IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 30, 2020, accepted December 31, 2020, date of publication January 8, 2021, date of current version January 15, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3050038

A Survey on the Current Security Landscape of Intelligent Transportation Systems

AYYOUB LAMSSAGGAD[1], NABIL BENAMAR[2], ABDELHAKIM SENHAJI HAFID[3], AND MOUNIRA MSAHLI[4]

[1]Department of Mathematics and Computer Science, Faculty of Sciences, Moulay Ismail University of Meknes, Meknes 50000, Morocco
[2]IMAGE Laboratory, Department of Computer Engineering, School of Technology, Moulay Ismail University of Meknes, Meknes 50000, Morocco
[3]Montreal Blockchain Laboratory, Department of Computer Science and Operational Research, University of Montreal, Montreal, QC H3C 3J7, Canada
[4]Department of Computer Sciences and Networks (INFRES), Télécom Paris, 91120 Paris, France

Corresponding author: Ayyoub Lamssaggad (a.lamssaggad@edu.umi.ac.ma)

This work was supported in part by the Natural Sciences and Engineering Research Council of Canada.

ABSTRACT With the proliferation of embedded technologies and wireless capabilities, today's vehicles are no longer isolated mechanical machines. They become part of a hyper-connected system -Intelligent Transportation Systems (ITS)- that has the potential to support multiple levels of autonomy and intelligence improving considerably the safety, efficiency, and sustainability of transportation networks. However, this raises new security issues that make the whole system prone to cybersecurity attacks that threaten both the safety and privacy of all road-users. This article gives a short background tutorial on the main security issues and the different attacks that hinder Intelligent Transport Systems. To enable secure and safe ITS applications, this article provides a comprehensive analysis of existing solutions and highlights their strengths and limitations. Finally, this survey presents key challenges in the field, and discusses recent trends that must be factored in by researchers, implementers, and car manufactures to improve the security of ITS.

INDEX TERMS Intelligent transportation systems, vehicular networks, attacks, security, privacy.

I. INTRODUCTION

In recent years, Intelligent Transport Systems (ITS) have gained increasing attention as a promising field of research in academia and also within standardization bodies, such as the Internet Engineering Task Force (IETF). ITS are playing a critical role in designing future smart roads; they are one of the main components of smart cities [1]. Vehicular Ad-Hoc Networks (VANET) [2] represent the most important component of ITS. Indeed, a study by the US Department of Transport (DOT) reported that VANET have the potential to address more than 79 % of all crashes involving unimpaired drivers. In VANET, vehicles cooperatively collect and share information with each other, with road-side infrastructure, and with other vulnerable road users, such as pedestrians and bicycles. Indeed, vehicular communications develop the potential to promote global traffic control through exchanging safety messages, traffic conditions, and warning messages in case of accidents. Hence, they hold the promise to deal with complex road situations (e.g., reduce traffic jams, accident rates, and environmental pollution) [3], [4], and also to improve individual safety, comfort, and convenience, especially with the tremendous increase in various travel demands (e.g., vehicular traffic, public transportation, freight, and even pedestrian traffic).

The European Transport Safety Council (ETSC) [5] reports that ITS focus on the development of digital technologies (e.g., Electronic Control Units (ECU), sensors and actuators) to promote ''smartness'' in ITS components. In parallel, Cooperative-ITS (C-ITS) focus on the development of communication protocols to support interactions between ITS components. Thus, the objective of C-ITS is to enable applications that can improve the overall performance of vehicular networks [2], [6], [7]. In order to achieve higher levels of interconnectivity between different ITS components, vehicles are becoming cluttered with a diversity of information and communication technologies. These include wireless communication technologies, such as Bluetooth, Wi-Fi, satellite systems, 3G/4G, and more recently, the 5th Generation (5G), Visible Light Communication (VLC), and Millimeter Waves [8]. However, using such components for vast data collection and dissemination comes with a set of challenges,

The associate editor coordinating the review of this manuscript and approving it for publication was Yanli Xu.

particularly related to security and privacy issues. Modern vehicular networks are vulnerable to a wide range of security threats. An attacker can exploit the exposure of the system to gain access to vehicles and eventually control them; this may lead to dangerous driving situations causing life-threatening crashes.

The ability to perform a successful attack requires an in-depth knowledge of the targeted system. The first step for an attacker would be to evaluate attack surfaces to gain access and deliver malicious input to the system. Then, the attacker has to search for exploitable vulnerabilities to control the external and internal vehicular network. Consequently, security must be guaranteed to establish reliable communications between different ITS components. To this end, a large number of studies (e.g., [9]–[16]) have been conducted (as we will discuss deeply in this article) aiming to provide appropriate protection against the threats facing ITS. A good security approach should provide protection against attacks without degrading the quality of service of the system; this is more critical in the case of systems that involve mobility and are delay-sensitive. Indeed, implementing security mechanisms generates overhead, in terms of computation and communication, which may degrade the system performance [17]. Thus, a trade-off should be found between the level of security and the performance of the system. The current survey reviews the state-of-the-art security solutions in ITS and highlights their strengths and limitations. The following sub-sections discuss existing surveys related to security issues in ITS and present the main contributions of the current survey.

A. EXISTING SURVEYS AND CONTRIBUTION

In recent years, several research articles have been published covering various security-related issues associated with ITS [18]–[27]. Lu *et al.* [18] provide a comprehensive security analysis in the field of vehicular networks with a special emphasis on anonymous authentication schemes, used to protect the privacy of vehicle users, and trust management models. Similarly, Huang *et al.* [19] provide an in-depth review of the state-of-the-art solutions concerning security and privacy for V2X communications. However, both contributions did not cover new emerging security solutions (e.g., machine learning-based defense mechanisms and 5G-V2X security technologies). Hussain and Zeadally [20] provide an in-depth study of the security features, including issues, solutions, and standards of 5G and their applicability to VANET. However, this study did not address the current trends in machine learning. Alnasser *et al.* [21] analyze the threats for V2X and some traditional security solutions. Hahn *et al.* [22] and Parkinson *et al.* [23] identify security challenges, risks, and vulnerabilities that can subsequently be used to motivate a future roadmap to address cyber security-related challenges. However, the challenges and the mitigating solutions, they did cover, are outdated due to the emergence of newer technologies (e.g., 5G technologies, machine learning-based schemes, Blockchain) that can boost the development of better security solutions. There are also several surveys that cover specific kinds of security solutions. For example, van der Heijden *et al.* [24] and Sharma and Kaul [25] are concerned with detecting misbehaviors and intrusions in the network. Petit *et al.* [26] cover pseudonymous schemes and Hussain *et al.* [27] focus more on trust management. Table 1 summarizes the features of existing related surveys and highlights the enhancements in this article.

We conclude that existing surveys have investigated ITS security from different perspectives, such as risks, threat assessment, and security countermeasures. However, to the best of our knowledge, there is no survey that fully addresses the major aspects of ITS security including newer challenges and technologies, and the corresponding security solutions. In this regard, this article presents a systematic review that aims to fill this gap through an in-depth analysis to cover recent advancements in ITS security.

B. MAIN CONTRIBUTIONS

In this article, we build upon existing security solutions in ITS to present a comprehensive review of related works published so far. More specifically, we cover recent publications (in the last seven years) from Q1 journals [28] (see Figure 1); the objective is to provide a detailed security analysis where vulnerabilities are surveyed and potential attacks are discussed. We provide a in-depth analysis of the current security landscape in ITS with the objective to help in identifying the missing elements in the design of existing security solutions. We also classify emerging defense mechanisms that provide solutions to the shortcomings of existing countermeasures and newer/emerging cyberattacks. Furthermore, we identify promising future research directions in ITS security. The main contributions of this article can be summarized as follows:

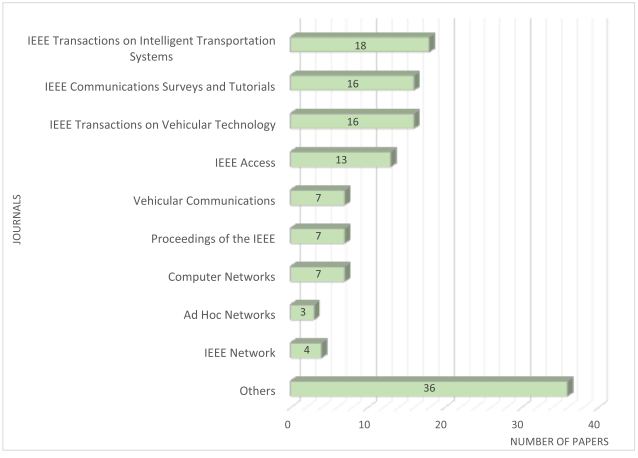

FIGURE 1. Articles related to ITS security per journal in the last 10 years.

- We present a general overview to describe the concept of ITS with a special emphasis on Vehicular Ad-hoc Networks, describing the architecture and the currently used technologies.

TABLE 1. Related survey articles.

Ref.	Journal	Vulnerability assessment	Attacks classification	Authentication schemes	ML-approaches	5G-V2X security	Research challenges	Major Contributions	Common points with our survey	Enhancements in our paper
Lu *et al.* [18]	IEEE Transactions on Intelligent Transportation Systems	*	✓	✓	*	*	*	Analysis of anonymous authentication schemes and trust management models used in VANET.	Evaluation of authentication-based security mechanisms.	Focus on most recently published papers on security, privacy, and trust in ITS.
Huang *et al.* [19]	IEEE Open Journal of Vehicular Technology	*	✓	✓	*	*	✓	State-of-the-art solutions security and privacy for V2X.	Evaluation of authentication-based security mechanisms.	Coverage of new emerging technologies (e.g., ML and 5G-V2X).
Hussain *et al.* [20]	Future Generation Computer Systems	*	✓	*	*	✓	✓	In-depth study of the security features of 5G and their applicability to VANET.	Exploration of recent security trends in 5G-V2X technologies.	Coverage of the current trends of ML-dominant approaches in ITS.
Alnasser *et al.* [21]	Computer Networks	*	✓	✓	*	*	*	Comprehensive taxonomy of existing security threats and solutions for V2X.	Classification of security attacks and the corresponding mitigation mechanisms.	Detailed classification of security attacks and recent security countermeasures in ITS.
Hahn *et al.* [22]	IEEE Intelligent Transportation Systems Magazine	✓	✓	*	*	*	✓	Analysis of security and privacy vulnerabilities in ITS and short discussion of main challenges and mitigation techniques.	Assessment of vulnerabilities and discussion of potential mitigation techniques.	Deep investigation of potential attacks to identify the missing security elements in the design of security solutions.
Parkinson *et al.* [23]	IEEE Transactions on Intelligent Transportation Systems	✓	✓	*	*	*	*	Analysis of most relevant cyber security knowledge gaps.	Assessment of vulnerabilities and discussion of potential mitigation techniques.	Coverage of recent contributions in ITS security with more focus on their limitation and challenges.
Van Der Heijden *et al.* [24]	IEEE Communications Surveys & Tutorials	*	✓	✓	*	*	✓	A survey of misbehavior detection mechanisms in cooperative-ITS.	Security analysis of cooperative ITS.	Evaluation of various security solutions to enhance security of ITS.
Sharma *et al.*, [25]	Vehicular Communications	*	✓	*	*	*	*	A survey of intrusion detection systems with an analysis and comparison of different detection techniques and strategies.	Evaluation of the applicability of intrusion detection systems in ITS.	Evaluation of recent mechanisms that address the applicability of ML-approaches.
Petit *et al.* [26]	IEEE Communications Surveys Tutorials	*	*	✓	*	*	✓	Analysis of challenges and requirements of pseudonymous authentication schemes for vehicular networks.	Evaluation of authentication-based security mechanisms.	Holistically addresses the problematic of security in ITS.
Hussain *et al.* [27]	IEEE Transactions on Intelligent Transportation Systems	*	*	✓	*	*	✓	State-of-the-art solutions on trust management in VANET.	Evaluation of trust establishment approaches used in VANET.	In-depth review of the problematic of security in ITS including trust establishment.
Proposed survey	—	✓	✓	✓	✓	✓	✓	A comprehensive survey that addresses the current security landscape of Intelligent Transportation Systems.	—	—

- We conduct an in-depth security analysis that investigates the nature of cyber-threats faced by ITS; the objective is to classify vulnerabilities and identify their root causes. We also provide a classification of the main attacks on ITS to understand the impact of these attacks and how to react accordingly.
- We evaluate the current state of the art of emerging defense strategies. In addition, we provide a comparative analysis of these strategies with a focus on their performance and the challenges.
- We draw insights and present promising future research directions to secure ITS.

The remainder of this article is organized as follows. Section 2 briefly presents the concept of ITS with an emphasis on Vehicular Ad-hoc Networks. Section 3 presents an extensive ITS security analysis including vulnerabilities, attacks, and attack surfaces. Section 4 presents the state of the art of ITS security solutions. Finally, section 5 concludes this article. Figure 2 shows the global organization of the survey.

II. INTELLIGENT TRANSPORT SYSTEMS OVERVIEW

In this section, we present essential background information on Intelligent Transportation Systems.

A. INTEGRATION OF INTERNET OF THINGS WITH INTELLIGENT TRANSPORTATION SYSTEMS

Over the past few decades, we have experienced the domination of novel types of communication between humans and things and among things themselves leading to the emergence of a new paradigm called the Internet of Things (IoT) [29]. The IoT paradigm has demonstrated its potential to reshape the future of Internet communication, bringing vast improvements and radical transformation to human lives. It consists of a multitude of leading-edge information and communication technologies that bridge the physical world (e.g., vehicles and smart appliances) to the digital world to form a new intelligent system; such a system will improve every aspect of human life, including homes, transportation systems, environment and even the human body. In particular, Guerrero-Ibanez *et al.* [29] report that IoT will play a pivotal role in complementing the evolution of intelligent

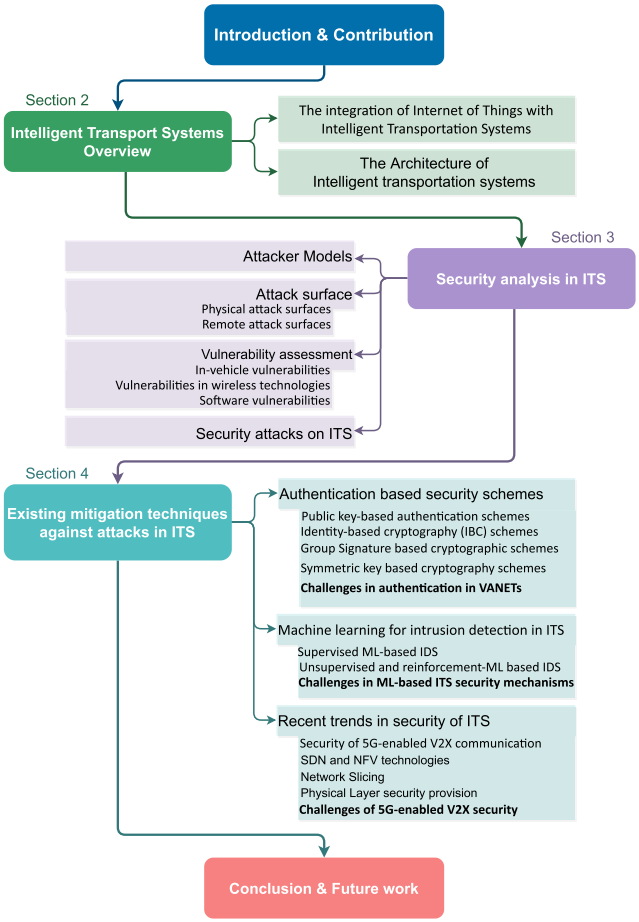

FIGURE 2. Organization of the survey.

transportation systems. Indeed, IoT represents a breakthrough in terms of trends and traffic management approaches to satisfy the need for safer and comfortable experiences on roads [30]. To realize such a breakthrough, the active development of ITS along with IoT requires a combination of data collection, processing, and disseminating technologies. In the following, we briefly overview these technologies [1], [31].

1) DATA COLLECTION

Data collection is the first step in data journey through ITS applications. It provides the capability to gather all basic observable measurements (e.g., location, speed, neighboring vehicles, road traffic condition, and average travel time) from multiple sources of data (e.g., road data, vehicle data, driver/passenger/pedestrian data, and traffic flow data) to be exchanged between vehicles and roadside units [32]. Because of the significant safety implication related to vehicular networks, it is critical to develop reliable collection solutions that take into account VANET characteristics (e.g., mobility and time sensitivity). In the literature, several contributions propose different architectures and schemes to support efficient data collection. In [33], Touil *et al.* propose a data collection scheme based on a clustering approach; the objective is to reduce the impact of mobility and density on the data collection stations. Khan *et al.* [34] propose a data forwarding algorithm for data collection; it is based on a ranking scheme of On-Board Units (OBUs) and the hop count of data traffic. The authors in [35] propose a Quality-oriented Data Collection (QDC) to provide high quality data for vehicular application and services. Moreover, QDC maintains the time sensitivity and accuracy required for vehicular services while keeping communication overheads at minimum levels; this was shown via simulations results.

2) INFORMATION PROCESSING

The data collected from ITS can be used in developing ITS applications. However, this requires the capability to clean, transform, and discover patterns in the data in order to extract useful information. Recently, the explosive growing number of complex data collection technologies has increased the demand for large-scale and real-time data processing frameworks. This led to the emergence of considerable research efforts in the field of data analytics that take advantage of new technologies to introduce advanced frameworks that provide on-demand decision support. In [36], Nie *et al.* propose a novel processing framework for vehicular sensor networks, called Vehdoop. This framework uses the computing capability of vehicles to efficiently process sensor data in parallel across a large number of vehicles in a decentralized manner.

3) DATA DISSEMINATION

The basic idea behind ITS is to build a cooperative awareness among network members to enhance road safety and transport efficiency. In VANET, the data dissemination component plays a pivotal role in distributing and delivering information from Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and from Vehicle-to-Everything (V2X) [37]. Thus, it is important to build an efficient and reliable data dissemination scheme that guarantees full network coverage while maintaining a high data delivery ratio and minimum overheads [38]. However, the key challenge remains on how to ensure efficient data dissemination considering, the high mobility of nodes (moving vehicles), stringent delay requirements, and adequate trust management [39]. In this vein, Zhao *et al.* [40] provide an Optimal Transmission Reliability Enhancement Mechanism (OTREM) designed to improve the quality of Emergency Warning Messages (EWM) propagation in vehicular cooperative driving systems. The main idea of OTREM is to use an improved finite automata to minimize transmission delays, error rate, and redundancy. The experimental results show that OTREM effectively reduces transmission delays and redundancy and increases propagation accuracy rates of EWM. Trust is another key factor that affects the performance of data dissemination strategies [27]. Therefore, the authors in [41] describe the trust relationship among vehicles and propose a trust evaluation model for VANET; the model considers the trust uncertainty of fuzziness and randomness in the interactions among vehicles.

B. INTELLIGENT TRANSPORTATION SYSTEMS ARCHITECTURE AND COMPONENTS

The high-level architecture of ITS provides a description of the functionality and communication links between ITS nodes (e.g., vehicles). It consists of a set of interconnected components organized into two main domains: Intra-vehicle and Inter-vehicle (see Figure 3) [21].

1) INTRA-VEHICLE DOMAIN

The number of electrical components and embedded devices in modern vehicles is continually increasing. A multitude of interconnected embedded computer systems, called Electronic Control Units (ECUs), have been widely used in vehicles forming a distributed network to control a broad range of automobile functions [42] including powertrain and in-vehicle infotainment. In general, ECUs can communicate with each other over many in-vehicle bus communication networks [42]–[44]: Controller Area Network (CAN), Local Interconnect Network (LIN), FlexRay, Media Oriented System Transport (MOST), and Ethernet (see Table 2)). The use of each one of them depends on the criticality, cost, bandwidth, and timing requirements of the desired functions.

TABLE 2. Current automotive physical layer technologies.

Bus name	Transfer Rate	Access Control
Controller Area Network	1Mbits/s	CSMA/CA and AMD
Local Interconnect Network	20Kbits/s	Polling
FlexRay	10Mbits/s	TDMA
Media Oriented System Transport	150Mbits/s	CSMA/CD and TDM
Ethernet	100Mbits/s	TDMA and TDD

CAN and FlexRay are mainly designed to provide a low-cost and fast data transmission; this makes them more appropriate for critical applications, such as powertrain and safety control. LIN is designed for functions that require smaller transmission speed, such as controlling lights, doors, air conditioning, and seats. MOST is a high-speed bus designed for multimedia applications in the automotive environment.

Due to the diversity of in-vehicle bus communication networks, a gateway ECU is required to coordinate between the different buses and manage communication protocols of the intra-vehicle domain. Furthermore, ECU plays a crucial role in bridging the communication to external networks allowing a great flexibility and convenience in the system design [44].

2) INTER-VEHICLE DOMAIN

The inter-vehicle paradigm covers the communication between vehicles and their surrounding environments, including other vehicles, pedestrians, bicycles, or what is commonly named Vulnerable Road Users (VRU), and the regional infrastructure as well. Each vehicle equipped with an OBU can become a part of the network and able to send and receive messages related to a variety of applications (e.g., safety, traffic management, and infotainment). Inter-vehicle

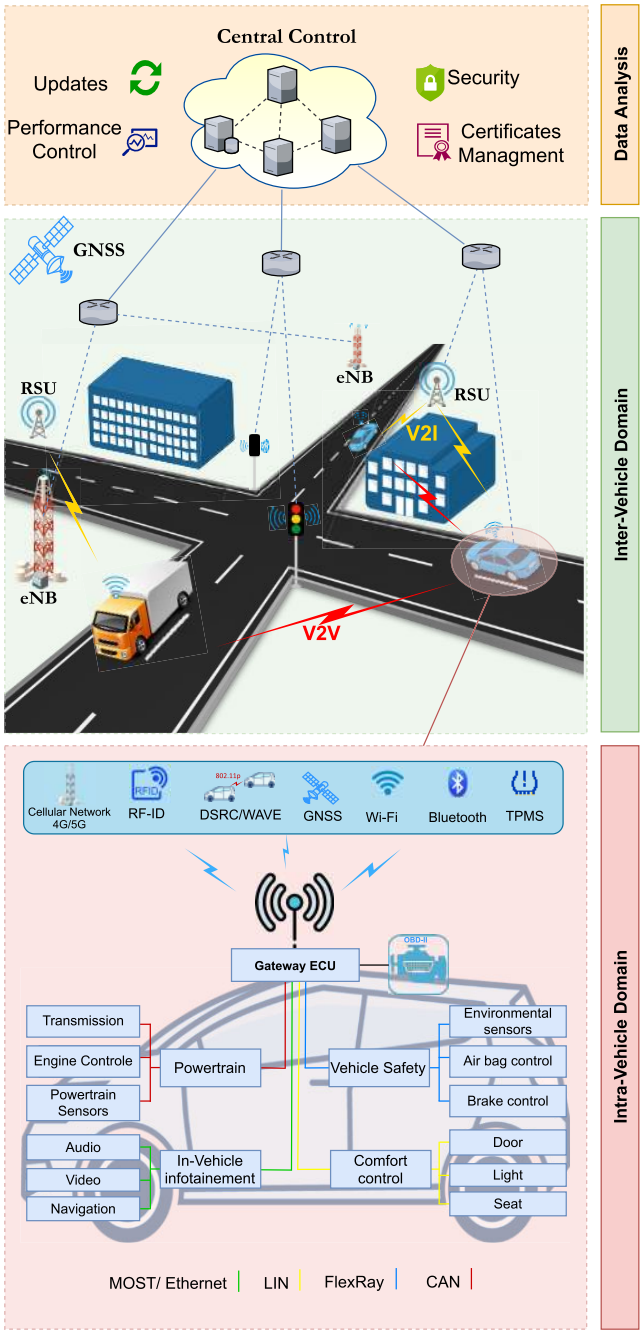

FIGURE 3. Architecture and key components of an Intelligent Transport Systems.

communication may refer to V2X (Vehicle to everything), which incorporates more specific types of communication depending on the targeted entities [45]. This includes Vehicle-to-Vehicle (V2V) [46], [47], Vehicle-to-Infrastructure (V2I) [48], [49], Vehicle-to-Pedestrian (V2P) [50]–[52] and Vehicle-to-Grid (V2G) communication [53], [54]. To support such communications, Dedicated Short-Range Communication (DSRC) and Wireless Access in Vehicular Environment (WAVE) are one of the most promising wireless standards deployed in the field of transportation [55].

In 1999, the Federal Communications Commission (FCC) allocated 75 MHz of spectrum in the range of 5.85-5.925 GHz to be used exclusively for DSRC services in ITS [56]. DSRC is mainly designed to provide high data transfers over two basic units: Road-Side Unit (RSU) and On-Board Unit (OBU) with low communication latency [57]; hence, covering a wide range of applications, such as V2V emergency warning and collision avoidance applications. The development of the DSRC standard has resulted in the IEEE 802.11p standards along with IEEE 1609.x, which makes it close to the WAVE standard [57]. Recently, the IEEE 802.11p standard has been replaced by IEEE 802.11-OCB, which refers to a special mode of communication outside the context of the basic service set [58].

To expand the range of VANET's applications, there exists a wide range of other communication standards, such as cellular technologies (Long-Term Evolution (LTE) and LTE-Advanced), Wi-Fi, Visible Light Communication (VLC), and WiMAX. However, not all of these standards have the ability to provide reliable communications for safety applications [59]. For instance, Wi-Fi can exhibit a very high market that can be exploited to provide low cost and efficient wireless access in VANET; however, it suffers from limited coverage and intermittent connectivity due to the high mobility of vehicles [60]. V2X-LTE provides ubiquitous coverage that supports VANET and solves bandwidth problems; however, it leads to higher latency, which is a challenge for safety and real-time applications [59], [61].

III. SECURITY ANALYSIS IN ITS

With the fast and active development of IoT, it comes with no surprise the considerable increase of security attacks targeting IoT systems. Generally, smart IoT devices (e.g., wearable heath monitors, connected appliances and vehicles) carry sensitive information. Thus, any attacks on data integrity, availability, or confidentiality can have serious impact (e.g., financial/human losses) on the victims of these attacks. Attackers may initially target IoT technologies (e.g., sensors), embedded in the system (e.g., ITS) under attack, with the objective to compromise the whole system [62]. Security is a main concern of any system; however, it becomes more critical when human lives are involved, such as the case in ITS. Due to the high accessibility, complexity, and interdependency of communication technologies in ITS, the probability of security breaches is high. Figure 4 shows that attackers can exploit vulnerabilities discovered in entry points, called attack surfaces, which provide direct access to vehicular communication systems. The ability to execute successful attacks may cause serious damage in ITS [63]. In this section, we provide a detailed analysis of the current security landscape in ITS.

A. ATTACKER MODELS

The operations of ITS are entirely controlled by the embedded software in the vehicle without the need of human intervention. This makes it possible for attackers to control the vehicle if they succeed in penetrating the system remotely. Hence, understanding the attack models is a fundamental step towards designing efficient schemes to predict the behavior of attackers and counter their malicious activities. By analyzing the potential attack characteristics (e.g., the attack method and the attack scope) and interactions of attackers with the system under attack (e.g., membership and motivation), we categorize the attackers into several classes [64]–[66].

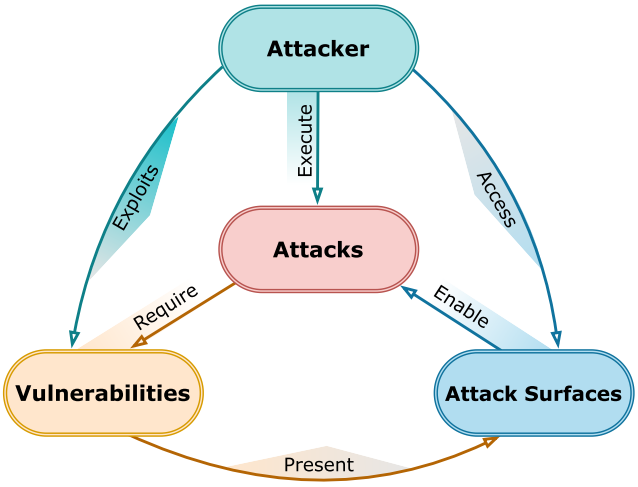

FIGURE 4. Relation between security relevant terms.

1) **Active vs. Passive:** Active attackers generate malicious packets to be transmitted to other nodes causing harmful effects on the network. Generally, these attackers have the authorization to operate within the network; thus, they could perpetrate almost any kind of attacks, such as DoS attacks, Sybil attacks, and blackholes wormholes. Passive attackers present the opposite characteristics of active attackers. They attempt to silently monitor and eavesdrop the network traffic to extract useful information that can be used to prepare future attacks; these attackers are generally outsiders and cause no direct damage to the network, which make them very difficult to detect.
2) **External vs. Internal:** External or outsider attackers perpetrate their attacks from outside the network; they are not authorized to operate in the network. Generally, they are limited in terms of attacks they can launch. They must successfully bypass system defenses, such as firewalls and IDSs, to be able to operate within the network. In contrast, internal attackers are mainly legitimate members or part of the network; this makes them able to access basic network resources according to their access privilege. These attackers can cause serious damage due to their ability to perpetrate almost any kind of attack targeting the confidentiality, availability, and integrity of the system.
3) **Local vs. Extended:** Local attackers operate within a limited scope targeting only nearby vehicles or RSUs. Extended attackers expand the scope of their attacks

which can be performed from anywhere via the internet; in this case, the physical location of attackers becomes irrelevant.

4) **Malicious vs. Rational:** The main goal of malicious attackers is to cause disruption and damage to the network without considering the consequences. These kinds of attackers are usually seeking no personal benefits from their attacks [64]. On the other hand, rational attackers can be more dangerous by launching their attacks targeting specific victims to draw attention and also to maximize their benefits.

B. ATTACK SURFACE

Due to the growing number of internetworking control units in VANET, new attack surfaces are created, where an attacker could gain access to compromise the security of the network [67]. Thus, the identification of those attack surfaces can help both Original Equipment Manufacturers (OEMs) and drivers to better prevent possible attacks.

1) PHYSICAL ATTACK SURFACES

VANET provide several physical interfaces installed in both moving cars, such as On-Board Diagnostics (OBD) port that allow access to the car's internal networks and regional roadside infrastructure. Having open access to those critical components makes the whole in-vehicle system highly reachable to anyone, including attackers. This increases the ability of attackers to explore the system offline, discover exploitable vulnerabilities, and test possible attack scenarios until performing a successful one. It is worth mentioning that the OBD-II port remains one of the most critical interfaces used to compromise the full range of automotive systems. This interface is available in almost every vehicle to provide efficient diagnostic codes to detect faults in ECUs. It also provides direct access to the vehicle's internal network. Once an attacker can get a physical connection to this port, he/she will be able to inject messages, jam signals, and/or eavesdrop on exchanged keys between ECUs and different entities. This may result in car theft or control of various components of the automobile (e.g., brake, engine, and locks). Other ways to gain physical access to the vehicle are those used for entertainment systems, such as disc reader or USB port, where the attacker creates multimedia files that can change code in the system to spy on other parts of the vehicle. Practically, it is hard for an attacker to gain such physical access to the vehicle's internal network. Therefore, attackers seek to find other possible attack surfaces to initiate remote attacks on the vehicle's internal network by injecting malicious codes, or placing devices, with wireless features, to read messages bridged from the targeted network [68], [69].

2) REMOTE ATTACK SURFACES

ITS rely on wireless connectivity to ensure flexible and extensible communications between different ITS components. By exploiting the vulnerabilities and sensitive nature of this connectivity, these components can be ultimately hacked and controlled remotely over the Internet. Checkoway *et al.* [70] identify attack surfaces for modern automobiles. Wireless attack surfaces can be categorized based on the range of wireless access. For short-range wireless access, attackers should be located nearby to the attack target (generally, between 5 and 300 meters) to be able to wirelessly compromise desired ECUs and read messages bridged from the vehicle internal network. Particularly, they can send and execute malicious code (e.g., Trojan Horse, Virus, and Worm) compromising vehicle safety. Several technologies can be used as an entry point to hack the system; these include Bluetooth, Wi-Fi, Remote Keyless Entry (RKE), RFIDs, and Tire Pressure Monitoring Systems (TPMS). For long-range access (e.g., greater than 1 km), attacks can be launched from anywhere. This kind of attacks focus on the exploitation of addressable channels like Internet services or cellular capabilities integrated into the telematics units, or Broadcast channels including Global Navigation Satellite Systems (GNSS), Satellite Radio, Radio Data System (RDS), and Traffic Message Channel (TMC) [70].

C. VULNERABILITY ASSESSMENT

To execute successful attacks, hackers must have a deep knowledge of the targeted system. Thus, they can precisely scan and monitor specific elements of the network to discover possible vulnerabilities. Generally, a vulnerability exists because of a limitation or a weakness in the system design, which can be exploited to compromise security services, such as confidentiality, availability, and integrity. A good security approach requires the identification of vulnerabilities to prioritize the testing; this will help security experts to recognize the weakest entities in order to develop appropriate countermeasures and improve the security of future vehicles. Figure 5 shows possible security vulnerabilities.

1) IN-VEHICLE VULNERABILITIES

In the design phase of in-vehicle network protocols, security issues were not a primary concern since vehicles were rarely connected to the external world. However, due to the increased number of external interfaces and the ability to connect to outside networks, in-vehicle networks have become heavily exposed to many cyber-security threats, such as eavesdropping, spoofing, and denial of service. Indeed, in-vehicle bus networks are simple message broadcasting networks; an attacker can easily attach a fake ECU with an illegitimate, malicious program and receive broadcast messages.

Due to the lack of security protection (e.g., no confidentiality, no privacy, and no authentication), particularly in CAN buses [71], the attacker can easily analyze the transmitted frames based on id-based priority schemes (priority arbitration: message with a lower identifier gets higher priority); this allows the attacker to determine the target ECU and its priority. Thus, he/she can exploit the priority arbitration to keep the network busy by sending spoofed messages causing resource exhaustion (Denial-of-Service) and other frames to back off.

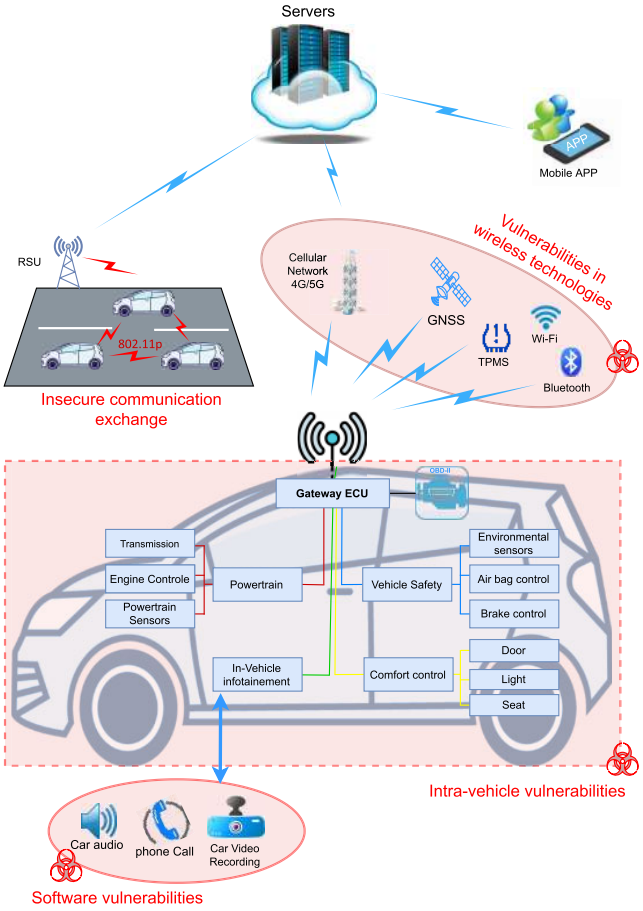

FIGURE 5. Map of security vulnerabilities in automotive systems.

Furthermore, because internal bus networks are universally connected, the attacker can compromise the whole in-vehicle security and take control of all vehicle components leading to serious safety threats.

Recently, many studies on security vulnerabilities (see Table 3) highlight the weaknesses in internal bus networks that allow direct access without any restriction. Several contributions [43], [72]–[75] focus on the security of CAN bus. In [72], Iehira *et al.* propose an attack that combines bus-off attacks with spoofing attacks exploiting the absence of security protection in the CAN buses. According to the simulation results, the proposed attacks have successfully prevented the transmission of regular messages without any resistance from legitimate ECUs; this shows the feasibility of these attacks and the potential threats to vehicles. Currie [75] studies the overall insecurity of the CAN bus architecture. The author shows that it is easy to manipulate the CAN bus using basic computer hardware. He proposes basic guidelines for security researchers on how to gain access to internal vehicle systems and manipulate the vehicle by reverse engineering.

The security research community did produce several contributions [76]–[78] related to potential threats of exploiting CAN buses. However, there are limited studies concerning the security of other network buses (e.g. FlexRay, LIN). Mousa *et al.* [76] report that FlexRay suffers from the same lack of security protection as CAN buses (e.g., no confidentiality, no authentication, and no privacy). They present a lightweight authentication protocol based on the implementation of Light Weight CAN Authentication Protocol (LCAP) over FlexRay. Murvay and Groza [77] discuss the feasibility of attacks on FlexRay. They first identify network behavior and features for a better understanding of targeted attacks including DoS attacks and messages spoofing. They put these attacks into practice and analyzed them in terms of feasibility.

In addition to CAN and FlexRay, LIN is another commonly used in-vehicle's internal network. Takahashi *et al.* [78] evaluate the resistance of LIN against cyber-threats. They present sample attacks that use the characteristics of an error handling mechanism [79]; the main concept behind the proposed mechanism is to inject any value of false response using the error handling mechanism. This injects a collision between the responses to induce the bit error and injects a false response after an error occurs. According to the experimental results, the proposed mechanism [78] shows great effectiveness in this type of attacks.

2) VULNERABILITIES IN WIRELESS TECHNOLOGIES

Although wireless communication technologies provide many advantages, they introduce security vulnerabilities. Attackers can exploit these vulnerabilities to gain remote access to the internal vehicular network and compromise the whole system. This section aims to shed light on the main security vulnerabilities introduced by the implementation of wireless technologies used in ITS, such as DSRC/WAVE, Cellular-V2X, Bluetooth, and Global Navigation Satellite Systems (GNSS).

a: IEEE 802.11p

VANET mainly adopt IEEE 802.11p as a dominant vehicular Radio Frequency (RF) technology. Although IEEE 802.11p provides reliable vehicular communication, this technology remains vulnerable to attacks. A vulnerability analysis did show the existence of gaps in the current technology, especially with the usage of omnidirectional antennas [86]. This makes it vulnerable to jamming attacks since anyone in the scope of radio communication can send jamming signals to the victims [87]. Lyamin *et al.* [88] investigate the jamming DoS attacks in IEEE 802.11p that are possible when the exchanged beacons in a platoon are corrupted. The authors propose a simple real-time detector of jamming DoS; it is validated in terms of detection and false alarm probabilities for the proposed scenarios. Recently, the IEEE standard has replaced the IEEE 802.11p by the IEEE 802.11-OCB specification [58], where OCB stands for outside the context of a basic service set. It is worth noting that 802.11-OCB does not provide any cryptographic protection since it operates in OCB mode, where there is no need for Association Request/Response or Challenge messages. Consequently, attackers can eavesdrop and/or modify the traffic while within

TABLE 3. Cyber-incident against vehicular network.

	Automotive cyber incidents	References	Attack Surfaces	Attacks range	Attack methodologies
Intra-vehicle vulnerabilities	Exploiting the vulnerability of the CAN buses led to bus-off attacks.	Iehira *et al*. [72]	ECUs, CAN buses	Physical attack	Spoofing attacks, bus-off attacks against an ECU
	Hacking the CAN bus: manipulation of a modern automobile through CAN bus.	Currie, 2017, [75]	OBD-II port	Physical attack	Reverse engineering
	Practical security exploits of FlexRay.	Murvay *et al*. [77]	OBD-II port, FlexRay	Physical attack	Malicious frames injection
Vulnerabilities in wireless technologies	Hacking TESLA: use wireless communication to access CAN buses.	Nie *et al*. 2017, [80]	Wireless capabilities (Wi-Fi/Cellular)	Remote, Long-range attack	Internet attacks, unauthorized attack
	Remotely compromising the gateway, BCM, and autopilot ECU of TESLA cars.	Nie *et al*, 2017, [81]	Infotainment, Wi-Fi, ECU, CAN bus, Gateway,	Remote, Long and Short-range attack	Malicious Wi-Fi hotspot, code signing bypass, local privilege escalation
	Injecting malicious codes into Volkswagen mobile applications.	CVE-2018-1170, [82]	Mobile applications	Remote, Long-range	Malicious CAN bus massage injection
	Wirelessly attacking connected cars using security vulnerabilities of In-Vehicle CAN buses.	Woo *et al*. 2015, [73]	Cellular network, Mobile applications.	Remote, Long-range attack	CAN buses vulnerabilities, Malicious mobile applications
Software Vulnerabilities	Tesla cross-site scripting (XSS) vulnerability.	Sam Curry, 2019, [83]	Infotainment, servers	Physical, Short-range attack	Cross-site scripting (XSS)
	Discovering Buffer Overflow vulnerabilities in widely used vehicles telematics control modules.	CVE-2017-9647, [84]	Telematics control modules	Long range attacks	Buffer overflow
	Hacking Tesla car via its browser.	CVE-2019-9977, [85]	Infotainment	Physical, Short-range attacks	Vulnerability exploits

range of a vehicle or IP-RSU. Therefore, such a link is less protected than traditional 802.11 links [58].

b: CELLULAR NETWORKS

Cellular networks (e.g., LTE and LTE-A) are another mode of wireless communication used by vehicles to support long-range Internet connectivity. In fact, connecting the Internet to cellular networks is a major contributor to cellular network vulnerabilities. The cellular architecture at its core is based on Internet Protocol (IP) to support full interworking with heterogeneous radio access networks. However, this introduces more security threats by exposing the system in question to IP-based attacks, such as false information injection, eavesdropping attacks, spoofing, DDoS attacks, and others [20], [89]. Besides, due to the unpredictable and the ephemeral connectivity among nodes in VANET, management of (re)authentication and record of trust pose a serious challenge for cellular communication, putting the security and network performance at risk [20].

c: BLUETOOTH

Bluetooth is an open standard for short-range Radio Frequency (RF) communication that has been widely integrated into many industry segments including the automotive industry for media connectivity purposes. According to the National Institute of Standards and Technology (NIST) guide to Bluetooth security [90], Bluetooth is susceptible to several known attacks, such as DoS attacks, eavesdropping, and message modification. Security vulnerabilities of the latest version of Bluetooth technology include (for more details, we refer the reader to [90], [91]): (a) Authentication requests: there is no waiting interval for authentication challenge requests; this gives attackers the ability to collect a large number of challenge responses and break secret link keys; (b) keys: if secrete keys are not properly protected, attackers can easily read and modify them; (c) user authentication: in Bluetooth technology, devices, and not users, are authenticated; (d) end-to-end security: an intermediary can decrypt the transmitted data due to the absence of end-to-end encryption; (e) discoverability: vehicles need to be discoverable all the time; this makes them prone to several attacks; and (g) lack of audit and non-repudiation.

d: GLOBAL NAVIGATION SATELLITE SYSTEMS (GNSS)

GNSS is now an integral part of all aspects of our lives. It provides global coverage, accurate position, velocity, and timing information to support a wide range of critical applications. Due to the increasing dependence on GNSS, security vulnerabilities became a prime concern because of a growing record of interference incidents that need to be properly addressed [92], [93]. Generally, GNSS vulnerabilities can be classified into three categories: System-related vulnerabilities, propagation channel-related vulnerabilities, and interference (unintentional or intentional)

related vulnerabilities [94]. System-related vulnerabilities, propagation channel-related vulnerabilities, and unintentional interference-related vulnerabilities are out of the scope of the current study and may need a dedicated survey. Due to the low signal strength in GNSS, interference signals can be easily generated to intentionally block or mislead receivers into false positioning, incorrect timing, and wrong velocity. This falls into two distinct forms of intentional interference with GNSS signals: jamming and spoofing [94].

Jamming: The basic principle of GNSS signal jamming is to generate and transmit powerful noise signals toward the victim's receiver aiming to prevent legitimate signals from being distinguishable by the GNSS receiver. The objective is to disrupt the operations of GNSS. This could be done through the use of low-cost jammer devices that disrupt GNSS-based services in extended geographical areas. The availability of such illegal and low-cost devices is alarming, especially due to the serious damaging impact they may cause. Borio *et al.* [95] review the characteristics of jamming signals and their impact on GNSS receivers; they also present the state-of-the-art methods for jamming detection. Another study [96] provides an overview of various methods used to protect GNSS receivers from jamming and interference.

Spoofing: It is the act of broadcasting false signals which can appear to be genuine GNSS signals; the goal is to mislead the GNSS receiver into providing erroneous positions, velocities, and time information (see Figure 6). In comparison with jamming (that can be easily detected by receivers), a successful spoofing attack may have disastrous consequences, especially for emerging applications (e.g., autonomous vehicle navigation), because it is difficult to detect. In this context, a number of contributions have investigated spoofing attacks. To name a few, Psiaki and Humphreys [97] review the state of GNSS spoofing and provided a detailed description of spoofing attacks and the corresponding defense methods. The authors in [98] propose a novel scheme to detect and localize spoofing attacks on vehicular navigation GPS by correlating Doppler measurements from multiple vehicles connected with V2V communication. However, it only supports perfectly straight trajectory, which is not always the case. Similarly, authors in [99] have reported the lack of proper security measures applied to vehicular sensor networks. Hence, they propose a new approach to detect sensor spoofing attacks against automotive radars by effectively applying multiple beamforming in an automotive MIMO radar.

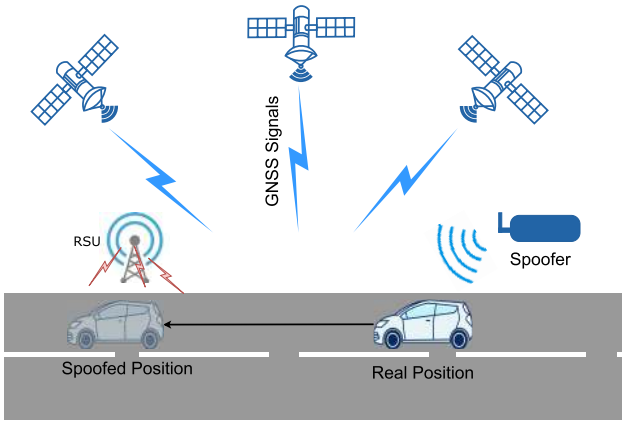

FIGURE 6. Illustration of a GNSS spoofing attack.

3) SOFTWARE VULNERABILITIES

To provide innovative features, most connected vehicle functions are controlled by software with over 100 million lines of code. However, softwares are never perfect. It is commonly assumed the existence of many vulnerabilities that can be exploited to cause unexpected behaviors using malware leading to life-threatening situations [100]. Software vulnerabilities are caused by software errors and flaws introduced during the design or implementation phases. The identification and categorization of security vulnerabilities have become one of the most active areas of software security research, where multiple vulnerability databases (lists) have been maintained; these include the CWE (Common Weakness Enumeration) list, the CVE (Common Vulnerabilities and Exposures) list, and NVD (National Vulnerability Database).

In VANET, several common software vulnerabilities exist, such as buffer overflow, code injection and weak access control or authentication (see the CWE and CVE lists) to name a few. Buffer Overflow or buffer overrun is always considered one of the most dangerous software coding errors. It is specified as CWE-120 under the CWE dictionary of weakness types. Typically, it occurs when a program overruns the buffer's boundary and overwrites adjacent memory locations while writing data into a memory buffer. By the exploiting this vulnerability, it becomes easy to inject malicious code into a program to gain illegitimate access to the targeted system. In 2017, a stack-based buffer overflow issue was discovered by Shkatov *et al.* [84] in several vehicles, including BMW and INFINITI. These vehicles had telematics control modules (TCUs) which are built by Continental AG; they contain the S-Gold 2 (PMB 8876). The exploitation of this vulnerability allows the attacker to disable the infotainment system and affect the functional features of the vehicle.

There are advanced types of injection vulnerabilities. SQL injection (SQLi) and Cross-site Scripting (XSS) are common injection vulnerabilities used to insert untrusted input due to the lack of sufficient query validation process in legitimate user infotainment systems [101]. Li *et al.* [102] report that traditional detection methods have many limitations and cannot deal with the increasingly complex injection attacks in ITS. They propose an SQL injection attack detection method which can automatically learn the effective representation of data. In 2019, the white hat hacker, Sam Curry, discovered a stored cross-site scripting (XSS) vulnerability in the software of his Tesla Model 3; the exploitation of this vulnerability allows the attacker to obtain vehicle private information [83]. In advanced attacks, attackers may exploit additional privilege escalation vulnerabilities combined with weak access control or authentication to gain an extended control of all

TABLE 4. Classification of Security Issues in ITS.

Attacks	Type of attacker		Attacks on security objectives	Target of attacks	Purpose behind attacks
	active	passive			
D-Dos attacks [103]–[106]	✓	x	Availability	Wireless channels, hardware and software, backend servers	• Disrupt network availability • Drop vehicular traffic • Exhaust network resources • Take down vehicular services and applications
Black hole attacks [107]–[110]	✓	x	Availability, Integrity	Wireless channels, routing protocols	• Direct routing paths through malicious nodes • Selectively or fully drop incoming packets
Malware attacks [100], [111], [112]	✓	x	Availably, Confidentiality	Software and hardware, wireless channels, vehicular services	• Remotely control vehicles • Steal sensitive information • Disrupt regular functioning of vehicles • Use vehicles as zombies to perform other attacks
Sybil attacks [113]–[118]	✓	x	Authentication, Availability	Software, wireless channels, routing protocols	• Pretend convincingly having multiple identities • Create deep illusion of trust to trap vehicles • Mislead vehicles and change their own paths • Launch DDoS attacks by exploiting multiple Sybil nodes
Wormhole attacks [119]–[121]	✓	✓	Availability, Confidentiality	Wireless channels, routing protocols	• Modify the logical topology of the network • Prevent nodes from discovering other paths • Route all traffic through the malicious nodes
Passive Attacks [122]–[124]	x	✓	Confidentiality	Wireless channels, software and hardware, In-vehicle components	• Eavesdrop on network communication to capture legitimate packets • Gain access to sensitive information • Prepare for more sophisticated attacks
Replay attack [107], [125]	✓	x	Authentication, Confidentiality, Integrity	Wireless channels, intra-vehicular systems	• Store packets and retransmit them later • Impersonate a legitimate Vehicle/RSU • Inject bogus information
Bush Telegraph attacks [25]	✓	x	Availability, Integrity	Wireless channels, software and hardware	• Accumulate enough errors (i.e., bogus information) to drop vehicular traffic
Timing attacks [126]–[128]	✓	x	Availability, Integrity	Wireless channels, software and hardware	• Add intentionally some timeslots to the original message to impact information freshness • Flood or jam the communication channels to increase packet delays and losses

network resources which are protected from normal application users. Given the large amount of code installed in today's vehicles, it is extremely difficult and expensive to test and verify such codes. Thus, securing the various heterogeneous software platforms is a challenging task.

D. SECURITY ATTACKS ON ITS

Although there are significant technological improvements, ITS are still vulnerable to various security attacks (see Table 4). We observe that the risks presented by cyberattacks against ITS can be extremely dangerous; indeed, they could threaten both the safety and privacy of all road-users. In the following, we describe major attacks that can target ITS.

1) ATTACKS ON AVAILABILITY

Attacks targeting availability may cause a temporary outage in an attempt to prevent access to any kind of network resources. This can cause serious damage due to the real-time nature of several applications of ITS.

a: DENIAL OF SERVICE (DoS) ATTACKS

DoS attacks are one of the most typical cyber-attacks in communication networks. They have been extensively used to disrupt network availability. They occur when an attacker tries to flood a legitimate user (e.g., a vehicle) with a large amount of illegitimate traffic in an attempt to overload the victim. This may cause congestion resulting in legitimate traffic being dropped [103]. Launching a DOS attack by a single attacker is computationally expensive to execute. Thus, attackers resort to Distributed DoS (DDoS) attacks to overwhelm the target's resources, such as network bandwidth and processing power, with illegitimate traffic [104]. To launch DDoS attacks, the attacker (e.g., bot-master) generally needs to control a large number of compromised devices

(called zombies). Each zombie sends a huge volume of illegitimate traffic to deny services to legitimate users of the target (e.g., vehicle or RSU).

DoS and DDoS attacks can cause serious harm to the network. Several efforts toward the mitigation and the prevention of such attacks have been carried out. In [105], Liu *et al.* report the shortcomings of the classic pseudonymous authentication schemes subject to severe DoS attacks; they propose a puzzle-based co-authentication (PCA) scheme to mitigate these attacks. The key idea behind the proposed solution is to increase the publishing cost of certificates and to design a collaborative verification of legitimate vehicles. This restricts the attacker's capability to release forged pseudonymous certificates and improves the efficiency of certificate verification. The authors did show, via simulations, the effectiveness of their method in mitigating DoS attacks. In order to prevent most of the automated DDoS attacks, Poongodi *et al.* [106] propose a reCAPTCHA controller mechanism to filter the attack traffic by using the source side integrity checks. According to the authors, this solution has practically proved its high performance compared with existing systems and its ability to minimize the generated overhead in terms of latency and energy consumption.

b: BLACK HOLE ATTACKS

Black hole attacks are among the common attacks against vehicular networks that have serious implications on network performance [107]. In such attacks, the attacker works his way to become a part of the network and thus be able to exchange messages with other nodes. Then, he/she could exploit existing vulnerabilities in routing protocols, such as Ad hoc On-Demand Distance Vector (AODV) [108], to broadcast bogus routing information to its neighboring nodes. A research analysis conducted by Afdhal *et al.* [109] investigate the impact of the black hole attacks on the performance of AODV and AOMDV (Ad hoc On-demand Multipath Distance Vector) routing protocols in VANET. The goal of the attacker is to convince neighboring nodes that they are on the shortest path in order to increase the likelihood of its route being chosen. Once the attacker starts receiving data, it may selectively drop incoming packets evading detection; this is known as a gray hole attack. A black hole attack happens when the attacker drops all incoming packets. The detection of black hole attacks is a complex task since the attacker can drop packets periodically. The isolation of malicious nodes is more challenging, particularly in VANET. Tobin *et al.* [110] develop a countermeasure for black hole attacks in VANET. The proposed solution focus on multiple steps consisting of (a) attack detection through route backtracking and detecting discrepancies; (b) node accusation; and (c) blacklisting malicious nodes from participating in the network. However, the proposed solution can only detect one single malicious node and the solution requirements cannot be always satisfied.

c: MALWARE ATTACK

For the implementation of communication protocols, hardware drivers, as well as user applications, modern vehicular software could have more than 100 million lines of code exposed to all kinds of software vulnerabilities [100]. This gives opportunities for attackers to design effective malware to gain unauthorized access and disrupt the regular functioning of vehicles. Malware is a general term that refers to all types of malicious software (e.g., spyware, adware, worms, virus, and trojan) that can easily infect a huge number of vehicles. Malware attacks originate from computer networks, but they have been found in almost every existing data-enabled network including VANET. The attacker may have physical access to the vehicle, thus, the ability to install malware through the OBD-II port or via the in-vehicle infotainment system. Also, the attacker may exploit the vehicle's telematics system to deliver malware that allows him remote access (e.g., via 4G LTE or Bluetooth) to install malware. The characterization of malwares used against VANET are investigated in [100], [111]. It is worth to mention that malware can self-replicate and spread rapidly in VANET, which is the case of worms. Zhang and Boukerche [112] examine the characteristics of spreading worms in VANET. They propose a countermeasure-based Malicious Vehicle Screening Unit (MSVU); it serves as a particular type of RSUs to sniff the malicious behavior, broadcast and blacklist immunization. According to the simulation results, the proposed method outperforms other existing methods in terms of complexity and quality.

2) ATTACKS ON AUTHENTICITY

Attacks targeting authenticity allow illegitimate users to gain unauthorized access to private information through stealing or falsifying the identity of legitimate network members.

a: SYBIL ATTACK

Sybil attacks are among the hardest attacks to detect in VANET. Douseur [113] defines a Sybil attack as an identity-based attack. Due to the distributed characteristics of VANET [114], an attacker could create several pseudonymous fake identities (e.g., by stealing or falsifying the identities of legitimate nodes (Sybil nodes) [115]) and pretend convincingly having different identities. The main objective of this attack is to gain greater influence on the network by creating a deep illusion of trust to trap other vehicles (see Figure 7) [116]. For instance, an attacker can exploit the number of fake identities to report the existence of a severe traffic jam at certain locations; this would mislead vehicles to change their own paths to avoid the congested area [117]. Moreover, Sybil attacks can be used to launch DDoS attacks by exploiting multiple Sybil nodes to flood the target with massive illegitimate traffic to paralyze the whole system functionalities. According to Baza *et al.* [118], several solutions to detect Sybil attacks have failed since they suffer from technical limitations. For example, (a) identity

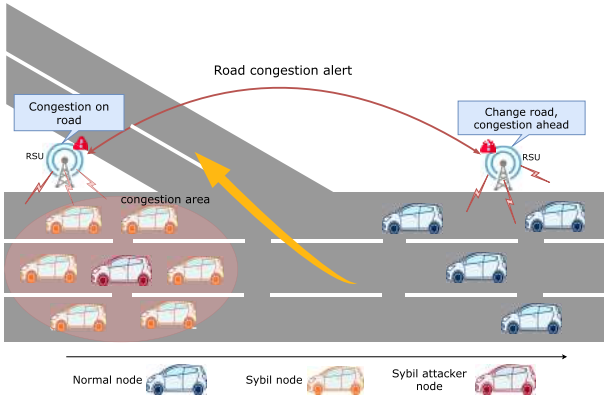

FIGURE 7. Sybil attack in VANET.

registration based techniques [129], [130] fail when the attacker pretends multiple identities; (b) position verification-based schemes [131] fail because of the high mobility of vehicles; (c) trajectory-based schemes [132] fail when the attacker succeeds in compromising an RSUs and thus can get a large number of valid trajectories. In this context, the authors in [118] propose a novel detection technique, using proof of work and location in VANET, which shows a high level of performance with acceptable overhead.

b: WORMHOLE ATTACKS

Wormhole attacks can severely affect routing protocols without being detected since the attacker can function as a legitimate node [119]. Such attacks typically require at least two colluding nodes, geographically separated, to create a tunnel (wormhole link) to forward packets among each other for end-to-end communication [120], [121]. Figure 8 shows that the malicious nodes involve themselves in many routes pretending to have the shortest path to any destination due to the smaller number of hops or minimum end-to-end delays. The goal of this type of attacks is to modify the logical topology of the network to prevent nodes from discovering other paths and route all traffic through the malicious nodes; this puts the attackers in a position to control and manipulate

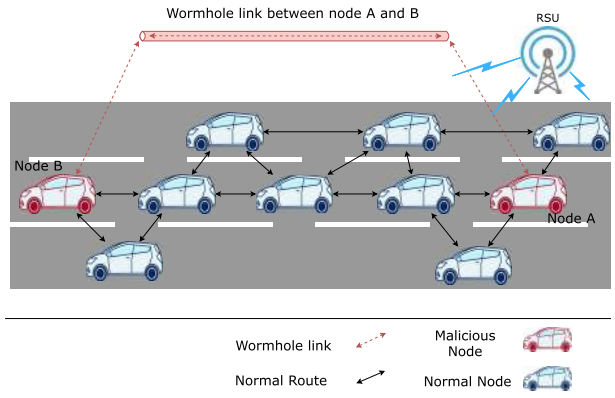

FIGURE 8. Wormhole Attack in VANET.

network traffic. Albouq and Fredericks [119] report that the severity of wormhole attacks can be maximized if attackers resort to cooperative wormhole attacks where several attackers cooperate. In classical attacks, an attacker may not be able to establish the wormhole link to cover long-range communications. Cooperative wormhole attacks serve not only to extend the range of the established links between attackers, but also to confuse existing detection techniques that rely on time analysis. To counter these attacks, the authors in [119] propose a lightweight protocol for detecting and mitigating wormhole attacks in VANET.

3) ATTACKS ON CONFIDENTIALITY

Attacks targeting confidentiality aim to disclose network sensitive's information to an unauthorized party. Due to the message broadcast characteristic in VANET, data exchanges could be easily compromised. Passive attacks (AKA Eavesdropping, sniffing, or snooping attacks) do not disrupt the operation of the network; they passively target weakened and unsecured connections to cause privacy leakage. The basic idea is to maliciously intercept relevant traffic in order to gain access to sensitive information such as credentials, personal location, or node configuration. Based on the extracted information, the attacker may continuously capture and analyze broadcast messages to track nodes based on their physical positions [122]–[124]. The impact of passive attacks could be very high since it could be used as a preliminary stage to perform more sophisticated and destructive attacks (e.g., DoS, blackhole, wormhole, and impersonation attacks) that require prior knowledge of the targeted system. Therefore, it is of great importance to secure communications and guarantee network confidentiality.

4) ATTACKS ON INTEGRITY

Attacks targeting integrity aim to alter or manipulate exchanged messages between different network members.

a: REPLAY ATTACKS

This type of attacks presents a serious breach of authenticity, confidentiality, and integrity. Replay attacks have a close association to the man in the middle attacks, where attackers eavesdrop on network communication to capture legitimate packets on their way to the destination (usually between vehicles and RSUs). Thus, the attacker can store packets and retransmit them later even when they are no longer valid. Furthermore, the attacker could exploit the information gathered from intercepted packets, including login credentials, to impersonate a legitimate Vehicle/RSU and deceive other nodes into believing the attacker is, in fact, an authenticated user [125]. It is very difficult to detect replay attacks since, in most cases, attackers are highly mobile and do not operate abnormally by altering packets. In this context, only the implementation of robust encryption methods and the inclusion of timestamps restrict the likelihood of these attacks.

b: TIMING ATTACKS

Several ITS applications require real-time traffic transmission; thus, there are major concerns on attacks that may impact the time synchronization, transmission delays, and packets losses [126]. Timing attacks target communication timing to cause serious safety problems, especially in dense traffic. Performing timing attacks can be done by flooding or jamming the communication channels to increase packet delays and losses. In [126], Zheng *et al.* have demonstrated how timing attacks could seriously impair the effectiveness of delay-sensitive applications in VANET. They propose a delay-tolerant intersection management protocol that considers the impact of communication delays in single and multiple interconnected intersections for intelligent intersection management systems. Timing attacks can be performed by an attacker who intentionally adds some extra timeslots to forwarded messages aiming to impact information freshness [127]. Another study conducted by Arsalan and Rehman [128] discusses thoroughly timing attacks in VANET. They propose a scheme, called Timing Attack Prevention (TAP), to detect and mitigate this type of attacks. The proposed scheme eliminates the risks of delayed and duplicated emergency packets by controlling the broadcasted messages. This is done through the use of Software Defined Network (SDN) controllers and Named Data Networking (NDN) communication paradigm in VANET.

c: BUSH TELEGRAPH ATTACKS

This type of attacks is an advanced version of bogus information attacks. The attacker attempts to gain access to a large number of nodes spread over several wireless hops. Then, he/she appends incremental errors to the packets at each hop. Thus, after passing several hops, the packet accumulates enough errors (i.e., bogus information) to be dropped [25]. This happens because, upon receipt of the packet, a node checks whether the corresponding error is small; if the response is yes, it forwards the packet; otherwise, it drops it.

E. LESSONS LEARNED FROM THE CURRENT SECURITY LANDSCAPE OF ITS

The driving motivation behind this chapter is to answer the following two questions 1) what are the current security issues of modern ITS, and 2) what are the root causes of these security issues. In our attempt to answer these questions, we explored and analyzed existing relevant literature to provide an overall picture of the ITS security landscape. The current architectural design of automotive systems has shown to be vulnerable due to the increasing number of new services and capabilities integrated into modern vehicles. Indeed, this results in introducing additional fraud risks and data-breach incidents, threatening the safety of road users. Based on our analysis, we believe that the enforcement of appropriate security requirements is needed and challenging at the same time. Even with the availability of conventional security mechanisms, there is a lack of proper mechanisms that consider the current security threats while taking into account the stringent requirements of ITS. We also believe that the analysis, presented in this article, is much needed since it helps determine what type of solutions can be used to minimize the likelihood of successful attacks targeting the security of ITS.

IV. EXISTING MITIGATION TECHNIQUES AGAINST ATTACKS IN ITS

Mitigating techniques can be classified into two categories: Proactive and reactive approaches. Typically, in ITS, it is crucial to implement proactive cybersecurity strategies in order to enforce security policies. This category consists of defining a baseline level of cybersecurity, which is considered as a preventative measure to deal with potential threats. This includes mechanisms, such as integrity and authenticity checks (e.g., verifying digital signatures and certificates) and access control mechanisms. However, since it is impossible to predict all possible threats and dificult to counter internal attacks, reactive approaches must be deployed to react to attacks when proactive measures are not effective. In this context, intrusion and misbehavior detection systems are widely deployed in mitigating the impacts of attacks and restricting their propagation [24], [25]. To provide the reader with a comprehensive review of existing defense mechanisms against attacks in VANET, it is crucial to systematically review these solutions and analyze them thoroughly. In this section, we briefly introduce recent security mechanisms which can be used to mitigate the risk of cyberattacks we did address in section III.

A. AUTHENTICATION BASED SECURITY SCHEMES

Due to the diversity of security attacks (e.g., replay, injection and eavesdropping attacks), safety messages must be authenticated. In this regard, cryptographic algorithms are considered as the backbone of security and privacy protection for ITS applications; this allows to ensure the legitimacy of exchanged messages with functions of auditability in case of misbehaving. Most existing schemes in VANET are developed to guarantee authentication and integrity with privacy and anonymity preservation. These schemes can be divided into four classes: Public Key-based Authentication (PKA) schemes, Identity-based Authentication (IBA) schemes, Group Signature-based Authentication (GSA) schemes, and Symmetric Key based Authentication (SKA) schemes [26], [133]. In this subsection, we walk through the most recent contributions that use cryptography to improve security in VANET. More specifically, we describe existing schemes and identify their limitations. Table 5 summarizes the list of security mechanisms we cover in this subsection.

1) PUBLIC KEY-BASED AUTHENTICATION (PKA) SCHEMES

In particular, public key-based cryptographic schemes have been employed pervasively to achieve reliable node authentication for pseudonymous vehicular communication [26].

TABLE 5. Authentication based security schemes for VANET.

	Security solutions	Effort year	Technique	Performance metrics	Main mitigated attacks	Shortcoming
Public Key-based Authentication (PKA) schemes	Azees *et al.* [9]	2017	• The use of bilinear pairing to offer message authentication and privacy preservation for VANET. • Provide an efficient conditional privacy tracking mechanism in case of dispute.	Fast verification of certificates and signatures	Bogus message, impersonation and modification attacks	High computational overhead due to the bilinear pairing operations.
	Dua *et al.* [10]	2018	• The use of the concept of clustering in VANET to design two levels of authentication: selected and authenticated cluster heads will be responsible for authentication of vehicles in the second level authentication.	Better storage, communication and computation costs	Man-in-middle, replay, modification and brute force attacks	The number of verification steps is not scalable in the case of high-density networks
	Islam *et al.* [134]	2018	• The implementation of Password-based Conditional Privacy Preserving Authentication and Group-Key Generation (PW-CPPA-GKA) scheme for VANET.	Short execution time of message authentication (generation and verification phase)	Replay, impersonation, modification and off-line password guessing attacks	Lack of simulation results in specific scenarios
	Huang *et al.* [14]	2020	• The exploitation of the 5G technology to introduce a new scheme that makes use of elliptic-curve public-key cryptography and Registration List (RL) to secure VANET.	lower average message delay and average packet loss ratio even in dense scenarios	DoS, eavesdropping and message modification attacks	Assumption of reliable wireless networks and access points
Identity-based Authentication (IBA) schemes	Tangade *et al.* [135]	2018	• The use of asymmetric ID-based cryptography and the symmetric HMAC to implement a Decentralized Privacy Preserving Authentication (DSPA) scheme.	Lower communication and computation overheads	Impersonation, modification, identity-disclosure and sybil attacks	infeasibility against man-in-the-middle replay and plain-text attacks
	Zhang *et al.* [136]	2017	• Implementation of Cryptographic Mix-Zones (CMIX) using One-time Identity-Based Authenticated Asymmetric Group Key Agreement (OTIBAAGK).	Efficient key update and certificate management	Eavesdropping	Limited protection against attacks other than eavesdropping
	Asaar *et al.* [137]	2018	• The implementation of identity-based message authentication with privacy preservation scheme using proxy vehicles (ID-MAP).	Lower average message delay and average packet loss ratio.	Impersonation, replay modification, and man-in-middle attacks	Master keys might be compromised since they are stored in every vehicle
Group Signature based Authentication (GSA) schemes	Yue *et al.* in [138]	2018	• The implementation of a new decentralized authentication scheme for VANET based on the framework of group signatures. • Ensure more advanced security requirements like forward security, CCA2-anonymous, non-frameablility, unforgeability and traceability.	Efficient verification and revocation feature	Forgery and untraceable signature, ID disclosure, revoked key exposure and framing attacks	Vulnerable to Denial of Service (DoS) attacks when false data is injected.
	Zhang *et al.* [139]	2019	• The adoption of batch group signature verification and Group Session Key (GSK)-based revocation strategy for efficient message authentication protocol for VANET.	Lower computation cost, authentication delay and message loss rate	Impersonation, tracking, sybil, replay and DoS attacks	Unable to guarantee the integrity of the sender's message content
	Jiang *et al.* [140]	2020	• The adoption of a pseudonym mechanism and identity based group signature for anonymous authentication. • Involve the RTA for extra computational efficiency.	Acceptable storage, communication and computation costs	Tracking attacks, eavesdropping, ID disclosure and sybil attacks	Only supports vehicle-to-infrastructure communications
Symmetric key based Authentication (SKA) schemes	Jiang *et al.* [11]	2016	• The use of HMAC to substitute the utilization of time-consuming CRL for a lightweight anonymous batch authentication scheme. • The use of IBS for privacy preserving.	Better efficiency, Lower computational overhead and verification delay	Modification, replay, injection, Impersonation and colluding attacks	Heavily relies on the security of trusted authorities.
	Benyamina *et al* [141]	2019	• The implementation of MAC-based authentication technique to ensure lightweight message authentication, privacy-preservation and non-repudiation.	Lower delay, computation and communication overhead	Location tracking, impersonation, compromise RSUs and stolen OBUs attacks	The lack of strong cryptographic operations to protect the privacy of the exchanged information

The initial stage of communication involves the registration process of the vehicles to authenticate themselves to a trusted authority and obtain a set of public key certificates and corresponding public/private key pairs. Therefore, a vehicle signs outgoing packets with its private key and attaches the resulting signature and corresponding certificate to the message. It requires the sending vehicle to have a valid public key certificate to be authenticated properly by receivers [18]. To support the management of public keys, the European Telecommunications Standards Institute (ETSI) and the National Highway Traffic Safety Administration (NHTSA) have defined a Vehicular Public Key Infrastructure (VPKI) where only legitimately registered nodes within the domain are able to communicate securely [142].

Azees *et al.* [9] propose an efficient anonymous authentication scheme with conditional privacy preserving (EAAP) for VANET. EAAP supports efficient authentication for vehicles and RSUs while preserving their anonymity; it allows preventing attacks like impersonation and masquerading. EAAP outperforms several schemes, such as BLS [143], ECPP [144], CAS [145], GSB [146], and KPSD [147], in terms of the verification process of certificates and signatures. Moreover, it provides conditional tracking capability which allows trusted authorities to trace the identity of vehicles in case they misbehave. However, EAAP is costly in terms of computational overhead due to the bilinear pairing operation. It also suffers from the limitations caused by the centralized authentication design which relies on the security of the trusted authority. Islam *et al.* [134] report that the use of either elliptic curve or bilinear-pairing causes a heavy computational burden making them infeasible for VANET. Thus, to overcome this issue, they introduce a password-based conditional privacy preserving authentication and group-key generation (PW-CPPA-GKA) scheme for VANET. The usage of this scheme allows vehicles to join or leave a regional group of nodes and also facilitates password updates. In terms of communication overhead and latency, PW-CPPA-GKA outperforms other existing schemes [148]–[150]. However, the authors [134] did not simulate the proposed scheme in realistic scenarios (e.g., urban or highway scenarios) that consider traffic density, speed of moving vehicles, or some other metrics. Huang *et al.* [14] investigate the possibility of exploiting the potential of the 5G technology in supporting higher data rates with larger numbers of connected devices to overcome the issues of public-key cryptography. The authors propose a novel scheme that makes uses of elliptic-curve public-key cryptography and a registration list (RL) to secure VANET. This approach only requires two light-weighted hash operations to be effective against attacks like eavesdropping, message modification, and DoS attacks. The simulation results show that the scheme achieves negligible authentication delay even in high vehicle density scenarios. However, it relies on a non-realistic assumption of reliable wireless networks and access points. Similarly, Dua *et al.* [10] propose a novel scheme to ensure secure message communication among vehicles using two-level authentication key exchange. In the first authentication level, a Cluster Head (CH) is selected among a group of vehicles in a cluster by a trusted certification authority. In the second level, the selected CHs are responsible for the authentication of vehicles within their clusters. Simulation results show that the scheme [10] is efficient in terms of computational cost and response time; this is explained by the fact that it is implemented using Elliptic Curve Cryptographic (ECC) technique. However, the number of verification steps executed by the certificate authority is not scalable in the case of high-density networks.

2) IDENTITY-BASED AUTHENTICATION (IBA) SCHEMES

Identity-based Authentication (IBA) schemes extend the idea of PKA-based schemes. In IBA, the receiver can exploit the explicit identity, included in the message, to derive the public key of the sender. Thus, compared with PKA, IBA eliminates the requirement of certificates since the sender's identifier is sufficient to verify messages [26]. Consequently, IBA eliminates the overhead caused by including certificates in the exchanged messages [151].

Tangade *et al.* [135] propose a Decentralized and Scalable Privacy Preserving Authentication (DSPA) scheme that enjoys the benefits of both asymmetric Identity-Based (ID-based) authentication and the Symmetric Hash Message Authentication Code (HMAC). Indeed, DSPA allows reducing communication and computation overheads. However, it is not suitable for direct V2V communication because of the large number of messages that should be exchanged between nodes and RSUs/base stations [152]. Furthermore, DSPA is not effective against passive attacks such as man-in-the-middle and replay plain-text attacks [152]. Since other well-known approaches (e.g., digital signatures combined with pseudonymous [153], [154] and group signatures [155], [156]) are insufficient to stand against attacks that target vehicles privacy (e.g. location tracking), Zhang [136] address the problem of location privacy; they propose a new method that relies on the One-Time Identity-Based Authenticated Asymmetric Group Key Agreement (OTIBAAGKA) to establish Cryptographic mix-zones (CMIXs). Unlike previous related contributions [157], [158], OTIBAAGKA allows vehicles to update their pseudonyms while sending vehicular safety messages. Since none can trust RSUs, OTIBAAGKA makes use of semi-trusted RSUs which cannot decrypt messages broadcasted by the vehicles in CMIXs. However, this scheme can only protect VANET from passive attacks like eavesdropping and location tracking. Asaar *et al.* [137] propose a novel identity-based message authentication with a privacy preservation scheme using proxy vehicles (ID-MAP). ID-MAP is based on an earlier contribution by Liu *et al.* [159] which examines the benefits of proxy vehicles in reducing the centralized computational overhead of RSUs through simultaneous verification of signatures. More specifically, ID-MAP extends the scheme in [159] to satisfy the security and privacy requirements of VANET as well as the traceability of misbehaving vehicles. However, the master keys are

stored in every vehicle which might increase the risk of key lackage.

3) GROUP SIGNATURE BASED AUTHENTICATION (GSA) SCHEMES

Group signature based Authentication (GSA) schemes introduce a group-wide public key such that any vehicle within a specific group can sign messages on behalf of the group. However, it is infeasible for anyone except for the group manager to reveal the signer's identity. In addition to the effective and anonymous vehicle's authentication, the implementation of GSA extends security requirements to cover more services for vehicular networks, including accountability, unlinkability, and unforgeability [160]. Once a vehicle is found to be malicious, only a designated group manager who operates as a semi-trusted entity can link the signature to the identity of the signer after deciding to revoke the malicious member.

The tradeoff between privacy preservation and conditional anonymity has led Yue *et al.* [138] to propose a new authentication scheme based on the framework of group signatures. The proposed scheme offers a decentralized management model to offload the heavy burden of generating group certificates for vehicles and avoid the cost of creating and updating revocation lists. The scheme can guarantee more advanced security requirements (e.g., forward security, CCA2-anonymous, non-frameablility, unforgeability, and traceability) which cannot be completely satisfied in existing schemes. However, the proposed scheme is found to be vulnerable to Denial of Service (DoS) attacks when false data is injected. Similarly, Jiang *et al.* [140] propose an Anonymous Authentication scheme based on group signature (AAAS). AAAS allows a good level of performance since it adopts a pseudonym mechanism and identity based group signature to eliminate the overhead generated by the management of public key certificates. It makes use of Region Trust Authority (RTA) as a group manager to reduce the computation and communication costs of the central trusted authority and also to relieve the pressure on RSUs. However, this scheme is limited in scope since it only supports vehicle-to-infrastructure communications. Zhang *et al.* [139] introduce a novel scheme that adopts (a) batch group signature verification to minimize the computational cost of signatures verification; and (b) Group Session Key (GSK)-based revocation strategy to quickly check whether the message sender has been revoked or not. The scheme is effective against several attacks (e.g., impersonation attacks, tracking attacks, Sybil attacks, replay attacks, and DoS attacks) with an acceptable level of performance in terms of computation, authentication delay, and message loss rate. However, this scheme is unable to guarantee the integrity of the sender's message content; thus, vehicles could not verify the legitimacy of responses from RSUs.

4) SYMMETRIC KEY BASED AUTHENTICATION (SKA) SCHEMES

It is widely known that symmetric cryptography can provide high computational efficiency and reduce communication overhead because of the utilization of one single key for both the signing and verification processes [26]. However, for reliable node authentication, the secret keys should not be compromised during transportation. Thus, it is essential to establish secure channels to safely exchange keys between vehicles and RSUs. In symmetric cryptographic schemes, a Hash Message Authentication Code (HMAC) is used for lightweight message authentication. Since the utilization of symmetric cryptography alone is questionable, several authentication schemes have combined the use of HMAC with other cryptographic techniques to achieve better performance.

Jiang *et al.* [11] address the problem caused by the Certificate Revocation List (CRL) (e.g., communication overhead and lack of privacy). They propose a lightweight Anonymous Batch Authentication scheme (ABAH) that relies on calculating the Hash Message Authentication Code (HMAC). ABAH makes use of identity-based signature (IBS) to achieve privacy-preserving and realize batch authentication. Simulation results show that ABAH achieves significant improvement in terms of communication and computational overhead. However, the average transmission delay provided by ABAH is not good enough to outperform other schemes like IBV [161]. Similarly, Benyamina *et al.* [141] propose a novel efficient and lightweight authentication scheme (ANEL) that enjoys the benefits of the MAC-based authentication, which is much more efficient in terms of computational overhead. ANEL uses biological password authentication, system key updates, and biological password updates. It is resistant to location tracking, impersonation, RSU compromise, and stolen OBU attacks to prevent the disclosure of any sensitive information. Simulation results show that ANEL ensures fast and reliable authentication suitable for VANET.

5) AUTHENTICATION CHALLENGES IN VANET

According to the DSRC and IEEE 1609.2 standards, vehicles are required to satisfy real-time transmission of periodic safety messages in order to realize ITS services. However, due to the diversity of security attacks (e.g., replay, injection, and eavesdropping attacks), safety messages must be authenticated. The implementation of robust authentication schemes may impose a heavy burden on participating entities resulting in violating the requirements of delay-sensitive applications. In [162], the authors investigate the sources of overhead caused by security mechanisms. They show that the overhead may lead to serious performance degradation. Therefore, vehicles have to be equipped with tailored authentication schemes that satisfy the strict requirements of VANET. Indeed, all existing schemes aim to make a tradeoff between vigorous authentication and computational/communication overhead. However, there are still significant research challenges because of the nature of pseudonym approaches and underlying cryptographic primitives that are used. For instance, SKA schemes have demonstrated high computational efficiency with minimum overhead. However, they present some limitations related to the key distribution problem and the key management problem; this in addition to the

inability to support non-repudiation services, which makes them not suitable for sensitive communication in VANET. In contrast, PKA schemes support well the security requirements of VANET; however, they cause large storage and communication overhead because of the certificate management. IBA schemes allow reducing the overhead (since no certificates are attached); however, they fully rely on the security of trusted authorities (as PKA schemes do), which cannot always be guaranteed. GSA schemes enable vehicles within the group to produce signatures without revealing their identities; however, they cause considerable computation overhead during the verification of signatures [18], [26], [163].

The pseudonyms in all these schemes (except GSA) are static in nature and need to be changed frequently to avoid the linkage among different communications [164]. This may result in sending messages with inconsistent sets of identifiers making the receiver unable to verify signatures and thus, increasing packet losses [26]. Revocation is another key challenge to maintain reliable communication. Since the Certificate Revocation Lists (CRL) can be extremely massive due to the unpredictable scale of VANET, the distribution and checking process of CRL makes the authentication not practical, especially in dense traffic scenarios.

B. MACHINE LEARNING BASED SECURITY MECHANISMS

With the explosive growth in the size and the complexity of VANET, it becomes increasingly challenging to manage such networks. Therefore, the necessity to migrate towards more sophisticated solutions that promote autonomy for analysis and decision making using Artificial Intelligence (AI) [165]–[167]. Machine learning (ML), as a subset of AI, is playing a leading role in the creation of next-generation systems due to the recent success in supporting a wide variety of applications and industries [168]. By applying ML approaches in ITS, significant improvement can be achieved by making defense strategies (e.g., intrusion detection, software, and malware detection) smarter, adaptive, and highly efficient. In this section, we review security schemes in ITS that use machine learning and, in particular, deep learning methods that effectively prevent and mitigate the impact of cyber-attacks. Table 6 summarizes the list of security mechanisms we cover in this subsection.

1) MACHINE LEARNING TECHNIQUES FOR INTRUSION DETECTION IN ITS

The proliferation of embedded devices and wireless technologies in today's vehicular communications has increased the risk of being exposed to cyber-attacks. Thus, detecting and isolating anomalies are crucial tasks. In ITS, the implementation of proactive security countermeasures such as cryptographic-based solutions might not be reliable due to their inherent characteristics and the highly generated overhead. In this context, considerable attention has been paid to Intrusion Detection Systems (IDSs) to detect possible cyber-attacks. By investigating incoming and outgoing traffic from a specific location, an IDS can provide adequate protection against any suspicious activities manifested by malicious users [25]. One common usage of ML is designing effective IDSs. By considering classification algorithms of supervised learning, clustering algorithms of unsupervised learning, and reinforcement learning, different classes of detection strategies have shown a respectable performance in detecting a wide range of attacks and anomalies in networks.

a: SUPERVISED ML-BASED IDS

Signature-based IDS consists of matching an observed activity with a predefined set of rules (signatures) and patterns characterizing a well-known threat. With the use of this detection strategy, the system can accurately identify known attacks without exhausting the computational resources of the network. Supervised ML based schemes represent good candidates to outperform signature-based IDS algorithms since both rely on classification and knowledge databases [176]. Hence, making predicting outcomes for unforeseen data becomes effective and more accurate. In the literature, there are numerous contributions (e.g., [12], [169]–[172]) that have investigated the use of supervised ML algorithms along with signature-based IDS to examine their applicability in enhancing security in VANET.

Song *et al.* [12] study the feasibility of supervised ML in designing an IDS to protect the in-vehicle network (i.e., CAN bus). The proposed model uses a Deep Convolutional Neural Network (DCNN) architecture, called Inception-ResNet [177], due to its superior performance in natural image classification tasks. The authors build a new DCNN model optimized for data traffic in CAN bus that provides better detection and latency performance. Simulation results show that the proposed model outperforms existing machine learning models, such as Support Vector Machine (SVM), K-Nearest Neighbors, and Decision Trees in terms of detection accuracy, training cost, and latency. However, the model [12] is unable to detect unlearned types of attacks. Unlike the previous work [12] that address the security of in-vehicle network, Eziama *et al.* [169] report that existing categories of trust management models (e.g., entity centric trust and data centric trust) are not always successful in capturing the behavior of malicious nodes especially in highly dynamic networks like VANET. Thus, they propose a new trust model based on machine/deep learning; more specifically, they modeled trust as a classification process and employed the Bayesian Neural Network (BNN) to extract relevant features from the network with higher performance prediction, classification accuracy, and low detection latency. Gyawali *et al.* [171] report that proactive security measures like cryptographic methods are vulnerable to internal attacks (e.g., false alert generation and position falsification attacks), which are carried out by authenticated vehicles. To counter these attacks, the authors propose a decentralized misbehavior detection system for 5G vehicular networks. The proposed system makes use of (a) a hybrid collaborative ML scheme that uses K-Nearest Neighbor, Logistic Regression, Decision Tree, and Random Forest; the objective is to detect

TABLE 6. Machine learning defense techniques for vehicular networks.

	Security solutions	Effort year	Technique	Performance metrics	Main mitigated attacks	Shortcoming
Supervised learning	Song *et al.* [12]	2019	• The adoption of a recent deep convolutional neural network architecture, called Inception-ResNet, to protect in-vehicle network.	Lower false negative, error rates, training cost and latency	DoS, spoofing, injection attacks	Poor performance in detecting unlearned types of attacks
	Eziama *et al.* [169]	2018	• The use of a hybrid model-based Bayesian Neural Network that combines deep learning with probabilistic modeling for malicious node detection.	High prediction and classification accuracy, low detection latency	Timing, Sybil and false position attacks	No estimation of node behavior
	So *et al.* [170]	2018	• The use of a combination of K-Nearest Neighbors, K-NN and SVM to improve the overall detection precision for misbehaviors in messages.	Higher precision recall	Position forging attacks	Limited protection against attacks other than location spoofing attacks
	Gyawali *et al.* [171]	2020	• The implementation of a hybrid collaborative ML that uses K-Nearest Neighbors, Logistic regression, Decision Tree, and Random forest. • The use of reputation to identify the trustworthiness of vehicles. • The use of a Dempster-Shafer theory to combine resulted feedback and beta distributions for reputation update.	Superior results for precision, recall, and F1-score	False alert and position falsification attacks	Limited protection against online or active attacks
	Zhang *et al.* [172]	2018	• The implementation of a privacy-preserving ML based collaborative IDS (PML-CIDS) using ADMM to construct a distributed ERM problem. • The use of DVP to ensure dynamic differential privacy in the collaborative learning of IDS.	Fast convergence of collaborative Learning, small training data size, security-privacy tradeoff	Denial of service, probing and unauthorized access attacks	Cannot precisely identify the type of attack
Unsupervised & Reinforcement learning	Karagiannis *et al.* [13]	2018	• The use of k-means algorithm to process the variation of relative speed to distinguish intentional from unintentional jamming as well as identify the unique characteristics of each jamming attack.	Better clustering ability, accurate attack identification	RF jamming attacks	Limited protection against attacks other than RF jamming attacks
	Hanselmann *et al.* [173]	2020	• The implementation of a new neural network architecture, called LSTM, to handle the challenging structure of CAN data and effectively calculate anomaly scores.	Reliable attack detection, high true positive and true negative rates	Plateau, Continuous change, Playback, Flooding and Suppress attacks	Expensive cost of training models
	Xing *et al.* [174]	2019	• The use of Q-learning based incentive model to report intrusion in autonomous driving vehicles.	Detection rate and accuracy	GPS jamming/ spoofing and camera blind attacks, fake road information attacks	The integrity of intrusion reports is not guaranteed during the transmission.
	Xiao *et al.* [175]	2018	• The use of Policy Hill Climbing (PHC)-based UAV relay strategy to improve the anti-jamming performance of the VANET communication.	Lower error rate, higher utility	Smart jamming attacks	The high computation and communication overhead, limited protection against attacks other than smart jamming attacks

misbehavior in messages; (b) a reputation mechanism to score the trustworthiness of a vehicle; the score is slowly incremented by quickly dropped; (c) Dempster-Shafer theory to combine resulted feedback and beta distributions for reputation update.

Moreover, the authors in [172] propose a privacy-preserving ML-based collaborative IDS (PML-CIDS) for VANET. The proposed system uses the Alternating Direction Method of Multipliers (ADMM) to construct a distributed Empirical Risk Minimization (ERM) problem; this allows the classifier to be trained in a decentralized fashion to detect the intrusions. The PML-CIDS enjoys the advantages of collaborative IDS; indeed, it allows vehicles to share their knowledge - already trained data- with each other to boost the training data size while reducing the workload of each vehicle. To protect the privacy of vehicles during the knowledge exchange, the authors adopt a Dual Variable Perturbation (DVP) to ensure dynamic differential privacy in the collaborative learning. Simulation results, based on the NSL-KDD dataset, show that the proposed system outperforms existing schemes in

terms of the convergence of collaborative Learning, the minimum training data size, and the security-privacy tradeoff. However, it cannot precisely identify the type of attacks. Furthermore, the authors in [170] propose a new model that uses plausibility checks and ML to detect and mitigate the risks of location spoofing attacks in VANET. In this model, a combination of K-Nearest Neighbors (K-NN) and Support Vector Machine (SVM) has been adopted to classify misbehaviors for further mitigation plans. Moreover, the authors have introduced a friendly version of the VeReMi dataset [178], which is created specifically to train the ML-based models with a wide range of misbehaving traffic scenarios for testing V2X security. They show that the model can achieve a significant improvement in classification accuracy and precision-recall characteristics. However, the model is not resistant against attacks other than location spoofing attacks.

b: UNSUPERVISED AND REINFORCEMENT-ML BASED IDS

Because datasets cannot be exhaustive, it is extremely difficult to catch unknown threats for which no characterizing patterns are available. Thereby, considerable attention has been paid to anomaly-based IDS approaches. It provides the capability to overcome the limitations of signature-based IDS in ensuring an effective detection of abnormal behaviors by continuously checking network traffic for any deviation from legitimate network profiles [179]. Recently, anomaly-based detection strategies can benefit from advances in the field of machine/deep learning, particularly unsupervised and reinforcement learning. The operational logic of unsupervised learning helps models crafting representative features of legitimate profiles and also generating analytic insights from patterns and structures in unlabeled data [180]. In this regard, various anomaly-based approaches have been proposed. Furthermore, the constructed knowledge can be labeled with signatures to enrich datasets for hybrid detection strategies [165].

The authors in [13] introduce a new mechanism based on unsupervised ML to detect a specific type of DDoS attacks, namely RF jamming attacks. Through clustering using the K-means algorithm, the authors have evaluated the capability of a new metric, called Relative Speed Variation (RSV), in distinguishing intentional from unintentional jamming and identifying the unique characteristics of each jamming attack. The authors do not rely on the specific characteristics of k-means algorithm [13]. This opens up the door for further studies using different clustering algorithms (e.g., [179], [181]) especially, with the potential demonstrated by RSV. For in-vehicle security design, Hanselmann *et al.* [173] propose a scheme to secure CAN buses. They propose CANet as a new deep learning-based IDS to process signals to catch unknown attacks and to detect earlier technical failures. They implemented CANet using a new neural network architecture, called Long Short-Term Memory (LSTM), to handle the challenging structure of CAN data and calculate anomaly scores. One of the strongest points of CANet, compared to existing techniques (e.g., [182], [183]) is (a) its capability to work on signals of multiple CAN IDs simultaneously; (b) its high true negative rate, which is necessary for real-world applications; and (c) its reliability in detecting unknown attacks. Furthermore, Xing *et al.* [174] introduce a novel intrusion detection strategy for Autonomous Vehicle Networks (AVN) based on an assessment of Autonomous Driving Vehicles (ADVs) and a reinforcement Q-learning method. The proposed method focus on three steps consisting of (a) evaluate the trust of ADVs behaviors through direct and indirect assessment; (b) establish the intrusion detection scheme based on intrusion reports provided by ADVs;and (c) use an incentive paradigm based on Q-learning to participate in the intrusion reporting. The proposed method has shown its efficiency by providing a higher detection rate. Xiao *et al.* [175] propose a new mechanism to improve the communication performance of VANET against smart jammers. The main idea of the proposed scheme is to employ a hotbooting Policy Hill Climbing (PHC)-based Unmanned Aerial Vehicles (UAV) relay strategy to achieve optimal resistance against smart jamming without requiring prior knowledge about the jamming and UAV channel model. Simulation results show the efficiency of the proposed strategy in improving the anti-jamming transmission in VANET.

2) CHALLENGES IN ML-BASED SECURITY MECHANISMS

Machine learning, deep learning, and reinforcement learning (RL) are one of the most rapidly growing fields to realize next-generation ITS. However, to achieve the full potential of ML/DL, many challenges and open issues still need further investigation. Successful ML applications require a sufficient amount of representative datasets that can be used to train models. The generation of such datasets is particularly challenging in high scale and heterogeneous systems like VANET [184]. Even with the richness of data, it is yet challenging to develop a suitable model that processes data collected from various sources (e.g., vehicular sensors, wireless technology, and network traffic). Complex and time-consuming steps in preprocessing and cleaning of datasets are required in order to accurately reflect the actual environment and avoid data anomalies and misinterpretation. To cope with the challenges of the availability of datasets, the authors in [178] introduce the Vehicular Reference Misbehavior (VeReMi) as a first public extensible dataset specifically designed to train ML-models for the evaluation of misbehavior detection mechanisms for VANET. Security applications are not static in nature; this means ML/DL models must continuously monitor activities and analyze behaviors looking for deviations. Therefore, whenever there is an adjustment in the state of the network, ML/DL models need to be retrained according to the freshly acquired data; this leads to another challenge, namely the cost of training ML/DL models. For real-time VANET applications, it is difficult to frequently retrain ML/DL models since the process is expensive in terms processing and storage overhead. Hence, it is of great importance to carefully plan for future (re)training

processes to adapt to network changes and execute particular processing (e.g., model reduction and compression) to lower the overhead without causing any performance degradation.

Furthermore, we cannot imagine a successful usage of ML/DL models without the capacity to generate meaningful insights that contribute to a better understanding of questionable problems and effective decision-making processes [185]. In fact, complex ML/DL models such as Neural Network (NN) and Deep-NN often produce unpredictable and hard to interpret or explain outputs because of the uncertainty of the layered structure [186]. When presenting the generated outputs of ML/DL models, it is important to make sure that correct interpretations are achieved to guarantee the expected model performance. Otherwise, the misinterpretation could result in misleading/inaccurate decisions making these models not suitable for the critical security of VANET. ML/DL models are sensitive to changes in the data; indeed, even small changes in the initial input could have a significant impact on the resulting output. Recently, this has been exploited in an adversarial setting where the attacker attempted to add noise to the model input aiming to fool the learning process and result in corrupted output [186]. Consequently, it is of great importance to address all these challenges before the full integration of ML/DL models into realistic scenarios of VANET.

C. RECENT TRENDS IN SECURITY OF ITS

1) SECURITY OF 5G-ENABLED V2X COMMUNICATIONS

Over the previous decades, we have experienced the fastest growth of communication technologies bringing vast improvements to the capabilities of ITS. These trends are expected to go far, especially, with the active development/deployment of the Fifth Generation Cellular Technology (5G) [187]. According to the 5G Infrastructure Public Private Partnership (5G PPP) [188], the possibility to integrate V2X communication standards with 5G is promising. It is considered a great opportunity to provide more flexible and innovative services to migrate toward higher automation levels while maximizing the safety, efficiency, and sustainability of our transportation systems [189]–[191]. Currently, the link-layer protocol, used in V2X communication is 802.11p; it supports traditional mechanisms to protect system authentication and private data. However, with the growing demands of high reliability and ultra-low latency, the traditional design of security management has failed to satisfy the needs without additional overhead and costly operations [20].

The adoption of 5G in V2X communication might bring new security possibilities to overcome the shortcomings of DSRC, 802.11p, and LTE-V2X. Currently, the 5G security design has boosted the development of security in terms of flexibility as well as network programmability while fulfilling the unique security requirements of each network user and consistent Quality of Experience (QoE) provision. Software Defined Networking (SDN), Network Function Virtualization (NFV), and network slicing are including most technologies that support the security design of 5G-V2X communication in very innovative ways [20].

2) SDN AND NFV TECHNOLOGIES

The convergence of both SDN and NFV with vehicular networks are gaining high momentum since they offer great potential in addressing most system challenges. In SDN, the controllers hide network complexity and offload the heavy burden from nodes through decoupling control planes from data forwarding planes. Hence, significant enhancements in terms of flexibility, dynamicity, manageability, and network programmability can be projected to the current design of network security [192], [193]. This separation results in a flexible and logically centralized architecture that takes control of major security operations based on a holistic view of data plane connections. This feature can ease the network-wide security monitoring by retrieving network statistics information and flow request messages through the controller. Therefore, SDN enables instant threat identification by analyzing the network state changes, and reacts conveniently to mitigate risks by reprogramming the network accordingly [192]–[194].

The adoption of the NFV paradigm has been proposed to reshape the landscape of telecommunication industries in a flexible and scalable way. It provides the capability to replace expensive dedicated hardware appliances with generic servers that use virtualization technologies to build different virtual network slices. Thereby, it enables to design, deploy, and manage services (e.g., security capabilities) customized to meet the required characteristics by the use case under consideration (e.g., VANET [195]). Among the benefits of NFV is the capability to enhance the security of VANET through shifting the use of dedicated hardware-based security appliances (e.g., deep packet inspection (DPI), Firewalls, IPS, and IDS) into virtual security appliances (e.g., vDPI, vFirewalls, vIDS, and vIPS). This certainly has the potential to achieve a higher level of agility and enables optimal orchestration of resource allocation [193].

SDN and NFV paradigms are complementing each other, and both are essential parts of the 5G network. They have the potential to boost the development and deployment of secure network applications due to the capability of enabling unlimited creativity of network functionalities. Various protocols have been proposed to extend network security. In the context of security, Floodlight is a Java-based open-source SDN controller that supports virtual switches. This makes it easier to develop and test modules in a flexible and extendable way to react to changes in network configuration [196]. Security-Enhanced (SE) Floodlight controller [197] offers a comprehensive security mediation for the SDN control layer and adds a secure programmable northbound API, which specifically enforces the privilege separation principle. It assigns authorization roles to OpenFlow applications to improve inline flow rules for conflict detection. Furthermore, Floodlight also introduces an OpenFlow audit subsystem to track all security relevant-events that occur

between the control data plane and the application layer. Based on Floodlight Framework, Yu *et al.* [15] design a platform to efficiently detect and rapidly respond to the DDoS attacks in vehicular networks. Simulation results show that the proposed system significantly shortens the response time to the attack and reduces the burden on the controller. BENBI [198] is a scalable and dynamic security mechanism that allows SDN-based VANET applications to access resources on available controllers via the northbound interface. The proposed mechanism prevents attackers from manipulating network configurations and spoofing. However, it suffers from the single-point failure issue of SDN; the authors plan for a decentralized implementation using blockchain.

3) NETWORK SLICING

The next generation of vehicular communications are expected in order to support the high heterogeneity of network components in order to satisfy the need for safer and comfortable traffic experiences. In fact, with the traditional network architecture wherein dedicated hardware is reserved for each service [199], it would be extremely challenging to secure the strict requirement of transportation services. In this context, the concept of network slices has emerged as a novel technology targeted by different standardization bodies, including the 3rd Generation Partnership Project (3GPP) Release 16 [200], the European Telecommunications Standards Institute (ETSI) [201], and ITU-T (ITU Telecommunication Standardization Sector) [202]. Network slicing has a close association with the virtualization of the network paradigm; it can go towards SDN and NFV, but it can also be considered as an independent technology. Network slicing aims to provide service customization, network isolation, and multitenancy support for network services [203], [204]. It is intended as a set of logical network functions that enable flexible and efficient creation of specialized network services tailored to serve a particular purpose in terms of functionalities (e.g., security and mobility) and performance (e.g., latency and reliability).

Network slices are independent in nature. Because of this feature, the design of future security mechanisms has been improved. With elasticity, network slicing technology supports the isolation between slices in terms of traffic and resources. Therefore, it becomes easier to limit the scope of potential attacks (e.g., DoS attacks and side-channel attacks) by placing a particular kind of vehicular components (could be software or hardware) with common weaknesses in a dedicated slice. Then, each dedicated slice can be customized to operate with different security functionalities and policies enforcement, such as access control, firewalls and authentication schemes. This allows to ensure adequate protection for different vehicular slices.

4) PHYSICAL LAYER SECURITY PROVISION

Due to the fading, random location, and broadcast nature of the wireless medium in 5G-V2X networks, channels are exposed to a variety of attacks (e.g., jamming, eavesdropping and DoS). In the literature, the computational security paradigm, such as cryptographic techniques, has been proven to be effective against these attacks. However, this is not the case in all scenarios, especially for communications that require low latency and ultra-reliable connectivity between different components like vehicular communication. Thus, lightweight and efficient security solutions are needed. Unlike traditional security mechanisms that are heavily reliant on cryptographic mechanisms, Physical Layer Security (PLS) emerges as a potential strategy that offers a promising solution for securing wireless communications. In particular, PLS avoids the use of compute-intensive cryptographic techniques, which makes it more suitable for heterogeneous and ultra-reliable systems like vehicular networks [205], [206]. PLS exploits the properties of the wireless medium, such as noise, fading, and interference to degrade the signal quality intercepted/received by malicious users; thus, it prevents these users from acquiring confidential information from the signal [207], [208]. Recently, considerable research efforts have been devoted to improving the positive transmission rate at which information can be transmitted securely in the presence of malicious third parties; this is known as Secrecy Rate (SR). For instance, the authors in [209] introduce PLS-based secrecy transmission in VANET; their proposal achieves better performance in terms of secrecy rate and energy effectiveness while keeping vehicular communication secure. A comprehensive overview of physical-layer security strategies employed in V2X can be found in [210].

In 5G-V2X networks, technologies such as massive Multiple-Input Multiple-Output (MIMO) and millimeter Wave (mmWave) constitute the foundation to provide secure communication at the physical layer. With massive MIMO systems, the secrecy performance can be significantly enhanced [208]. By using arrays of antennas, massive MIMO provides high power and spectrum efficiencies. Therefore, the transmitted power is considerably reduced resulting in reduced Signal to Noise Ratio (SNR) at the eavesdropper's channel. MmWave is another enabling technology for 5G-V2X that is used for high transmission capacity and secure communication. By taking advantages from the high frequency signals offered by mmWave, a wealth of opportunities at the physical layer security can be achieved. Indeed, the high mmWave frequency is needed to reach a higher secrecy rate [211]. High frequency signals increase free space path losses, therefore, reduce the probability for third parties to overhear signals. In [16], the authors have studied the possibility to enhance the secrecy performance with mmWave in vehicular communication. More specifically, they proposed two Physical Layer (PHY) security techniques that take advantages of (a) a new hybrid transceiver architecture for mmWave to reduce the complexity and cost of fully digital antenna architectures; and (b) opportunistic noise injection to improve the secrecy rate to jam potential eavesdroppers with sensitive receivers.

TABLE 7. Current automotive physical layer technologies.

Acronyms	Definition	Acronyms	Definition
3GPP	3rd Generation Partnership Project	ML	Machine Learning
5G-PPP	5G Infrastructure Public Private Partnership	MOST	Media Oriented System Transport
CA	Certification Authorities	NFV	Network Function Virtualization
CALM	Communications Access for Land Mobiles	NIST	National Institute of Standards and Technology
CAM	Cooperative Awareness Message	OBD	On-Board Diagnostics
CAN	Controller Area Network	OBU	On-Board Unit
CRL	Certificate Revocation List	PCA	Pseudonym Certificate Authority
CVE	Common Vulnerabilities and Exposures	PKA	Public Key-based Authentication
CWE	Common Weakness Enumeration	PKI	Public Key Infrastructure
DSRC	Dedicated Short-Range Communications	PLS	Physical Layer Security
DoS	Denial of Service	QoE	Quality of Experience
ECU	Electronic Control Units	QoS	Quality-of-Service
ETSI	European Telecommunications Standards Institute	RF	Radio Frequency
FCC	Federal Communications Commission	RL	Reinforcement Learning
GNSS	Global Navigation Satellite System	RSU	Road-side Unit
GS	Group Signature	SDN	Software Defined Networking
GSA	Group signature based Authentication	SKA	Symmetric key based Authentication
IBA	Identity-based Authentication	SVM	Support Vector Machine
IDS	Intrusion Detection System	V2G	Vehicle-to-Grid
ITS	Intelligent Transportation System	V2I	Vehicle-to-Infrastructure
IoT	Internet of Things	V2P	Vehicle-to-Pedestrian
IoV	Internet of Vehicles	V2V	Vehicle-to-Vehicle
LIN	Local Interconnect Network	V2X	Vehicle-to-Everything
LTE	Long Term Evolution	VANET	Vehicular Adhoc NETwork
MAC	Message Authentication Code	VPKI	Vehicular Public Key Infrastructure
ML	Machine Learning	WAVE	Wireless Access in Vehicular Environment

5) SECURITY CHALLENGES OF 5G-ENABLED V2X COMMUNICATION

Despite the great success of 5G-V2X in developing the next generation of intelligent vehicular networks through the softwarization and virtualization of network functions, the security of the overall architecture is still questionable [191]. This paradigm change may adversely impact the network security and opens up doors for various new challenges in securing 5G-V2X platforms that manage virtual resources and their relationships with the application layer for a fully trusted system. As recently stated by Hussain and Zeadally [20], security is one of the crucial challenges that need further investigation to guarantee seamless integration of 5G technology with VANET. In the 5G context, technologies like SDN and network virtualization have extended the range of security vulnerabilities. On the one hand, SDN-based VANET has been planned without considering security as a top priority. In particular, SDN controllers can be targeted by various attacks (e.g., saturation, misconfiguration, poisoning, and DDoS attacks). The flexibility provided by Application Programming Interfaces (APIs) between different layers can also be exploited to produce destructive malware to take control of the whole system. For more details about SDN attacks, the reader is referred to [189], [212], [213].

Furthermore, the high degree of heterogeneity in the 5G-V2X network is another major challenge for the efficiency and the accuracy of security controls and monitoring solutions. 5G-V2X must carry a large amount of network traffic and comprise many heterogeneous devices. Having such a large-scale network can create significant attack surfaces and enable threats to move across large portions of the global network. Hence, it creates serious concerns on how establishing trustworthy relationships between devices and networks. According to Hussain and Zeadally [20], traditional security and trust models may not work in addressing the emerging issues facing the integration of 5G technology in VANET. Therefore, it is of great importance to carry out a novel exhaustive investigation that focuses on the current situations of LTE-V2X and 5G-V2X to design and optimize adaptative security standards; the objective is to address properly the different security challenges faced by the next generation of vehicular communication.

V. CONCLUSION

Modern transport systems are continuously evolving, bringing benefits that promote smartness and multiple levels of autonomy. As systems become more open and technologically more complex, attacks on security, privacy, and trust become more sophisticated. However, a few studies have focused on the plethora of security issues in ITS and their mitigation. In this article, we have analyzed security issues in ITS based on recently published articles to identify the root causes of vulnerabilities. We also investigated potential attacks to identify the missing security elements in the design of existing security solutions. We covered the most relevant defense mechanisms, which are considered the best candidates to dominate the future of ITS security. In particular, we presented a comparative study of existing solutions highlighting their strengths and shortcomings to draw lessons learned. We also placed a special emphasis on classifying mitigating security schemes in the context of ITS. Finally, we have pointed out existing gaps that warrant additional research. Table 7 shows the list of relevant abbreviations used throughout this article.

ACKNOWLEDGMENT

The authors would like to thank the editors and the anonymous reviewers for their valuable and enriching comments and suggestions to improve the content of this article.

REFERENCES

[1] A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil, M. Guizani, and A. Al-Fuqaha, "Smart cities: A survey on data management, security, and enabling technologies," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2456–2501, 4th Quart., 2017.

[2] E. Ahmed and H. Gharavi, "Cooperative vehicular networking: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 3, pp. 996–1014, Mar. 2018.

[3] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, "Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2377–2396, 4th Quart., 2015.

[4] 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 Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 584–616, 4th Quart., 2011.

[5] *Briefing: Cooperative Intelligent Transport Systems (C-ITS)*, Eur. Transp. Saf. Council (ETSC), Brussels, Belgium, Nov. 2017.

[6] M. Seredynski and F. Viti, "A survey of cooperative ITS for next generation public transport systems," in *Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2016, pp. 1229–1234.

[7] V. Astarita, D. C. Festa, P. Giofrè, G. Guido, and D. W. E. Mongelli, "Co-operative ITS: ESD a smartphone based system for sustainability and transportation safety," *Procedia Comput. Sci.*, vol. 83, pp. 449–456, Jan. 2016.

[8] P. K. Singh, S. K. Nandi, and S. Nandi, "A tutorial survey on vehicular communication state of the art, and future research directions," *Veh. Commun.*, vol. 18, Aug. 2019, Art. no. 100164.

[9] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2467–2476, Sep. 2017.

[10] A. Dua, N. Kumar, A. K. Das, and W. Susilo, "Secure message communication protocol among vehicles in smart city," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4359–4373, May 2018.

[11] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 8, pp. 2193–2204, Aug. 2016.

[12] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," *Veh. Commun.*, vol. 21, Jan. 2020, Art. no. 100198.

[13] D. Karagiannis and A. Argyriou, "Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning," *Veh. Commun.*, vol. 13, pp. 56–63, Jul. 2018.

[14] J. Huang, Y. Qian, and R. Q. Hu, "Secure and efficient privacy-preserving authentication scheme for 5G software defined vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 8542–8554, Aug. 2020.

[15] Y. Yu, L. Guo, Y. Liu, J. Zheng, and Y. Zong, "An efficient SDN-based DDoS attack detection and rapid response platform in vehicular networks," *IEEE Access*, vol. 6, pp. 44570–44579, 2018.

[16] M. E. Eltayeb, J. Choi, T. Y. Al-Naffouri, and R. W. Heath, "Enhancing secrecy with multiantenna transmission in millimeter wave vehicular communication systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8139–8151, Sep. 2017.

[17] M. A. Javed, E. B. Hamida, A. Al-Fuqaha, and B. Bhargava, "Adaptive security for intelligent transport system applications," *IEEE Intell. Transp. Syst. Mag.*, vol. 10, no. 2, pp. 110–120, 2018.

[18] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2019.

[19] J. Huang, D. Fang, Y. Qian, and R. Q. Hu, "Recent advances and challenges in security and privacy for V2X communications," *IEEE Open J. Veh. Technol.*, vol. 1, pp. 244–266, 2020.

[20] R. Hussain, F. Hussain, and S. Zeadally, "Integration of VANET and 5G security: A review of design and implementation issues," *Future Gener. Comput. Syst.*, vol. 101, pp. 843–864, Dec. 2019.

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

[22] D. A. Hahn, A. Munir, and V. Behzadan, "Security and privacy issues in intelligent transportation systems: Classification and challenges," *IEEE Intell. Transp. Syst. Mag.*, early access, Apr. 11, 2019, doi: 10.1109/MITS.2019.2898973.

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

[24] R. W. van der Heijden, S. Dietzel, T. Leinmuller, and F. Kargl, "Survey on misbehavior detection in cooperative intelligent transportation systems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 779–811, 1st Quart., 2019.

[25] S. Sharma and A. Kaul, "A survey on intrusion detection systems and honeypot based proactive security mechanisms in VANETs and VANET cloud," *Veh. Commun.*, vol. 12, pp. 138–164, Apr. 2018.

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

[27] R. Hussain, J. Lee, and S. Zeadally, "Trust in VANET: A survey of current solutions and future research opportunities," *IEEE Trans. Intell. Transp. Syst.*, early access, Mar. 5, 2020, doi: 10.1109/TITS.2020.2973715.

[28] *Scimago Institution Rankings*. Accessed: Jun. 14, 2020. [Online]. Available: https://www.scimagojr.com/journalrank.php

[29] J. A. Guerrero-ibanez, S. Zeadally, and J. Contreras-Castillo, "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and Internet of Things technologies," *IEEE Wireless Commun.*, vol. 22, no. 6, pp. 122–128, Dec. 2015.

[30] R. I. Meneguette, R. E. De Grande, and A. A. F. Loureiro, *Intelligent Transport System in Smart Cities*. Cham, Switzerland: Springer, 2018.

[31] A. Sumalee and H. W. Ho, "Smarter and more connected: Future intelligent transportation system," *IATSS Res.*, vol. 42, no. 2, pp. 67–71, Jul. 2018.

[32] S. M. Khan, M. Rahman, A. Apon, and M. Chowdhury, "Characteristics of intelligent transportation systems and its relationship with data analytics," in *Data Analytics for Intelligent Transportation Systems*. Amsterdam, The Netherlands: Elsevier, 2017, pp. 1–29.

[33] A. Touil, A. Sbai, and F. Ghadi, "Cluster-based data collection scheme for vehicular ad-hoc networks," *Procedia Comput. Sci.*, vol. 148, pp. 62–69, Jan. 2019.

[34] M. A. Khan, S. Sargento, and M. Luis, "Data collection from smart-city sensors through large-scale urban vehicular networks," in *Proc. IEEE 86th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2017, pp. 1–6.

[35] W. Nie, V. C. S. Lee, D. Niyato, Y. Duan, K. Liu, and S. Nutanong, "A quality-oriented data collection scheme in vehicular sensor networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 5570–5584, Jul. 2018.

[36] W. Nie, K. Liu, V. C. S. Lee, Y. Duan, and S. Nutanong, "Vehdoop: A scalable analytical processing framework for vehicular sensor networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 8, pp. 3104–3114, Aug. 2019.

[37] S. Ilarri, T. Delot, and R. Trillo-Lado, "A data management perspective on vehicular networks," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2420–2460, 4th Quart., 2015.

[38] M. Chaqfeh, H. El-Sayed, and A. Lakas, "Efficient data dissemination for urban vehicular environments," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 4, pp. 1226–1236, Apr. 2019.

[39] L. Aparecido, "Data dissemination in vehicular networks: Challenges, solutions, and future perspectives," in *Proc. 7th Int. Conf. New Technol., Mobility Secur. (NTMS)*, Jul. 2015, pp. 1–5.

[40] H. Zhao, H. Yue, T. Gu, and W. Li, "CPS-based reliability enhancement mechanism for vehicular emergency warning system," *Int. J. Intell. Transp. Syst. Res.*, vol. 17, no. 3, pp. 232–241, Mar. 2019.

[41] D. Sun, H. Zhao, and S. Cheng, "A novel membership cloud model-based trust evaluation model for vehicular ad hoc network of T-CPS," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 5710–5723, Dec. 2016.

[42] S. Tuohy, M. Glavin, C. Hughes, E. Jones, M. Trivedi, and L. Kilmartin, "Intra-vehicle networks: A review," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 534–545, Apr. 2015.

[43] J. Huang, M. Zhao, Y. Zhou, and C.-C. Xing, "In-vehicle networking: Protocols, challenges, and solutions," *IEEE Netw.*, vol. 33, no. 1, pp. 92–98, Jan. 2019.

[44] W. Zeng, M. A. S. Khalid, and S. Chowdhury, "In-vehicle networks outlook: Achievements and challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1552–1571, 3rd Quart., 2016.
[45] A. Zekri and W. Jia, "Heterogeneous vehicular communications: A comprehensive study," *Ad Hoc Netw.*, vols. 75–76, pp. 52–79, Jun. 2018.
[46] R. I. Meneguette, R. E. De Grande, and A. A. F. Loureiro, "Vehicle-to-Vehicle Communication," in *Intelligent Transport System in Smart Cities: Aspects and Challenges of Vehicular Networks and Cloud*. Cham, Switzerland: Springer, 2018, pp. 79–112.
[47] J. Harding, G. Powell, R. Yoon, J. Fikentscher, C. Doyle, D. Sade, M. Lukuc, J. Simons, and J. Wang, "Vehicle-to-vehicle communications: Readiness of V2V technology for application," Nat. Highway Traffic Safety Admin., Washington, DC, USA, Tech. Rep. DOT HS 812 014, 2014, p. 327.
[48] R. I. Meneguette, R. E. De Grande, and A. A. F. Loureiro, "Vehicle-to-infrastructure communication," in *Intelligent Transport System in Smart Cities: Aspects and Challenges of Vehicular Networks and Cloud*. Cham, Switzerland: Springer, 2018, pp. 53–77.
[49] E. Ndashimye, S. K. Ray, N. I. Sarkar, and J. A. Gutiérrez, "Vehicle-to-infrastructure communication over multi-tier heterogeneous networks: A survey," *Comput. Netw.*, vol. 112, pp. 144–166, Jan. 2017.
[50] M. G. Doone, S. L. Cotton, D. W. Matolak, C. Oestges, S. F. Heaney, and W. G. Scanlon, "Pedestrian-to-vehicle communications in an urban environment: Channel measurements and modeling," *IEEE Trans. Antennas Propag.*, vol. 67, no. 3, pp. 1790–1803, Mar. 2019.
[51] S. El Hamdani, N. Benamar, and M. Younis, "A protocol for pedestrian crossing and increased vehicular flow in smart cities," *J. Intell. Transp. Syst., Technol., Planning, Oper.*, vol. 24, no. 5, pp. 514–533, 2020.
[52] S. El Hamdani, N. Benamar, and M. Younis, "Pedestrian support in intelligent transportation systems: Challenges, solutions and open issues," *Transp. Res. C Emerg. Technol.*, vol. 121, Dec. 2020, Art. no. 102856.
[53] A. Sharma and S. Sharma, "Review of power electronics in vehicle-to-grid systems," *J. Energy Storage*, vol. 21, pp. 337–361, Feb. 2019.
[54] N. S. Pearre and H. Ribberink, "Review of research on V2X technologies, strategies, and operations," *Renew. Sustain. Energy Rev.*, vol. 105, pp. 61–70, May 2019.
[55] J. E. Siegel, D. C. Erb, and S. E. Sarma, "A survey of the connected vehicle Landscape—Architectures, enabling technologies, applications, and development areas," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 8, pp. 2391–2406, Aug. 2018.
[56] *FCC Report and Order: FCC-03-324*, FCC, Washington, DC, USA, Oct. 2004.
[57] Y. L. Morgan, "Notes on DSRC & WAVE standards suite: Its architecture, design, and characteristics," *IEEE Commun. Surveys Tuts.*, vol. 12, no. 4, pp. 504–518, 4th Quart., 2010.
[58] N. Benamar, J. Härri, J. Lee, and T. Ernst, "Basic support for IPv6 networks operating outside the context of a basic service set over IEEE Std 802.11," Internet Eng. Task Force (IETF), Fremont, CA, USA, Tech. Rep. RFC 8691, Dec. 2019. [Online]. Available: https://tools.ietf.org/html/rfc8691
[59] A. Ghosal and M. Conti, "Security issues and challenges in V2X: A survey," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107093.
[60] N. Lu, N. Zhang, N. Cheng, X. Shen, J. W. Mark, and F. Bai, "Vehicles meet infrastructure: Toward Capacity–Cost tradeoffs for vehicular access networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 3, pp. 1266–1277, Sep. 2013.
[61] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of DSRC and cellular network technologies for V2X communications: A survey," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 9457–9470, Dec. 2016.
[62] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3453–3495, 4th Quart., 2018.
[63] Y. Li, Y. Tu, Q. Fan, C. Dong, and W. Wang, "Influence of cyber-attacks on longitudinal safety of connected and automated vehicles," *Accident Anal. Prevention*, vol. 121, pp. 148–156, Dec. 2018.
[64] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2015.
[65] A. K. Malhi, S. Batra, and H. S. Pannu, "Security of vehicular ad-hoc networks: A comprehensive survey," *Comput. Secur.*, vol. 89, Feb. 2020, Art. no. 101664.
[66] F. Qu, Z. Wu, F. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.
[67] X. Li, Y. Yu, G. Sun, and K. Chen, "Connected Vehicles' security from the perspective of the in-vehicle network," *IEEE Netw.*, vol. 32, no. 3, pp. 58–63, May 2018.
[68] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," IOActive, Washington, DC, USA, Tech. Rep., 2014, pp. 1–90.
[69] H. Olufowobi and G. Bloom, "Connected cars: Automotive cybersecurity and privacy for smart cities," in *Smart Cities Cybersecurity Privacy*, D. B. Rawat and K. Z. Ghafoor, Eds. Amsterdam, The Netherlands: Elsevier, 2018, pp. 227–240.
[70] 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 *Proc. 20th USENIX Secur. Symp.* Berkeley, CA, USA: USENIX Association, 2011, pp. 77–92.
[71] J. Liu, S. Zhang, W. Sun, and Y. Shi, "In-vehicle network attacks and countermeasures: Challenges and future directions," *IEEE Netw.*, vol. 31, no. 5, pp. 50–58, Sep. 2017.
[72] K. Iehira, H. Inoue, and K. Ishida, "Spoofing attack using bus-off attacks against a specific ECU of the CAN bus," in *Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2018, pp. 1–4.
[73] S. Woo, H. Jin Jo, and D. Hoon Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 993–1006, Apr. 2015.
[74] S. Woo, D. Moon, T.-Y. Youn, Y. Lee, and Y. Kim, "CAN ID shuffling technique (CIST): Moving target defense strategy for protecting in-vehicle CAN," *IEEE Access*, vol. 7, pp. 15521–15536, 2019.
[75] R. Currie, "Hacking the CAN bus: Basic manipulation of a modern automobile through CAN bus reverse engineering," SANS Technol. Inst., Columbia, MD, USA, Tech. Rep., 2017, pp. 1–32.
[76] A. R. Mousa, P. NourElDeen, M. Azer, and M. Allam, "Lightweight authentication protocol deployment over FlexRay," in *Proc. 10th Int. Conf. Informat. Syst. (INFOS)*. New York, NY, USA: Association for Computing Machinery, 2016, pp. 233–239.
[77] P. Murvay and B. Groza, "Practical security exploits of the FlexRay in-vehicle communication protocol," in *Risks and Security of Internet and Systems* (Lecture Notes in Computer Science), vol. 11391. Cham, Switzerland: Springer, 2019, pp. 172–187.
[78] J. Takahashi, Y. Aragane, T. Miyazawa, H. Fuji, H. Yamashita, K. Hayakawa, S. Ukai, and H. Hayakawa, "Automotive attacks and countermeasures on LIN-bus," *J. Inf. Process.*, vol. 25, no. 0, pp. 220–228, 2017.
[79] National Instruments. (2011). *Introduction to the Local Interconnect Network (LIN) Bus*. pp. 2–5. [Online]. Available: http://www.ni.com/white-paper/9733/en/
[80] S. Nie, L. Liu, and Y. Du, "Free-fall: Hacking tesla from wireless to can bus," in *Proc. Black Hat USA*, 2017, pp. 1–16. [Online]. Available: https://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf
[81] S. Nie, L. Liu, Y. Du, and W. Zhang, "Over-the-air: How we remotely compromised the gateway, BCM, and autopilot ECUs of tesla cars," in *Proc. Defcon*, vol. 1, 2018, pp. 1–19. [Online]. Available: http://www.w3.org/2000/svg
[82] (Feb. 2018). *(CVE)-2018-1170*. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1170
[83] (2019). *Tesla Cross-Site Scripting (XSS) Vulnerability*. [Online]. Available: https://www.bankinfosecurity.com/blogs/how-big-rock-revealed-10k-tesla-xss-vulnerability-p-2772
[84] M. Shkatov, J. Michae, and O. Bazhaniuk. (2017). *CVE-2017-9647 Detail*. [Online]. Available: https://www.us-cert.gov/ics/advisories/ICSA-17-208-01
[85] (Mar. 2019). *(CVE)-2019-9977*. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-9977
[86] S. Ucar, S. C. Ergen, and O. Ozkasap, "Security vulnerabilities of IEEE 802.11p and visible light communication based platoon," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2016, pp. 1–4.
[87] S. Ishihara, R. V. Rabsatt, and M. Gerla, "Improving reliability of platooning control messages using radio and visible light hybrid communication," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2015, pp. 96–103.
[88] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo, "Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 110–113, Jan. 2014.
[89] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE—A networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 283–302, 1st Quart., 2014.

[90] J. Padgette, J. Bahr, M. Batra, M. Holtmann, R. Smithbey, L. Chen, and K. Scarfone, "Guide to Bluetooth security guide to Bluetooth security," Tech. Rep. 2, May 2017. [Online]. Available: https://doi.org/10.6028/nist.sp.800-121r2

[91] P. Cope, J. Campbell, and T. Hayajneh, "An investigation of Bluetooth security vulnerabilities," in *Proc. IEEE 7th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2017, pp. 1–7.

[92] M. G. Amin, P. Closas, A. Broumandan, and J. L. Volakis, "Vulnerabilities, threats, and authentication in satellite-based navigation systems [scanning the issue]," *Proc. IEEE*, vol. 104, no. 6, pp. 1169–1173, Jun. 2016.

[93] E. Falletti, D. Margaria, G. Marucco, B. Motella, M. Nicola, and M. Pini, "Synchronization of critical infrastructures dependent upon GNSS: Current vulnerabilities and protection provided by new signals," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2118–2129, Sep. 2019.

[94] R. T. Ioannides, T. Pany, and G. Gibbons, "Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques," *Proc. IEEE*, vol. 104, no. 6, pp. 1174–1194, Jun. 2016.

[95] D. Borio, F. Dovis, H. Kuusniemi, and L. Lo Presti, "Impact and detection of GNSS Jammers on consumer grade satellite navigation receivers," *Proc. IEEE*, vol. 104, no. 6, pp. 1233–1245, Jun. 2016.

[96] G. X. Gao, M. Sgammini, M. Lu, and N. Kubo, "Protecting GNSS receivers from jamming and interference," *Proc. IEEE*, vol. 104, no. 6, pp. 1327–1338, Jun. 2016.

[97] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.

[98] C. Sanders and Y. Wang, "Localizing spoofing attacks on vehicular GPS using vehicle-to-vehicle communications," *IEEE Trans. Veh. Technol.*, early access, Oct. 16, 2020, doi: 10.1109/TVT.2020.3031576.

[99] P. Kapoor, A. Vora, and K.-D. Kang, "Detecting and mitigating spoofing attack against an automotive radar," in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Aug. 2018, pp. 1–6.

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

[101] H. Alnabulsi and R. Islam, "Protecting code injection attacks in intelligent transportation system," in *Proc. 18th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./13th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2019, pp. 799–806.

[102] Q. Li, F. Wang, J. Wang, and W. Li, "LSTM-based SQL injection detection method for intelligent transportation system," *IEEE Trans. Veh. Technol.*, vol. 68, no. 5, pp. 4182–4191, May 2019.

[103] Z. Abdollahi Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3893–3902, Dec. 2018.

[104] M. Shabbir, M. A. Khan, U. S. Khan, and N. A. Saqib, "Detection and prevention of distributed denial of service attacks in VANETs," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2016, pp. 970–974.

[105] P. Liu, B. Liu, Y. Sun, B. Zhao, and I. You, "Mitigating DoS attacks against pseudonymous authentication through puzzle-based co-authentication in 5G-VANET," *IEEE Access*, vol. 6, pp. 20795–20806, 2018.

[106] M. Poongodi, V. Vijayakumar, F. Al-Turjman, M. Hamdi, and M. Ma, "Intrusion prevention system for DDoS attack on VANET with reCAPTCHA controller using information based metrics," *IEEE Access*, vol. 7, pp. 158481–158491, 2019.

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

[108] C. Panos, C. Ntantogian, S. Malliaros, and C. Xenakis, "Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks," *Comput. Netw.*, vol. 113, pp. 94–110, Feb. 2017.

[109] A. Afdhal, S. Muchallil, H. Walidainy, and Q. Yuhardian, "Black hole attacks analysis for AODV and AOMDV routing performance in VANETs," in *Proc. Int. Conf. Electr. Eng. Informat. (ICELTICs)*, Oct. 2017, pp. 29–34.

[110] J. Tobin, C. Thorpe, and L. Murphy, "An approach to mitigate black hole attacks on vehicular wireless networks," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Jun. 2017, pp. 1–7.

[111] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 10–21, Feb. 2014.

[112] Q. Zhang and A. Boukerche, "A novel infrastructure-based worm spreading countermeasure for vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2188–2203, Jul. 2018.

[113] J. R. Douceur, "The Sybil attack," in *Peer-to-Peer Systems* (Lecture Notes in Computer Science), vol. 2429, P. Druschel, F. Kaashoek, and A. Rowstron, Eds. Berlin, Germany: Springer, 2002, pp. 251–260.

[114] A. Vasudeva and M. Sood, "Survey on Sybil attack defense mechanisms in wireless ad hoc networks," *J. Netw. Comput. Appl.*, vol. 120, pp. 78–118, Oct. 2018.

[115] A. M. Bhise and S. D. Kamble, "Review on detection and mitigation of Sybil attack in the network," *Procedia Comput. Sci.*, vol. 78, pp. 395–401, Apr. 2016.

[116] M. Ayaida, N. Messai, S. Najeh, and K. Boris Ndjore, "A macroscopic traffic model-based approach for sybil attack detection in VANETs," *Ad Hoc Netw.*, vol. 90, Jul. 2019, Art. no. 101845.

[117] 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 Trans. Mobile Comput.*, vol. 18, no. 2, pp. 362–375, Feb. 2019.

[118] M. Baza, M. Nabil, M. M. E. A. Mahmoud, N. Bewermeier, K. Fidan, W. Alasmary, and M. Abdallah, "Detecting sybil attacks using proofs of work and location in vanets," *IEEE Trans. Depend. Sec. Comput.*, p. 1, 2020.

[119] S. S. Albouq and E. M. Fredericks, "Detection and avoidance of wormhole attacks in connected vehicles," in *Proc. 6th ACM Symp. Develop. Anal. Intell. VehicularNetworks Appl. (DIVANet)*. New York, NY, USA: Association for Computing Machinery, 2017, pp. 107–116.

[120] S. Ali, P. Nand, and S. Tiwari, "Secure message broadcasting in VANET over wormhole attack by using cryptographic technique," in *Proc. Int. Conf. Comput., Commun. Autom. (ICCCA)*, May 2017, pp. 520–523.

[121] D. S. K. Tiruvakadu and V. Pallapa, "Confirmation of wormhole attack in MANETs using honeypot," *Comput. Secur.*, vol. 76, pp. 32–49, Jul. 2018.

[122] K. Emara, W. Woerndl, and J. Schlichter, "Vehicle tracking using vehicular network beacons," in *Proc. IEEE 14th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2013, pp. 1–6.

[123] Y. Zou and G. Wang, "Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack," *IEEE Trans. Ind. Informat.*, vol. 12, no. 2, pp. 780–787, Apr. 2016.

[124] M. S. Sheikh, J. Liang, and W. Wang, "Security and privacy in vehicular ad hoc network and vehicle cloud computing: A survey," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–25, Jan. 2020.

[125] J. Lastinec and M. Keszeli, "Analysis of realistic attack scenarios in vehicle ad-hoc networks," in *Proc. 7th Int. Symp. Digit. Forensics Secur. (ISDFS)*, Jun. 2019, pp. 1–6.

[126] B. Zheng, M. O. Sayin, C.-W. Lin, S. Shiraishi, and Q. Zhu, "Timing and security analysis of VANET-based intelligent transportation systems: (Invited paper)," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2017, pp. 984–991.

[127] I. A. Sumra, J. L. Ab Manan, and H. Hasbullah, "Timing attack in vehicular network," in *Proc. Recent Res. Comput. Sci.-Proc. 15th WSEAS Int. Conf. Comput., 15th WSEAS CSCC Multiconf.* Stevens Point, WI, USA: World Scientific and Engineering Academy and Society (WSEAS), 2011, pp. 151–155.

[128] A. Arsalan and R. A. Rehman, "Prevention of timing attack in software defined named data network with VANETs," in *Proc. Int. Conf. Frontiers Inf. Technol. (FIT)*, Dec. 2018, pp. 247–252.

[129] D. S. Reddy, V. Bapuji, A. Govardhan, and S. S. V. N. Sarma, "Sybil attack detection technique using session key certificate in vehicular ad hoc networks," in *Proc. Int. Conf. Algorithms, Methodol., Models Appl. Emerg. Technol. (ICAMMAET)*, Feb. 2017, pp. 1–5.

[130] K. E. Defrawy and G. Tsudik, "Privacy-preserving location-based on-demand routing in MANETs," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 1926–1934, Dec. 2011.

[131] K. Rabieh, M. M. E. A. Mahmoud, T. N. Guo, and M. Younis, "Cross-layer scheme for detecting large-scale colluding sybil attack in VANETs," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 7298–7303.

[132] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: Detecting Sybil attacks in urban vehicular networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 6, pp. 1103–1114, Jun. 2012.

[133] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, and Y. Park, "Authentication protocols in Internet of vehicles: Taxonomy, analysis, and challenges," *IEEE Access*, vol. 8, pp. 54314–54344, 2020.

[134] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Gener. Comput. Syst.*, vol. 84, pp. 216–227, Jul. 2018.
[135] S. Tangade, S. S. Manvi, and P. Lorenz, "Decentralized and scalable privacy-preserving authentication scheme in VANETs," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8647–8655, Sep. 2018.
[136] L. Zhang, "OTIBAAGKA: A new security tool for cryptographic mix-zone establishment in vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 12, pp. 2998–3010, Dec. 2017.
[137] M. R. Asaar, M. Salmasizadeh, W. Susilo, and A. Majidi, "A secure and efficient authentication technique for vehicular ad-hoc networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 5409–5423, Jun. 2018.
[138] X. Yue, B. Chen, X. Wang, Y. Duan, M. Gao, and Y. He, "An efficient and secure anonymous authentication scheme for VANETs based on the framework of group signatures," *IEEE Access*, vol. 6, pp. 62584–62600, 2018.
[139] C. Zhang, X. Xue, L. Feng, X. Zeng, and J. Ma, "Group-signature and group session key combined safety message authentication protocol for VANETs," *IEEE Access*, vol. 7, pp. 178310–178320, 2019.
[140] Y. Jiang, S. Ge, and X. Shen, "AAAS: An anonymous authentication scheme based on group signature in VANETs," *IEEE Access*, vol. 8, pp. 98986–98998, 2020.
[141] Z. Benyamina, K. Benahmed, and F. Bounaama, "ANEL: A novel efficient and lightweight authentication scheme for vehicular ad hoc networks," *Comput. Netw.*, vol. 164, Dec. 2019, Art. no. 106899.
[142] P. Cincilla, O. Hicham, and B. Charles, "Vehicular PKI scalability-consistency trade-offs in large scale distributed scenarios," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2016, pp. 1–8.
[143] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Advances in Cryptology—EUROCRYPT 2003*, E. Biham, Ed. Berlin, Germany: Springer, 2003, pp. 416–432.
[144] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE 27th Conf. Comput. Commun. (INFOCOM)*, Apr. 2008, pp. 1229–1237.
[145] Z. Gong, Y. Long, X. Hong, and K. Chen, "Two certificateless aggregate signatures from bilinear maps," in *Proc. 8th ACIS Int. Conf. Softw. Eng., Artif. Intell., Netw., Parallel/Distrib. Comput. (SNPD)*, vol. 3, Jul. 2007, pp. 188–193.
[146] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.
[147] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 86–96, Jan. 2012.
[148] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.
[149] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for VANETs with batch verification," *Wireless Netw.*, vol. 21, no. 5, pp. 1733–1743, Jul. 2015.
[150] N.-W. Lo and J.-L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 5, pp. 1319–1328, May 2016.
[151] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey," *Veh. Commun.*, vol. 16, pp. 45–61, Apr. 2019.
[152] T. Limbasiya and D. Das, "Secure message confirmation scheme based on batch verification in vehicular cloud computing," *Phys. Commun.*, vol. 34, pp. 310–320, Jun. 2019.
[153] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 3, pp. 516–526, Mar. 2017.
[154] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, "Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response," *IEEE Trans. Comput.*, vol. 65, no. 8, pp. 2562–2574, Aug. 2016.
[155] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 4, pp. 1606–1617, May 2010.
[156] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, and B. Liu, "Practical secure and privacy-preserving scheme for value-added applications in VANETs," *Comput. Commun.*, vol. 71, pp. 50–60, Nov. 2015.
[157] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J. Hubaux, "Mix-zones for location privacy in vehicular networks," in *Proc. 1st Int. Workshop Wireless Netw. Intell. Transp. Syst. (WiN-ITS)*, 2007.
[158] M. Jadliwala, I. Bilogrevic, and J.-P. Hubaux, "Optimizing mix-zone coverage in pervasive wireless networks1," *J. Comput. Secur.*, vol. 21, no. 3, pp. 317–346, Jul. 2013.
[159] Y. Liu, L. Wang, and H.-H. Chen, "Message authentication using proxy vehicles in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3697–3710, Aug. 2015.
[160] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *Proc. Mobile Netw. Veh. Environ.*, May 2007, pp. 103–108.
[161] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. IEEE 27th Conf. Comput. Commun. (INFOCOM)*, Apr. 2008, pp. 246–250.
[162] S. Bittl, K. Roscher, and A. A. Gonzalez, "Security overhead and its impact in VANETs," in *Proc. 8th IFIP Wireless Mobile Netw. Conf. (WMNC)*, Oct. 2015, pp. 192–199.
[163] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Veh. Commun.*, vol. 9, pp. 19–30, Jul. 2017.
[164] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 770–790, 1st Quart., 2018.
[165] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future intelligent and secure vehicular network toward 6G: Machine-learning approaches," *Proc. IEEE*, vol. 108, no. 2, pp. 292–307, Feb. 2020.
[166] J. Wang, C. Jiang, H. Zhang, Y. Ren, K.-C. Chen, and L. Hanzo, "Thirty years of machine learning: The road to Pareto-optimal wireless networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1472–1514, 3rd Quart., 2020.
[167] M. A. Hossain, R. M. Noor, K.-L.-A. Yau, S. R. Azzuhri, M. R. Z'aba, and I. Ahmedy, "Comprehensive survey of machine learning approaches in cognitive radio-based vehicular ad hoc networks," *IEEE Access*, vol. 8, pp. 78054–78108, 2020.
[168] L. Liang, H. Ye, and G. Y. Li, "Toward intelligent vehicular networks: A machine learning framework," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 124–135, Feb. 2019.
[169] E. Eziama, K. Tepe, A. Balador, K. S. Nwizege, and L. M. S. Jaimes, "Malicious node detection in vehicular ad-hoc network using machine learning and deep learning," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, pp. 1–6.
[170] S. So, P. Sharma, and J. Petit, "Integrating plausibility checks and machine learning for misbehavior detection in VANET," in *Proc. 17th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2018, pp. 564–571.
[171] S. Gyawali, Y. Qian, and R. Q. Hu, "Machine learning and reputation based misbehavior detection in vehicular communication networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 8871–8885, Aug. 2020.
[172] T. Zhang and Q. Zhu, "Distributed privacy-preserving collaborative intrusion detection systems for VANETs," *IEEE Trans. Signal Inf. Process. Over Netw.*, vol. 4, no. 1, pp. 148–161, Mar. 2018.
[173] M. Hanselmann, T. Strauss, K. Dormann, and H. Ulmer, "CANet: An unsupervised intrusion detection system for high dimensional CAN bus data," *IEEE Access*, vol. 8, pp. 58194–58205, 2020.
[174] R. Xing, Z. Su, and Y. Wang, "Intrusion detection in autonomous vehicular networks: A trust assessment and Q-learning approach," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2019, pp. 79–83.
[175] L. Xiao, X. Lu, D. Xu, Y. Tang, L. Wang, and W. Zhuang, "UAV relay in VANETs against smart jamming with reinforcement learning," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4087–4097, May 2018.
[176] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Veh. Commun.*, vol. 23, Jun. 2020, Art. no. 100214.
[177] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2016, pp. 770–778.
[178] 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, Switzerland: Springer, 2018, pp. 318–337.

[179] M. Usama, J. Qadir, A. Raza, H. Arif, K.-L.-A. Yau, Y. Elkhatib, A. Hussain, and A. Al-Fuqaha, "Unsupervised machine learning for networking: Techniques, applications and research challenges," *IEEE Access*, vol. 7, pp. 65579–65615, 2019.
[180] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," *Appl. Sci.*, vol. 9, no. 20, p. 4396, Oct. 2019.
[181] G. Casolla, S. Cuomo, V. S. D. Cola, and F. Piccialli, "Exploring unsupervised learning techniques for the Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 4, pp. 2621–2628, Apr. 2020.
[182] A. Taylor, S. Leblanc, and N. Japkowicz, "Anomaly detection in automobile control network data with long short-term memory networks," in *Proc. IEEE Int. Conf. Data Sci. Adv. Anal. (DSAA)*, Oct. 2016, pp. 130–139.
[183] M. Weber, G. Wolf, E. Sax, and B. Zimmer, "Online detection of anomalies in vehicle signals using replicator neural networks," in *Proc. 6th ESCAR USA*, 2018, p. 14.
[184] 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 Veh. Technol. Mag.*, vol. 13, no. 2, pp. 94–101, Jun. 2018.
[185] L. H. Gilpin, D. Bau, B. Z. Yuan, A. Bajwa, M. Specter, and L. Kagal, "Explaining explanations: An overview of interpretability of machine learning," in *Proc. IEEE 5th Int. Conf. Data Sci. Adv. Analytics (DSAA)*, Oct. 2018, pp. 80–89.
[186] F. Hussain, S. A. Hassan, R. Hussain, and E. Hossain, "Machine learning for resource management in cellular and IoT networks: Potentials, current solutions, and open challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1251–1275, 2nd Quart., 2020.
[187] G. Arfaoui, P. Bisson, R. Blom, R. Borgaonkar, H. Englund, E. Félix, F. Klaedtke, P. Kumar Nakarmi, M. Näslund, P. O'Hanlon, J. Papay, J. Suomalainen, M. Surridge, J.-P. Wary, and A. Zahariev, "A security architecture for 5G networks," *IEEE Access*, vol. 6, pp. 22466–22479, 2018.
[188] 5G Automotive Vision. (2015). *The 5G Infrastructure Public Private Partnership*. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White-Paper-on-Automotive-Vertical-Sectors.pdf%0Ahttps://5g-ppp.eu/white-papers/
[189] R. Lu, L. Zhang, J. Ni, and Y. Fang, "5G vehicle-to-everything services: Gearing up for security and privacy," *Proc. IEEE*, vol. 108, no. 2, pp. 373–389, Feb. 2020.
[190] Y. Yang and K. Hua, "Emerging technologies for 5G-enabled vehicular networks," *IEEE Access*, vol. 7, pp. 181117–181141, 2019.
[191] C. Lai, R. Lu, D. Zheng, and X. Shen, "Security and privacy challenges in 5G-enabled vehicular networks," *IEEE Netw.*, vol. 34, no. 2, pp. 37–45, Mar. 2020.
[192] S. Shin, L. Xu, S. Hong, and G. Gu, "Enhancing network security through software defined networking (SDN)," in *Proc. 25th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Aug. 2016, pp. 1–9.
[193] I. Farris, T. Taleb, Y. Khettab, and J. Song, "A survey on emerging SDN and NFV security mechanisms for IoT systems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 812–837, 1st Quart., 2019.
[194] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in software defined networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2317–2346, Fou. 2015.
[195] M. Condoluci and T. Mahmoodi, "Softwarization and virtualization in 5G mobile networks: Benefits, trends and challenges," *Comput. Netw.*, vol. 146, pp. 65–84, Dec. 2018.
[196] L. V. Morales, A. F. Murillo, and S. J. Rueda, "Extending the floodlight controller," in *Proc. IEEE 14th Int. Symp. Netw. Comput. Appl.*, Sep. 2015, pp. 126–133.
[197] P. Porras, S. Cheung, M. Fong, K. Skinner, and V. Yegneswaran, "Securing the software defined network control layer," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2015.
[198] J.-S. Weng, J. Weng, Y. Zhang, W. Luo, and W. Lan, "BENBI: Scalable and dynamic access control on the northbound interface of SDN-based VANET," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 822–831, Jan. 2019.
[199] C. Campolo, A. Molinaro, A. Iera, and F. Menichella, "5G network slicing for Vehicle-to-Everything services," *IEEE Wireless Commun.*, vol. 24, no. 6, pp. 38–45, Dec. 2017.
[200] 3GPP. (2020). *Release 16*. pp. 3–6. [Online]. Available: https://www.3gpp.org/release-16
[201] *ETSI GR NGP 011 V1.1.1: Next Generation Protocols (NGP); E2E Network Slicing Reference Framework and Information Model*, ETSI, Sophia Antipolis, France, 2018, pp. 1–32.
[202] I. T. S. Sector. (2018). *Y.3112: Framework for the Support of Network Slicing in the IMT-2020 Network*. [Online]. Available: https://www.itu.int/rec/T-REC-Y.3112-201812-I
[203] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2429–2453, 3rd Quart., 2018.
[204] C. Campolo, R. Fontes, A. Molinaro, C. E. Rothenberg, and A. Iera, "Slicing on the road: Enabling the automotive vertical through 5G network softwarization," *Sensors*, vol. 18, no. 12, p. 4435, Dec. 2018.
[205] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: A review," *China Commun.*, vol. 14, no. 12, pp. 1–14, Dec. 2017.
[206] J. D. Vega Sanchez, L. Urquiza-Aguiar, and M. C. Paredes Paredes, "Physical layer security for 5G wireless networks: A comprehensive survey," in *Proc. 3rd Cyber Secur. Netw. Conf. (CSNet)*, Oct. 2019, pp. 122–129.
[207] L. Sun, K. Tourki, Y. Hou, and L. Wei, "Safeguarding 5G networks through physical layer security technologies," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–2, Sep. 2018.
[208] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.
[209] H. Song, H. Wen, J. Tang, Y. Chen, F. Xie, R.-F. Liao, and S. Chen, "PLS-based secrecy transmission for VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7596–7608, Jul. 2020.
[210] B. M. ElHalawany, A. A. A. El-Banna, and K. Wu, "Physical-layer security and privacy for Vehicle-to-Everything," *IEEE Commun. Mag.*, vol. 57, no. 10, pp. 84–90, Oct. 2019.
[211] Y. Zhu, L. Wang, K.-K. Wong, and R. W. Heath, "Secure communications in millimeter wave ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3205–3217, May 2017.
[212] W. Ben Jaballah, M. Conti, and C. Lal, "A survey on software-defined VANETs: Benefits, challenges, and future directions," *CoRR*, vol. abs/1904.0, pp. 1–17, Apr. 2019.
[213] W. Ben Jaballah, M. Conti, and C. Lal, "Security and design requirements for software-defined VANETs," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107099.

AYYOUB LAMSSAGGAD received the M.S. degree in information systems security from the School of Applied Sciences, University of Ibn Tofail, Morocco, in 2019. He is currently pursuing the Ph.D. degree with the Faculty of Sciences, Moulay Ismail University, Morocco. His research interest includes security in intelligent transportation systems.

NABIL BENAMAR is currently an Associate Professor of computer networks. He is an IPv6 expert (he.net certified) and IPv6 trainer with many international organizations, such as RIPE/MENOG, AFRINIC, and Agence Universitaire de Francophonie. He became an Expert in Internet Governance after completion of ISOC Next generation e-learning program. He has authored or coauthored several journal articles in highly ranked journals and conferences. He has authored an RFC and other IETF Internet documents. His main research topics are IPv6, vehicular networks, ITS, DTNs, and IoT. He is a member of G6 Association for IPv6 and one of the contributors to the IPv6 MOOC. He is also a TPC member in different IEEE flagship conferences, including Globecom, ICC, and PIMRC. He is an ISOC Ambassador to IGF in 2012 and 2013, a Google Panelist in the first Arab-IGF, an ISOC Fellow of IETF'89, IETF'92, IETF'95, IETF'99, and ICANN'50 and ICANN'54. He is the Chair of the Task Force for Arabic IDNs. He is an Associate Editor of IEEE Access and *Wireless Communications and Mobile Computing*, and a reviewer of different journals.

ABDELHAKIM SENHAJI HAFID spent several years as a Senior Research Scientist with Bell Communications Research (Bellcore), NJ, USA, working in the context of major research projects on the management of next generation networks. He was also an Assistant Professor with Western University (WU), Canada, the Research Director with the Advance Communication Engineering Center (venture established by WU, Bell Canada, and Bay Networks), Canada, a Researcher with CRIM, Canada, a Visiting Scientist with GMD-Fokus, Germany, and a Visiting Professor with the University of Evry, France. He is currently a Full Professor with the University of Montreal. He is the Founding Director of the Network Research Laboratory and Montreal Blockchain Laboratory. He is also a Research Fellow with CIRRELT, Montreal, Canada. He co-founded Tipot Technologies, Inc. (research and development platform for IoT). He consulted for a number of telecommunication companies and startups in North America. He has extensive academic and industrial research experience in the area of the management and design of next generation networks. He supervised to graduation over 50 graduate and postgraduate students. He has authored or coauthored over 250 journal and conference papers. He also holds three U.S. patents. His current research interests include the IoT, fog/edge computing, blockchain, and intelligent transport systems. He also gave talks/keynotes in a number of international conferences.

MOUNIRA MSAHLI received the M.Sc. degree in network from Pierre and Marie Curie University, France, and the Ph.D. degree from Télécom Paris, Paris. She is currently an Associate Professor with the Network and Computer Science Department (INFRES), Télécom Paris, Paris, a member of the CCN Research Team, and the Co-Head of the postmaster's degree in digital enterprise architecture. Her current research interests include the areas of vehicular network security and the use of IA for cybersecurity.