learning techniques can thus be exploited to deal with such dynamic and volatile V2X scenarios [352]. Active learning is a form of online learning, in which the algorithm is provisioned to choose relevant data for training and collects only specific samples. This class of learning techniques is useful in V2X, particularly when communication and computation are expensive for sample acquisition from all variables of interest.

2) Authentication and access control

Emerging AI-driven techniques are deemed essential towards efficient and scalable vehicle authentication without the need to rely on cryptographic attributes [353], [354], [360]. This stems from their ability to enforce adaptive access-control policies, by exploiting the time-varying non-cryptographic features which are intrinsically associated with vehicles' behaviors and the environment.

In particular, ML-based techniques can opportunistically leverage multidimensional physical-layer information (e.g., time, frequency and network architecture) rendering it difficult for an adversary to infer legitimate data based on the received signals and observations. Such intelligent authentication approaches are presented in [361] for complex environments, aiming to provide cost-effective, continuous, and situation-aware validation. In [362], an attribute-based access control system for cloud-assisted ITS infrastructures is introduced, with a fine-grained policy for authorization based on location, direction, and speed attributes.

A holistic authentication and authorization scheme based on online learning is proposed in [355], tailored for large-scale networks with resource-constrained nodes, as in V2X. The proposed access control policy is able to refine access policies on run-time by exploiting the time-varying features of the transmitter. The work in [356] propose an AI-based V2X authentication scheme to mitigate spoofing signal attacks originated from malicious edge nodes. The proposed framework uses the packet arrival interval and RSSI values of the ambient radio signals, received along the vehicular driving traces, to detect spoofing packets sent by rogue edge nodes. Transfer learning and deep reinforcement learning (DRL) are also applied to save the convergence time in the authentication process and decrease the authentication error, respectively. Finally, a two-way authentication and security monitoring method enhanced with a random forest algorithm is proposed in [357]. Compared to benchmark approaches, the scheme exhibits higher authentication accuracy and better adaptability to high-speed IoV environments. An FL-assisted collaborative authentication protocol is introduced in [358] to guarantee integrity of messages exchanged among vehicles and resistance against various attack types, such as replay, Sybil and MitM. A communication-computation tradeoff analysis also reveals that the communication efficiency of the proposed solution can be drastically improved at the expense of a slightly increased computational cost.

TABLE 10: Overview of AI/ML applicability for authentication and access control in V2X

Paper	Methodology	Attack/Threat type	Connectivity mode(s)	Data/Simulator	Key remarks and limitations
[353]	Convolutional neural network, Support vector domain description	Illegal/unauthorized drivers	V2X	Experimental setup for data collection	Proposed fingerprinting scheme can dynamically match the driver's identity in real-time without affecting the normal driving. Higher accuracy in driver identification and illegal driver detection compared to related work. The identification accuracy decreases as the number of drivers to be identified increases.
[354]	Long short-term memory, Support vector domain description, Feedforward neural network	Illegal/unauthorized drivers	V2X	Experimental setup for data collection	Illegal driver detection is successfully applied in different types of vehicles. The proposed scheme takes into account the long-term dependencies of driving behavior characteristics in contrast to baseline approaches. The identification accuracy decreases as the number of drivers to be identified increases. Insufficient vehicle data may lead to inadequate model training and inaccurate outcomes.
[355]	Support vector machine, Online learning	Unauthorized nodes, False data injection	V2X	Customized simulator	Proposed scheme achieves continuous authentication in the time-domain and lower complexity compared to a baseline physical layer key generation scheme. Prevention of potential key leakage and reduction of communication latency are reported. Decision making at a high layer is required for modeling the holistic authentication and authorization.
[356]	DRL, Transfer learning, Game theory	Spoofing	VANET	Customized simulator, Experimental setup	Authentication policy is optimized agnostic to the packet generation model, the VANET channel model and the spoofing model. Authentication performance gains over benchmark schemes in terms of miss detection and false alarm rates are reported. More accurate authentication is achieved at the cost of increased communication and computational overhead.
[357]	Random forest, Bagging, Elliptic curve cryptography	Replay, Masquerade, Impersonation, MitM	V2N, V2I	SUMO [177]	The proposed method ensures high behavioral consistency of vehicles. The impact of vehicle speed on authentication accuracy is also evaluated, demonstrating consistent trend with the classification performance. Monitoring accuracy also decreases with increasing vehicle variation probability.
[358]	Federated learning	Tampering, Replay, Sybil, MitM	V2V, V2N, V2I	SUMO [177], OMNeT++ [359]	A federated learning collaborative authentication protocol is proposed to reduce the number of vehicle certifications for each dynamic RSU. The packet loss rate of data transmitted and shared by vehicles is the main indicator of protocol security.

3) **Privacy preservation**

Among distributed ML techniques, FL emerges as a promising option for mission-critical vehicular scenarios with stringent low-latency and data-privacy requirements [379]. In contrast to conventional methods of data sharing in edge-cloud ML, FL implementations are privacy-preserving by design, eliminating the need to upload local training data to a cloud server for global aggregation. Instead, FL nodes only need to upload model parameters to servers, thus minimizing the risk of data breaches as well as the need to transfer raw data to an untrusted third-party curator. The potential of FL for privacy-preserving collaborative learning has recently attracted notable research interest, exploiting the concept of vehicular edge computing [363], [364], [367], [368].

A resilient two-phase scheme for mitigating vehicular data leakage is introduced in [370], using an FL model which addresses the privacy concerns associated with the vulnerability of a centralized curator. In a similar line of research, the authors in [372] propose a differentially private asynchronous FL approach for secure resource sharing in vehicular networks. The proposed scheme is evaluated with real-world datasets and exhibits good performance in terms of accuracy, as well as in protecting the privacy of training data. Federated averaging, a widely used FL technique, alternates between the computation of a local model at each vehicle and a round of communication with the server for learning of a global model [386]. Such an approach is adopted in [375] to avoid privacy breaches in the detection of misbehaving vehicles. The work in [376] addresses the problem of incentive mechanism design in FL-based IoV, by leveraging game-theoretic tools in the presence of multiple model owners and federations. Finally, the authors in [377] and [378] propose an FL-based collaborative-learning system to preserve privacy for IoV applications where resource-

TABLE 11: Overview of AI/ML applicability for privacy preservation in V2X

Paper	Methodology	Attack/Threat type	Connectivity mode(s)	Data/Simulator	Key remarks and limitations
[363]	Deep Q-network, Federated learning	Privacy leakage	V2N, V2I, V2V	Customized simulator	Fast convergence, low-latency performance and effective privacy protection over three baseline data sharing schemes. Multi-tasking data migration may, however, result in high complexity. Constant speed and single heading direction assumptions for vehicles. MEC needs to be synchronized with up-to-date vehicle status data.
[364]	Hierarchical federated learning	Privacy leakage	V2N, V2I	Synthetic data [365], Federated extended MNIST [366]	The method outperforms the baseline approach in terms of testing accuracy (improvement by 6.31%) and communication optimization (improvement by 2.15 times) with faster convergence speed. Tradeoff between local computing and global communication overheads.
[367]	Federated learning, Homomorphic threshold cryptosystem	Privacy leakage, Dishonest vehicles	V2N, V2I	Customized simulator	Improved computational efficiency over two traditional schemes. Robustness against dishonest users. Tradeoff between the privacy level and computational complexity is investigated. Key establishment relies on a homomorphic cryptosystem which is computationally heavy.
[368]	Federated learning, Adversarial autoencoder	Privacy leakage, Outdated content	V2N, V2I	MovieLens data [369]	Improved cache effectiveness over four baseline caching schemes. Protection of nodes' privacy and significantly reduced communication costs. Fully asynchronous federated learning may better cope with the highly dynamic environments and diverse computing capabilities.
[370]	Federated learning, Differential privacy	Privacy leakage	V2N, V2I, V2V	20 Newsgroups dataset [371]	Detection accuracy of the proposed data leakage defending scheme is higher than a baseline scheme. It is also capable of achieving near-real-time performance. Avoiding the eavesdropping of the model parameters in federated learning remains an open issue.
[372]	Federated learning, Differential privacy	Privacy leakage, Eavesdropping, Byzantine attack	V2N, V2I, V2V	20 Newsgroups dataset [371], Reuters dataset [373], Ohsumed dataset [374]	Higher average accuracy than three benchmark schemes. Model accuracy is hardly affected by the increase in data providers. Due to parallel local training, the running time increases little as the data size increases.
[375]	Federated averaging	Privacy leakage, Position falsification	VANET	VeReMi	Higher detection accuracy and significantly lower communication cost compared to a centralized training method. Privacy of the training process can be further improved using homomorphic encryption or differential privacy.
[376]	Federated learning, Coalitional game theory	Privacy leakage	V2X	Customized simulator	Model owners are shown to prefer joining federations that meet a minimum threshold of data quantity and quality. Fair distribution of payoffs based on each model owner's marginal contribution, even in the presence of information asymmetry. The impact of heterogeneous cooperation costs on the collaboration of model owners is not explored.
[377], [378]	Federated learning, Contract theory	Privacy leakage, Misreports	V2N, V2I	Customized simulator	Profit maximization guarantees with the highest utility derived only when data are reported truthfully to the model owner. Multiple sources of heterogeneity (e.g., different data quantities) do not affect the matching outcomes.

constrained vehicular components are aided by the deployment of UAVs. Their incentive mechanism relies on contract theory principles, and aims to match the optimal UAV to each sensing subregion while accounting for the heterogeneity in UAV types.

4) **Trust management**

Data-driven techniques have been also applied to foster and manage trust and liability in V2X systems, by enhancing confidence between entities and ensuring compliance with regulations. The authors in [380] introduce a hybrid ML and reputation-based scheme to enhance the detection accuracy of false alert and position falsification attacks in V2X. The proposed scheme leverages an edge-based local authority and a centralized certificate authority to manage the reputation scores of vehicles. An RL-driven data-centric trust scheme is proposed in [381] to improve reliability of shared vehicular information and secure the driving decision-making process. Trust evaluation can learn from historical feedback and dynamically determine the best strategy to address constantly varying vehicular scenarios. In [383], trustworthiness scores

TABLE 12: Overview of AI/ML applicability for trust management in V2X

Paper	Methodology	Attack/Threat type	Connectivity mode(s)	Data/Simulator	Key remarks and limitations
[380]	K-nearest neighbor, Logistic regression, Decision tree, Random forest, Bagging, Reputation scheme	False alert, Position falsification	V2X	VeReMi	Proposed hybrid scheme outperforms standalone ML-based schemes. Dempster-Shafer theory is used for combining evidences from multiple vehicles, while reputations are updated using the beta distribution. Detection performance is negatively correlated with the reputation score of malicious vehicles. Detection of online/active attacks is an open issue.
[381]	RL-driven trust evaluation, Information entropy theory	Bogus information	VANET	Veins simulator [184]	Adaptive scheme to different driving scenarios with negligible time overhead, regardless of the proportion of malicious nodes. Higher evaluation precision rate compared to three benchmark trust models. Trust management may be subject to adversarial attacks, which exploit vulnerabilities by faking pseudonyms, and mislead the RL model.
[382]	Q-learning, Fuzzy logic	Untrustworthy vehicles	VANET	NS-2 [173]	Proposed method leverages fuzzy logic for trust evaluation of one-hop neighbors, and Q-learning for indirect trust evaluation of nodes outside the directly observable region. The effect of vehicle velocity on packet forwarding ratio is not considered in the packet drop estimation, which may lead to inaccurate trust estimation for the honest vehicles propagating messages already altered by malicious ones.
[383]	Trust-aware control policies based on deep Q-learning	Untrustworthy vehicles	V2X	AIM simulator [384]	Proposed method decreases the collision rate and maintains stable low collision rate even when all vehicles are untrustworthy. Trade-off between performance (throughput) and safety (collision avoidance). The generalizability of the trust framework needs to be verified in a broader range of multi-agent setups.
[385]	Deep feedforward network, Blockchain	Compromised vehicles/RSUs (simple, bad mouth, and zigzag attacks)	V2V, V2I	NS-2 [173] SUMO [177]	Proposed scheme performs better than two baseline approaches by managing the trust of vehicles and detecting malicious ones in an accurate and efficient manner. How to effectively evaluate trust while maintaining the privacy of vehicles remains an open issue.

Continued on next page.

of traffic participants are used to synthesize trust-aware controllers for ITS, utilizing a DRL-based approach.

A DL-based trust management system is introduced in [385] to evaluate the trust of vehicles, RSUs, and exchanged information in an automatic and dynamic manner. Local and global trust level calculations are performed with the aid of a feedforward neural network algorithm, which identifies malicious vehicles and learns the potential correlation among them. Aiming to ensure content trustworthiness in AV-navigation systems, the work in [387] adopts an AI-empowered trust-information-centric architecture where content credibility decisions are determined using DRL. Finally, the works in [389], [392] focus on the optimal routing selection problem in software-defined vehicular networks, by employing a trust-based DRL scheme which extracts useful features from the available routing information. A similar methodology has been recently proposed in [391], where DRL is used to determine the most secure communication link policy under the effect of malicious vehicles.

C. Threats and Vulnerabilities

The integration of data-driven techniques in V2X systems is a double-edge sword. As illustrated in Figure 16, AI/ML models, albeit offering novel solutions to challenging security problems, constitute a source of new attack vectors. The automation and self-managing capabilities offered by AI expands the attack surface, giving rise to finely targeted, stealthier, and scalable attacks. In particular, ML techniques are susceptible to attacks targeting both training (i.e., poisoning attacks) and test (i.e., evasion attacks) phases. In *poisoning* attacks, an attacker intentionally tampers the training data, by injecting carefully crafted malicious samples or contaminating the original data to influence the learning outcome. The authors in [395] assess the impact of a Sybil-based data poisoning attack against an IoV service placement mechanism empowered by DRL. The performance degradation in terms of delay and resource congestion is quantified for different proportions of Sybil vehicles. In *evasion* attacks, the attacker attempts to bypass the learned model by introducing small perturbations to the test instances (adversarial examples). An evasion attack in autonomous driving scenarios is introduced in [396], where the adversary's goal is to increase the probability that the targeted test sample is misclassified in a traffic sign recognition process. Data disclosure threats also exist in ML setups, pertaining to the possibility of leakage of all or partial information about the applied model. Finally, failures or malfunctions of the ML application components are also possible, e.g., due to

Paper	Methodology	Attack/Threat type	Connectivity mode(s)	Data/Simulator	Key remarks and limitations
[387]	DRL-enabled content credibility decision, Blockchain	Untrusted content	V2X	Customized simulator	Proposed method can determine whether the content is trusted intelligently based on content status and nodes' behaviors. Cumulative time delay of the consensus phase increases with the blockchain height. Due to the transparency of blockchain for all participants, privacy (e.g., patterns of behaviors) may be extracted by attackers.
[388]	DRL, Blockchain	Information leakage	V2N, V2I	Customized simulator	Blockchain technology is jointly applied with a DRL algorithm to prevent information leakage and ensure trust evaluation decisions for vehicular service offloading and migration. As the average transaction size increases, the system throughput of decreases, while an increase in vehicular speed leads to increased task execution overhead.
[389]	Deep Q-learning	Random packet drop	VANET	OPNET 14.5 [390]	Performance gains in terms of packet delivery ratio and average network throughput compared to two baseline schemes. Impact of learning rate on the convergence performance is studied. Packet delivery ratio deteriorates with increasing number of vehicles, since misbehavior of the malicious nodes increases the possibility of packet loss.
[391]	Deep Q-learning	Tampering	VANET	Customized simulator	Proposed method is shown to improve performance of data forwarding, link quality, and security of connected vehicles under different architectures of deep Q-networks. Expected transmission count delay increases with increasing number of vehicles, posing a scalability challenge. Privacy concerns not taken into account.
[392]	Dueling deep Q-network	Random packet drop	VANET	OPNET 14.5 [390]	Average network throughput gains compared to two baseline schemes, at the cost of a slightly higher average end-to-end delay. Average end-to-end delay increases with increasing number of vehicles, posing a scalability challenge. Privacy concerns not taken into account.
[393]	Federated learning, Blockchain	Untrustworthy vehicles, Poisoning attack	V2N, V2I, V2V	KDDCup99 [394]	A dynamically updated intrusion detection system is maintained by vehicles and RSUs for accurate model aggregation and sharing. A blockchain incentive mechanism is proposed to ensure privacy-preservation and high accuracy of the federated learning model training. The considered dataset contains general purpose network traffic, and it is not directly associated with vehicular environments.

inappropriate format of input data caused by a malicious action (sponge example).

Besides the lack of robustness and vulnerabilities of AI/ML models and algorithms, the malevolent use of AI can potentially create highly sophisticated types of adversarial attacks, such as AI-empowered malware, AI-augmented DDoS attacks and deep generative models for false data generation [397]. Attackers are able to make malicious use of AI techniques while constantly improving their attack strategy with the use of evolving adversarial examples. Among others, DeepLocker [398], i.e., a highly targeted and evasive malware, and PassGAN [399], i.e., a fully automated password guessing technique based on DL, can be highlighted as two exemplary case studies of AI-based cyber-attacks. Therefore, it is of paramount importance that V2X networks become resilient against hostile threats stemming from the malicious AI use. In this context, ETSI has recently launched a new industry specification group on securing AI (ISG-SAI) with the aim to create high-quality technical standards to preserve and improve the security of new AI technologies [400].

D. Lessons Learned

5G and AI transformational paradigms are already driving research towards the realization of fully automated networks. In this context, AI/ML-based techniques constitute promising and future-proof enablers to empower key V2X security functions, such as efficient prediction and detection of anomalies linked to security incidents, authentication, privacy preservation and trust enhancement. The advanced and automated capabilities of AI/ML schemes hold the promise of addressing the limitations of traditional proactive/reactive security approaches in emerging IoV environments. However, their direct integration in networks with highly dynamic topologies, ephemeral connectivity and distributed setups is inherently challenging.

The envisioned benefits of AI/ML techniques should not overlook the potential risks of their use. Consequently, the growing enthusiasm for AI/ML adoption in V2X security could be waned if security concerns related to the malevolent use of AI are not addressed. Therefore, significant research efforts are required to materialize AI-driven intelligent security mechanisms in V2X systems. We foresee that research

groups around the world and standards developing organizations will steer their efforts to integrate data-empowered security mechanisms in future V2X networks. Over the next years, network operators are also expected to advance the implementation of automated, closed-loop security enforcement and control functionalities for vehicular systems.

Finally, the importance of explainability has been recently highlighted in the context of AI-based solutions for safety-critical V2X, as a means of reducing model vulnerabilities against external attacks [401]. Explainability can be achieved either via the adoption of post-hoc explainability techniques or with the design of inherently interpretable built-in models. The incorporation of such methodologies would foster trustworthiness in AI-enabled V2X systems, as well as their legal and regulatory compliance.

VII. Open Challenges and Future Research Paths

While V2X standardization and deployment phases are progressing, a growing body of research evolves around security and privacy in V2X, with the potential of developing efficient solutions by satisfying emerging V2X applications' requirements. This survey has focused on security and privacy implications introduced by ubiquitous V2X connectivity, with a close look at potential cyber threats and appropriate prevention, detection and mitigation mechanisms. In this context, we offer a comprehensive review of existing proactive and reactive solutions, as well as emerging methods relying on the nascent AI paradigm.

Although several technical challenges are discussed throughout the survey, this section highlights additional open issues and key research paths to effectively address cybersecurity concerns in future V2X systems. As outlined in Table 13, our envisioned security roadmap covers three distinct yet intertwined areas of V2X communication and networking, with the overarching goal of enriching research agendas with promising directions and security guidelines. We provide the details in the following.

A. Architectural Plane

1) Deployment limitations of V2X network components

Efficiency and effectiveness of security reporting-response mechanisms depend on the available V2X information, which may not be the same at various network entities and levels. In a local vehicular network, for example, vehicles are able to acquire mobility data from neighboring vehicles in their communication range. However, as highlighted in Section V, such information might be insufficient for detecting DDoS or misbehavior executed in a distributed manner [14]. In such scenarios, the tendency is to aggregate distributed data into a central entity (e.g., an RSU or MEC) and perform data-driven detection based on historical information. Vehicles are typically geographically clustered using metrics such as density, velocity, and geographical location [402]. Nevertheless, in terms of network availability, RSUs and MEC servers are sparsely deployed due to incurred installation and operational costs [403]. Network coverage and road traffic conditions are further considered essential for the deployment of stationary infrastructure nodes.

Such limitations may hinder the efficacy of security mechanisms from a practical implementation perspective. Distributed data transfer to a central location may also result in excessive resource consumption and latency, which, in turn, may violate the stringent V2X performance requirements. A rather unexplored research direction to overcome V2X deployment limitations, is to exploit the underlying physics of traffic with consistency checks against fundamental physical laws dictated by traffic flow theory [404]. For example, the incorporation of domain knowledge, e.g., traffic density, kinematics laws of motion, and vehicular physics, in the design of data-driven security enablers, may overcome the incomplete vehicular measurement streams owing to deployment limitations, and reduce the computational burden pertaining to the limited capabilities at the vehicular edge.

2) Multi-tenant infrastructure

Vehicular services are typically multi-tenant, involving multiple stakeholders, e.g., road authorities, municipalities, original equipment manufacturers, network operators and service providers. In contrast to previous mobile network generations, 5G architecture leverages cloud-native concepts to allow the disaggregation of network functions. 5G-enabled vehicular infrastructure is thus able to host multiple logical networks at the same time, allowing multi-service and multi-tenancy deployments. By leveraging cloud computing, software-defined networking and network functions virtualization, V2X services can be instantiated in a flexible manner, following a network-as-a-service model.

In this setting, new challenges for end-to-end security and trust are introduced. For example, multi-tenant infrastructures shared among multiple virtual network operators require strict resource isolation at multiple levels to avoid misuse of the network resources and maintain integrity of vehicles' information [64]. The agile orchestration of multi-domain and multi-tenant security policies is, thus, of paramount importance, complementing traditional perimetral protection technologies. Real-time monitoring of security service level agreements becomes indispensable, while advanced mechanisms are required to foster trustworthiness by empowering trust in software components and AI/ML-based techniques. In this context, distributed ledger technologies, e.g., blockchain, can be adopted to achieve trustworthy interoperability across various parties involved in the V2X service chain. As discussed in Section II-C, blockchain technology allows managing the complexity of a multi-stakeholder V2X framework with automated settlements using smart contracts [405]. Its distributed nature and immutability features can play a pivotal role in fostering trust in distributed AI/ML models [406]. In this context, a recent

TABLE 13: Summary of open challenges and future research directions in V2X security

	Area	Open challenges	Potential research directions
Architectural	Deployment limitations of V2X network components	• Sparse installation of edge nodes • Insufficient information available for attack detection/mitigation • Heterogeneous computational capabilities	• Dynamic clustering solutions • Incorporation of vehicular domain knowledge and physical laws • Consistency checks against traffic flow theory
	Multi-tenant infrastructure	• Trust management across stakeholders • Conflicting security policies • Infeasible service level agreements	• Trustworthy interoperability with blockchain • Agile security policy orchestration • Dynamic liability chains
	Zero-touch security service provisioning	• Compromised software components • API-based vulnerabilities • Threats related to intent-based interfaces	• Trusted execution environments • Use of API gateways with customized features • AI-based API security
Computational	Practical implications of PKI implementation	• Equipment interoperability • Lack of practical feasibility studies and real-world testing at large-scale • Scalability limitations of asymmetric cryptography	• Crypto-agile V2X systems • Scalable pseudonym reusage policies and revocation mechanisms • Impact of sporadic V2X connectivity links
	Quantum-safe cryptography	• Unexplored trade-offs with energy consumption and deployment cost • Quantum-based adversaries • Large key size of public-key ciphers	• Quantum-resistant enhancements in current ciphersuites • Quantum key distribution for long distances • Lattice-based cryptography
	Over-the-air computing	• Manipulation of summation operation • Asymmetric computation, storage, communication capabilities • Adversarial attacks using channel information	• Alliance with differential privacy techniques • Probabilistic crypto-less over-the-air key establishment protocols • Active attack mitigation aided by PLS schemes
Learning	Availability of datasets	• Limited open-source vehicular data • Unbalanced and irregular attack information • Deviance from real-world scenarios	• Openness and reproducibility of vehicular data • Feature engineering • Resampling strategies
	Vulnerabilities of decentralized learning solutions	• Data manipulation at training/inference phase • Model replacement attack at local level • Vulnerabilities due to server-client architecture	• Hybrid learning with local differential privacy • Hierarchical blockchain-based schemes • Integration of vehicle dynamics in learning phase
	Trustworthiness of AI-based security	• Model extraction/inversion attacks • Information integrity and availability risks • Privacy violation via reverse-engineering methodologies	• Adversarial ML • Explainable AI and physics-informed learning • Ensemble learning models to address adversarial concept drift

work in [407] proposes a blockchain-based strategy with hierarchical incentive mechanisms, utilizing FL to prevent privacy leakage and ensure accurate and fair trust evaluation.

3) Zero-touch security service provisioning

The pervasive integration of AI/ML and SDN/NFV technologies in beyond-5G vehicular networks is envisioned to increase the level of security management automation towards real-time zero-touch orchestration across multiple domains. In particular, security service provisioning is expected to be guided by intelligent decision engines with agile and self-dynamic capabilities, in line with the ETSI zero-touch network and service management (ZSM) reference architecture [408]. Besides its benefits, a fully automated V2X network rollout comes inadvertently with security risks and compelling attack surfaces that can be exploited for malicious purposes. Software entities involved in the security management operations (e.g., SDN controllers, NFV orchestrators) may become themselves malicious or compromised, leading to adverse effects on network performance and security. For example, compromised virtual network functions (VNFs) could execute a poisoning attack, as discussed in Section VI-C, and provide wrong monitoring data that may mislead AI/ML models in a ZSM-based security system.

To establish VNF confidentiality and integrity at runtime, trusted execution environments (TEEs) are considered a promising option in the presence of V2X introspection attacks [409]. TEEs achieve the isolation of data and operations in a secure enclave that allows access only through an attested link supported by hardware-secured technologies. However, the adoption of TEEs in V2X virtual environments is challenged by the limited computational capacity at the vehicular edge, their relatively complex use and the incurred performance overhead. In an effort to improve scalability, a recent work in [410] proposes a decentralized trust management system with a parallel consensus model which jointly considers TEEs and blockchain technology to secure trust evaluation. In addition, while open APIs play an integral role for the realization of security management automation, they introduce notable vulnerabilities which can be exploited in vehicular API-based attacks. Although API security is a rela-

tively new concept, the associated attacks performed through the APIs are not; examples include identity, MitM, and DoS attacks [411]. Such attacks may result in information leakage/alteration, identity theft, as well as vehicular service unavailability. A common approach to enhance API security is the use of API gateways with customizable parameters, to perform rate limiting, fine-grained authentication and authorization, and content routing for reliable access to backend services. AI-based API security is also gaining ground to strengthen API capabilities; it may, however, expand the attack surface with additional threats, as discussed in Section VI-C.

B. Computational Plane

1) Practical implications of PKI implementation

As discussed in Section IV, authentication and integrity protection mechanisms reduce attack surfaces by restricting severe outsider attacks (e.g., Sybil, spoofing and DoS). To this end, solutions based on PKI and digital signatures have been standardized and extensively studied in V2X communication. However, the validation techniques summarized in Table 6 reveal that there are still feasibility gaps between existing academic research and real-world testing of PKI practices at large-scale for V2X services. The stringent V2X security and privacy requirements have led to even more complex PKI architectures with many entities and layers that make it harder to scale. Experimental assessment of such approaches has only been conducted under limited operating conditions, which may hinder the transition of PKIs to practice [171]. Additional feasibility and comparative studies are thus necessary to discover and resolve possible computational issues, owing to ambiguous specifications in standards, interoperability of equipment from different vendors, and scalability of computationally intensive asymmetric cryptography schemes [412].

To overcome hardware constraints, crypto-agile V2X systems, capable of coupling asymmetric and certificate-based cryptography with more traditional symmetric cryptographic algorithms, appear as a promising approach. Pseudonym reusage policies and revocation mechanisms need to be carefully managed to account for massive connectivity in IoV environments. In existing PKI methods, trade-offs between computational aspects, such as CRL size, complexity, delay overhead, and RSU availability, deserve further research attention, as outlined in Section IV-D. The impact of the sporadic availability of communication channel among the vehicle, the road infrastructure and the back-end servers needs also to be further explored. Finally, since the existence of a PKI architecture does not guarantee per se the enactment of trust between the involved entities, the roles of different stakeholders in the PKI need to be properly defined.

2) Quantum-safe cryptography

The advent of quantum computing paradigm with its powerful processing capacity is expected to play an important role in emerging autonomous-driving scenarios, e.g., traffic flow control optimization. However, as essential it is to the realization of autonomous driving as an accessible service, quantum technology introduces vulnerabilities and security risks [413], [414]. In particular, traditional symmetric and asymmetric cryptographic techniques are threatened by the prospect of adversaries with quantum computing capabilities. Quantum algorithms have the disruptive potential to effectively break cryptography schemes which are in widespread use in existing V2X communication systems. Thus, cryptographic primitives described in Section IV, such as hash functions and symmetric key encryption, become vulnerable to quantum cyberattacks and require increasing the key length, leading to higher computing power. Further, large-scale quantum computers may be able to quickly (i.e., in the order of minutes or hours) break asymmetric encryption solutions that base their security on integer factorization or discrete logarithms, which otherwise could take hundreds of years on today's most powerful computers.

The introduced vulnerabilities and quantum computing security risks in V2X systems render the development of post-quantum cryptographic techniques, such as quantum key distribution (QKD) and quantum-resistant algorithms, imperative to address quantum-era cyberattacks [415]. QKD leverages the laws of quantum physics to protect data exchange inside the backend V2X infrastructure by offering forward secrecy and ensuring anti-eavesdropping of the encryption keys. A quantum-resistant cryptography scheme based on location-aware lattices is introduced in [416] to address collusion and quantum attacks, revealing a trade-off between the network performance metrics (i.e., delay, throughput, energy efficiency) and security robustness. Lattice-based cryptographic solutions are generally capable of providing an additional level of quantum defense by properly concealing data in complex and abstract mathematical structures exploiting the hardness of short vectors in lattices [417], [418]. The trade-offs among key sizes, signature lengths, network performance, and security raise intriguing research questions in the upcoming post-quantum era [419].

3) Over-the-air computing

V2X entities are asymmetric in terms of computational capabilities, with particularly limited resources available at the vehicular edge. Although MEC servers are capable of aggregating data from different sources, the incurred computational burden may limit the execution of heavy and complex tasks, e.g., decentralized learning [420]. In particular, large and structured training datasets are necessary for data-driven detection schemes to function adequately [421]. Handling such high volumes of vehicular data at the edge entails high computational power, high convergence time to obtain

sufficient training and test accuracy, and memory shortage risks.

In this context, over-the-air (OTA) computing emerges as a promising alternative to relieve computational burden, by exploiting the signal superposition property to calculate functions of the individual signals over the air. This novel parallel computing paradigm synergistically merges the communication and computation tasks to establish secure communication links with minimum resource consumption and sizable performance gains over classical separation-based approaches. OTA mechanisms are gradually gaining momentum for privacy preservation in decentralized learning environments. Secure OTA computing with differential privacy is recently proposed in [422] to prevent the inference of private data in FL setups. In a similar line, the privacy-for-free mechanism in [423] shows that enforcing a differentially private constraint into an OTA scheme keeps the learning performance unaltered compared to a non-private design. However, vulnerabilities at the vehicular edge and adversarial attacks may compromise the integrity, availability and/or privacy of OTA-based learning, thus challenging the trustworthiness of the approach. For example, active attacks, described in Section III-B, may manipulate the OTA computation process, leading to wrong computational model learning and service failure. The heterogeneity in computation, storage, and communication capabilities across the V2X entities constitutes an additional research challenge in OTA-based learning systems.

C. Learning Plane

1) Availability of datasets

The majority of misbehavior detection mechanisms are data-centric, and require a considerable volume of data to obtain effective outcomes. As discussed in Section VI, complete and well-structured training datasets allow AI/ML models to obtain relevant knowledge for the detection and identification of attacks. Since the availability and quality of training data become crucial for the effectiveness of solutions, it is essential to include *sufficient* attack information and create *balanced* datasets while representing real-world characteristics. Similarly, test datasets are also necessary to evaluate and compare both accuracy and performance against benchmark approaches. In the context of AI/ML-based security, acquiring high-quality datasets with adequate realizations of V2X attack types, is a non-trivial task.

In their vast majority, security mechanisms are validated through system-level simulations and theoretical model assessment. However, existing simulators are rather limited in fully characterizing the complexity and dynamics of real V2X communication systems. Notably, most of the presented studies are focusing on specific attack scenarios and have incorporated strict assumptions on their theoretical models that may not reflect V2X characteristics in reality. Further, as elucidated in Tables 9–12, many researchers have not made publicly available the datasets used in the evaluation; in turn, this lowers the possibility of reproducibility and comparative feasibility studies, posing unprecedented challenges in the assessment of security proposals under common real-world V2X scenarios. It is noted, though, that most research works are restricted from accessing real-world V2X datasets due to various reasons, such as internal policies of automakers and infrastructure providers and/or data protection laws (e.g., GDPR). On the other hand, field measurement tests of security architectures can be prohibitively expensive, while the execution of attack scenarios may not be practically feasible with real vehicular fleets involved. Access to V2X-compatible infrastructure is not currently widespread due to the lack of extensive and large-scale deployments. Considering all aforementioned challenges, evaluating detection/mitigation mechanisms by simulating cyberattacks seems to be the most viable option and equally important as coming up with novel methods. Further efforts are needed towards generating open-source datasets and making them publicly available for the research community.

2) Vulnerabilities of decentralized learning solutions

Distributed learning methods hold the promise of exploiting the edge components in large-scale vehicular networks to decrease learning time and improve resource efficiency [424]. By diffusing distributed intelligence in a V2X system, vehicles turn into smart cooperative agents and can perform collaborative learning tasks without centralized orchestration. Collaborative learning underpins local decisions and allows vehicles to exchange their locally trained model parameters. As discussed in Section VI-B, albeit FL approaches are gradually gaining momentum towards the realization of privacy-by-design V2X (e.g., anonymous data collection and/or retrieval [425]), they still rely on a server-client architecture, rendering them vulnerable to several attacks (e.g., due to faulty software, hardware invasions, and unreliable communication channel). In addition, locally trained ML models may suffer from data poisoning and adversarial manipulations (e.g., malicious samples deliberately crafting the model).

To this end, the development of robust FL designs against these attacks constitutes an open research challenge. A recent work in [426] combines FL and local differential privacy to prevent adversaries from deducing the exact location information of vehicles even when the uploaded gradients to the cloud are compromised. The authors in [427] introduce a hierarchical FL framework empowered by blockchain ledgers to enhance security and facilitate the distributed knowledge-sharing process. The proposed scheme is shown to adapt well to large-scale vehicular networks with diverse regional characteristics and effectively defend against malicious nodes during the sharing process. In a similar direction, a blockchain-based collective learning approach is presented in [428] to further protect the distributed learned models.

The integration of underlying vehicle dynamics to control the learning phases in FL, and the consideration of time-varying connectivity links to manage the coexistence of outdated or partially trained models with highly automated ones, constitute promising future research paths [429].

3) Trustworthiness of AI-based security

One of the key concerns related to the integration of AI-based techniques in V2X security refers to adversarial attacks which may cause trained models to behave in undesired ways, as discussed in Section VI-C. Depending on the attacker's level of knowledge, attacks against AI/ML can be divided in two categories [430]: *i*) *white-box* attacks, which assume that the attacker has complete knowledge about the training data, the algorithm and its hyper-parameters; *ii*) *black-box* attacks, which assume that the attacker has no knowledge about the algorithm and its hyper-parameters. In the latter case, the attacker first observes the AI-based system's response to its query and uses this outcome to craft adversarial examples. These data manipulation attacks render AI/ML models vulnerable by introducing integrity, availability and/or privacy-violation risks. Integrity risks result in indecisiveness, delayed decisions, poor or even wrong decisions, while availability perils usually refer to the considerable rise of classification errors up to such levels where the system becomes effectively unusable. Privacy violation may also occur when private V2X information is disclosed by reverse-engineering the learning algorithm.

Dealing with adversarial attacks is non-trivial and requires solutions to foster trust and stimulate confidence in AI/ML models. In this context, AI model interpretability and adversarial ML can contribute towards the elevation of trustworthiness in AI-based solutions [431], [432]. Model interpretability (or explainable AI) aims at ensuring accountability, reliability and transparency, by explaining how and why decisions are taken based on training data. An interpretable scheme has been recently proposed in [433] for the detection of location forging attacks, which leverages a boosting decision tree ensemble to elevate the trust in the predicted security decisions. Explainable AI frameworks for trust management have been recently proposed in [434], [435]. The challenge here resides in balancing the resulting trade-off between interpretability and model accuracy. In an effort to render ML techniques resilient to adversarial attacks, adversarial AI aims at assessing the security robustness of learning algorithms and designing appropriate countermeasures [432]. While adversarial AI has already attracted considerable interest in the field of computer vision, future research efforts need to be devoted to mastering how AI-based attacks are launched in V2X environments and ensuring the safety of AI models. In this research line, a DRL algorithm aimed to maximize the robustness of AV dynamics against false data injection attacks has been recently introduced in [436].

VIII. Summary

This survey has compiled and reviewed recent developments in V2X security, offering a thorough assessment of state-of-the-art security enhancements proposed to date. Our methodology is based on three main pillars. First, we have presented a classification of threat/attack vectors that may hinder secure and safe operation of V2X systems. Second, a taxonomy of existing mechanisms, based on their proactive/reactive defensive attitude, has been proposed to help determine their feasibility in preserving fundamental security and privacy requirements against V2X attacks. Third, as AI poses elevated merit in addressing identified and foreseen limitations, we have thoroughly explored the applicability of data-driven techniques in V2X security. Finally, in an effort to motivate and foster further contributions in the field, we have summarized key open challenges in V2X security and provided relevant research guidelines.

REFERENCES

[1] S. K. Datta, R. P. F. Da Costa, J. Härri, and C. Bonnet, "Integrating connected vehicles in Internet of Things ecosystems: Challenges and solutions," in *2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2016, pp. 1–6.

[2] S. K. Datta, J. Härri, C. Bonnet, and R. Ferreira Da Costa, "Vehicles as Connected Resources: Opportunities and Challenges for the Future," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 26–35, 2017.

[3] M. Muhammad and G. A. Safdar, "Survey on existing authentication issues for cellular-assisted V2X communication," *Vehicular Communications*, vol. 12, pp. 50–65, 2018.

[4] V. Marojevic, "C-V2X security requirements and procedures: Survey and research directions," 2018. [Online]. Available: arXiv:1807.09338v1.

[5] K. Bian, G. Zhang, and L. Song, "Security in Use Cases of Vehicle-to-Everything Communications," in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, 2017, pp. 1–5.

[6] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications*, vol. 44, pp. 1–13, 2014.

[7] ETSI, "Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)," Tech. Rep. TR 102 893 V1.2.1, March 2017.

[8] A. Ghosal and M. Conti, "Security issues and challenges in V2X: A survey," *Computer Networks*, vol. 169, p. 107093, 2020.

[9] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017.

[10] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[11] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Vehicular Communications*, vol. 9, pp. 19–30, 2017.

[12] A. Alnasser, H. Sun, and J. Jiang, "Cyber security challenges and solutions for V2X communications: A survey," *Computer Networks*, vol. 151, pp. 52–67, 2019.

[13] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, p. 100214, 2020.

[14] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing Vehicle-to-Everything (V2X) Communication Platforms," *IEEE Transactions on Intelligent Vehicles*, pp. 1–1, 2020.

[15] J. Huang, D. Fang, Y. Qian, and R. Q. Hu, "Recent Advances and Challenges in Security and Privacy for V2X Communications," *IEEE Open Journal of Vehicular Technology*, vol. 1, pp. 244–266, 2020.

[16] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)," *Vehicular Communications*, vol. 25, p. 100247, 2020.

[17] A. Talpur and M. Gurusamy, "Machine Learning for Security in Vehicular Networks: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 346–379, 2022.

[18] S. Khan, F. Luo, Z. Zhang, M. A. Rahim, M. Ahmad, and K. Wu, "Survey on Issues and Recent Advances in Vehicular Public-key Infrastructure (VPKI)," *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2022.

[19] D. P. M. Osorio, I. Ahmad, J. D. V. Sánchez, A. Gurtov, J. Scholliers, M. Kutila, and P. Porambage, "Towards 6G-Enabled Internet of Vehicles: Security and Privacy," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 82–105, 2022.

[20] R. Sedar, C. Kalalas, F. Vázquez-Gallego, and J. Alonso-Zarate, "Intelligent Transport System as an Example of a Wireless IoT System," in *Wireless Networks and Industrial IoT: Applications, Challenges and Enablers*, N. H. Mahmood, N. Marchenko, M. Gidlund, and P. Popovski, Eds. Cham: Springer International Publishing, 2021, pp. 243–262.

[21] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *Journal of network and computer applications*, vol. 37, pp. 380–392, 2014.

[22] X. Shen, R. Fantacci, and S. Chen, "Internet of Vehicles [Scanning the Issue]," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 242–245, 2020.

[23] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C. Lin, and X. Liu, "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[24] 3GPP, "Architecture enhancements for V2X services (Release 17)," Tech. Rep. TS 23.285 v17.1.0, July 2022.

[25] 3GPP, "Architecture Enhancements for 5G System (5GS) to Support Vehicle-to-Everything (V2X) Services (Release 16)," Tech. Rep. TS 23.287 v16.7.0, July 2022.

[26] ——, "Architectural enhancements for 5G multicast-broadcast services (Release 17)," Tech. Rep. TS 23.247 v17.4.0, September 2022.

[27] A. García Olmos, F. Vázquez-Gallego, R. Sedar, V. Samoladas, F. Mira, and J. Alonso-Zarate, "An Automotive Cooperative Collision Avoidance Service Based on Mobile Edge Computing," in *Ad-Hoc, Mobile, and Wireless Networks*, M. R. Palattella, S. Scanzio, and S. Coleri Ergen, Eds. Cham: Springer International Publishing, 2019, pp. 601–607.

[28] L. Li, Y. Li, and R. Hou, "A Novel Mobile Edge Computing-Based Architecture for Future Cellular Vehicular Networks," in *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, 2017, pp. 1–6.

[29] Z. Xu, X. Li, X. Zhao, M. H. Zhang, and Z. Wang, "DSRC versus 4G-LTE for Connected Vehicle Applications: A Study on Field Experiments of Vehicular Communication Performance," *Journal of Advanced Transportation*, vol. 2017, pp. 1–10, 2017.

[30] S. Chen, J. Hu, Y. Shi, Y. Peng, J. Fang, R. Zhao, and L. Zhao, "Vehicle-to-Everything (V2X) Services Supported by LTE-Based Systems and 5G," *IEEE Communications Standards Magazine*, vol. 1, no. 2, pp. 70–76, 2017.

[31] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments," in *VTC Spring 2008 - IEEE Vehicular Technology Conference*, 2008, pp. 2036–2040.

[32] J. B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[33] A. Festag, "Cooperative intelligent transport systems standards in Europe," *IEEE Communications Magazine*, vol. 52, no. 12, pp. 166–172, 2014.

[34] K. Sjoberg, P. Andres, T. Buburuzan, and A. Brakemeier, "Cooperative Intelligent Transport Systems in Europe: Current Deployment Status and Outlook," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 89–97, 2017.

[35] IEEE, "IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments," Tech. Rep. IEEE Std 802.11p-2010, July 2010.

[36] ETSI, "Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band." Tech. Rep. EN 302 663 V1.3.1, October 2019.

[37] ——, "Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part." Tech. Rep. TS 102 687 V1.2.1, April 2018.

[38] ETSI, "Intelligent Transport Systems (ITS); LTE-V2X Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band," Tech. Rep. EN 303 613 V1.1.1, January 2020.

[39] SAE International, *Dedicated Short Range Communications (DSRC) Message Set Dictionary*, March 2016.

[40] ETSI, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service ," Tech. Rep. EN 302 637-2 V1.3.2, November 2014.

[41] ——, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service," Tech. Rep. EN 302 637-3 V1.3.1, April 2019.

[42] IEEE, "IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages," Tech. Rep. IEEE Std 1609.2-2016, March 2016.

[43] ETSI, "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2," Tech. Rep. TS 102 940 V2.1.1, July 2021.

[44] B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn, and R. Goudy, "A Security Credential Management System for V2X Communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 3850–3871, 2018.

[45] DSRC Technical Committee. (2020, April) SAE J2945/1 - On-board System Requirements for V2V Safety Communications. [Online]. Available: https://saemobilus.sae.org/content/j2945/1_202004

[46] A. Sabella, R. Irons-Mclean, and M. Yannuzzi, *Orchestrating and Automating Security for the Internet of Things: Delivering Advanced Security Capabilities from Edge to Cloud for IoT*. Cisco Press, 2018.

[47] C. Laurendeau and M. Barbeau, "Threats to Security in DSRC/WAVE," in *Ad-Hoc, Mobile, and Wireless Networks*, T. Kunz and S. S. Ravi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 266–279.

[48] A. M. Abdelgader, F. Shu, W. Zhu, and K. Ayoub, "Security challenges and trends in vehicular communications," in *2017 IEEE conference on systems, process and control (ICSPC)*. IEEE, 2017, pp. 105–110.

[49] 3GPP, "Service requirements for V2X services (Release 14)," Tech. Rep. TS 22.185 v14.4.0, July 2018.

[50] Continental. (2018, December) Cellular V2X: Continental Successfully Conducts Field Trials in China. [Online]. Available: https://www.continental.com/en/press/press-releases/2017-12-18-cellular-v2x-116994

[51] M. Alleven. (2018, January) NTT DoCoMo, Ericsson, Qualcomm to carry out C-V2X trials in Japan. [Online]. Available: https://www.fiercewireless.com/wireless/ntt-docomo-ericsson-qualcomm-to-carry-out-c-v2x-trials-japan

[52] 5G Americas. (2018, March) Cellular V2X Communications Towards 5G. [Online]. Available: https://www.5gamericas.org/wp-content/uploads/2019/07/2018_5G_Americas_White_Paper_Cellular_V2X_Communications_Towards_5G__Final_for_Distribution.pdf

[53] 3GPP, "Architecture enhancements for V2X services (Release 14)," Tech. Rep. TS 23.285 v14.9.0, January 2020.

[54] ——, "Architecture enhancements for V2X services (Release 15)," Tech. Rep. TS 23.285 v15.4.0, January 2020.

[55] D. Garcia-Roger, E. E. González, D. Martín-Sacristán, and J. F. Monserrat, "V2X Support in 3GPP Specifications: From 4G to 5G and Beyond," *IEEE Access*, vol. 8, pp. 190 946–190 963, 2020.

[56] 3GPP, "Proximity-based services (ProSe); Stage 2 (Release 13)," Tech. Rep. TS 23.303 v13.6.0, January 2017.

[57] L. Miao, J. J. Virtusio, and K.-L. Hua, "PC5-Based Cellular-V2X Evolution and Deployment," *Sensors*, vol. 21, no. 3, 2021.

[58] 3GPP, "Procedures for the 5G System (5GS) (Release 16)," Tech. Rep. TS 23.502 v16.14.0, September 2022.

[59] K. Ganesan, J. Lohr, P. B. Mallick, A. Kunz, and R. Kuchibhotla, "NR Sidelink Design Overview for Advanced V2X Service," *IEEE Internet of Things Magazine*, vol. 3, no. 1, pp. 26–30, 2020.

[60] 3GPP, "Security aspect for LTE support of Vehicle-to-Everything (V2X) services (Release 17)," Tech. Rep. TS 33.185 v17.0.0, April 2022.

[61] 3GPP, "Proximity-based Services (ProSe); Security aspects (Release 17)," Tech. Rep. TS 33.303 v17.1.0, September 2022.

[62] 3GPP, "Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services (Release 17)," Tech. Rep. TS 33.536, v17.1.0, July 2022.

[63] S. A. A. Shah, E. Ahmed, M. Imran, and S. Zeadally, "5G for Vehicular Communications," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 111–117, 2018.

[64] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G Security Challenges and Solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.

[65] 3GPP, "Security architecture and procedures for 5G System (Release 17)," Tech. Rep. TS 33.501 v17.7.0, September 2022.

[66] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, and L. Xiong, "A Survey on Security Aspects for 3GPP 5G Networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 170–195, 2020.

[67] Z. Liu, H. Lee, M. O. Khyam, J. He, D. Pesch, K. Moessner, W. Saad, H. V. Poor *et al.*, "6G for Vehicle-to-Everything (V2X) Communications: Enabling Technologies, Challenges, and Opportunities," 2020. [Online]. Available: arXiv:2012.07753.

[68] Wards IS Automotive. (2018, January) Storage Almost Full: Driverless Cars Create Data Crunch. [Online]. Available: https://www.wardsauto.com/technology/storage-almost-full-driverless-cars-create-data-crunch

[69] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on Multi-Access Edge Computing for Internet of Things Realization," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2961–2991, 2018.

[70] Verizon. (2019, March) 5G and edge computing. [Online]. Available: https://www.verizon.com/business/solutions/5g/edge-computing/5g-and-edge-computing/

[71] Fierce Wireless. (2021, January) Verizon extends 5G MEC to two more cities, tests C-V2X and XR applications. [Online]. Available: https://www.fiercewireless.com/operators/verizon-extends-5g-mec-to-two-more-cities-tests-c-v2x-and-xr-applications

[72] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A Survey on Mobile Edge Computing: The Communication Perspective," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2322–2358, 2017.

[73] K. Zhang, Y. Mao, S. Leng, Y. He, and Y. Zhang, "Mobile-Edge Computing for Vehicular Networks: A Promising Network Paradigm with Predictive Off-Loading," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 36–44, 2017.

[74] M. Emara, M. C. Filippou, and D. Sabella, "MEC-Assisted End-to-End Latency Evaluations for C-V2X Communications," in *2018 European Conference on Networks and Communications (EuCNC)*, 2018, pp. 1–9.

[75] A. Moubayed, A. Shami, P. Heidari, A. Larabi, and R. Brunner, "Edge-Enabled V2X Service Placement for Intelligent Transportation Systems," *IEEE Transactions on Mobile Computing*, vol. 20, no. 4, pp. 1380–1392, 2021.

[76] ETSI. (2022, September) MEC security: Status of standards support and future evolutions. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP-46-2nd-Ed-MEC-security.pdf

[77] K. Sha, T. A. Yang, W. Wei, and S. Davari, "A survey of edge computing-based designs for IoT security," *Digital Communications and Networks*, vol. 6, no. 2, pp. 195–202, 2020.

[78] K. Ramezanpour and J. Jagannath, "Intelligent Zero Trust Architecture for 5G/6G Tactical Networks: Principles, Challenges, and the Role of Machine Learning," 2021. [Online]. Available: arXiv:2105.01478.

[79] S. W. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," *NIST*, 2020.

[80] S. Lai, R. Zhao, S. Tang, J. Xia, F. Zhou, and L. Fan, "Intelligent secure mobile edge computing for beyond 5G wireless networks," *Physical Communication*, vol. 45, p. 101283, 2021.

[81] G. Americas. (2021, October) 5G veritical use cases. [Online]. Available: https://www.5gamericas.org/wp-content/uploads/2021/10/5G-Vertical-Use-Cases-WP-InDesign.pdf

[82] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network Slicing and Softwarization: A Survey on Principles, Enabling Technologies, and Solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2429–2453, 2018.

[83] J. Mei, X. Wang, and K. Zheng, "Intelligent Network Slicing for V2X Services Toward 5G," *IEEE Network*, vol. 33, no. 6, pp. 196–204, 2019.

[84] R. F. Olimid and G. Nencioni, "5G Network Slicing: A Security Overview," *IEEE Access*, vol. 8, pp. 99 999–100 009, 2020.

[85] R. Vilalta, P. Alemany, R. Sedar, C. Kalalas, R. Casellas, R. Martínez, F. Vázquez-Gallego, J. Ortiz, A. Skarmeta, J. Alonso-Zarate, and R. Muñoz, "Applying Security Service Level Agreements in V2X Network Slices," in *2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, 2020, pp. 114–115.

[86] J. Ni, X. Lin, and X. S. Shen, "Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 3, pp. 644–657, 2018.

[87] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Comput. Surv.*, vol. 52, no. 3, July 2019.

[88] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and beyond networks: A state of the art survey," *Journal of Network and Computer Applications*, vol. 166, p. 102693, 2020.

[89] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, C. Yuen, S. Sun, K.-Y. Lam, and L. H. Koh, "Blockchain for the Internet of Vehicles Towards Intelligent Transportation Systems: A Survey," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4157–4185, 2021.

[90] T. Alladi, V. Chamola, N. Sahu, V. Venkatesh, A. Goyal, and M. Guizani, "A Comprehensive Survey on the Applications of Blockchain for Securing Vehicular Networks," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 1212–1239, 2022.

[91] ETSI, "Multi-access Edge Computing (MEC); V2X Information Service API ," Tech. Rep. GS MEC 030 V2.2.1, May 2022.

[92] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4660–4670, 2019.

[93] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-Based Decentralized Trust Management in Vehicular Networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2019.

[94] C. Peng, C. Wu, L. Gao, J. Zhang, K.-L. Alvin Yau, and Y. Ji, "Blockchain for Vehicular Internet of Things: Recent Advances and Open Issues," *Sensors*, vol. 20, no. 18, 2020.

[95] 3GPP, "Service requirements for enhanced V2X scenarios (Release 17)," Tech. Rep. TS 22.186 v17.0.0, April 2022.

[96] ETSI, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions," Tech. Rep. Standard ETSI TR 102 638 V1.1.1, June 2009.

[97] 5GAA. (2020, December) C-V2X Use Cases and Service Level Requirements Volume. [Online]. Available: https://5gaa.org/wp-content/uploads/2020/12/5GAA_T-200111_TR_C-V2X_Use_Cases_and_Service_Level_Requirements_Vol_I-V3.pdf

[98] M. Boban, A. Kousaridas, K. Manolakis, J. Eichinger, and W. Xu, "Connected Roads of the Future: Use Cases, Requirements, and Design Considerations for Vehicle-to-Everything Communications," *IEEE Vehicular Technology Magazine*, vol. 13, no. 3, pp. 110–123, 2018.

[99] 3GPP, "Study on new services and markets technology enablers (Release 14)," Tech. Rep. TR 22.891, v14.2.0, September 2016.

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

[101] M. Villarreal-Vasquez, B. Bhargava, and P. Angin, "Adaptable Safety and Security in V2X Systems," in *2017 IEEE International Congress on Internet of Things (ICIOT)*, 2017, pp. 17–24.

[102] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *Journal of Network and Computer Applications*, vol. 101, pp. 55–82, 2018.

[103] ETSI, "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management," Tech. Rep. TS 102 941 V1.4.1, January 2021.

[104] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *20th USENIX security symposium (USENIX Security 11)*, 2011.

[105] I. Ivanov, C. Maple, T. Watson, and S. Lee, "Cyber security standards and issues in V2X communications for Internet of Vehicles," in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 2018, pp. 1–6.

[106] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of computer security*, vol. 15, no. 1, pp. 39–68, 2007.

[107] R. Lu, L. Zhang, J. Ni, and Y. Fang, "5G Vehicle-to-Everything Services: Gearing Up for Security and Privacy," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 373–389, 2020.

[108] S. Sharma, A. Kaul, S. Ahmed, and S. Sharma, "A detailed tutorial survey on VANETs: emerging architectures, applications, security issues, and solutions," *International Journal of Communication Systems*, vol. 34, no. 14, p. e4905, 2021.

[109] J. Kamel, M. Wolf, R. W. van der Hei, A. Kaiser, P. Urien, and F. Kargl, "VeReMi Extension: A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs," in *2020 IEEE International Conference on Communications*, 2020, pp. 1–6.

[110] J. Lastinec and M. Keszeli, "Analysis of Realistic Attack Scenarios in Vehicle Ad-hoc Networks," in *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, 2019, pp. 1–6.

[111] J. Kamel, F. Haidar, I. B. Jemaa, A. Kaiser, B. Lonc, and P. Urien, "A Misbehavior Authority System for Sybil Attack Detection in C-ITS," in *2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2019, pp. 1117–1123.

[112] P. Zhu, K. Zhu, and L. Zhang, "Security Analysis of LTE-V2X and A Platooning Case Study," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2020, pp. 532–537.

[113] Nishtha and M. Sood, "Exploring the Possibility of Sybil Attack in Position Based Routing Protocols in VANETs: A Case Study of Greedy Perimeter Coordinator Routing (GPCR)," in *International Conference on Recent Developments in Science, Engineering and Technology*. Springer, 2019, pp. 79–89.

[114] K. J. Ahmed and M. J. Lee, "Secure LTE-Based V2X Service," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3724–3732, 2018.

[115] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical attacks against privacy and availability in 4G/LTE mobile communication systems," in *23rd Annual Network and Distributed System Security Symposium (NDSS 2016)*. Internet Society, 2016.

[116] C. Vitale, N. Piperigkos, C. Laoudias, G. Ellinas, J. Casademont, J. Escrig, A. Kloukiniotis, A. S. Lalos, K. Moustakas, R. D. Rodriguez *et al.*, "CARAMEL: results on a secure architecture for connected and autonomous vehicles detecting GPS spoofing attacks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, pp. 1–28, 2021.

[117] J. S. Warner and R. G. Johnston, "A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing," *Journal of security administration*, vol. 25, no. 2, pp. 19–27, 2002.

[118] J. Shen, J. Y. Won, Z. Chen, and Q. A. Chen, "Drift with devil: Security of multi-sensor fusion based localization in high-level autonomous driving under GPS spoofing," in *USENIX Security Symposium*, 2020, pp. 931–948.

[119] R. Mit. (2021, August) Two years since the Tesla GPS hack. [Online]. Available: https://www.gpsworld.com/two-years-since-the-tesla-gps-hack/

[120] K. C. Zeng, S. Liu, Y. Shu, D. Wang, H. Li, Y. Dou, G. Wang, and Y. Yang, "All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 1527–1544.

[121] J. Cassou-Mounat, H. Labiod, and R. Khatoun, "Simulation of Cyberattacks in ITS-G5 Systems," in *International Workshop on Communication Technologies for Vehicles*. Springer, 2020, pp. 3–14.

[122] E. P. Valentini, R. I. Meneguette, and A. Alsuhaim, "An attacks detection mechanism for intelligent transport system," in *2020 IEEE International Conference on Big Data (Big Data)*. Ieee, 2020, pp. 2453–2461.

[123] G. Twardokus and H. Rahbari, "Vehicle-to-Nothing? Securing C-V2X Against Protocol-Aware DoS Attacks," in *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*, 2022, pp. 1629–1638.

[124] N. Trkulja, D. Starobinski, and R. A. Berry, "Denial-of-Service Attacks on C-V2X Networks," in *Proceedings Third International Workshop on Automotive and Autonomous Vehicle Security*. Internet Society, 2021. [Online]. Available: https://doi.org/10.14722/autosec.2021.23006

[125] H. Pirayesh, P. K. Sangdeh, S. Zhang, Q. Yan, and H. Zeng, "JammingBird: Jamming-Resilient Communications for Vehicular Ad Hoc Networks," in *2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, 2021, pp. 1–9.

[126] G. Twardokus, J. Ponicki, S. Baker, P. Carenzo, H. Rahbari, and S. Mishra, "Targeted Discreditation Attack against Trust Management in Connected Vehicles," in *ICC 2021 - IEEE International Conference on Communications*, 2021, pp. 1–6.

[127] W. Xu, C. Yan, W. Jia, X. Ji, and J. Liu, "Analyzing and Enhancing the Security of Ultrasonic Sensors for Autonomous Vehicles," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 5015–5029, 2018.

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

[129] J. Billman and V. Hellström, "Abusing Keep-Alive Forwarding to flood a VANET: When safety messages become a safety risk," 2016, [Online]. Available: https://www.diva-portal.org/smash/get/diva2:1034703/ATTACHMENT01.pdf.

[130] E. Kovacs. (2021, March) Tesla Car Hacked Remotely From Drone via Zero-Click Exploit. [Online]. Available: https://www.securityweek.com/tesla-car-hacked-remotely-drone-zero-click-exploit

[131] O. Bittner, T. Krachenfels, A. Galauner, and J.-P. Seifert, "The Forgotten Threat of Voltage Glitching: A Case Study on Nvidia Tegra X2 SoCs," in *2021 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*, 2021, pp. 86–97.

[132] S. Gyawali and Y. Qian, "Misbehavior Detection using Machine Learning in Vehicular Communication Networks," in *2019 IEEE International Conference on Communications (ICC)*, 2019, pp. 1–6.

[133] X. Luo, Y. Liu, H.-H. Chen, and Q. Guo, "Physical Layer Security in Intelligently Connected Vehicle Networks," *IEEE Network*, vol. 34, no. 5, pp. 232–239, 2020.

[134] A. Greenberg. (2016, October) A New Wireless Hack Can Unlock 100 Million Volkswagens. [Online]. Available: https://www.wired.com/2016/08/oh-good-new-hack-can-unlock-100-million-volkswagens/

[135] F. D. Garcia, D. Oswald, T. Kasper, and P. Pavlidès, "Lock It and Still Lose It - on the (in)Security of Automotive Remote Keyless Entry Systems," in *Proceedings of the 25th USENIX Conference on Security Symposium*, ser. SEC'16. USA: USENIX Association, 2016, p. 929–944.

[136] I. Rouf, R. D. Miller, H. A. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study," in *USENIX Security Symposium*, vol. 10, 2010.

[137] K. Kate. (2015, July) Shock at the wheel: your Jeep can be hacked while driving down the road. [Online]. Available: https://www.kaspersky.com/blog/remote-car-hack/9395/

[138] F. Ahmad, A. Adnane, V. N. L. Franqueira, F. Kurugollu, and L. Liu, "Man-In-The-Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackers' Strategies," *Sensors*, vol. 18, no. 11, 2018.

[139] K. Stundefinedpień and A. Poniszewska-Marańda, "Security Solution Methods in the Vehicular Ad-Hoc Networks," in *Proceedings of the 17th International Conference on Advances in Mobile Computing & Multimedia*. Association for Computing Machinery, 2019, p. 127–135.

[140] S. E. Huang, W. Wong, Y. Feng, Q. A. Chen, Z. M. Mao, and H. X. Liu, "Impact evaluation of falsified data attacks on connected vehicle based traffic signal control," 2020. [Online]. Available: arXiv:2010.04753.

[141] K.-T. Cho and K. G. Shin, "Fingerprinting Electronic Control Units for Vehicle Intrusion Detection," in *Proceedings of the 25th USENIX Conference on Security Symposium*. USA: USENIX Association, 2016, p. 911–927.

[142] P. T. Partners. (2016, June) Hacking the Mitsubishi Outlander PHEV hybrid. [Online]. Available: https://www.pentestpartners.com/security-blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/

[143] S. Kamkar, "Drive it like you Hacked it: New Attacks and Tools to Wireless," 2015, [Online]. Available: https://av.tib.eu/media/36433.

[144] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, no. S 91, 2015.

[145] N. Lo and H. Tsai, "Illusion Attack on VANET Applications - A Message Plausibility Problem," in *2007 IEEE Globecom Workshops*, 2007, pp. 1–8.

[146] G. Costantino, A. La Marra, F. Martinelli, and I. Matteucci, "CANDY: A social engineering attack to leak information from infotainment system," in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, 2018, pp. 1–5.

[147] CISA. (2017, April) Hyundai Blue Link Vulnerability. [Online]. Available: https://www.cisa.gov/uscert/ics/advisories/ICSA-17-115-03

[148] J. R. Douceur, "The Sybil Attack," in *Revised Papers from the First International Workshop on Peer-to-Peer Systems*, ser. IPTPS '01. Berlin, Heidelberg: Springer-Verlag, 2002, p. 251–260.

[149] E. Koutrouli and A. Tsalgatidou, "Reputation Systems Evaluation Survey," *ACM Comput. Surv.*, vol. 48, no. 3, Dec. 2015.

[150] I. A. Sumra, I. Ahmad, H. Hasbullah, and J. bin Ab Manan, "Classes of attacks in VANET," in *2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC)*, 2011, pp. 1–5.

[151] B. Mokhtar and M. Azab, "Survey on Security Issues in Vehicular Ad Hoc Networks," *Alexandria Engineering Journal*, vol. 54, no. 4, pp. 1115–1126, 2015.

[152] K. C. Zeng, Y. Shu, S. Liu, Y. Dou, and Y. Yang, "A Practical GPS Location Spoofing Attack in Road Navigation Scenario," in *Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications*. Association for Computing Machinery, 2017, p. 85–90.

[153] J. Bhatti and T. E. Humphreys, "Hostile control of ships via false GPS signals: Demonstration and detection," *NAVIGATION, Journal of the Institute of Navigation*, vol. 64, no. 1, pp. 51–66, 2017.

[154] S. Tariq, H. Kim, and J. Ryoo, "AuthGPS: Lightweight GPS Authentication against GPS and LTE Spoofing (poster)," in *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services*, 2019, pp. 547–548.

[155] X. Lin and X. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 7, pp. 3339–3348, 2013.

[156] Y. Xie, S. Zhang, X. Li, and Y. Li, "An efficient cooperative message authentication based on reputation mechanism in vehicular ad hoc networks," *International Journal of Distributed Sensor Networks*, vol. 15, no. 6, pp. 1–10, 2019.

[157] O. Puñal, A. Aguiar, and J. Gross, "In VANETs We Trust? Characterizing RF Jamming in Vehicular Networks," in *Proceedings of the Ninth ACM International Workshop on Vehicular Inter-Networking, Systems, and Applications*. New York, NY, USA: Association for Computing Machinery, 2012, p. 83–92.

[158] The Tesla Team. (2016, June) A Tragic Loss. [Online]. Available: https://www.tesla.com/blog/tragic-loss

[159] S. Zhang, Y. Wang, and W. Zhou, "Towards secure 5G networks: A Survey," *Computer Networks*, vol. 162, p. 106871, 2019.

[160] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2, pp. 760–776, 2019.

[161] I. Yaqoob, E. Ahmed, M. H. ur Rehman, A. I. A. Ahmed, M. A. Al-garadi, M. Imran, and M. Guizani, "The rise of ransomware and emerging security challenges in the Internet of Things," *Computer Networks*, vol. 129, pp. 444–458, 2017.

[162] M. Azees, P. Vijayakumar, and L. Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks," *IET Intelligent Transport Systems*, vol. 10, pp. 379–388, 2016.

[163] M. Jakobsson, S. Wetzel, and B. Yener, "Stealth attacks on ad-hoc wireless networks," in *2003 IEEE 58th Vehicular Technology Conference VTC 2003-Fall*, vol. 3, 2003, pp. 2103–2111.

[164] A. Serban, E. Poll, and J. Visser, "A Security Analysis of the ETSI ITS Vehicular Communications," in *SAFECOMP Workshops*, 2018.

[165] J. Grover, V. Laxmi, and M. S. Gaur, "Attack models and infrastructure supported detection mechanisms for position forging attacks in vehicular ad hoc networks," *CSI transactions on ICT*, vol. 1, no. 3, pp. 261–279, 2013.

[166] M. Arif, G. Wang, M. Zakirul Alam Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges," *Vehicular Communications*, vol. 19, p. 100179, 2019.

[167] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, D. Boneh *et al.*, "Location privacy via private proximity testing," in *NDSS*, vol. 11, 2011.

[168] K. Norrman, M. Näslund, and E. Dubrova, "Protecting IMSI and User Privacy in 5G Networks," in *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications*, ser. MobiMedia '16, 2016, p. 159–166.

[169] A. Jovanovic, C. Botteron, and P. Fariné, "Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers," in *2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014*, 2014, pp. 1258–1271.

[170] PRESERVE. (2013, December) Deliverable 5.3 - Deployment Issues Report v3. [Online]. Available: https://www.preserve-project.eu/www.preserve-project.eu/sites/preserve-project.eu/files/PRESERVE-D5.3-Deployment_Issues_Report_V3.pdf

[171] T. Giannetsos and I. Krontiris, "Securing V2X Communications for the Future: Can PKI Systems Offer the Answer?" in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, ser. ARES '19. New York, NY, USA: Association for Computing Machinery, 2019.

[172] N. Kumar, R. Iqbal, S. Misra, and J. J. Rodrigues, "An intelligent approach for building a secure decentralized public key infrastructure in VANET," *Journal of Computer and System Sciences*, vol. 81, no. 6, pp. 1042–1058, 2015.

[173] "NS-2 Network Simulator," http://nsnam.sourceforge.net/wiki/index.php/Main_Page, Accessed: 2021-11-29.

[174] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication," *Journal of Communications and Networks*, vol. 11, no. 6, pp. 574–588, 2009.

[175] S. Bao, W. Hathal, H. Cruickshank, Z. Sun, P. Asuquo, and A. Lei, "A lightweight authentication and privacy-preserving scheme for VANETs using TESLA and Bloom Filters," *ICT Express*, vol. 4, no. 4, pp. 221–227, 2018.

[176] "NS-3 Network Simulator," https://www.nsnam.org/, Accessed: 2021-12-01.

[177] P. A. Lopez, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y.-P. Flötteröd, R. Hilbrich, L. Lücken, J. Rummel, P. Wagner, and E. Wiessner, "Microscopic Traffic Simulation using SUMO," in *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, 2018, pp. 2575–2582.

[178] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "SPACF: A Secure Privacy-Preserving Authentication Scheme for VANET With Cuckoo Filter," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10 283–10 295, 2017.

[179] B. Ying and A. Nayak, "Anonymous and Lightweight Authentication for Secure Vehicular Networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 10 626–10 636, 2017.

[180] J. Härri, F. Filali, C. Bonnet, and M. Fiore, "VanetMobiSim: Generating Realistic Mobility Patterns for VANETs," in *Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks*. New York, NY, USA: Association for Computing Machinery, 2006, p. 96–97.

[181] K. Lim and D. Manivannan, "An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks," *Vehicular Communications*, vol. 4, pp. 30–37, 2016.

[182] Y. Yang, Z. Wei, Y. Zhang, H. Lu, K.-K. R. Choo, and H. Cai, "V2X security: A case study of anonymous authentication," *Pervasive and Mobile Computing*, vol. 41, pp. 259–269, 2017.

[183] U. Rajput, F. Abbas, and H. Oh, "A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANET," *IEEE Access*, vol. 4, pp. 7770–7784, 2016.

[184] C. Sommer, R. German, and F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3–15, 2011.

[185] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, "2FLIP: A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 2, pp. 896–911, 2016.

[186] B. Blanchet, "An Efficient Cryptographic Protocol Verifier Based on Prolog Rules," in *14th IEEE Computer Security Foundations Workshop (CSFW-14)*. IEEE Computer Society, Jun. 2001, pp. 82–96.

[187] A. Keränen, J. Ott, and T. Kärkkäinen, "The ONE Simulator for DTN Protocol Evaluation," in *SIMUTools '09: Proceedings of the 2nd International Conference on Simulation Tools and Techniques*. New York, NY, USA: ICST, 2009.

[188] C. Xu, X. Huang, M. Ma, and H. Bao, "A Secure and Efficient Message Authentication Scheme for Vehicular Networks based on LTE-V," *KSII Trans. Internet Inf. Syst.*, vol. 12, pp. 2841–2860, 2018.

[189] Apache. The MIRACL Core Cryptographic Library. [Online]. Available: https://github.com/miracl/MIRACL

[190] L. Buttyán, T. Holczer, and I. Vajda, "On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs," in *Security and Privacy in Ad-hoc and Sensor Networks*, F. Stajano, C. Meadows, S. Capkun, and T. Moore, Eds. Springer Berlin Heidelberg, 2007, pp. 129–141.

[191] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J. Hubaux, "Mix-Zones for Location Privacy in Vehicular Networks," in *First International Workshop on Wireless Networking for Intelligent Transportation Systems*, 2007.

[192] C. Vaas, M. Khodaei, P. Papadimitratos, and I. Martinovic, "Nowhere to hide? Mix-Zones for Private Pseudonym Change using Chaff Vehicles," in *2018 IEEE Vehicular Networking Conference (VNC)*, 2018, pp. 1–8.

[193] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacy for VANET," Washington Univ Seattle Dept of Electrical Engineering, Tech. Rep., 2005.

[194] D. Liu, J. Ni, X. Lin, and X. S. Shen, "Anonymous Group Message Authentication Protocol for LTE-based V2X Communications," *Internet Technology Letters*, vol. 1, no. 2, p. e25, 2018.

[195] P. Vijayakumar, M. Azees, S. A. Kozlov, and J. J. P. C. Rodrigues, "An Anonymous Batch Authentication and Key Exchange Protocols for 6G Enabled VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 2, pp. 1630–1638, 2022.

[196] L. Zhou, L. Yu, S. Du, H. Zhu, and C. Chen, "Achieving Differentially Private Location Privacy in Edge-Assistant Connected Vehicles," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4472–4481, 2019.

[197] H. Cui, R. H. Deng, and G. Wang, "An Attribute-Based Framework for Secure Communications in Vehicular Ad Hoc Networks," *IEEE/ACM Transactions on Networking*, vol. 27, no. 2, pp. 721–733, 2019.

[198] J. A. Akinyele, M. D. Green, and A. D. Rubin, "Charm: A framework for rapidly prototyping cryptosystems," Cryptology ePrint Archive, Paper 2011/617, 2011, https://eprint.iacr.org/2011/617. [Online]. Available: https://eprint.iacr.org/2011/617

[199] D. Huang and M. Verma, "ASPE: attribute-based secure policy enforcement in vehicular ad hoc networks," *Ad Hoc Networks*, vol. 7, no. 8, pp. 1526–1535, 2009, Privacy and Security in Wireless Sensor and Ad Hoc Networks. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870509000456

[200] T. Leinmuller, E. Schoch, and C. Maihofer, "Security requirements and solution concepts in vehicular ad hoc networks," in *2007 Fourth Annual Conference on Wireless on Demand Network Systems and Services*, 2007, pp. 84–91.

[201] *Public Key Infrastructure for Vehicle Networks*. John Wiley and Sons, Ltd, 2012, ch. 15, pp. 209–236. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118452189.ch15

[202] J. Petit and Z. Mammeri, "Authentication and consensus overhead in vehicular ad hoc networks," *Telecommunication systems*, vol. 52, no. 4, pp. 2699–2712, 2013.

[203] T. Weil, "Service management for its using wave (1609.3) networking," in *2009 IEEE Globecom Workshops*. IEEE, 2009, pp. 1–6.

[204] PRESERVE. (2014, January) Deliverable 1.3 - V2X Security Architecture v2. [Online]. Available: https://www.preserve-project.eu/www.preserve-project.eu/sites/preserve-project.eu/files/PRESERVE-D1.3-V2X_Security_Architecture_V2.pdf

[205] "OpenSSL Cryptography and SSL/TLS toolkit," https://www.openssl.org/, Accessed: 2021-12-19.

[206] "OpenCA Labs; Open-source Security and Identity Management Solutions," https://www.openca.org/, Accessed: 2021-12-19.

[207] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[208] N. Alexiou, S. Gisdakis, M. Laganà, and P. Papadimitratos, "Towards a secure and privacy-preserving multi-service vehicular architecture," in *2013 IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, 2013, pp. 1–6.

[209] S. Gisdakis, M. Laganà, T. Giannetsos, and P. Papadimitratos, "Serosa: Service oriented security architecture for vehicular communications," in *2013 IEEE Vehicular Networking Conference*, 2013, pp. 111–118.

[210] H. Krishnan and A. Weimerskirch, "Verify-on-demand - A practical and scalable approach for broadcast authentication in vehicle-to-vehicle communication," *SAE Int. J. Passeng. Cars – Mech. Syst.*, vol. 4, pp. 536–546, 2011.

[211] F. Haidar, A. Kaiser, and B. Lonc, "On the Performance Evaluation of Vehicular PKI Protocol for V2X Communications Security," in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, 2017, pp. 1–5.

[212] 3GPP, "Specification of the MILENAGE algorithm set: Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General (Release 17)," Tech. Rep. TS 35.205 v17.0.0, April 2022.

[213] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A Formal Analysis of 5G Authentication," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 1383–1396.

[214] C. Kalalas and J. Alonso-Zarate, "Lightweight and Space-efficient Vehicle Authentication based on Cuckoo Filter," in *2020 IEEE 3rd 5G World Forum (5GWF)*, 2020, pp. 139–144.

[215] R. Sedar, C. Kalalas, J. Alonso-Zarate, and F. Vazquez-Gallego, "Multi-domain Denial-of-Service Attacks in Internet-of-Vehicles: Vulnerability Insights and Detection Performance," in *2022 IEEE International Conference on Network Softwarization (NetSoft)*, 2022.

[216] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," *Rsa Cryptobytes*, vol. 5, no. 2, pp. 2–13, 2002.

[217] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in *Advances in Cryptology*, G. R. Blakley and D. Chaum, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 47–53.

[218] D. He, S. Zeadally, B. Xu, and X. Huang, "An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[219] C. Feng, K. Yu, M. Aloqaily, M. Alazab, Z. Lv, and S. Mumtaz, "Attribute-Based Encryption With Parallel Outsourced Decryption for Edge Intelligent IoV," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13 784–13 795, 2020.

[220] J. Ma, T. Li, J. Cui, Z. Ying, and J. Cheng, "Attribute-Based Secure Announcement Sharing Among Vehicles Using Blockchain," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10 873–10 883, 2021.

[221] L. Cheng, J. Liu, G. Xu, Z. Zhang, H. Wang, H.-N. Dai, Y. Wu, and W. Wang, "SCTSC: A Semicentralized Traffic Signal Control Mode With Attribute-Based Blockchain in IoVs," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, pp. 1373–1385, 2019.

[222] B. M. ElHalawany, A. A. A. El-Banna, and K. Wu, "Physical-Layer Security and Privacy for Vehicle-to-Everything," *IEEE Communications Magazine*, vol. 57, no. 10, pp. 84–90, 2019.

[223] H. M. Furqan, M. S. J. Solaija, J. M. Hamamreh, and H. Arslan, "Intelligent Physical Layer Security Approach for V2X Communication," 2020. [Online]. Available: arXiv:1905.05075v3.

[224] S. Kavaiya, D. K. Patel, Z. Ding, Y. L. Guan, and S. Sun, "Physical Layer Security in Cognitive Vehicular Networks," *IEEE Transactions on Communications*, pp. 1–1, 2020.

[225] S. Kavaiya, D. K. Patel, Y. L. Guan, S. Sun, Y. C. Chang, and J. M. Y. Lim, "On Physical Layer Security over $\alpha - \eta - \kappa - \mu$ Fading for Relay based Vehicular Networks," in *2020 International Conference on Signal Processing and Communications (SPCOM)*, 2020, pp. 1–5.

[226] Y. Ai, M. Cheffena, A. Mathur, and H. Lei, "On Physical Layer Security of Double Rayleigh Fading Channels for Vehicular Communications," *IEEE Wireless Communications Letters*, vol. 7, no. 6, pp. 1038–1041, 2018.

[227] A. Pandey and S. Yadav, "Physical Layer Security in Cooperative Vehicular Relay Networks," in *5G and Beyond Wireless Systems: PHY Layer Perspective*, M. Mandloi, D. Gurjar, P. Pattanayak, and H. Nguyen, Eds. Singapore: Springer Singapore, 2021, pp. 365–390.

[228] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, K. Adhikari, X. Li, M. Quiroz-Castellanos, and R. Kharel, "Reconfigurable intelligent surfaces-enabled vehicular networks: A physical layer security perspective," 2020. [Online]. Available: arXiv:2004.11288v1.

[229] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, X. Li, and R. Kharel, "Physical Layer Security in Vehicular Networks with Reconfigurable Intelligent Surfaces," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, 2020, pp. 1–6.

[230] A. Abdelaziz, C. Emre Koksal, R. Burton, F. Barickman, J. Martin, J. Weston, and K. Woodruff, "Beyond PKI: Enhanced Authentication in Vehicular Networks via MIMO," in *2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2018, pp. 1–5.

[231] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[232] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[233] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[234] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[235] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [Security and Privacy in Emerging Wireless Networks]," *IEEE Wireless Communications*, vol. 17, no. 5, pp. 56–62, 2010.

[236] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[237] J. Li, A. P. Petropulu, and S. Weber, "On Cooperative Relaying Schemes for Wireless Physical Layer Security," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4985–4997, 2011.

[238] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober, "Robust and Secure Resource Allocation for Full-Duplex MISO Multicarrier NOMA Systems," *IEEE Transactions on Communications*, vol. 66, no. 9, pp. 4119–4137, 2018.

[239] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, 2010.

[240] J. Tang, M. Dabaghchian, K. Zeng, and H. Wen, "Impact of Mobility on Physical Layer Security Over Wireless Fading Channels," *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 7849–7864, 2018.

[241] X. Yu, D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, "Robust and Secure Wireless Communications via Intelligent Reflecting Surfaces," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 11, pp. 2637–2652, 2020.

[242] A. Khisti and G. W. Wornell, "Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, 2010.

[243] L. Liu, R. Zhang, and K. Chua, "Secrecy Wireless Information and Power Transfer With MISO Beamforming," *IEEE Transactions on Signal Processing*, vol. 62, no. 7, pp. 1850–1863, 2014.

[244] M. Cui, G. Zhang, and R. Zhang, "Secure Wireless Communication via Intelligent Reflecting Surface," *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1410–1414, 2019.

[245] Q. Wu and R. Zhang, "Towards Smart and Reconfigurable Environment: Intelligent Reflecting Surface Aided Wireless Network," *IEEE Communications Magazine*, vol. 58, no. 1, pp. 106–112, 2020.

[246] Z. Chu, W. Hao, P. Xiao, D. Mi, Z. Liu, M. Khalily, J. R. Kelly, and A. P. Feresidis, "Secrecy Rate Optimization for Intelligent Reflecting Surface Assisted MIMO System," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1655–1669, 2021.

[247] L. Dong and H. Wang, "Secure MIMO Transmission via Intelligent Reflecting Surface," *IEEE Wireless Communications Letters*, vol. 9, no. 6, pp. 787–790, 2020.

[248] L. Dong and H. M. Wang, "Enhancing Secure MIMO Transmission via Intelligent Reflecting Surface," *IEEE Transactions on Wireless Communications*, vol. 19, no. 11, pp. 7543–7556, 2020.

[249] S. Hong, C. Pan, H. Ren, K. Wang, and A. Nallanathan, "Artificial-Noise-Aided Secure MIMO Wireless Communications via Intelligent Reflecting Surface," *IEEE Transactions on Communications*, vol. 68, no. 12, pp. 7851–7866, 2020.

[250] X. Guan, Q. Wu, and R. Zhang, "Intelligent Reflecting Surface Assisted Secrecy Communication: Is Artificial Noise Helpful or Not?" *IEEE Wireless Communications Letters*, vol. 9, no. 6, pp. 778–782, 2020.

[251] S. S. Kaushik, "Review of different approaches for privacy scheme in VANETs," *International Journal of Advances in Engineering & Technology*, vol. 5, no. 2, p. 356, Jan 2013.

[252] J. M. De Fuentes, A. I. González-Tablas, and A. Ribagorda, "Overview of security issues in vehicular ad-hoc networks," in *Handbook of research on mobility and computing: Evolving technologies and ubiquitous impacts*. IGI global, 2011, pp. 894–911.

[253] A. R. Beresford and F. Stajano, "Mix zones: user privacy in location-aware services," in *IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second*, 2004, pp. 127–131.

[254] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 584–616, 2011.

[255] C. Vaas, M. Roeschlin, P. Papadimitratos, and I. Martinovic, "Poster: Tracking Vehicles Through Encrypted Mix-Zones Using Physical Layer Properties," in *2018 IEEE Vehicular Networking Conference (VNC)*, 2018, pp. 1–2.

[256] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey," *Vehicular Communications*, vol. 16, pp. 45–61, 2019.

[257] D. Chaum and E. van Heyst, "Group signatures," in *Advances in Cryptology — EUROCRYPT '91*, D. W. Davies, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1991, pp. 257–265.

[258] F. Anjum, D. Subhadrabandhu, and S. Sarkar, "Signature based intrusion detection for wireless ad-hoc networks: a comparative study of various routing protocols," in *2003 IEEE 58th Vehicular Technology Conference VTC 2003-Fall*, vol. 3, 2003, pp. 2152–2156.

[259] L. Bilge and T. Dumitraş, "Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, 2012, p. 833–844.

[260] A. Ganesan, J. Rao, and K. Shin, "Exploiting Consistency among Heterogeneous Sensors for Vehicle Anomaly Detection," *SAE Technical Paper*, pp. 1–9, 2017.

[261] R. E. Haas, D. P. F. Möller, P. Bansal, R. Ghosh, and S. S. Bhat, "Intrusion detection in connected cars," in *2017 IEEE International Conference on Electro Information Technology (EIT)*, 2017, pp. 516–519.

[262] M.-J. Kang and J.-W. Kang, "Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security," *PLOS ONE*, vol. 11, no. 6, pp. 1–17, 06 2016.

[263] F. A. Ghaleb, M. Aizaini Maarof, A. Zainal, M. A. Rassam, F. Saeed, and M. Alsaedi, "Context-aware data-centric misbehaviour detection scheme for vehicular ad hoc networks using sequential analysis of the temporal and spatial correlation of the consistency between the cooperative awareness messages," *Vehicular Communications*, vol. 20, p. 100186, 2019.

[264] T. Leinmüller, E. Schoch, F. Kargl, and C. Maihöfer, "Decentralized position verification in geographic ad hoc routing," *Security and Communication Networks*, vol. 3, no. 4, pp. 289–302, 2010.

[265] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, "On Data-Centric Misbehavior Detection in VANETs," in *2011 IEEE Vehicular Technology Conference (VTC Fall)*, 2011, pp. 1–5.

[266] R. W. van der Heijden, S. Dietzel, T. Leinmüller, and F. Kargl, "Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 779–811, 2019.

[267] F. A. Ghaleb, A. Zainal, and M. A. Rassam, "Data verification and misbehavior detection in vehicular ad-hoc networks," *Jurnal Teknologi*, vol. 73, no. 2, 2015.
[268] F. Kargl, P. Papadimitratos, L. Buttyan, M. Müter, E. Schoch, B. Wiedersheim, T. Thong, G. Calandriello, A. Held, A. Kung, and J. Hubaux, "Secure vehicular communication systems: implementation, performance, and research challenges," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 110–118, 2008.
[269] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1557–1568, 2007.
[270] M. Hadded, O. Shagdar, and P. Merdrignac, "Augmented Perception by V2X Cooperation (PAC-V2X): Security issues and misbehavior detection solutions," in *15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 2019, pp. 907–912.
[271] X. Chen and L. Wang, "A trust evaluation framework using in a vehicular social environment," in *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2017, pp. 1004–1005.
[272] ETSI, "Intelligent Transport Systems (ITS); Security; Pre-standardization study on Misbehaviour Detection; Release 2," Tech. Rep. TR 103 460, v2.1.1, October 2020.
[273] J. Hortelano, J. C. Ruiz, and P. Manzoni, "Evaluating the Usefulness of Watchdogs for Intrusion Detection in VANETs," in *2010 IEEE International Conference on Communications Workshops*, 2010, pp. 1–5.
[274] J. Hortelano, M. Nacher, J.-C. Cano, C. Calafate, and P. Manzoni, "Castadiva: A Test-Bed Architecture for Mobile Ad Hoc Networks," in *2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2007, pp. 1–5.
[275] A. Daeinabi and A. G. Rahbar, "Detection of Malicious Vehicles (DMV) through Monitoring in Vehicular Ad-Hoc Networks," vol. 66, no. 2, p. 325–338, Sep. 2013.
[276] A. Hamieh, J. Ben-Othman, and L. Mokdad, "Detection of Radio Interference Attacks in VANET," in *GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference*, 2009, pp. 1–5.
[277] N. Lyamin, D. Kleyko, Q. Delooz, and A. Vinel, "AI-Based Malicious Network Traffic Detection in VANETs," *IEEE Network*, vol. 32, no. 6, pp. 15–21, 2018.
[278] W. Li and H. Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, 2016.
[279] X. Zeng, R. Bagrodia, and M. Gerla, "GloMoSim: a library for parallel simulation of large-scale wireless networks," in *Proceedings. Twelfth Workshop on Parallel and Distributed Simulation PADS '98*, 1998, pp. 154–161.
[280] J. Cui, X. Zhang, H. Zhong, Z. Ying, and L. Liu, "RSMA: Reputation System-Based Lightweight Message Authentication Framework and Protocol for 5G-Enabled Vehicular Networks," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6417–6428, 2019.
[281] T. H.-J. Kim, A. Studer, R. Dubey, X. Zhang, A. Perrig, F. Bai, B. Bellur, and A. Iyer, "VANET Alert Endorsement Using Multi-Source Filters," in *Proceedings of the Seventh ACM International Workshop on VehiculAr InterNETworking*, ser. VANET '10, 2010, p. 51–60.
[282] C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, "TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs," *Vehicular Communications*, vol. 9, pp. 254–267, 2017.
[283] M. Sun, M. Li, and R. Gerdes, "A data trust framework for VANETs enabling false data detection and secure vehicle tracking," in *2017 IEEE Conference on Communications and Network Security (CNS)*, 2017, pp. 1–9.
[284] A. Jaeger, N. Bißmeyer, H. Stübing, and S. A. Huss, "A novel framework for efficient mobility data verification in vehicular ad-hoc networks," *International Journal of Intelligent Transportation Systems Research*, vol. 10, no. 1, pp. 11–21, 2012.
[285] N. Bißmeyer, H. Stübing, M. Mattheß, J. P. Stotz, J. Schütte, M. Gerlach, and F. Friederici, "simTD security architecture: Deployment of a security and privacy architecture in field operational tests," in *7th ESCAR Embedded Security in Cars Conference*, 2009.
[286] Y. Yao, B. Xiao, G. Wu, X. Liu, Z. Yu, K. Zhang, and X. Zhou, "Multi-Channel Based Sybil Attack Detection in Vehicular Ad Hoc Networks Using RSSI," *IEEE Transactions on Mobile Computing*, vol. 18, no. 2, pp. 362–375, 2019.
[287] S. So, J. Petit, and D. Starobinski, "Physical Layer Plausibility Checks for Misbehavior Detection in V2X Networks," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 84–93.
[288] T. Leinmüller, E. Schoch, and F. Kargl, "Position Verification Approaches for Vehicular ad hoc Networks," *IEEE Wireless Communications*, vol. 13, no. 5, pp. 16–21, 2006.
[289] G. Yan, S. Olariu, and M. C. Weigle, "Providing VANET security through active position detection," *Computer Communications*, vol. 31, no. 12, pp. 2883–2897, 2008.
[290] R. K. Schmidt, T. Leinmüller, E. Schoch, A. Held, and G. Schäfer, "Vehicle behavior analysis to enhance security in vanets," in *Proceedings of the 4th IEEE Vehicle-to-Vehicle Communications Workshop (V2VCOM2008)*. Citeseer, 2008.
[291] M. Tsukada, S. Arii, H. Ochiai, and H. Esaki, "Misbehavior Detection Using Collective Perception under Privacy Considerations," in *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2022, pp. 808–814.
[292] T. Leinmüller, C. Maihöfer, E. Schoch, and F. Kargl, "Improved Security in Geographic Ad Hoc Routing through Autonomous Position Verification," ser. VANET '06. New York, NY, USA: Association for Computing Machinery, 2006, p. 57–66.
[293] H. Füßler, M. Mauve, H. Hartenstein, M. Käsemann, and D. Vollmer, "A comparison of routing strategies for vehicular ad hoc networks," *Technical reports*, vol. 2, 2002.
[294] J. Grover, M. S. Gaur, V. Laxmi, and N. K. Prajapati, "A Sybil Attack Detection Approach Using Neighboring Vehicles in VANET," in *Proceedings of the 4th International Conference on Security of Information and Networks*, ser. SIN '11. New York, NY, USA: Association for Computing Machinery, 2011, p. 151–158.
[295] V. Naumov, R. Baumann, and T. Gross, "An Evaluation of Inter-Vehicle Ad Hoc Networks Based on Realistic Vehicular Traces," in *Proceedings of the 7th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, ser. MobiHoc '06. New York, NY, USA: Association for Computing Machinery, 2006, p. 108–119.
[296] J. Rezgui and S. Cherkaoui, "Detecting faulty and malicious vehicles using rule-based communications data mining," in *2011 IEEE 36th Conference on Local Computer Networks*, 2011, pp. 827–834.
[297] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '00. Association for Computing Machinery, 2000, p. 255–265.
[298] J. Zhang, "A Survey on Trust Management for VANETs," in *2011 IEEE International Conference on Advanced Information Networking and Applications*, 2011, pp. 105–112.
[299] H. Hasrouny, C. Bassil, A. E. Samhat, and A. Laouiti, "Security Risk Analysis of a Trust Model for Secure Group Leader-Based Communication in VANET," in *Vehicular Ad-Hoc Networks for Smart Cities*, A. Laouiti, A. Qayyum, and M. N. Mohamad Saad, Eds. Springer Singapore, 2017, pp. 71–83.
[300] A. A. Ghorbani, W. Lu, and M. Tavallaee, *Network intrusion detection and prevention: concepts and techniques*. Springer Science & Business Media, 2009, vol. 47.
[301] J. Kamel, I. B. Jemaa, A. Kaiser, L. Cantat, and P. Urien, "Misbehavior Detection in C-ITS: A comparative approach of local detection mechanisms," in *2019 IEEE Vehicular Networking Conference (VNC)*, 2019, pp. 1–8.
[302] 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 Journal on Wireless Communications and Networking*, vol. 2018, no. 1, pp. 1–17, 2018.
[303] ETSI, "Intelligent Transport Systems (ITS); Security; Misbehaviour Reporting service; Release 2," Tech. Rep. TS 103 759, v0.0.10, June 2022.
[304] ——, "Intelligent Transport Systems (ITS); Security; Security header and certificate formats; Release 2," Tech. Rep. TS 103 097, v2.1.1, October 2021.
[305] UN Regulation, "Cyber security and cyber security management system," Tech. Rep. No. 155, March 2021.

[306] ——, "Software update and software update management system," Tech. Rep. No. 156, March 2021.
[307] ISO/SAE, "Road vehicles - Cybersecurity engineering," Tech. Rep. 21434:2021, August 2021.
[308] D. Nilsson and U. Larson, "A Defense-in-Depth Approach to Securing the Wireless Vehicle Infrastructure," *J. Networks*, vol. 4, pp. 552–564, 2009.
[309] H. Ye, L. Liang, G. Ye Li, J. Kim, L. Lu, and M. Wu, "Machine Learning for Vehicular Networks: Recent Advances and Application Examples," *IEEE Vehicular Technology Magazine*, vol. 13, no. 2, pp. 94–101, 2018.
[310] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and Beyond," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3682–3722, 2019.
[311] N. Argyropoulos, P. S. Khodashenas, O. Mavropoulos, E. Karapistoli, A. Lytos, P. A. Karypidis, and K.-P. Hofmann, "Addressing Cybersecurity in the Next Generation Mobility Ecosystem with CARAMEL," *Transportation Research Procedia*, vol. 52, pp. 307–314, 2021.
[312] M. Kang and J. Kang, "A Novel Intrusion Detection Method Using Deep Neural Network for In-Vehicle Network Security," in *2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*, 2016, pp. 1–5.
[313] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, p. 102419, 2020.
[314] C. Zhang, P. Patras, and H. Haddadi, "Deep Learning in Mobile and Wireless Networking: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2224–2287, 2019.
[315] D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, "A survey of deep learning-based network anomaly detection," *Cluster Computing*, vol. 22, no. 1, pp. 949–961, 2019.
[316] T. Alladi, V. Kohli, V. Chamola, and F. R. Yu, "Securing the Internet of Vehicles: A Deep Learning-Based Classification Framework," *IEEE Networking Letters*, vol. 3, no. 2, pp. 94–97, 2021.
[317] N. Kaloudi and J. Li, "The AI-Based Cyber Threat Landscape: A Survey," *ACM Comput. Surv.*, vol. 53, no. 1, Feb. 2020.
[318] Y. Zeng, H. Gu, W. Wei, and Y. Guo, "Deep-Full-Range: A Deep Learning Based Network Encrypted Traffic Classification and Intrusion Detection Framework," *IEEE Access*, vol. 7, pp. 45 182–45 190, 2019.
[319] Y. Zeng, M. Qiu, Z. Ming, and M. Liu, "Senior2Local: A Machine Learning Based Intrusion Detection Method for VANETs," in *Smart Computing and Communication*, M. Qiu, Ed. Cham: Springer International Publishing, 2018, pp. 417–426.
[320] J. Grover, N. K. Prajapati, V. Laxmi, and M. S. Gaur, "Machine Learning Approach for Multiple Misbehavior Detection in VANET," in *Advances in Computing and Communications*, A. Abraham, J. L. Mauri, J. F. Buford, J. Suzuki, and S. M. Thampi, Eds. Springer Berlin Heidelberg, 2011, pp. 644–653.
[321] S. Y. Wang and C. L. Chou, "NCTUns 5.0 Network Simulator for Advanced Wireless Vehicular Network Researches," in *2009 Tenth International Conference on Mobile Data Management: Systems, Services and Middleware*, 2009, pp. 375–376.
[322] P. K. Singh, S. Gupta, R. Vashistha, S. K. Nandi, and S. Nandi, "Machine Learning Based Approach to Detect Position Falsification Attack in VANETs," in *Security and Privacy*, S. Nandi, D. Jinwala, V. Singh, V. Laxmi, M. S. Gaur, and P. Faruki, Eds. Springer Singapore, 2019, pp. 166–178.
[323] S. So, P. Sharma, and J. Petit, "Integrating Plausibility Checks and Machine Learning for Misbehavior Detection in VANET," in *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)*, 2018, pp. 564–571.
[324] P. Sharma and H. Liu, "A Machine-Learning-Based Data-Centric Misbehavior Detection Model for Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4991–4999, 2021.
[325] A. Sharma and A. Jaekel, "Machine Learning Based Misbehaviour Detection in VANET Using Consecutive BSM Approach," *IEEE Open Journal of Vehicular Technology*, vol. 3, pp. 1–14, 2022.
[326] J. Grover, V. Laxmi, and M. S. Gaur, "Misbehavior Detection Based on Ensemble Learning in VANET," in *Advanced Computing, Networking and Security*, P. S. Thilagam, A. R. Pais, K. Chandrasekaran, and N. Balakrishnan, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 602–611.
[327] S. Ercan, M. Ayaida, and N. Messai, "Misbehavior Detection for Position Falsification Attacks in VANETs Using Machine Learning," *IEEE Access*, vol. 10, pp. 1893–1904, 2022.
[328] F. Hawlader, A. Boualouache, S. Faye, and T. Engel, "Intelligent Misbehavior Detection System for Detecting False Position Attacks in Vehicular Networks," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2021, pp. 1–6.
[329] Z. Yang, K. Zhang, L. Lei, and K. Zheng, "A Novel Classifier Exploiting Mobility Behaviors for Sybil Detection in Connected Vehicle Systems," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2626–2636, 2019.
[330] D. Chuxing. GAIA initiative. [Online]. Available: https://gaia.didichuxing.com
[331] Y. Xu, J. Xia, H. Wu, and L. Fan, "Q-Learning Based Physical-Layer Secure Game Against Multiagent Attacks," *IEEE Access*, vol. 7, pp. 49 212–49 222, 2019.
[332] R. Sedar, C. Kalalas, F. Vazquez-Gallego, and J. Alonso-Zarate, "Reinforcement Learning Based Misbehavior Detection in Vehicular Networks," in *ICC 2022 - IEEE International Conference on Communications*, 2022, pp. 3550–3555.
[333] Z. Li, Y. Kong, C. Wang, and C. Jiang, "DDoS Mitigation Based on Space-Time Flow Regularities in IoV: A Feature Adaption Reinforcement Learning Approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 3, pp. 2262–2278, 2022.
[334] S. Yang, C. Wang, L. Yang, and C. Jiang, "iLogBook: Enabling Text-Searchable Event Query Using Sparse Vehicle-Mounted GPS Data," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 12, pp. 4328–4338, 2019.
[335] F. Jameel, M. A. Javed, S. Zeadally, and R. Jäntti, "Secure Transmission in Cellular V2X Communications Using Deep Q-Learning," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–10, 2022.
[336] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, "Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning," *IEEE Access*, vol. 6, pp. 3491–3508, 2018.
[337] T. Alladi, V. Kohli, V. Chamola, F. R. Yu, and M. Guizani, "Artificial Intelligence (AI)-Empowered Intrusion Detection Architecture for the Internet of Vehicles," *IEEE Wireless Communications*, vol. 28, no. 3, pp. 144–149, 2021.
[338] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten, "The WEKA Data Mining Software: An Update," *SIGKDD Explor. Newsl.*, vol. 11, no. 1, p. 10–18, Nov. 2009.
[339] R. W. van der Heijden, T. Lukaseder, and F. Kargl, "VeReMi: A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs," in *Security and Privacy in Communication Networks*, R. Beyah, B. Chang, Y. Li, and S. Zhu, Eds. Cham: Springer International Publishing, 2018, pp. 318–337.
[340] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future Intelligent and Secure Vehicular Network Toward 6G: Machine-Learning Approaches," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 292–307, 2020.
[341] H. al-Khateeb, G. Epiphaniou, A. Reviczky, P. Karadimas, and H. Heidari, "Proactive Threat Detection for Connected Cars Using Recursive Bayesian Estimation," *IEEE Sensors Journal*, vol. 18, no. 12, pp. 4822–4831, 2018.
[342] L. Liang, H. Ye, and G. Y. Li, "Toward Intelligent Vehicular Networks: A Machine Learning Framework," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 124–135, 2019.
[343] M. Salehi and L. Rashidi, "A Survey on Anomaly Detection in Evolving Data: [With Application to Forest Fire Risk Prediction]," *SIGKDD Explor. Newsl.*, vol. 20, no. 1, p. 13–23, May 2018.
[344] G. Pang, A. van den Hengel, C. Shen, and L. Cao, "Toward Deep Supervised Anomaly Detection: Reinforcement Learning from Partially Labeled Anomaly Data," in *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery; Data Mining*. New York, NY, USA: Association for Computing Machinery, 2021, p. 1298–1308.
[345] C. Huang, Y. Wu, Y. Zuo, K. Pei, and G. Min, "Towards experienced anomaly detector through reinforcement learning," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 32, no. 1, 2018.
[346] Z. Ning, P. Dong, X. Wang, L. Guo, J. J. P. C. Rodrigues, X. Kong, J. Huang, and R. Y. K. Kwok, "Deep Reinforcement Learning for Intelligent Internet of Vehicles: An Energy-Efficient Computational

Offloading Scheme," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 4, pp. 1060–1072, 2019.
[347] X. Zhu, Y. Luo, A. Liu, M. Z. A. Bhuiyan, and S. Zhang, "Multiagent Deep Reinforcement Learning for Vehicular Computation Offloading in IoT," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9763–9773, 2021.
[348] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, and A. Sadeghi, "DÏoT: A Federated Self-learning Anomaly Detection System for IoT," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, 2019, pp. 756–767.
[349] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y. C. Liang, Q. Yang, D. Niyato, and C. Miao, "Federated Learning in Mobile Edge Networks: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 2031–2063, 2020.
[350] H. H. Bosman, G. Iacca, A. Tejada, H. J. Wörtche, and A. Liotta, "Ensembles of incremental learners to detect anomalies in ad hoc sensor networks," *Ad Hoc Networks*, vol. 35, pp. 14–36, 2015.
[351] Y. Zhang, N. Meratnia, and P. Havinga, "Adaptive and Online One-Class Support Vector Machine-Based Outlier Detection Techniques for Wireless Sensor Networks," in *2009 International Conference on Advanced Information Networking and Applications Workshops*, 2009, pp. 990–995.
[352] M. Almgren and E. Jonsson, "Using active learning in intrusion detection," in *17th IEEE Computer Security Foundations Workshop*, 2004, pp. 88–98.
[353] Y. Xun, J. Liu, N. Kato, Y. Fang, and Y. Zhang, "Automobile Driver Fingerprinting: A New Machine Learning Based Authentication Scheme," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1417–1426, 2020.
[354] Y. Xun, J. Liu, and Z. Shi, "Multitask Learning Assisted Driver Identity Authentication and Driving Behavior Evaluation," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 10, pp. 7093–7102, 2021.
[355] H. Fang, A. Qi, and X. Wang, "Fast Authentication and Progressive Authorization in Large-Scale IoT: How to Leverage AI for Security Enhancement," *IEEE Network*, vol. 34, no. 3, pp. 24–29, 2020.
[356] X. Lu, L. Xiao, T. Xu, Y. Zhao, Y. Tang, and W. Zhuang, "Reinforcement Learning Based PHY Authentication for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 3, pp. 3068–3079, 2020.
[357] L. Song, G. Sun, H. Yu, X. Du, and M. Guizani, "FBIA: A Fog-Based Identity Authentication Scheme for Privacy Preservation in Internet of Vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5403–5415, 2020.
[358] P. Zhao, Y. Huang, J. Gao, L. Xing, H. Wu, and H. Ma, "Federated Learning-Based Collaborative Authentication Protocol for Shared Data in Social IoV," *IEEE Sensors Journal*, vol. 22, no. 7, pp. 7385–7398, 2022.
[359] "OMNeT++ Discrete Event Simulator," https://omnetpp.org/, Accessed: 2022-07-06.
[360] C. Benzaïd and T. Taleb, "AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?" *IEEE Network*, vol. 34, no. 6, pp. 140–147, 2020.
[361] H. Fang, X. Wang, and S. Tomasin, "Machine Learning for Intelligent Authentication in 5G and Beyond Wireless Networks," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 55–61, 2019.
[362] M. Gupta, F. M. Awaysheh, J. Benson, M. Alazab, F. Patwa, and R. Sandhu, "An Attribute-Based Access Control for Cloud Enabled Industrial Smart Vehicles," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4288–4297, 2021.
[363] X. Li, L. Cheng, C. Sun, K.-Y. Lam, X. Wang, and F. Li, "Federated-Learning-Empowered Collaborative Data Sharing for Vehicular Edge Networks," *IEEE Network*, vol. 35, no. 3, pp. 116–124, 2021.
[364] S. Liu, J. Yu, X. Deng, and S. Wan, "FedCPF: An Efficient-Communication Federated Learning Approach for Vehicular Edge Computing in 6G Communication Networks," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–14, 2021.
[365] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, "Federated Optimization in Heterogeneous Networks," 2020. [Online]. Available: arXiv:1812.06127v5.
[366] G. Cohen, S. Afshar, J. Tapson, and A. van Schaik, "EMNIST: Extending MNIST to handwritten letters," in *2017 International Joint Conference on Neural Networks (IJCNN)*, 2017, pp. 2921–2926.
[367] Q. Kong, F. Yin, R. Lu, B. Li, X. Wang, S. Cui, and P. Zhang, "Privacy-Preserving Aggregation for Federated Learning-Based Navigation in Vehicular Fog," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 12, pp. 8453–8463, 2021.
[368] Z. Yu, J. Hu, G. Min, Z. Zhao, W. Miao, and M. S. Hossain, "Mobility-Aware Proactive Edge Caching for Connected Vehicles Using Federated Learning," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5341–5351, 2021.
[369] F. M. Harper and J. A. Konstan, "The MovieLens Datasets: History and Context," *ACM Trans. Interact. Intell. Syst.*, vol. 5, no. 4, 2015.
[370] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Federated Learning for Data Privacy Preservation in Vehicular Cyber-Physical Systems," *IEEE Network*, vol. 34, no. 3, pp. 50–56, 2020.
[371] T. Mitchell. 20 newsgroups dataset. [Online]. Available: http://www.qwone.com/~jason/20Newsgroups
[372] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Differentially Private Asynchronous Federated Learning for Mobile Edge Computing in Urban Informatics," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2134–2143, 2020.
[373] D. D. Lewis. Reuters dataset. [Online]. Available: http://www.daviddlewis.com/resources/testcollections/reuters21578/
[374] A. Moschitti. Ohsumed dataset. [Online]. Available: http://disi.unitn.it/moschitti/corpora/ohsumed-all-docs.tar.gz
[375] A. Uprety, D. B. Rawat, and J. Li, "Privacy Preserving Misbehavior Detection in IoV Using Federated Machine Learning," in *2021 IEEE 18th Annual Consumer Communications Networking Conference (CCNC)*, 2021, pp. 1–6.
[376] W. Y. B. Lim, Z. Xiong, D. Niyato, J. Huang, X.-S. Hua, and C. Miao, "Incentive Mechanism Design for Federated Learning in the Internet of Vehicles," in *2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*, 2020, pp. 1–5.
[377] W. Y. Bryan Lim, J. Huang, Z. Xiong, J. Kang, D. Niyato, X.-S. Hua, C. Leung, and C. Miao, "Multi-Dimensional Contract-Matching for Federated Learning in UAV-Enabled Internet of Vehicles," in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, 2020, pp. 1–6.
[378] W. Y. B. Lim, J. Huang, Z. Xiong, J. Kang, D. Niyato, X.-S. Hua, C. Leung, and C. Miao, "Towards Federated Learning in UAV-Enabled Internet of Vehicles: A Multi-Dimensional Contract-Matching Approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5140–5154, 2021.
[379] P. Kairouz *et al.*, "Advances and Open Problems in Federated Learning," 2021. [Online]. Available: arXiv:1912.04977v3.
[380] S. Gyawali, Y. Qian, and R. Q. Hu, "Machine Learning and Reputation Based Misbehavior Detection in Vehicular Communication Networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 8871–8885, 2020.
[381] J. Guo, X. Li, Z. Liu, J. Ma, C. Yang, J. Zhang, and D. Wu, "TROVE: A Context-Awareness Trust Model for VANETs Using Reinforcement Learning," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6647–6662, 2020.
[382] S. Guleng, C. Wu, X. Chen, X. Wang, T. Yoshinaga, and Y. Ji, "Decentralized Trust Evaluation in Vehicular Internet of Things," *IEEE Access*, vol. 7, pp. 15 980–15 988, 2019.
[383] M. Cheng, J. Zhang, S. Nazarian, J. Deshmukh, and P. Bogdan, "Trust-aware Control for Intelligent Transportation Systems," in *2021 IEEE Intelligent Vehicles Symposium (IV)*, 2021, pp. 377–384.
[384] "Aim4 1.0-snapshot api," http://www.cs.utexas.edu/~aim/aim4sim/aim4-release-1.0.3/aim4-root/target/site/apidocs/index.html, Accessed: 2021-11-29.
[385] C. Zhang, W. Li, Y. Luo, and Y. Hu, "AIT: An AI-Enabled Trust Management System for Vehicular Networks Using Blockchain Technology," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3157–3169, 2021.
[386] J. Konečný, H. B. McMahan, D. Ramage, and P. Richtárik, "Federated Optimization: Distributed Machine Learning for On-Device Intelligence," 2016. [Online]. Available: arXiv:1610.02527v1.
[387] Q. Pan, J. Wu, J. Li, W. Yang, and Z. Guan, "Blockchain and AI Empowered Trust-Information-Centric Network for Beyond 5G," *IEEE Network*, vol. 34, no. 6, pp. 38–45, 2020.
[388] Y. Ren, X. Chen, S. Guo, S. Guo, and A. Xiong, "Blockchain-Based VEC Network Trust Management: A DRL Algorithm for Vehicular Service Offloading and Migration," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 8, pp. 8148–8160, 2021.

[389] D. Zhang, F. R. Yu, and R. Yang, "A Machine Learning Approach for Software-Defined Vehicular Ad Hoc Networks with Trust Management," in *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 1–6.

[390] "OPNET 14.5," https://opnetprojects.com/opnet-modeler-14-5/, Accessed: 2021-11-29.

[391] D. Zhang, F. R. Yu, R. Yang, and L. Zhu, "Software-Defined Vehicular Networks With Trust Management: A Deep Reinforcement Learning Approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 2, pp. 1400–1414, 2022.

[392] D. Zhang, F. R. Yu, R. Yang, and H. Tang, "A Deep Reinforcement Learning-Based Trust Management Scheme for Software-Defined Vehicular Networks," in *Proceedings of the 8th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, ser. DIVANet'18. New York, NY, USA: Association for Computing Machinery, 2018, p. 1–7.

[393] H. Liu, S. Zhang, P. Zhang, X. Zhou, X. Shao, G. Pu, and Y. Zhang, "Blockchain and Federated Learning for Collaborative Intrusion Detection in Vehicular Edge Computing," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 6073–6084, 2021.

[394] V. Bolón-Canedo, N. Sánchez-Maroño, and A. Alonso-Betanzos, "Feature selection and classification in multiple class datasets: An application to KDD Cup 99 dataset," *Expert Systems with Applications*, vol. 38, no. 5, pp. 5947–5957, 2011. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417410012650

[395] A. Talpur and M. Gurusamy, "Adversarial Attacks Against Deep Reinforcement Learning Framework in Internet of Vehicles," 2021, [Online]. Available: https://arxiv.org/abs/2108.00833.

[396] W. Jiang, H. Li, S. Liu, X. Luo, and R. Lu, "Poisoning and Evasion Attacks Against Deep Learning Algorithms in Autonomous Vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4439–4449, 2020.

[397] Y. Deng, T. Zhang, G. Lou, X. Zheng, J. Jin, and Q.-L. Han, "Deep learning-based autonomous driving systems: A survey of attacks and defenses," 2021, [Online]. Available: https://arxiv.org/abs/2104.01789.

[398] D. Kirat, J. Jang, and M. Stoecklin, "Deeplocker–concealing targeted attacks with ai locksmithing," *Blackhat USA*, 2018.

[399] B. Hitaj, P. Gasti, G. Ateniese, and F. Perez-Cruz, "PassGAN: A Deep Learning Approach for Password Guessing," in *Applied Cryptography and Network Security*, R. H. Deng, V. Gauthier-Umaña, M. Ochoa, and M. Yung, Eds. Cham: Springer International Publishing, 2019, pp. 217–237.

[400] ETSI, "Securing Artificial Intelligence (SAI); Problem Statement," Tech. Rep. GR SAI 004 V1.1.1, December 2020.

[401] M. Scalas and G. Giacinto, "On the Role of Explainable Machine Learning for Secure Smart Vehicles," in *2020 AEIT International Conference of Electrical and Electronic Technologies for Automotive (AEIT AUTOMOTIVE)*, 2020, pp. 1–6.

[402] R. S. Bali, N. Kumar, and J. J. Rodrigues, "Clustering in vehicular ad hoc networks: Taxonomy, challenges and solutions," *Vehicular Communications*, vol. 1, no. 3, pp. 134–152, 2014.

[403] Convex. (2020, March) Deliverable D4.1: Roadside ITS Station Specification. [Online]. Available: https://convex-project.de/onewebmedia/D4.1_Roadside-ITS-Station-Specification_rev1.pdf

[404] M. Ranaweera, A. Seneviratne, D. Rey, M. Saberi, and V. V. Dixit, "Detection of anomalous vehicles using physics of traffic," *Vehicular Communications*, vol. 27, p. 100304, 2021.

[405] B. Nour, A. Ksentini, N. Herbaut, P. A. Frangoudis, and H. Moungla, "A Blockchain-Based Network Slice Broker for 5G Services," *IEEE Networking Letters*, vol. 1, no. 3, pp. 99–102, 2019.

[406] H. Kim, J. Park, M. Bennis, and S.-L. Kim, "Blockchained On-Device Federated Learning," *IEEE Communications Letters*, vol. 24, no. 6, pp. 1279–1283, 2020.

[407] X. Wang, S. Garg, H. Lin, G. Kaddoum, J. Hu, and M. M. Hassan, "Heterogeneous Blockchain and AI-Driven Hierarchical Trust Evaluation for 5G-Enabled Intelligent Transportation Systems," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–10, 2021.

[408] ETSI, "Zero-touch network and Service Management (ZSM); Reference Architecture," Tech. Rep. GS ZSM 002 V1.1.1, August 2019.

[409] S. Hu, Q. A. Chen, J. Joung, C. Carlak, Y. Feng, Z. M. Mao, and H. X. Liu, "CVShield: Guarding Sensor Data in Connected Vehicle with Trusted Execution Environment," ser. AutoSec '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 1–4.

[410] X. Chen, J. Ding, and Z. Lu, "A Decentralized Trust Management System for Intelligent Transportation Environments," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 1, pp. 558–571, 2022.

[411] C. Benzaid and T. Taleb, "ZSM Security: Threat Surface and Best Practices," *IEEE Network*, vol. 34, no. 3, pp. 124–133, 2020.

[412] V. H. Le, J. den Hartog, and N. Zannone, "Security and privacy for innovative automotive applications: A survey," *Computer Communications*, vol. 132, pp. 17–41, 2018.

[413] O. S. Althobaiti and M. Dohler, "Cybersecurity Challenges Associated With the Internet of Things in a Post-Quantum World," *IEEE Access*, vol. 8, pp. 157 356–157 381, 2020.

[414] H. Xiao, A. T. Chronopoulos, and Z. Zhang, "An Efficient Security Scheme for Vehicular Communication Using a Quantum Secret Sharing Method," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 1, pp. 1101–1105, 2020.

[415] K.-A. Shim, "A Survey on Post-Quantum Public-Key Signature Schemes for Secure Vehicular Communications," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–18, 2021.

[416] O. S. Althobaiti and M. Dohler, "Quantum-Resistant Cryptography for the Internet of Things Based on Location-Based Lattices," *IEEE Access*, vol. 9, pp. 133 185–133 203, 2021.

[417] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2018, no. 1, p. 238–268, Feb. 2018.

[418] S. Ha, H. Lee, D. Won, and Y. Lee, "Quantum-resistant Lattice-based Authentication for V2X Communication in C-ITS," in *2020 14th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, 2020, pp. 1–8.

[419] E. Zeydan, Y. Turk, B. Aksoy, and Y. Y. Tasbag, "Post-Quantum Era in V2X Security: Convergence of Orchestration and Parallel Computation," 2021, [Online]. Available: https://arxiv.org/abs/2112.06814.

[420] L. Liu, C. Chen, Q. Pei, S. Maharjan, and Y. Zhang, "Vehicular edge computing and networking: A survey," *Mobile Networks and Applications*, pp. 1–24, 2020.

[421] T. Wang, S. Wang, and Z.-H. Zhou, "Machine learning for 5G and beyond: From model-based to data-driven mobile wireless networks," *China Communications*, vol. 16, no. 1, pp. 165–175, 2019.

[422] Y. Koda, K. Yamamoto, T. Nishio, and M. Morikura, "Differentially Private Aircomp Federated Learning with Power Adaptation Harnessing Receiver Noise," in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, 2020, pp. 1–6.

[423] D. Liu and O. Simeone, "Privacy for Free: Wireless Federated Learning via Uncoded Transmission With Adaptive Power Control," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 1, pp. 170–185, 2021.

[424] M. Brambilla, M. Nicoli, G. Soatti, and F. Deflorio, "Augmenting Vehicle Localization by Cooperative Sensing of the Driving Environment: Insight on Data Association in Urban Traffic Scenarios," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 4, pp. 1646–1663, 2020.

[425] E. Zavvos, E. H. Gerding, V. Yazdanpanah, C. Maple, S. Stein, and m. schraefel, "Privacy and Trust in the Internet of Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–16, 2021.

[426] Y. Zhao, J. Zhao, M. Yang, T. Wang, N. Wang, L. Lyu, D. Niyato, and K.-Y. Lam, "Local Differential Privacy-Based Federated Learning for Internet of Things," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8836–8853, 2021.

[427] H. Chai, S. Leng, Y. Chen, and K. Zhang, "A Hierarchical Blockchain-Enabled Federated Learning Algorithm for Knowledge Sharing in Internet of Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 3975–3986, 2021.

[428] Y. Fu, F. R. Yu, C. Li, T. H. Luan, and Y. Zhang, "Vehicular Blockchain-Based Collective Learning for Connected and Autonomous Vehicles," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 197–203, 2020.

[429] S. Savazzi, M. Nicoli, M. Bennis, S. Kianoush, and L. Barbieri, "Opportunities of Federated Learning in Connected, Cooperative, and Automated Industrial Systems," *IEEE Communications Magazine*, vol. 59, no. 2, pp. 16–21, 2021.

[430] C. Xiao, B. Li, J. yan Zhu, W. He, M. Liu, and D. Song, "Generating Adversarial Examples with Adversarial Networks," in *Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence*, 7 2018, pp. 3905–3911.

[431] V. S. Silva, A. Freitas, and S. Handschuh, "On the semantic interpretability of artificial intelligence models," 2019. [Online]. Available: arXiv:1907.04105.

[432] L. Huang, A. D. Joseph, B. Nelson, B. I. Rubinstein, and J. D. Tygar, "Adversarial machine learning," in *Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence*, ser. AISec '11. New York, NY, USA: Association for Computing Machinery, 2011, p. 43–58.

[433] M. A. Elsayed and N. Zincir-Heywood, "BoostGuard: Interpretable Misbehavior Detection in Vehicular Communication Networks," in *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, 2022, pp. 1–9.

[434] B. Mahbooba, M. Timilsina, R. Sahal, M. Serrano, and A. M. Khalil, "Explainable Artificial Intelligence (XAI) to Enhance Trust Management in Intrusion Detection Systems Using Decision Tree Model," *Complexity*, 2021. [Online]. Available: https://doi.org/10.1155/2021/6634811

[435] H. Mankodiya, M. S. Obaidat, R. Gupta, and S. Tanwar, "XAI-AV: Explainable Artificial Intelligence for Trust Management in Autonomous Vehicles," in *2021 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI)*, 2021, pp. 1–5.

[436] I. Rasheed, F. Hu, and L. Zhang, "Deep reinforcement learning approach for autonomous vehicle systems for maintaining security and safety using LSTM-GAN," *Vehicular Communications*, vol. 26, p. 100266, 2020.