IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 26 February 2024, accepted 9 May 2024, date of publication 20 May 2024, date of current version 30 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3402946

SURVEY

Safeguarding the V2X Pathways: Exploring the Cybersecurity Landscape Through Systematic Review

KEVIN HERMAN MURARO GULARTE[1], JOSÉ ALFREDO RUIZ VARGAS[1,2], (Member, IEEE), JOÃO PAULO JAVIDI DA COSTA[1,2,3,4], (Senior Member, IEEE), ANTONIO SANTOS DA SILVA[2,4,5,6], GIOVANNI ALMEIDA SANTOS[2], YUMING WANG[2], CHRISTIAN ALFONS MÜLLER[7], CHRISTOPH LIPPS[8], (Member, IEEE), RAFAEL TIMÓTEO DE SOUSA JÚNIOR[3], (Senior Member, IEEE), WALTER DE BRITTO VIDAL FILHO[9], PHILIPP SLUSALLEK[7,10], AND HANS DIETER SCHOTTEN[8,11], (Member, IEEE)

[1]Graduate Program in Mechatronic Systems (PPMEC), University of Brasília (UnB), Brasília 70910-900, Brazil
[2]Department 2 Lippstadt, Hamm-Lippstadt University of Applied Sciences (HSHL), 59063 Hamm, Germany
[3]Professional Postgraduate Program in Electrical Engineering (PPEE), University of Brasília (UnB), Brasília 70910-900, Brazil
[4]Graduate School for Applied Research in North Rhine-Westphalia (PK NRW), 44801 Bochum, Germany
[5]Karlsruhe Institute of Technology (KIT), 76133 Karlsruhe, Germany
[6]Graduate Program in Computing (PPGC), Federal University of Rio Grande do Sul (UFRGS), Porto Alegre 91501-970, Brazil
[7]German Center for Artificial Intelligence (DFKI), 66123 Saarbrücken, Germany
[8]German Center for Artificial Intelligence (DFKI), 67663 Kaiserslautern, Germany
[9]Department of Mechanical Engineering, University of Brasília (UnB), Brasília 70910-900, Brazil
[10]Computer Graphics Lab, Saarland University, 66123 Saarbrücken, Germany
[11]Department of Electrical and Computer Engineering, University of Kaiserslautern-Landau (RPTU), 67663 Kaiserslautern, Germany

Corresponding author: José Alfredo Ruiz Vargas (vargas@unb.br)

This work was suported in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior–Brasil (CAPES) under Grant 001, in part by the University of Brasília, and in part by the Bundesamt für Sicherheit in der Informationstechnik (BSI) through the project Beyond 5G Virtuelle Umgebung für Cybersicherheitstests von V2X-Systemen (B5GCyberTestV2X).

ABSTRACT Vehicle-to-Everything (V2X) communication, essential for enhancing road safety, driving efficiency, and traffic management, must be robust against cybersecurity threats for successful deployment and acceptance. This survey comprehensively explores V2X security challenges, focusing on prevalent cybersecurity threats such as jamming, spoofing, Distributed Denial of Service (DDoS), and eavesdropping attacks. These threats were selected due to their prevalence and ability to compromise the integrity and reliability of V2X systems. Jamming can disrupt communications, spoofing can lead to data and identity manipulation, DDoS attacks can saturate system resources, and eavesdropping can compromise user privacy and information confidentiality. Addressing these major threats ensures that V2X systems are robust and secure for successful deployment and widespread acceptance. This work makes significant contributions to the field of V2X cybersecurity, starting with a thorough review and categorization of existing survey papers, providing a clear map of the current research landscape, and identifying areas needing further study. An extensive review uncovered a global landscape of V2X cybersecurity research. We highlight contributions from the leading countries in scientific publications and patent innovations, with notable advancements from leading corporations. This work educates and informs on the current state of V2X cybersecurity and identifies emerging trends and future research directions based on a year-by-year analysis of the literature and patents. The findings underscore the evolving cybersecurity landscape in V2X systems and the importance of continued innovation and research in this critical field. The survey navigates the complexities of securing V2X communications, emphasizing the necessity for advanced security protocols and technologies, and highlights innovative approaches within the global scientific and patent research context. By providing a panoramic view of the field, this survey sets the stage for future advancements in V2X cybersecurity.

The associate editor coordinating the review of this manuscript and approving it for publication was Diana Gratiela Berbecaru.

INDEX TERMS Vehicle-to-everything, connected and automated vehicle, intellectual property in V2X cybersecurity, cyberattacks and attacks, V2X security.

I. INTRODUCTION

The levels of automation defined by the Society of Automotive Engineers (SAE) aptly capture the communication and connectivity aspect by outlining vehicles not only as transportation means but also as sophisticated hubs of connectivity and data exchange [1], [2]. From basic automation to full autonomy, such a shift mirrors the aspirations of society for safer, secure, intelligent, and efficient roadways. In this context, Vehicle-to-Everything (V2X) communication is vital in increasing safety and efficiency in autonomous vehicles by relying on rapid information exchange for cooperative and responsive driving [3]. As a result, V2X communication technology (CT) is increasingly recognized as a disruptive instrument for enhancing roadway safety and optimizing transportation [4]. Given its capabilities, V2X has captured significant interest for its role in ensuring the safety of both drivers and pedestrians, effectively orchestrating traffic movements, and introducing cutting-edge services [5], [6], [7]. As detailed in Table 1 and depicted in Figure 1, V2X is a framework including a variety of communication modalities, which are differentiated into specific categories [8], [9], [10], [11], [12], [13]. In Table 1, we present the definition of the five types of V2X communications, namely, Vehicle-to-Vehicle (V2V), Vehicle-to-Person/Pedestrian (V2P), Vehicle-to-Infrastructure (V2I), Vehicle-to-Network (V2N), and Vehicle-to-Grid (V2G).

TABLE 1. Five types of V2X communications, namely, V2V, V2P, V2I, V2N, and V2G.

V2X Type	Details
Vehicle-to-Vehicle	Direct interaction between vehicles
Vehicle-to-Person/Pedestrian	Interaction between vehicles and Vulnerable Road Users, such as pedestrians or cyclists
Vehicle-to-Infrastructure	Communication between vehicles and infrastructure components, such as traffic lights
Vehicle-to-Network	Connectivity between vehicles and network entities through a mobile network base station
Vehicle-to-Grid	Technology enabling Electric Vehicles to communicate and interact with the power grid

Figure 1 provides a detailed visualization of the five types of V2X communication, underscoring their significance in supporting various Driving Use Cases (DUCs) [14]. Among these, three key DUCs, adapted from the 3rd Generation Partnership Project (3GPP) [14], are prominently featured: 1) Left Turn Assist; 2) Vulnerable Road Users (VRU) alerts at blind intersections, and 3) Do Not Pass Warning (marked in Figure 1 corresponding to this numbering). This emphasis on these DUCs, in line with 3GPP guidelines, highlights their relevance in enhancing road safety in diverse driving scenarios. The Left Turn Assist is essential at intersections, facilitating safe left turns through real-time traffic information. VRU alerts ensure pedestrian safety at blind intersections by alerting drivers about obscured pedestrians or cyclists. Finally, the Do Not Pass Warning acts as a critical safety alert on both straight and curved roads, advising drivers against risky overtaking maneuvers [14].

Various situations can lead to accidents in many driving scenarios, including obstructed visibility due to other vehicles, the absence of traffic lights or adequate signage, and the recklessness of human drivers. Vehicles can exchange messages directly via V2V communication and messages with an Intelligent Transport System (ITS) through V2N communication to obtain more accurate information about traffic in the vicinity of the intersection in Left Turn Assist. The VRU Alerts at a Blind Intersection DUC is characterized by V2P communication, enabling the vehicle to communicate with devices carried by the pedestrian. This facilitates the vehicle to acquire information related to the position of the pedestrian, even when an obstruction hinders visual perception by the vehicle sensors, such as a camera or Light Detection and Ranging (LiDAR). In addition to V2P communication, this use case can also leverage V2I communication, allowing, for instance, the vehicle to receive messages from monitoring cameras supporting the detection of VRUs installed along the road. The Do Not Pass Warning DUC aims to assist vehicles during overtaking attempts, generating an alert if a dangerous situation is perceived, hindering the safe execution of the maneuver. In the specific scenario illustrated by marker 3 in Figure 1, the presence of a truck obstructs the view of a vehicle attempting to overtake. In contrast, another vehicle approaches from the opposite direction. Different V2X communication types, such as V2V and V2I, can be employed to provide the involved vehicles with additional information necessary for more precise decision-making.

Supporting the scenarios in Figure 1 requires a robust Information and Communication Technological (ICT) infrastructure. According to the 3GPP, Fifth-Generation (5G) technology, with ultra-low delay, ultra-high reliability, and ultra-large bandwidth, emerges as a pivotal enabler for reliable V2X communication [15]. Through V2X, vehicles are poised to share information in real time, making decisions that are timely, informed, and cooperative [7], [16]. However, the benefits of this hyper-connectivity are fraught with challenges. The risk escalates as vehicles transition from full-assistance modes to fully autonomous within the network [17]. Also, as V2X systems open communication channels with external entities, from vehicles to networks, infrastructure, other vehicles, pedestrians, or the electric grid, the susceptibility to cyber threats rises. The potential weaknesses in the remote control features of intelligent vehicles have garnered significant attention and concern from society [18]. As vehicles become more intelligent and interconnected, their security worries escalate, mirroring the

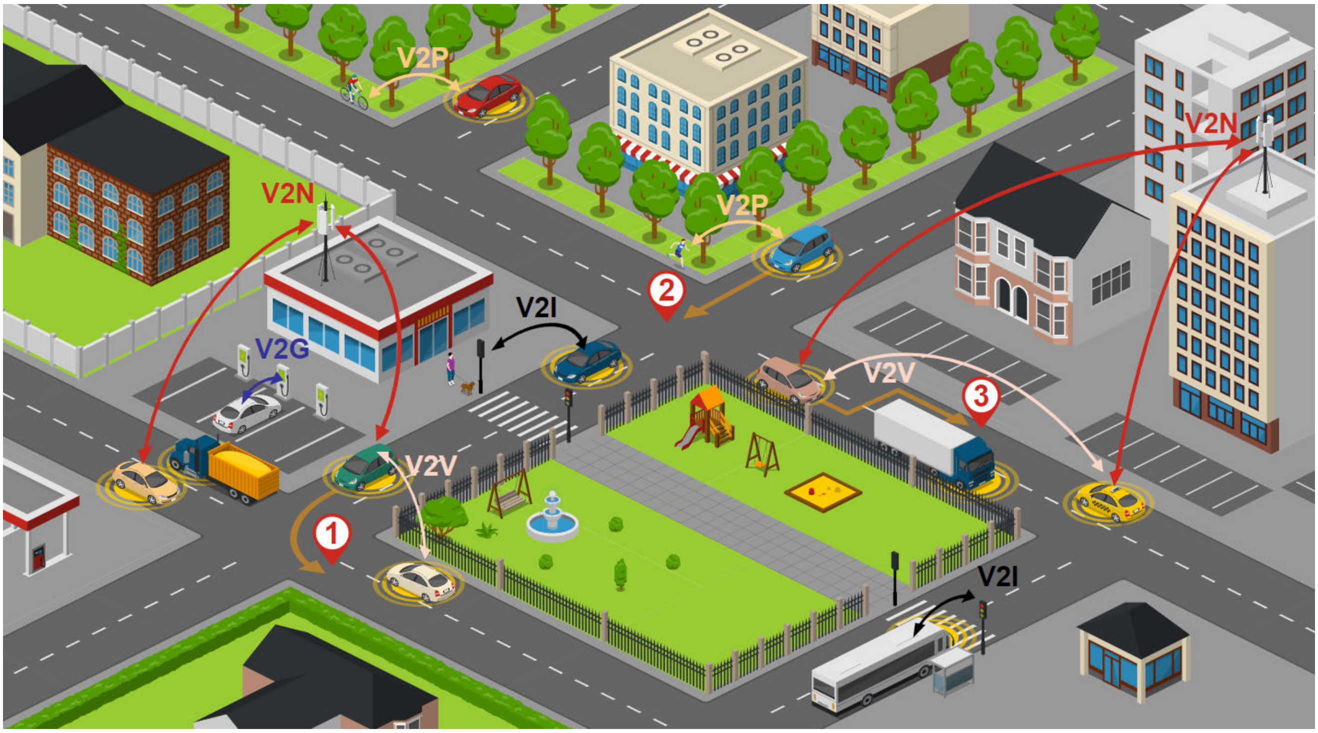


FIGURE 1. Representation of the V2X Communication Types V2V, V2G, V2I, V2P and V2N, and the DUCs Left Turn Assist (marker 1), VRU alerts at a blind intersection (marker 2), and Do not pass warning (marker 3).

significant security hurdles confronted by smartphones [18]. In addition, 5G network infrastructure is vulnerable to different kinds of cyber threats, potentially leading to data breaches and corruption [9].

Jamming and spoofing attacks, in particular, pose grave concerns to V2X communication. Jamming seeks to disrupt by overwhelming the communication channels, generally with noise. Another possibility is that the attacker interferes with the communication channel using a strong Radio Frequency (RF) signal with the same frequency occupying the channel with illegitimate traffic [19]. On the other hand, spoofing is an attack attempting to deceive while disguising itself as a trustworthy source when it is not. In message spoofing attacks, attackers send false messages with inaccurate information to disrupt vehicular communications [20]. The implications of jamming and spoofing attacks are profound, potentially compromising the safety and the integrity of V2X systems [7], [16]. In addition to the jamming and spoofing attacks, which respectively aim to saturate communication channels and deceive systems by masquerading as trustworthy sources [19], [20], Distributed Denial of Service (DDoS) [21] and eavesdropping attacks also pose significant risks. DDoS attacks disrupt networks by flooding them with excessive messages, often orchestrated by a primary attacker [22]. Eavesdropping involves unauthorized interception of vehicular messages, compromising communication confidentiality [20]. These collective threats can significantly undermine the safety and efficiency of the V2X ecosystem. In this context, this work provides a clear, tutorial-like overview to bridge the knowledge gap and foster a broader understanding of the dynamic interplay between V2X and security.

A. CONTRIBUTIONS

This work outlines seven primary contributions to the field of V2X cybersecurity. The initial contribution involves a detailed review and categorization of existing survey papers within this domain, as outlined in Subsection I-C. This examination maps the current research landscape and identifies potential areas lacking in-depth study. The second contribution expands the scope to the market relevance of V2X security, analyzed through annual publication metrics and identification of key industry players, as detailed in Subsection II-B. This analysis, supported by a comprehensive review of patents, provides insight into the evolving significance of V2X security in the marketplace.

The third contribution, described in Subsection II-C, assesses the impact of financial investments in V2X security, offering insights into funding trends and strategic priorities. This evaluation helps to quantify the economic emphasis placed on V2X security endeavors. In the fourth contribution, we focus on the academic sphere, examining the volume of research related to V2X security attacks and defenses, as discussed in Subsection II-D. This analysis highlights the concentrated academic efforts to address V2X security challenges.

The fifth contribution, presented in Subsection II-E, compiles and analyzes data from Scopus, providing a global overview of research efforts in V2X security by examining data from various years, countries, and funding bodies. This comprehensive overview offers a global perspective on the research dynamics in this field. The sixth contribution segments into an in-depth exploration of specific security threats to V2X communication, namely jamming, spoofing, DDoS, and eavesdropping attacks, as elaborated in Sections III, IV, V, and VI. This detailed review enhances the understanding of these particular vulnerabilities within V2X systems. Finally, the seventh contribution summarizes additional cyber threats to V2X communication, focusing on emergent and less common vulnerabilities as summarized in Section VII. This contribution broadens the discourse on V2X security by shedding light on a wider array of potential threats.

B. SURVEY ORGANIZATION AND SCOPE

The organization of the work is shown in Figure 2, including all sections and their respective subsections. Section II shows an overview of the V2X security area, showing statistics about scientific publications, investments, and patents. Sections III, IV, V, and VI provide in-depth analysis and brief review of the literature on jamming, spoofing, DoS, and eavesdropping attacks, respectively. The reason for this is, as will be seen in Section II that these attacks are the most commonly found in scientific literature and patents. Section VII briefly shows additional cyberattacks that threaten security in V2X communication. Finally, the conclusions are drawn in Section VIII.

According to Figure 2, the introduction section is divided into three subsections, where in Subsection I-A, the main contributions of this article are summarized. Subsection I-B is related to the overall organization of the paper, defining the scope of the paper. Finally, Subsection I-C contains state-of-the-art research on security surveys related to V2X.

As presented in this survey, V2X communication, in particular the areas of V2X security, has gradually received the attention of the academy and industry worldwide. Hence, this work distinguishes itself from the conventional V2X surveys by offering an exploration into V2X nuances, specifically emphasizing security challenges such as jamming, spoofing, DDoS, and eavesdropping. Areas related to V2X, including security, tend to have technical terms found in several works in the literature. Thus, the abbreviations used in the V2X area of security are summarized in the Abbreviations Section.

C. RELATED SURVEYS TO V2X SECURITY

This section provides a consolidated review of previously published surveys pertinent to the topics of V2X cybersecurity. This subsection underscores the unique positioning and contributions of this work, affording a deeper understanding of the topics at hand and pinpointing gaps that still need to be addressed in the existing literature. The works [9], [10], [17], [18], [19], [20], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34] are survey works related to field V2X security. Table 2 details the similarity of ideas between different survey papers related to V2X security and classifies them into different categories.

As detailed in Table 2, the surveys are organized into four categories, each thoroughly explored in respective subsubsections, focusing on diverse aspects of V2X communication. This revised structure begins with the first category, which is an exploration of security and communication challenges in V2X, which is discussed in Subsubsection I-C1. Following this, the second category is the examination of emerging technologies, and the role of Artificial Intelligence (AI) and Internet of Things (IoT) in V2X is presented in Subsubsection I-C2. This section delves into how these technologies collectively enhance the security and efficiency of vehicular networks. The third category combines the advancements in network infrastructure with the integration of cellular technologies in Connected Vehicles (CV) and is discussed in Subsubsection I-C3. As outlined in Table 2, this section provides a comprehensive look at the technological evolution and the significant role of cellular networks in V2X communication. The fourth category is the standards and legislation in vehicular communication, which is elaborated in Subsubsection I-C4. This part of the paper analyzes the regulatory landscape, discussing how various standards and legislative measures shape the future of vehicular communication. Finally, Subsubsection I-C5 synthesizes the findings from the surveyed literature, offering concluding remarks and drawing comparisons between our survey and others in the field, underscoring the unique contributions and insights presented in our study.

1) SECURITY AND COMMUNICATION CHALLENGES IN V2X

Addressing the evolving landscape of vehicular communication, a multitude of studies, including [9], [10], [20], [22], [23], [25], [28], [29], [30], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], and [42], delve into the security and communication challenges inherent in V2X systems, as shown in Table 2. In particular, [35] provides an extensive overview of the V2X ecosystem, reviewing security and privacy issues, current standardization activities, and defense mechanisms within the V2X domain, highlighting the need for layered defense strategies to improve system resilience. This aligns with the collective emphasis of these works on robust security and efficient communication in increasingly complex vehicular networks. The integration of IoT and the potential of cellular technologies, as highlighted by [9] and [29], are pivotal in enhancing vehicular applications but also introduce new security challenges. The advent of 5G, discussed in [32], further amplifies these concerns, necessitating advanced and adaptive security strategies.

In this dynamic environment, as detailed in Table 2, the role of AI, particularly Explainable AI (XAI) as explored in [25], emerges as a key factor in strengthening V2X security. This is complemented by insights into communication performance issues in specific scenarios, such as on-ramp merging, addressed by [23]. Such targeted investigations reveal the nuanced nature of ensuring safety and efficiency in diverse

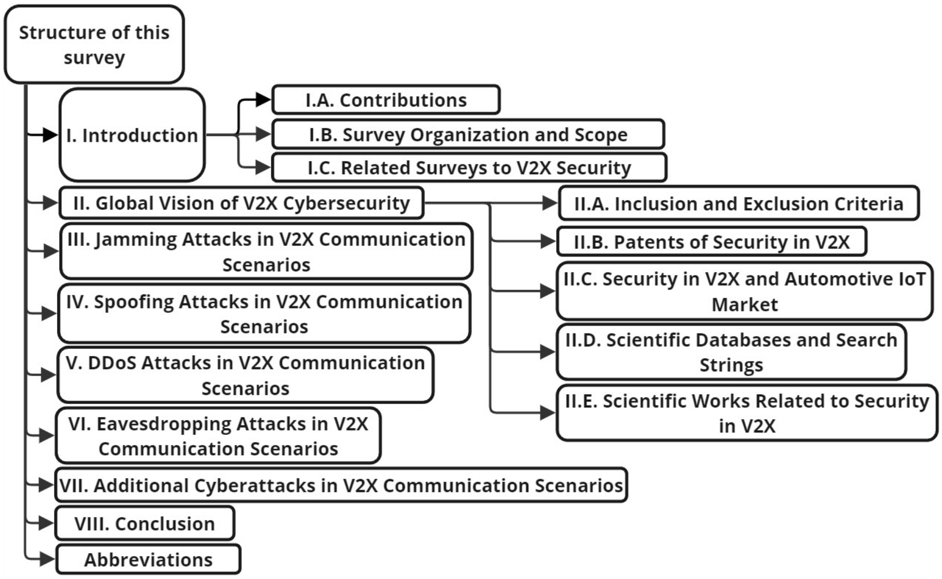


FIGURE 2. Organization of the survey.

TABLE 2. Papers surveys related to security in V2X grouped into four main topics: Security and Communication Challenges in V2X; Emerging Technologies and Role of AI and IoT in V2X; Advancements and Cellular Technologies for V2X Network Infrastructure; Standards and Legislation for V2X Vehicular Communication Security.

Topic	Description
Security and Communication Challenges in V2X	Papers such as [9], [10], [20], [22], [23], [25], [28]–[30], [32]–[42] focus on addressing security and communication challenges within V2X systems, including aspects related to autonomous vehicles and smart mobility. The emphasis is on robust security measures and reliable communication protocols for efficient and safe vehicular communication.
Emerging Technologies and Role of AI and IoT in V2X	Combining the realms of emerging technologies and the integration of AI and IoT, papers [17]–[19], [24], [25], [27], [31], [43]–[49] explore the potential of Software-Defined Networking (SDN), blockchain, AI, 5G, and IoT in enhancing V2X systems. These technologies are pivotal in augmenting security measures, creating Intelligent Transportation Systems (ITS), and providing comprehensive frameworks for threat mitigation.
Advancements and Cellular Technologies for V2X Network Infrastructure.	This category, merging advancements in network infrastructure with the utility of cellular technologies, includes papers [9], [17], [18], [20], [26], [28], [29], [32], [34], [50]–[52]. It discusses innovations such as blockchain, cellular communications, and advancements in vehicular networks that revolutionize V2X communications. The focus is on strategies to mitigate security threats and the role of cellular-based solutions in addressing communication challenges in V2X environments, including 5G advancements.
Standards and Legislation for V2X Vehicular Communication Security	Papers [10], [17], [18] examine existing standards and legislative measures in vehicular communication security. They identify gaps and propose enhancements to strengthen security and safety in vehicular communications, covering aspects of autonomous vehicles and comprehensive security strategies.

vehicular situations. Moreover, the focused discussions on autonomous vehicles and smart mobility in [20] and [30] integrate seamlessly into this broader narrative. They offer a lens through which the complexity of security in advanced autonomous systems can be viewed, underscoring the necessity for layered and sophisticated security frameworks. Complementing these perspectives, [10] and [19] bring in regulatory and AI-related aspects of vehicular network security. In contrast, [33] and [34] provide a more grounded view on implementing cryptographic and trust-based schemes in practical scenarios.

Also, [36] examines the spectrum of cyber-attacks and defenses in intelligent connected vehicles, reinforcing the critical need for enhanced security measures amidst the rapid technological evolution. Similarly, [37] focuses on the pivotal role of intrusion detection systems within intra-vehicle networks, underscoring a fundamental component of cybersecurity resilience. The exploration of pseudonymity in vehicular networks by [38] introduces a nuanced balance between security and privacy, exemplifying the complexities of V2X communications. Moreover, [39] provides insights into IP-based vehicular networking, illustrating how foundational communication protocols contribute to the overarching security architecture. In addition, [40] and [41] delve into the collaborative control systems of intelligent connected vehicles, shedding light on the communication security and testing challenges that are crucial for the development of reliable V2X interactions. Complementing these perspectives,

[42] employs knowledge mapping to forecast significant future research directions, including machine learning and V2X communication, which are essential for addressing security and efficiency in vehicular networks.

As systematically categorized in Table 2, these studies collectively paint a comprehensive picture of the security and communication challenges in V2X environments through this integrated approach. They highlight, in accordance with the structure depicted in Table 2, the importance of a multifaceted approach to security that accommodates the rapid technological advancements and the diverse needs of modern vehicular networks.

2) EMERGING TECHNOLOGIES AND ROLE OF AI AND IoT IN V2X

The confluence of emerging technologies in V2X, particularly 5G, AI, and IoT, is transforming the landscape of vehicular networks. Works [17] and [18] emphasize the critical role of 5G in revolutionizing vehicular network security, underscoring its capacity to enhance communication systems and integrate advanced technologies. This integration is pivotal in addressing the complex security challenges in V2X environments.

As explored in studies such as [19] and [25], the role of AI in vehicular networks extends to improving security measures and augmenting system efficiency. Reference [19] provides a detailed classification of V2X security threats and examines AI-driven solutions for their mitigation. Meanwhile, [25] discusses XAI in the context of Intelligent Connected Vehicles (ICVs), highlighting how AI enhances vehicular network security and transparency.

The transformative impact of IoT in V2X is also evident. Reference [31] discusses the integration of 5G and New Radio (NR) technology in V2X, illustrating how IoT contributes to developing more sophisticated and efficient vehicular communication systems. The collective insights from these studies underscore the importance of leveraging AI and IoT, along with emerging cellular technologies such as 5G, to tackle the security challenges in increasingly autonomous and smart vehicular systems.

It is worth noting that in the case of 5G, improvements in V2X communication security are achieved through advanced encryption and authentication protocols, network segmentation to limit unauthorized access, low latency, and high reliability. On the other hand, AI enables, for instance, the application of machine learning algorithms to detect anomalous patterns in V2X data traffic, allowing for the proactive identification and mitigation of attacks.

Adding to the discourse, [43] delves into the integration of cloud-controlled wireless networks and blockchain-based security mechanisms in CAVs, marking a significant step toward safer autonomous driving through lateral control and obstacle avoidance. Similarly, [44] outlines the effectiveness of C-V2X technology in mitigating accidents through advanced warning systems, showcasing the synergy between AI and network security. Furthermore, [45] highlights the role of IoT, edge intelligence, and blockchain in shaping a sustainable transportation ecosystem, pointing to a future where technology directly addresses the demands for safety, security, and reliability in AVs. Reference [46] expands this vision by exploring the radical changes expected from 5G and 6G technologies, emphasizing their potential to fulfill ubiquitous connectivity needs.

Moreover, [47] provides a critical analysis of technological gaps in autonomous driving, shedding light on the importance of V2X communications in enhancing road safety and efficiency. In [48], the discussion extends to connected vehicle architectures and the role of enabling technologies in fostering a collaborative, data-driven vehicle ecosystem. Lastly, [49] addresses the emerging communication and computational technologies in the context of plug-in electric vehicles, illustrating how advancements in machine learning and IoT are crucial for the development of V2G and G2V communications, thus further emphasizing the pivotal role of emerging technologies in the V2X paradigm.

3) ADVANCEMENTS AND CELLULAR TECHNOLOGIES FOR V2X NETWORK INFRASTRUCTURE

The intersection of advancements in network infrastructure and the incorporation of cellular technologies forms a cornerstone in the evolution of V2X systems. Works such as [17], [20], and [34] delve into the significant role of 5G in V2X, highlighting its potential to revolutionize vehicular network security and efficiency. Work [17] focuses on the architecture of 5G-V2X, while [20] addresses its application through a three-layer security model, underscoring the necessity for comprehensive security frameworks.

The evolution of cellular technologies within V2X, as discussed in [9] and [29], emphasizes the integration of IoT into cellular networks and the role of 3GPP standards in vehicular applications. These studies complement the insights on 5G-V2X provided by [32] and [34], which explore the practical implementation of V2X services supported by cellular networks and the security aspects of 3GPP 5G networks, respectively. Reference [26] introduces the role of blockchain technology in vehicular communications, particularly for audit and security purposes, adding a novel dimension to network infrastructure discussions. This perspective is crucial for understanding the broader implications of technological advancements in vehicular networks. Similarly, [28] expands the scope by surveying Vehicular Ad Hoc Networks (VANETs), exploring both architectural and security challenges, aligning with the overarching theme of evolving network infrastructures.

Conversely, [50] introduces the Multi-Radio Access Software-Defined Vehicular Networks (SDVN) concept, emphasizing the need for adaptable network management to support diverse vehicular applications. Similarly, [51] reviews the V2X operational modes in electric vehicles, highlighting the integration challenges and opportunities for enhancing grid services. Lastly, [52] explores the security implications of network slicing in 5G, which is crucial for supporting diverse V2X services while ensuring robust security measures.

Together, these studies paint a comprehensive picture of the ongoing transformation in V2X network infrastructure, marked by the integration of advanced cellular technologies such as 5G and blockchain. They highlight the continuous transition from Long-Term Evolution (LTE) V2X to more sophisticated 5G and Beyond 5G (B5G) systems, emphasizing the need for robust and scalable security solutions in this dynamic landscape.

4) STANDARDS AND LEGISLATION FOR V2X VEHICULAR COMMUNICATION SECURITY

This subsubsection focuses on the pivotal role of standards and legislative frameworks in vehicular communication as investigated in [10], [17], and [18], as shown in Table 2. These studies evaluate existing standards and legislative practices in vehicular communication security, pinpointing gaps and advocating for enhancements to bolster security and safety in this rapidly evolving field. Reference [10] offers a unique perspective on the legislative aspects of vehicular communication, especially within the European Union context. This paper highlights the necessity of aligning security standards with evolving legislative guidelines to ensure the harmonious development of vehicular communication technologies. In addition, [17] and [18] contribute significantly to the discourse by examining the impact of emerging technologies, such as 5G, on vehicular communication standards. Their work underscores the importance of updating and refining regulatory frameworks to accommodate the advancements and challenges presented by these new technologies.

5) CONCLUSION ON THE V2X SURVEYS

In synthesis, the surveys collectively highlight the growing importance of V2X communications in enhancing vehicular security and efficiency. However, with newer technologies such as B5G, and the increasing complexity of vehicular networks, ensuring security remains a constant concern. References [9], [10], [17], [18], [19], [20], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], and [34] propose innovative solutions, from blockchain integration to AI-driven mechanisms, showcasing the dynamic nature of the field and the constant pursuit of fortifying V2X security. As shown in Subsection I-C, the state of the art includes surveys dealing with V2X cybersecurity. However, there is a need for a more detailed overview of research and patents related to V2X security. Also, the literature needs to delve more deeply into the most common attacks in the context of V2X. Thus, this survey aims to fill out this gap in the area of V2X security, in particular, considering jamming, spoofing, DDoS, and eavesdropping.

II. GLOBAL VISION OF V2X CYBERSECURITY

This section provides a panoramic view to comprehensively understand the V2X security field, exploring findings from research articles indexed by Scopus, categorized by year, nation, and financial backers. It also reviews patents from the Scopus database and Google Patents. Furthermore, it includes studies from prominent academic databases, classifying them according to specific keywords or search queries.

This section is organized into five subsections. Subsection II-A briefly presents criteria for choosing papers and patents related to V2X security. Subsection II-B details the reasons, research bases, and comments on the results related to patents in V2X security. Subsection II-C presents information on financial investments in the area of V2X security and automotive cybersecurity. Tables showing the number of results found related to different tags in different relevant scientific bases are shown in the Subsection II-D. Subsection II-E shows various results related to papers found in scientific databases, showing results from different years, countries, and funding sponsors.

TABLE 3. Inclusion and exclusion criteria used in the papers selection procedure.

Counts	Inclusion criteria
1	Papers related to the subject security in V2X
2	Papers by titles, abstracts or keywords tags
Counts	**Exclusion criteria**
1	Duplicate studies

A. INCLUSION AND EXCLUSION CRITERIA

The selection of papers and patents is based on criteria delineated in Table 3.

a) Since the core of this study focuses on V2X and security, the main criterion for selection is its pertinence to the security field in V2X. The tags (“V2X” OR “vehicle-to-everything”) AND (“security” OR “cybersecurity”) are generally used.

b) The research shows that using “title, abstract, or keyword” tags produces fewer off-topic results than the “all fields” option. Therefore, the tag filtering is set to “title, abstract, or keyword”. The exception is patents in which the “all fields” tag filtering was chosen due to the lack of previous tag filtering.

c) Repetitions are excluded, as these are often just reiterations of original content found in lesser-known databases. This approach is primarily applied to the Google Scholar search, avoiding the “include citations” feature.

B. PATENTS OF SECURITY IN V2X

In the realm of V2X security, patents play a critical role. They serve as a tangible representation of innovations and progress within the sector. Evaluating patent trends uncovers ongoing Research and Development (R&D) directions and spotlights the primary movers and shakers of the industry. While scholarly articles share knowledge through theoretical frameworks and experimental findings, patents ground us in the real-world applications and the commercial side of things. Another facet to consider is that many ground-breaking technologies are patented and then detailed in academic journals. This sequence means patent reviews can sometimes preemptively unveil upcoming V2X security solutions. This

TABLE 4. Patents of security in V2X found in Google Patents and Scopus based on "all fields" filter criteria.

Year	Google Patents	% Google Patents	Scopus	% Scopus
2023	23457	36.12	8845	34.46
2022	16979	26.14	6662	25.96
2021	11192	17.23	4424	17.24
2020	7198	11.08	3003	11.70
2019	3413	5.26	1464	5.70
2018	1790	2.76	703	2.74
2017	571	0.88	353	1.38
2016	156	0.24	95	0.37
2015	66	0.10	44	0.17
2014	35	0.05	22	0.09
Pre-2014	86	0.13	52	0.20
Total	**64943**	**100.00**	**25667**	**100.00**

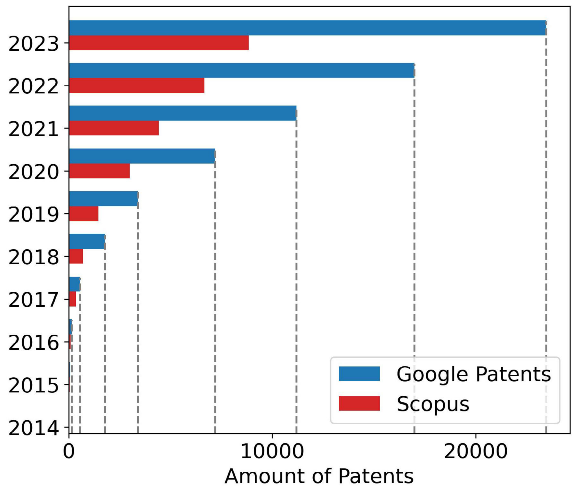


FIGURE 3. Patents in the security area in V2X separated by year and amount of patents.

patent-centric subsection aims to grant readers an encompassing view of V2X security, straddling academic insights and industrial progress.

Based on availability, accessibility, and extent of available data, we leaned on two primary repositories for our patent tally: a) Google Patents and b) Scopus, in the patent search function. All inquiries were carried out on a specific date, January 18, 2024, to maintain uniformity. The search criteria in Google Patents was the publication search parameter, indicating that results are recorded when an invention patent application was published, that is, made public. The search tags were ("V2X" OR "vehicle-to-everything") AND ("security" OR "cybersecurity"). Table 4 breaks down patents by year for a more granular understanding, while Figure 3 offer a visual digest of these findings. Both Table 4 and Figure 3 show that the number of patents in the area of V2X cybersecurity has grown significantly, signaling a heated market.

Our investigation highlighted several corporate entities with a strong patent portfolio. Their prominence and relative influence are detailed in Table 5. Table 5 also shows the headquarters of the different companies. It draws attention from Table 5 to the fact that 44.58 % of the patents are concentrated in just two companies: Qualcomm and LG Electronics. 84.55 % of the patents in this subsection are concentrated in seven companies: Qualcomm, LG, Huawei, Intel, Apple, Samsung, and Ericsson. Another interesting aspect is that only the companies in the top 10 have more than 1% of the total patents. The concentration of patents in two companies could be attributed to several factors. These companies may invest heavily in research and development (R&D), leading to more patent filings, or these companies may have strong intellectual property strategies. Furthermore, a few dominant players in the patent landscape could indicate industry specialization, in which bigger companies with more resources tend to dominate patent filings. It is important to say that it is possible that in Table 5, other companies could occupy the top 50 that the authors did not find.

In addition, what stands out is the recent upswing in patent registrations. Intriguingly, about 80% of these discoveries from Scopus data span just beyond a three years, hinting at a market in the midst of rapid expansion. There is, however, a variation in the volume of patents between Scopus and Google Patents, likely because Scopus adopts a stricter vetting process. However, this difference is a minor obstacle given our main aim to map out broad trends. Notably, the importance of each enterprise remains consistent across both databases, leading us to similar end insights. An important detail is that patents in the Scopus database cannot be searched by "title, abstract, or keyword," as can happen in scientific papers. This way, the search uses the "all fields" filter criteria. A consequence of this is that possibly many results found are not focused on the subject of security in V2X despite mentioning it. In this way, it is possible to have noisy data, that is, disconnected from the subject of V2X security, and the results found indicate only probable growth each year. This recognition underscores the importance of developing more refined methodologies for future research. As a suggestion for subsequent works, employing targeted strategies to mitigate these issues could significantly enhance the relevance and precision of data analysis. Such methodologies could include manual review processes or the application of more specific search criteria, aiming to focus exclusively on patents that directly pertain to the V2X security domain.

Note that the total amount of results in Table 5 is considerably high and, in the case of Scopus, is even higher than the total amount of results found in Table 4. The reason this happens is that the tags used in the global search ("V2X" OR "vehicle-to-everything") AND ("security" OR "cybersecurity") may encompass a wide range of patents, some of which may not be directly attributable to a specific company or may relate to diverse technologies and applications. On the other hand, when searching by company, the focus is on patents assigned explicitly to these entities, which can limit the scope. Another reason is that, in some cases, patents result from collaborations between multiple companies.

TABLE 5. Number of patents from different companies in the Google Patents and Scopus databases in the V2X security area.

	Companies	Country	Google Patents	% Google Patents	Scopus	% Scopus
1	Qualcomm	United States	15066	24.88	5868	19.41
2	LG	South Korea	11926	19.70	6258	20.70
3	Huawei	China	5615	09.27	2127	07.04
4	Intel	United States	5380	08.89	2343	07.75
5	Apple	United States	4726	07.81	2915	09.64
6	Samsung	South Korea	4652	07.68	1948	06.44
7	Ericsson	Sweden	3829	06.32	958	03.17
8	AMD	United States	2188	03.61	1215	04.02
9	Texas Instruments	United States	1356	02.24	976	03.23
10	Sony	Japan	947	01.56	798	02.64
11	Oppo	China	506	00.84	291	00.96
12	Lenovo	China	456	00.75	314	01.04
13	InterDigital	United States	450	00.74	182	00.60
14	Ford	United States	238	00.39	231	00.76
15	Nokia	Finland	209	00.35	198	00.65
16	Motional Ad Llc	United States	195	00.32	65	00.22
17	Convida Wireless	United States	185	00.31	183	00.61
18	Panasonic	Japan	180	00.30	288	00.95
19	Ofinno	United States	179	00.30	307	01.02
20	Denso	Japan	165	00.27	168	00.56
21	Hyundai	South Korea	162	00.27	161	00.53
22	ZTE	China	158	00.26	146	00.48
23	GM Global Technology Operations	United States	158	00.26	75	00.25
24	Toyota	Japan	148	00.24	162	00.54
25	NVIDIA	United States	146	00.24	218	00.72
26	DOCOMO	Japan	138	00.23	183	00.61
27	Volkswagen	Germany	116	00.19	85	00.28
28	Tesla	United States	108	00.18	155	00.51
29	Bosch	Germany	98	00.16	91	00.30
30	Asustek Computer	Taiwan	79	00.13	172	00.57
31	FG Innovation	China	76	00.13	122	00.40
32	Honda	Japan	75	00.12	75	00.25
33	Alphabet	United States	75	00.12	152	00.50
34	Mitsubishi	Japan	72	00.12	92	00.30
35	Philips	Netherlands	68	00.11	65	00.22
36	Comcast	United States	56	00.09	236	00.78
37	Blackberry Limited	Canada	47	00.08	120	00.40
38	Audi	Germany	44	00.07	33	00.11
39	BMW	Germany	43	00.07	41	00.14
40	Aptiv	Ireland	42	00.07	32	00.11
41	Ipla Holdings Inc.	United States	33	00.05	40	00.13
42	Geely	China	27	00.04	3	00.01
43	Mercedes	Germany	26	00.04	17	00.06
44	Siemens	Germany	19	00.03	19	00.06
45	ZF Friedrichshafen	Germany	19	00.03	6	00.02
46	Analog Devices	United States	18	00.03	27	00.09
47	Micron Technology	United States	16	00.03	24	00.08
48	Nissan	Japan	14	00.02	16	00.05
49	Hitachi	Japan	11	00.02	13	00.04
50	Cisco Systems	United States	10	00.02	17	00.06
-	**Total**	**-**	**60550**	**100.00**	**30231**	**100.00**

Table 6 shows different types of tags related to V2X security threats or attacks. Note from this table that there are many patents related to security related to V2X. The high number of results in Denial of Service (DoS) attacks may present a large number of noisy data due to the possibility of the word DoS being used in other contexts unrelated to V2X, even more so considering that these research bases are not case-sensitive. The concepts of each type of threat or attack are presented in detail in Section VII.

C. SECURITY IN V2X AND AUTOMOTIVE IoT MARKET

Insightful databases spotlight the significance of security in V2X in the context of financial commitments segmented by year. Drawing from the Statista resource [53], we have explored the financial infusions over multiple years, incorporating even upcoming forecasts. Two different surveys were carried out within the limitations of the platform. The first, carried out in january 2023, was to collect data on global financial investments in the V2X area, and its results can

TABLE 6. Searches for tags in the Google Patents and Scopus Patents database using different criteria.

Tag	Google Patents	Scopus
V2X*[a] AND ("security" OR "cybersecurity")	66418	26109
V2X*[a] AND ("attack" OR "attacks" OR "cyberattacks" OR "threat" OR "threats")	7047	3010
V2X*[a] AND ("Denial of Service" OR "DoS")	6140	2489
V2X*[a] AND ("jamming")	496	430
V2X*[a] AND ("spoofing")	280	412
V2X*[a] AND ("hacking")	255	383
V2X*[a] AND ("spamming")	237	15
V2X*[a] AND ("eavesdropping")	230	225
V2X*[a] AND ("Man-in-the-Middle" OR "MitM")	182	253
V2X*[a] AND ("viruses" OR "virus")	182	252
V2X*[a] AND ("replay attacks" OR "replay attack")	166	209
V2X*[a] AND ("malware" OR "malwares")	137	268
V2X*[a] AND ("Distributed Denial of Service" OR "DDoS")	117	176
V2X*[a] AND ("spam" OR "spams")	104	150
V2X*[a] AND ("masquerading" OR "impersonation attacks" OR "impersonation attack")	58	38
V2X*[a] AND ("sybil attacks" OR "sybil attack")	37	51
V2X*[a] AND ("phishing")	31	42
V2X*[a] AND ("trojans" OR "trojan")	34	67
V2X*[a] AND ("backdoor")	32	53
V2X*[a] AND ("ransomware")	28	48
V2X*[a] AND ("side-channel attacks" OR "side-channel attack")	22	37
V2X*[a] AND ("injection attacks" OR "injection attack")	20	22
V2X*[a] AND ("black hole" OR "blackhole" OR "black holes" OR "blackholes")	13	4
V2X*[a] AND ("physical layer attacks" OR "physical layer attack")	11	2
V2X*[a] AND ("timing attacks" OR "timing attack")	9	19
V2X*[a] AND ("Cross-Site Scripting" OR "XSS")	6	20
V2X*[a] AND ("Advanced Persistent Threats" OR "APTs")	6	8
V2X*[a] AND ("wormhole" OR "wormholes")	5	1
V2X*[a] AND ("SQL injection")	4	8
V2X*[a] AND ("zero-day exploits" OR "zero-day exploit")	2	5
V2X*[a] AND ("insider threats" OR "insider threat")	2	1

[a] "V2X*" represents the search terms ("V2X" OR "vehicle-to-everything").

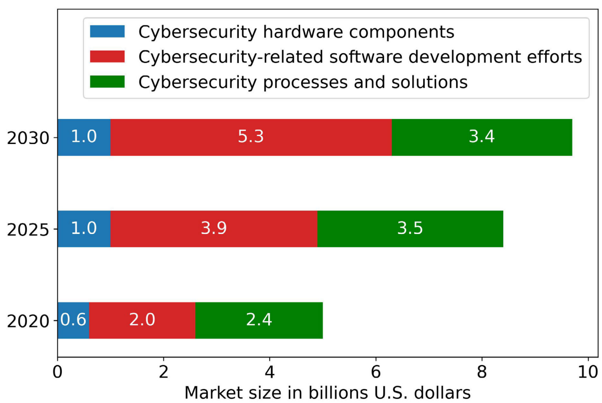


FIGURE 4. Automotive cybersecurity market size worldwide from Statista database [53].

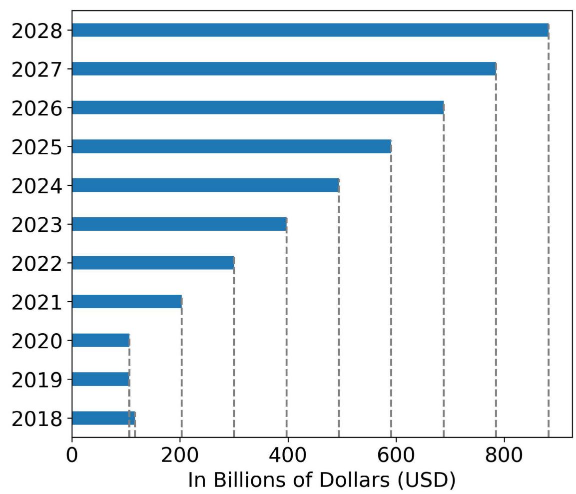


FIGURE 5. Financial investment in the security area in V2X worldwide from 2018 to 2028 from Statista database [53].

be seen in Figure 4. The second was carried out in August 2023 to obtain data on global financial investments in the area of automotive cybersecurity. Figure 5 shows the results of this second survey.

A closer inspection of Figures 4 and 5 reveals a consistent uptrend in investments, with predictions suggesting a fourfold increase from 2020 to 2030. An important observation is that according to Figure 5, in 2020, the total global investment in V2X was around 100 billion dollars. Figure 4 shows that, in 2020, the total investment in cyber security in automobiles alone was approximately 5 billion dollars. As the V2X security area is a subset of the automobile cybersecurity area, it is possible to infer through the combination of this data that the security area does not occupy more than 5% of the total investments made in the V2X area.

This estimation of 5% primarily considers cybersecurity-related software development efforts, encompassing measures for protecting against cyber threats, such as intrusion prevention systems and threat detection software. While it is acknowledged that countermeasures against jamming attacks include hardware components such as antenna arrays, these are part of broader hardware investments and are not confined solely to cybersecurity. Therefore, by concentrating on software development efforts for V2X security, it is deduced that these constitute a smaller fraction, at most 5%, of the total investment in V2X, which includes a wider range of technologies and infrastructure.

D. SCIENTIFIC DATABASES AND SEARCH STRINGS

Table 7 was drafted as a starting point for searches rooted in tags. It showcases an array of V2X-linked searches sourced from the Scopus academic database. Given the reputation of Scopus for exhaustive academic searches, it naturally became our chief source for the research. Our approach varied, sometimes scanning all content fields and narrowing the search to just the "title, abstract, or keyword" to minimize irrelevant hits. The outcomes of these foundational searches, documented on January 18, 2024, can be viewed in Table 7. It is unmistakable from the table that most of our hits were English-language entries, with Chinese works being the next most frequent, underlining the dominance of English in academic writing. Note that the rightmost column in Table 7 shows the number of V2X security works divided by total V2X works, providing something that suggests the percentage of security works in relation to the total works. Considering that the most probable number refers to works in "title, abstract, or keyword", this subsection concludes that security works are approximately 15% of the total works in V2X.

In addition, Table 8 represents an expanded search effort encompassing tags related to security, threats or attacks related to V2X. We harnessed mainstream databases such as Google Scholar and Scopus and delved into four specialized academic resources identified as particularly relevant. While searches from Elsevier were channeled through the Science Direct platform, the Institute of Electrical and Electronic Engineers (IEEE) searches were routed via the IEEE Xplore. All data collection efforts here, as before, are timestamped to January 18, 2024. The concepts of each type of threat or attack are presented in Section VII.

The primary focus of our search was on "title, abstract, or keyword" tags instead of delving into "all fields". This method proved effective in narrowing down results to the most relevant ones. Nevertheless, some databases, notably Google Scholar and Springer, did not offer this refined search, prompting us to rely solely on "title" or "all fields" searches. This way, we chose the search criteria from "all fields" in both Google Scholar and Springer. Notwithstanding these variations, we are confident in the relevance of the results.

From our insights in Table 8, the following key points can be deduced:

a) Among specialized academic resources, IEEE emerges as the leading platform for subjects related to V2X, including its security dimensions. MDPI, Elsevier, and Springer are close behind it in terms of prominence. Note that more results appear in the Springer database due to the more comprehensive "all fields" criteria.

b) Google Scholar displayed a higher count of results for complex queries than Scopus. While Google Scholar often outpaces Scopus in raw results due to its broader search criteria, it is crucial to note that our Scopus findings were based strictly on titles, abstracts, and keywords while Google Scholar results spanned all fields.

c) Some terms are used more in works than others. Words related to security are used more than words related to attacks. Furthermore, jamming is the attack most commonly found in papers.

E. SCIENTIFIC WORKS RELATED TO SECURITY IN V2X

In this subsection, we executed several unique searches on the Scopus platform for academic papers. This work was based on Scopus for a couple of reasons: 1) its reputation as a top-tier general academic repository, and 2) its ability to dissect search results in multiple informative ways, such as by annual trends, origin country, and funding entity. To streamline our search and minimize irrelevant hits, we concentrated on "title, abstract, and keywords". An additional criterion not used in other subsections of this work is to find results only from articles or conference papers. Adopting this approach enables the identification of academic sources that are more pertinent and insightful for uncovering emerging trends in the scholarly universe. Our January 1, 2024 search yielded an 689 papers tagged under ("V2X" OR "vehicle-to-everything") AND ("security" OR "cybersecurity").

When broken down by year, originating country, and funding entity, the data is captured in Tables 9-11, respectively. The cumulative term is the sum of the values from previous years from pre-2009 onwards in Table 9. Note that no pre-2009 results appeared in Table 9. Concurrently, Figures 6-7 visually interpret the annual and country-specific data. An intriguing observation from Table 9 is the consistent annual surge in publications centered on V2X. The most significant exception is 2021, where there was a slight drop, possibly due to reduced work production related to the COVID-19 pandemic.

Table 10 highlights the prominent role of China in V2X cybersecurity paper production, strengthening its central position in this field. According to Figure 7 and Table 10, not far behind, the USA also asserts a significance, ranking among the top contributors. Due to undefined results in the automatic search, the authors of our work manually found the

TABLE 7. Searches for tags in the Scopus database using different criteria.

Search Within	Language	Tags	Number of References	Tags	Number of References	%
All Fields	All	V2X*	6493	V2X*	18058	35.96
All Fields	English	V2X*	6374	V2X*	17653	36.11
TITLE-ABS-KEY	All	V2X*	801	V2X*	5527	14.49
TITLE-ABS-KEY	English	V2X*	789	V2X*	5434	14.52
TITLE	All	V2X*	82	V2X*	2342	03.50
TITLE	English	V2X*	80	V2X*	2291	03.49

"V2X*" represents the search terms ("V2X" OR "vehicle-to-everything") AND ("security" OR "cybersecurity")
"V2X*" represents the search terms ("V2X" OR "vehicle-to-everything")

TABLE 8. Number of results in searches for different tags on different scientific bases.

Tags \ Scientific basis	In Title, Abstract or Keyword				All Fields	
	Scopus	IEEE	MDPI	Elsevier	Google Scholar	Springer
V2X* AND ("security" OR "cybersecurity")	801	668	93	52	20800	2606
V2X* AND ("attack" OR "attacks" OR "cyberattacks" OR "threat" OR "threats")	382	377	61	32	14000	1878
V2X* AND ("Denial of Service" OR "DoS")	34	142	2	1	5090	894
V2X* AND ("jamming")	33	42	5	6	2900	1147
V2X* AND ("eavesdropping")	19	18	2	3	2350	461
V2X* AND ("spoofing")	14	35	1	1	2190	488
V2X* AND ("hacking")	12	10	3	1	1770	662
V2X* AND ("Distributed Denial of Service" OR "DDoS")	10	25	0	0	1670	432
V2X* AND ("malware" OR "malwares")	9	23	0	2	1770	484
V2X* AND ("Man-in-the-Middle" OR "MitM")	9	18	2	1	1760	428
V2X* AND ("sybil attacks" OR "sybil attack")	8	50	0	2	1220	244
V2X* AND ("black hole" OR "blackhole" OR "black holes" OR "blackholes")	6	8	72	1	920	239
V2X* AND ("injection attacks" OR "injection attack")	5	15	0	0	739	216
V2X* AND ("replay attacks" OR "replay attack")	4	46	1	0	1420	324
V2X* AND ("masquerading" OR "impersonation attacks" OR "impersonation attack")	3	18	34	0	953	231
V2X* AND ("wormhole" OR "wormholes")	3	0	1	1	426	131
V2X* AND ("side-channel attacks" OR "side-channel attack")	2	9	0	0	474	155
V2X* AND ("viruses" OR "virus")	2	2	120	0	1170	603
V2X* AND ("insider threats" OR "insider threat")	2	1	0	0	142	87
V2X* AND ("spam" OR "spams")	2	0	0	1	479	340
V2X* AND ("phishing")	2	0	0	0	449	265
V2X* AND ("ransomware")	1	2	0	0	438	234
V2X* AND ("physical layer attacks" OR "physical layer attack")	1	1	2	0	91	11
V2X* AND ("timing attacks" OR "timing attack")	1	0	10	0	276	109
V2X* AND ("Cross-Site Scripting" OR "XSS")	0	0	5	0	218	125

"V2X*" represents the search terms ("V2X" OR "vehicle-to-everything")

countries and funding sponsors of the undefined works, and Tables 10 and 11 were updated based on this. Note that the total results of Table 10 differ from 9 since some publications involve authors from more than one country. A deep dive into Table 11 showcases the influence of the National Natural Science Foundation of China, holding references that dwarf its closest competitor, further accentuating the academic progress of China.

III. JAMMING ATTACKS IN V2X COMMUNICATION SCENARIOS

V2X communication is susceptible to cybersecurity attacks, with jamming among the most prominent. This section delves into jamming - an attack characterized by the deliberate disruption of communication. The attacker generates interference signals, effectively halting legitimate traffic. As already seen in the previous section, this type of attack is probably

TABLE 9. Number of publications separated year by year in the V2X security area in the Scopus database using the title, abstract, and keywords criteria.

Year	Amount of Publications	% Amount of Publications	Cumulative	% Cumulative
2023	155	22.50	689	100.00
2022	143	20.75	534	77.50
2021	97	14.08	391	56.75
2020	106	15.38	294	42.67
2019	68	9.87	188	27.29
2018	52	7.55	120	17.42
2017	25	3.63	68	9.87
2016	14	2.03	43	6.24
2015	6	0.87	29	4.21
2014	7	1.02	23	3.34
2013	7	1.02	16	2.32
2012	4	0.58	9	1.31
2011	3	0.44	5	0.73
2010	1	0.15	2	0.29
2009	1	0.15	1	0.15
Total	**689**	**100.00**	**689**	**100.00**

TABLE 10. Number of publications separated country by country in the V2X security area in the Scopus database using the title, abstract, and keywords criteria.

Country	Amount of Publications	% Amount of Publications
China	159	17.38
United States	134	14.64
India	68	07.43
South Korea	63	06.89
Germany	58	06.34
United Kingdom	49	05.36
France	43	04.70
Canada	35	03.83
Spain	18	01.97
Italy	17	01.86
Saudi Arabia	17	01.86
Egypt	15	01.64
Japan	15	01.64
Pakistan	12	01.31
Portugal	12	01.31
Others	200	21.86
Total	**915**	**100.00**

TABLE 11. Number of publications in the different funding sponsors in the V2X security area in the Scopus database using the title, abstract, and keywords criteria.

Funding Sponsor	Amount of Publications
National Natural Science Foundation of China	72
National Science Foundation	30
National Key Research and Development Program of China	25
Horizon 2020 Framework Programme	24
National Research Foundation of Korea	21
Ministry of Science, ICT and Future Planning	21
Institute for Information and Communications Technology Promotion	16
Ministry of Science and ICT, South Korea	13
European Commission	11
Horizon 2020	9
Electronic Components and Systems for European Leadership	7
Key Research and Development Projects of Shaanxi Province	7
Fonds National de la Recherche Luxembourg	7
Agence Nationale de la Recherche	6
Conselho Nacional de Desenvolvimento Científico e Tecnológico	6
Engineering and Physical Sciences Research Council	6
European Regional Development Fund	6
Natural Sciences and Engineering Research Council of Canada	6

the most frequent attack that threatens V2X security. For this reason, it is natural that there are several different types or modalities of jamming attacks. Table 12 shows different types of jamming attacks.

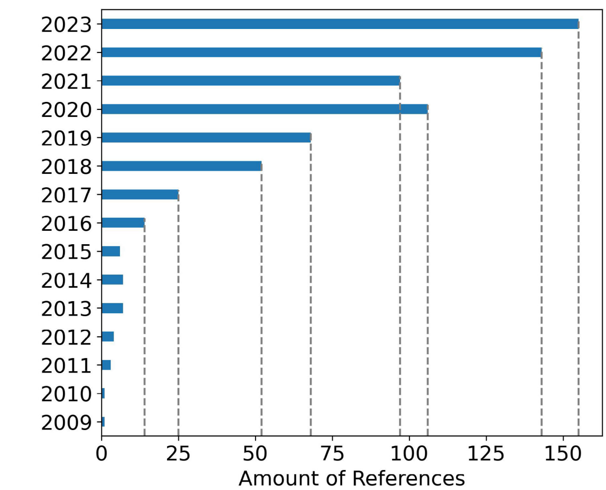


FIGURE 6. Number of references separated year by year in the V2X security area.

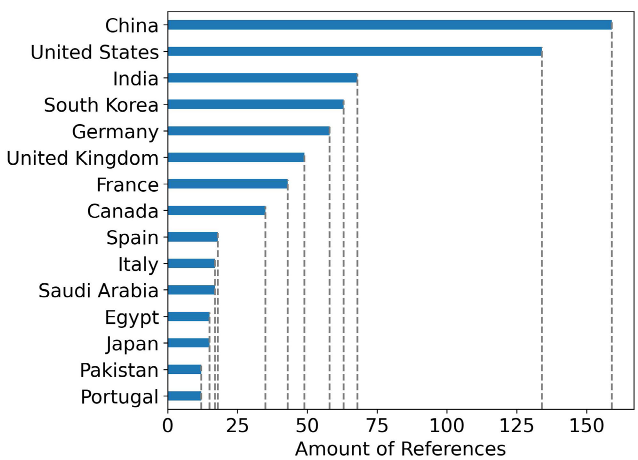


FIGURE 7. Number of references separated country by country in the V2X security area.

On other hand, Figure 8 presents a visualization of the scenario depicted in Figure 1, considering a jamming attack using several drones acting as jammers. The use of drones brings significant advantages to the attack, as the drone has better mobility, making it difficult to employ countermeasures for its detection and localization. In the Left Turn Assist DUC (marker 1 in the Figure 8), the jammer disrupts communication between vehicles, preventing the vehicle making a left turn from receiving adequate information about the presence and location of other vehicles. As a result, the risk of colliding with vehicles in the perpendicular lanes increases significantly. In the VRU Alerts at a Blind Intersection DUC (marker 2 in the Figure 8), the jammer disrupts the communication between the vehicle and the pedestrian. In this case, the vehicle is unable to receive the necessary information about the presence of the pedestrian. In the Do Not Pass Warning DUC (marker 3 in the Figure 8), the vehicle behind the truck may be unable to receive the necessary information to make a safe driving decision. As a result, it may proceed to turn left, potentially leading to a collision with the vehicle approaching from the opposite direction [14]. A plethora of research exists focusing on the threats posed by jammers. For instance, studies such as [14], [58], [61], [62], [63], [64], [65], [66], and [67] have delved into this domain.

The work in [61] is noteworthy for introducing an anti-jamming technique using a Deep Q-network (DQN). Concentrating on a multi-jammer environment with an eavesdropper jammer accompanied by four disruptive jammers, this study leverages machine learning to ensure secure V2V communication amidst these threats. Reference [62] investigates the efficacy of rate adaptation and power control in counteracting jamming within 802.11 networks. The research underlines the compromised performance due to standard rate adaptation under jamming conditions and suggests the Anti-Jamming Reinforcement System (ARES) as a potent countermeasure. Further adding to the knowledge repository, [63] proposes a jammer detection framework tailored for V2X communications. By harnessing Generalized Dynamic Bayesian Networks (GDBNs) and Modified Markov Jump Particle Filter (M-MJPF), this framework offers real-time monitoring and prediction of the V2X signal landscape, detecting jammers when discrepancies arise.

The vulnerabilities of 5G Cellular V2X communication, particularly at the Physical and Media Access Control layers, are explored in [64]. This research notably identifies two innovative DoS attacks - targeted sidelink jamming and sidelink resource exhaustion - and provides valuable insights through simulations that consider specific parameters such as C-V2X power levels and GPS synchronization. The article [65] accentuates the security challenges faced by ITS, especially concerning millimeter-wave cellular vehicle-to-everything (C-V2X) communications. A novel blockage-and-power-based jammer selection strategy is introduced, targeting eavesdroppers while minimizing interference to legitimate entities.

Emphasizing vehicular network safety, [61] models an attack in a Rayleigh fading environment, using parameters such as transmit power and noise power. In contrast, [66] simulates jamming effects on wireless channels using tools and techniques such as direct digital synthesis (DDS). Reference [67] offers a comprehensive categorization of jamming attacks on the Physical Layer. The article recommends novel countermeasures, highlighting the need for a multi-tiered defense strategy against jamming threats. Lastly, [68] showcases Adaptive Beamforming to enhance signal transmission. The research emphasizes the importance of a specific antenna configuration to maximize Adaptive Beamforming efficiency and provides a performance evaluation model for the LTE-A system.

Chaos-based communication has emerged as a significant body of research in recent years, driven by the compelling attributes of chaos, including its random-like behavior and strong sensitivity to initial conditions [69]. For instance, chaos synchronization has been used in wireless sensor networks to improve communication security and increase

TABLE 12. Classification of jamming attacks in V2X security.

Category	Attack Type	Description
Generic jamming attacks	Constant jammers	Continuous generation of high-powered noise as random bits, operating independently of MAC protocols and channel traffic [54]–[57].
	Random and Periodic jammers	Unpredictable functioning, alternating between sleep and jam intervals, impacting the Packet Delivery Ratio (PDR) [54], [55], [58].
	Deceptive jammers	Transmitting unauthorized packets to occupy channels, mimicking legitimacy to receivers [54], [55].
	Reactive jammers	Activating upon channel activity and corrupting legitimate packets [54], [55], [57], [58].
	Frequency Swept Jammer	Fluctuating across frequencies, transmitting signals at each step [54], [58].
Intelligent jammers	Short noise-based	Employing shot noise with protocol awareness to challenge FEC schemes [57], [59], [60].
	Brilliant Jamming	Modifying specific bit patterns within frames, requiring detailed target signal knowledge [54].

FIGURE 8. Representation of a Jamming swarming attack with several jammers interfering in the V2X communication.

the battery lifetime of the sensor nodes [70]. Many works found in the literature can be helpful to face the challenges represented by V2X communication. Notably, those based on chaos synchronization [71], [72] can offer attractive features, including enhanced security [73], [74], [75], low probability of detection [76], and anti-jamming capabilities [77], among others. In particular, synchronizers derived from Lyapunov theory [78] have been proposed to encrypt and decrypt confidential information [79], [80], [81], [82], [83], [84]. The main peculiarity of these works is their enhanced security and robustness against disturbances, including jamming signals.

IV. SPOOFING ATTACKS IN V2X COMMUNICATION SCENARIOS

Spoofing attacks, where attackers attempt to mislead target vehicles using falsified signals, present a significant challenge in the realm of vehicular communication [19]. Several seminal works delve deep into the intricacies of these threats, enriching our understanding and response mechanisms. This section synthesizes the insights and methodologies proposed by these contributions.

In their exploration, [85] detail an advanced RF-based spoofing technique that jeopardizes genuine V2V interactions. By capitalizing on RF Emissions Localization, adversaries craft "phantom cars" using distorted data from Global Navigation Satellite System (GNSS) and Inertial Measurement Unit (IMU) sensors. This research not only pinpoints crucial parameters but also proposes a synergy between Received Signal Strength Indicator (RSSI) and Time Difference of Arrival (TDOA) as an effective countermeasure.

Venturing further into the V2X domain, [86] presents a groundbreaking model, the Coupled Generalized Dynamic Bayesian Network (C-GDBN), positioned at Road Side

Units (RSUs). By interpreting vehicular positions from real-time RF signals, this research pioneers in identifying and counteracting spoofing vulnerabilities intrinsic to V2X communications. Transitioning to the larger framework of Connected Vehicles, [87] accentuates the potential perils within Traffic Signal Control (TSC) systems. Their research spotlighted the ETA attack and the phantom queue incursion as primary threat vectors, suggesting a comprehensive cybersecurity framework to counter these.

While CV technologies offer significant potential, they are vulnerable to data spoofing attacks. Recognizing this, [88] proposes a detection methodology for infrastructure-side CV applications, boasting an impressive 95% detection efficacy with minimal false positives. Further focusing on anomalous vehicular behaviors, [89] innovates with a Multi-Sensor Fusion-based spoofing attack model. Through their framework, two distinct threat models targeting the GPS channel and Integrated Modular Avionics are developed, adding layers to our understanding. In Global Positioning System (GPS) spoofing, the attacker aims to drag victim vehicles off to incorrect positions through fabricated spurious GPS signals [19]. Given the increasing reliance on 5G, [90] stresses its vulnerabilities, offering a virtual channel-based model for detecting spoofing within massive Multiple Input Multiple Output (MIMO) mm-wave networks. Similarly, [91] sheds light on 5G precision in positioning, presenting the In-Phase Quadrature Network (IQ-Net) defense mechanism against Selective-PRS-Spoofing (SPS).

The research by [92] brings forward a scalable solution for Next Generation Internet of Things (NGIoT) networks, leveraging beam pattern features of mmWave devices. In contrast, [93] and [94] provide varied methodologies, focusing on the 5G mmWave 60 GHz band and Akaike, Bayesian, and Generalized Information Criteria, respectively. Expanding the horizon, [95] and [96] delve into the potentials and challenges within wireless communications, with [97] concluding our discussion by introducing Thermal Pattern Analysis as a promising tool for spoofing attack prediction.

V. DOS AND DDOS ATTACKS IN V2X COMMUNICATION SCENARIOS

A DoS attack aims to disrupt the normal functions of a network by overwhelming the target with a flood of requests, rendering services unavailable to legitimate users. Expanding upon this, a DDoS attack, a specific type of DoS attack, utilizes multiple compromised systems as sources of attack traffic, significantly increasing the scale and effectiveness of the attack [22]. In the context of V2X security, DDoS attacks represent a substantial threat, even more significant than DoS, impacting the availability and reliability of crucial communication channels in vehicular networks. For this reason, more focus will be given to DDoS in this section, as DDoS represents a more significant threat than DoS. DoS attacks manifest when attackers perpetually transmit high-priority communications, thereby overshadowing and obstructing genuine messages of lower priority [20], [98]. Also, differing from jamming attacks that directly disrupt the signal, DDoS attacks inundate the network with excessive requests, overwhelming the system and impeding legitimate communications. Several studies have explored various aspects of DDoS attacks in V2X environments [99], [100], [101], [102]. A notable approach in detecting and locating DDoS attacks in LTE-based vehicular networks involves the application of Machine Learning techniques designed to handle the dynamic scenarios of moving vehicles and heterogeneous network entities such as Femtocells/Femto Access Points (FAPs) [103]. This method differs from traditional methods by addressing the unique challenges posed by mobile network components in V2X scenarios.

Another significant contribution is the development of a numerically efficient offline design algorithm to enhance platoon control law against DDoS attacks [104]. This research balances the need for resilience against DDoS attacks and the requirements for stability, safety, and scalability in vehicular networks. The emergence of 5G introduces new challenges for V2X communications. A study focusing on creating a DDoS attack model to test vulnerabilities in the Physical Layer of 5G Cellular V2X aims to develop countermeasures [64]. The model incorporates parameters such as transmission power, bandwidth, and modulation techniques, offering a deeper understanding of potential weaknesses in 5G networks. In addition to detection methods, the literature also discusses strategies to mitigate the effects of DDoS attacks. For example, a Central Aggregator-Intrusion Detection System (CA-IDS) was proposed for EVs, noted for its higher throughput, lower jitter, and accuracy [105]. This system monitors and analyzes incoming traffic to EVs, effectively identifying and blocking malicious vehicles.

The Detection of Anomalous Behavior in Smart Conveyance Operations (DAMASCO) system combines software and hardware solutions to detect DDoS attacks in VANETs, validated through simulations [106]. This system is particularly effective in ITS, where ensuring continuous network service is crucial for safety and efficiency. Using a multivariate approach, a novel multivariate statistical Intrusion Detection System (IDS) monitors vehicular networks for DDoS attacks, demonstrating its effectiveness in simulated environments with tools such as Objective Modular Network Testbed in C++ (OMNET++) and the Vehicles in Network Simulation (Veins) network mobility framework [107]. The literature also includes examples of combined attack models, such as a study demonstrating how spoofing and DDoS attacks can synergize, creating more complex challenges for vehicular networks [108]. This model emphasizes the need for less power for effective implementation, making it a realistic threat in real-world scenarios.

In the sphere of autonomous vehicles, research suggests channel switching in the IEEE 802.11p DSRC protocol as a countermeasure against DDoS attacks [21]. This approach aims to maintain continuous and secure communication by dynamically adapting to the presence of attacks on different channels. In summary, the research on DDoS attacks in V2X environments is extensive, covering various attack models, detection methods, and mitigation strategies. These studies underscore the complexity and evolving nature of threats in vehicular networks, emphasizing the need for advanced, adaptable solutions to ensure secure and reliable V2X communication.

VI. EAVESDROPPING ATTACKS IN V2X COMMUNICATION SCENARIOS

The burgeoning field of the IoT and autonomous vehicles has intensified the focus on wireless communication security, with eavesdropping attacks emerging as a critical concern. This type of attack, where unauthorized parties intercept confidential communications, poses a significant threat to the integrity of V2X communication systems. Studies have explored various aspects of eavesdropping attacks and corresponding countermeasures in wireless communication, especially in V2X contexts. In an eavesdropping attack, unauthorized parties intercept vehicular messages with the intent of capturing packet details and obtaining sensitive data [20]. Typically, these broadcasted messages encompass traffic safety information, which is usually deemed non-confidential [109].

Also, as discussed in [110], it examines scenarios involving Unmanned Aerial Vehicles (UAVs) in roles such as User Equipment (UE), Base Stations (BS), and moving relays, shedding light on anti-eavesdropping techniques such as the use of jamming UAVs to disrupt eavesdroppers. This approach underscores the potential of using existing technologies creatively to safeguard communications. Innovative countermeasures against eavesdropping continue to evolve. For instance, reference [111] proposes a V2V communication model where legal vehicles track an eavesdropping car. The system, comprising a preceptor, feedback channel, and executor, collaboratively adjusts transmission power and coding to secure communications. Similarly, [112] introduces Radio Frequency Fingerprinting (RF-FP) to locate hidden eavesdroppers, proving its efficiency through simulation results. Furthermore, the study in [113] highlights the complexities of ensuring physical layer security in V2V communication under challenging conditions such as double-Rayleigh fading channels.

The scope of research extends to related domains such as drone and satellite communications, providing valuable insights applicable to V2X security. For example, [114] discusses a system that tackles both eavesdropping and jamming attacks in UAV communications, offering a holistic view of the security challenges. Additionally, [115] explores satellite communication eavesdropping, suggesting a system model that employs cooperative jamming and full-duplex terrestrial relays to evade eavesdroppers. Recent studies have introduced novel methodologies to enhance eavesdropping detection and prevention in V2X communication. Reference [116] discusses an innovative approach that combines legal and eavesdropping links to improve attack detection, substantiated through simulation in a Rayleigh fading channel environment. Moreover, [61] and [117] propose techniques based on Wireless Power Transfer (WPT) and Deep Q-Network (DQN) architectures, respectively, highlighting the importance of adaptive and intelligent systems in countering eavesdropping risks. Further advancements in collaborative beamforming and UAV-assisted security measures have broadened the prospects for countering eavesdropping attacks. For instance, [118] and [119] delve into the use of UAV swarms and full-duplex transmission modes for securing data transmission against eavesdropping, emphasizing the potential of emerging technologies in enhancing V2X communication security.

In conclusion, eavesdropping attacks constitute a significant threat to V2X communications, necessitating ongoing research and development in this field. The studies reviewed here present a comprehensive understanding of current research trends, offering a range of methodologies and technological innovations aimed at fortifying wireless communication networks against such attacks.

VII. ADDITIONAL CYBERATTACKS IN V2X COMMUNICATION SCENARIOS

In addition to the most popular and high-impact attacks listed above, there are several other attacks, some of which are very specialized, that will be described below:

- **Advanced Persistent Threat (APT):** An APT is a sustained, focused cyber-attack where an intruder infiltrates critical infrastructure systems and maintains a stealthy presence, avoiding detection until causing significant damage to the target system [120]. An APT in the context of V2X involves sophisticated, stealthy cyber-attacks, typically state-sponsored or well-funded, focusing on prolonged access to crucial systems. Unlike conventional attacks, APTs utilize advanced tools and methods, bypassing standard anti-virus and IDS, to remain undetected and gather vital information over an extended period [121].
- **Backdoor attack:** In V2X systems, a backdoor attack involves malware installation by hackers, designed to circumvent the usual security of network and authentication measures [122].
- **Blackhole Attack:** In V2X systems, a blackhole attack, sometimes termed a packet drop attack, represents a variant of DoS attacks. Within this framework, an attacker purposely omits forwarding packets meant for relay [18], [123]. Essentially, by halting the relaying of packets to adjacent nodes, this compromised node denies legitimate users access to pertinent information [33].
- **Cross-Site Scripting (XSS):** XSS is a client-side code injection attack where an attacker executes malicious scripts within a legitimate web application. This type of vulnerability poses a risk to V2X systems and occurs

when a web application includes unencoded user input in its output. The key aspect of XSS is its indirect nature; rather than attacking directly, it exploits existing vulnerabilities within a website [124].

- **Gray-Hole Attack:** In blackhole and gray-hole attacks in the V2X context, an adversary diverts or discards network traffic using a fabricated node. The node is manipulated to appear as the most efficient route, attracting all traffic. While a blackhole attack involves dropping all redirected packets, a gray-hole attack is more selective, discarding only specific packets. These attacks can have varied impacts across different network levels [125].
- **Injection Attack:** In injection attacks, attackers introduce unauthorized and harmful messages into the V2X network, threatening the security and functionality of in-vehicle networks [20].
- **Insider Threats:** Insider threats in V2X communications pose a significant cybersecurity challenge, necessitating specialized detection systems for timely identification of malicious insiders. Despite various studies, limitations persist, including a lack of comprehensive understanding and real-case analyses. Addressing insider threats effectively requires advanced detection systems that can discern and mitigate such risks within organizations, especially in critical sectors such as V2X communications [126].
- **Malware Attack:** In this form of attack, an attacker introduces malicious software components, such as viruses, trojans, or worms, into the On-Board Units (OBUs) and Road-Side Units (RSUs) of the V2X network. This injection often occurs during periodic software updates and is more likely to be initiated by rogue insiders. The attack aims to disrupt access to devices by compromising their availability, with ransomware being a notable example. This can result in the malfunctioning of V2X network components, inflicting severe disruption to normal system operations [19].
- **Man-in-the-Middle (MitM) Attack:** This attack, in the V2X context, strategically positions an adversary between transmitting and receiving vehicles, enabling the interception and manipulation of vital safety and traffic information. The ramifications of such an attack are particularly grave due to the sensitive nature of the data in vehicular communications, potentially leading to significant property damage and loss of human lives [9].
- **Masquerading/Impersonation Attack:** In a masquerading or impersonation attack, the attacker assumes a valid identity to infiltrate V2X networks and access confidential information [33].
- **Phishing:** A significant cybersecurity threat involves fraudulent tactics such as deceptive emails to steal user credentials. Its relevance in V2X security arises from the increasing use of IoT devices in phishing attacks, which can compromise network integrity. Adaptability of phishing across various platforms, including V2X systems, necessitates advanced detection and security mechanisms to protect against data breaches and safeguard sensitive vehicular communications [127].
- **Physical Layer Attacks:** Physical Layer Attacks in V2X network target the foundational level of a network, where its physical traits are defined. Due to the broadcast nature of wireless communications, this layer is particularly susceptible to various interference and breaches, such as node tampering, hardware hacking, jamming, and eavesdropping [128].
- **Ransomware:** In V2X systems, ransomware is a form of malware that encrypts the computer of a victim, with decryption contingent upon ransom payment. Identifying these attacks is known as ransomware detection [129]. Ransomware is recognized as a highly effective and lucrative attack method in traditional information technology settings. Considering the growing number of connected vehicles, its potential impact on the automotive industry is substantial. Even a modest percentage of these cars being targeted by ransomware could have significant financial implications, underscoring the need for robust security measures in this sector [130].
- **Replay Attack:** In replay attacks, malicious actors rebroadcast previously transmitted V2X messages from vehicles, pedestrians, or infrastructure. This deceptive action can mislead receiving vehicles into responding to nonexistent traffic scenarios [18].
- **Side-channel Attack:** The adversary uses forensic techniques to glean information such as execution time and power consumption from hardware. These non-invasive attacks focus on the physical aspects of embedded hardware in V2X communication systems to extract encryption keys. To mitigate such attacks in the V2X field, countermeasures such as cryptographic safeguards, isolation strategies, proper system configurations, and secure implementation practices are essential [125].
- **Spamming Attack:** This strategy involves the injection of a copious volume of spam messages by an attacker into the network. Such an onslaught leads to resource collisions and bandwidth saturation, critically undermining the efficiency of V2X communication systems [19].
- **SQL Injection Vulnerabilities:** SQL injection vulnerabilities pose a significant threat to web applications by allowing attackers to access or corrupt underlying databases containing sensitive information. These vulnerabilities arise from inadequate validation of user input, making many web applications, including those in V2X systems, susceptible to such attacks. Addressing these vulnerabilities requires rigorous application of defensive coding practices, but the vast scope and

variations of SQL injection attacks make it challenging to fully safeguard systems [131].

- **Sybil Attack:** In a Sybil attack in V2X environments, an attacker employs several identities to disseminate varied messages to other vehicles, leading them to perceive that the messages originate from distinct vehicles. Consequently, this deception prompts the recipient vehicles to make erroneous decisions [9].
- **Trojans:** Trojans in V2X contexts masquerade as legitimate software, requiring user interaction for dissemination [132].
- **Wormhole Attack:** This attack involves establishing a clandestine tunnel within the V2X network by using controlled or fake nodes. It enables data interception at one point and its deceptive replay at another, corrupting routing information and impairing location-dependent protocols impairing location-dependent protocols essential for V2X communications. Beyond affecting data delivery and network functionality, the wormhole attack facilitates others, such as blackhole and DoS, presenting challenges to IDS due to late detection and considerable damage [125], [133].
- **Viruses:** Viruses in V2X systems, often dormant, become active upon executing an infected host program or file, spreading passively through copying or downloading [132].
- **Zero-Day Vulnerability:** A zero-day vulnerability in V2X systems is a newly discovered security flaw unknown to the vendor and without a patch. The risk escalates if the vulnerability becomes public before a fix is issued, as attackers can exploit it to target vulnerable systems. Delays in patching these vulnerabilities increase the likelihood of zero-day exploits, posing significant security threats. Hence, timely identification and patching of such vulnerabilities are crucial for IT vendors to protect their systems and users [134].

VIII. CONCLUSION

This work is a survey related to V2X cybersecurity. This paper conducted a comprehensive survey, presenting an in-depth examination of security in V2X communications. The authors provided a related survey on V2X security, highlighting the breadth and depth of research in this area. We also delved into various cybersecurity threats such as jamming, spoofing, Distributed Denial of Service, and eavesdropping, exploring how they impact V2X systems. Another interesting contribution was finding a long list of other types of attacks besides the four mentioned in the previous sentence and their respective concepts.

The main finding of our study is the identification of market and academic trends, indicating a significant and growing interest in V2X security and the threats it faces. Our extensive review reveals the most relevant companies and the leading role of China and the United States as pioneering countries in V2X cybersecurity solutions. The significance of this research area is clear, calling for ongoing efforts in research and development to tackle these ever-changing challenges.

Future work in the field of V2X security is poised to explore advanced defensive mechanisms, particularly in the context of 5G integration and the increasing application of AI. The convergence of growing concerns over V2X cybersecurity threats with the rise of 5G technology and AI-driven solutions suggests a potential shift towards more sophisticated, integrated security approaches. Additionally, encryption and secure communication protocols will probably become increasingly prevalent as standard protective tools in V2X cybersecurity. A key insight from this research is the emerging consensus on the necessity of layered defense tactics, evolving in step with the dynamic nature of cyber threats in the field of V2X.

Further research should also explore emerging technologies such as Quantum Cryptography and Zero Trust Architectures to assess their implications for V2X security. The potential of these technologies to enhance the security framework in V2X communications warrants deeper investigation. Moreover, conducting prototyping and simulation studies could provide valuable insights into the efficacy of new security protocols or systems, demonstrating their practical application and impact in a controlled environment. These future directions will not only extend the understanding of V2X cybersecurity, but also guide the development of more robust and effective security solutions, thereby significantly impacting the field.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

ABBREVIATIONS

The following abbreviations are used in this work:

3GPP	3rd Generation Partnership Project.
AI	Artificial Intelligence.
APT	Advanced Persistent Threat.
ARES	Anti-Jamming Reinforcement System.
B5G	Beyond 5G.
BS	Base Stations.
C-GDBN	Coupled Generalized Dynamic Bayesian Network.
C-V2X	Cellular Vehicle-to-Everything.
CA-IDS	Central Aggregator-Intrusion Detection System.
CT	Communication Technology.
CV	Connected Vehicles.
DAMASCO	Detection of Anomalous Behavior in Smart Conveyance Operations.
DDoS	Distributed Denial of Service.
DDS	Direct Digital Synthesis.
DoS	Denial of Service.
DQN	Deep Q-network.

DUCs	Driving Use Cases.
FAPs	Femtocells/Femto Access Points.
GDBNs	Generalized Dynamic Bayesian Networks.
GNSS	Global Navigation Satellite System.
GPS	Global Positioning System.
ICT	Information and Communication Technological.
ICVs	Intelligent Connected Vehicles.
IDS	Intrusion Detection System.
IEEE	Institute of Electrical and Electronic Engineers.
IMU	Inertial Measurement Unit.
IoT	Internet of Things.
IQ-NeT	In-Phase Quadrature Network.
ITS	Intelligent Transportation Systems.
LiDAR	Light Detection and Ranging.
LTE	Long-Term Evolution.
M-MJPF	Modified Markov Jump Particle Filter.
MIMO	Multiple Input Multiple Output.
MitM	Man-in-the-Middle.
NGIoT	Next Generation Internet of Things.
NR	New Radio.
OBUs	On-Board Units.
OMNeT++	Objective Modular Network Testbed in C++.
PDR	Packet Delivery Ratio.
R&D	Research and Development.
RF	Radio Frequency.
RSSI	Received Signal Strength Indicator.
RSUs	Road Side Units.
SAE	Society of Automotive Engineers.
SDN	Software-Defined Networking.
TDOA	Time Difference of Arrival.
UAVs	Unmanned Aerial Vehicles.
UE	User Equipment.
V2G	Vehicle-to-Grid.
V2I	Vehicle-to-Infrastructure
V2N	Vehicle-to-Network.
V2P	Vehicle-to-Person/Pedestrian
V2V	Vehicle-to-Vehicle.
V2X	Vehicle-to-Everything.
VANETs	Vehicular ad hoc Network.
Veins	Vehicles in Network Simulation.
WPT	Wireless Power Transfer.
VRU	Vulnerable Road Users.
XAI	Explainable AI.
XSS	Cross-Site Scripting.

ACKNOWLEDGMENT

The authors would like to acknowledge Daniel Valle de Lima for their assistance in the initial review phases of this work.

REFERENCES

[1] M. N. Ahangar, Q. Z. Ahmed, F. A. Khan, and M. Hafeez, "A survey of autonomous vehicles: Enabling communication technologies and challenges," *Sensors*, vol. 21, no. 3, p. 706, Jan. 2021, doi: 10.3390/s21030706.

[2] T. Ersal, I. Kolmanovsky, N. Masoud, N. Ozay, J. Scruggs, R. Vasudevan, and G. Orosz, "Connected and automated road vehicles: State of the art and future challenges," *Vehicle Syst. Dyn.*, vol. 58, no. 5, pp. 672–704, Mar. 2020, doi: 10.1080/00423114.2020.1741652.

[3] W. Tong, A. Hussain, W. X. Bo, and S. Maharjan, "Artificial intelligence for vehicle-to-everything: A survey," *IEEE Access*, vol. 7, pp. 10823–10843, 2019, doi: 10.1109/ACCESS.2019.2891073.

[4] H. Zhou, W. Xu, J. Chen, and W. Wang, "Evolutionary V2X technologies toward the Internet of Vehicles: Challenges and opportunities," *Proc. IEEE*, vol. 108, no. 2, pp. 308–323, Feb. 2020, doi: 10.1109/JPROC.2019.2961937.

[5] A. Alalewi, I. Dayoub, and S. Cherkaoui, "On 5G-V2X use cases and enabling technologies: A comprehensive survey," *IEEE Access*, vol. 9, pp. 107710–107737, 2021, doi: 10.1109/ACCESS.2021.3100472.

[6] Md. Noor-A-Rahim, Z. Liu, H. Lee, M. O. Khyam, J. He, D. Pesch, K. Moessner, W. Saad, and H. V. Poor, "6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities," *Proc. IEEE*, vol. 110, no. 6, pp. 712–734, Jun. 2022, doi: 10.1109/JPROC.2022.3173031.

[7] C. Shin, E. Farag, H. Ryu, M. Zhou, and Y. Kim, "Vehicle-to-everything (V2X) evolution from 4G to 5G in 3GPP: Focusing on resource allocation aspects," *IEEE Access*, vol. 11, pp. 18689–18703, 2023, doi: 10.1109/ACCESS.2023.3247127.

[8] 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, doi: 10.1109/TVT.2016.2591558.

[9] M. Muhammad and G. A. Safdar, "Survey on existing authentication issues for cellular-assisted V2X communication," *Veh. Commun.*, vol. 12, pp. 50–65, Apr. 2018, doi: 10.1016/j.vehcom.2018.01.008.

[10] T. Yoshizawa, D. Singelée, J. T. Muehlberg, S. Delbruel, A. Taherkordi, D. Hughes, and B. Preneel, "A survey of security and privacy issues in V2X communication systems," *ACM Comput. Surv.*, vol. 55, no. 9, pp. 1–36, Jan. 2023, doi: 10.1145/3558052.

[11] M. H. C. Garcia, A. Molina-Galan, M. Boban, J. Gozalvez, B. Coll-Perales, T. Sahin, and A. Kousaridas, "A tutorial on 5G NR V2X communications," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1972–2026, 3rd Quart., 2021, doi: 10.1109/COMST.2021.3057017.

[12] A. W. Thompson, "Economic implications of lithium ion battery degradation for vehicle-to-grid (V2X) services," *J. Power Sour.*, vol. 396, pp. 691–709, Aug. 2018, doi: 10.1016/j.jpowsour.2018.06.053.

[13] M. A. Rehman, M. Numan, H. Tahir, U. Rahman, M. W. Khan, and M. Z. Iftikhar, "A comprehensive overview of vehicle to everything (V2X) technology for sustainable EV adoption," *J. Energy Storage*, vol. 74, Dec. 2023, Art. no. 109304, doi: 10.1016/j.est.2023.109304.

[14] A. S. Da Silva, J. P. J. Da Costa, G. A. Santos, Z. Miri, M. I. B. M. Fauzi, A. Vinel, E. P. de Freitas, and K. Kastell, "Radio jamming in vehicle-to-everything communication systems: Threats and countermeasures," in *Proc. 23rd Int. Conf. Transparent Opt. Netw. (ICTON)*, Bucharest, Romania, Jul. 2023, pp. 1–4, doi: 10.1109/ICTON59386.2023.10207422.

[15] W. Duan, J. Gu, M. Wen, G. Zhang, Y. Ji, and S. Mumtaz, "Emerging technologies for 5G-IoV networks: Applications, trends and opportunities," *IEEE Netw.*, vol. 34, no. 5, pp. 283–289, Sep. 2020, doi: 10.1109/MNET.001.1900659.

[16] A. Bazzi, A. O. Berthet, C. Campolo, B. M. Masini, A. Molinaro, and A. Zanella, "On the design of sidelink for cellular V2X: A literature review and outlook for future," *IEEE Access*, vol. 9, pp. 97953–97980, 2021, doi: 10.1109/ACCESS.2021.3094161.

[17] V. Sharma, I. You, and N. Guizani, "Security of 5G-V2X: Technologies, standardization, and research directions," *IEEE Netw.*, vol. 34, no. 5, pp. 306–314, Sep. 2020, doi: 10.1109/MNET.001.1900662.

[18] 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, doi: 10.1109/JPROC.2019.2948302.

[19] R. Sedar, C. Kalalas, F. Vázquez-Gallego, L. Alonso, and J. Alonso-Zarate, "A comprehensive survey of V2X cybersecurity mechanisms and future research paths," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 325–391, 2023, doi: 10.1109/OJCOMS.2023.3239115.

[20] 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, doi: 10.1016/j.vehcom.2019.100214.

[21] S. Nazat and M. Abdallah, "Anomaly detection framework for securing next generation networks of platoons of autonomous vehicles in a vehicle-to-everything system," in *Proc. 9th ACM Cyber-Phys. Syst. Secur. Workshop*, Las Vegas, NV, USA, Jul. 2023, pp. 1–6, doi: 10.1145/3592538.3594274.

[22] A. Ghosal and M. Conti, "Security issues and challenges in V2X: A survey," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107093, doi: 10.1016/j.comnet.2019.107093.

[23] X. Tong, Y. Shi, Q. Zhang, and S. Chen, "Adaptive on-ramp merging strategy under imperfect communication performance," *Veh. Commun.*, vol. 44, Dec. 2023, Art. no. 100681, doi: 10.1016/j.vehcom.2023.100681.

[24] I. M. Varma and N. Kumar, "A comprehensive survey on SDN and blockchain-based secure vehicular networks," *Veh. Commun.*, vol. 44, Dec. 2023, Art. no. 100663, doi: 10.1016/j.vehcom.2023.100663.

[25] C. I. Nwakanma, L. A. C. Ahakonye, J. N. Njoku, J. C. Odirichukwu, S. A. Okolie, C. Uzondu, C. C. N. Nweke, and D.-S. Kim, "Explainable artificial intelligence (XAI) for intrusion detection and mitigation in intelligent connected vehicles: A review," *Appl. Sci.*, vol. 13, no. 3, p. 1252, Jan. 2023, doi: 10.3390/app13031252.

[26] C. Zidi, P. Sondi, N. Mitton, M. Wahl, and A. Meddahi, "Review and perspectives on the audit of vehicle-to-everything communications," *IEEE Access*, vol. 11, pp. 81623–81645, 2023, doi: 10.1109/ACCESS.2023.3301182.

[27] A. Balador, A. Bazzi, U. Hernandez-Jayo, I. de la Iglesia, and H. Ahmadvand, "A survey on vehicular communication for cooperative truck platooning application," *Veh. Commun.*, vol. 35, Jun. 2022, Art. no. 100460, doi: 10.1016/j.vehcom.2022.100460.

[28] N. H. Hussein, C. T. Yaw, S. P. Koh, S. K. Tiong, and K. H. Chong, "A comprehensive survey on vehicular networking: Communications, applications, challenges, and upcoming research directions," *IEEE Access*, vol. 10, pp. 86127–86180, 2022, doi: 10.1109/ACCESS.2022.3198656.

[29] I. Soto, M. Calderon, O. Amador, and M. Urueña, "A survey on road safety and traffic efficiency vehicular applications based on C-V2X technologies," *Veh. Commun.*, vol. 33, Jan. 2022, Art. no. 100428, doi: 10.1016/j.vehcom.2021.100428.

[30] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," *Comput. Secur.*, vol. 103, Apr. 2021, Art. no. 102150, doi: 10.1016/j.cose.2020.102150.

[31] R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, "Evolution of V2X communication and integration of blockchain for security enhancements," *Electronics*, vol. 9, no. 9, p. 1338, Aug. 2020, doi: 10.3390/electronics9091338.

[32] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, and L. Xiong, "A survey on security aspects for 3GPP 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 170–195, 1st Quart., 2020, doi: 10.1109/COMST.2019.2951818.

[33] 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, doi: 10.1016/j.comnet.2018.12.018.

[34] 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, doi: 10.1109/OJVT.2020.2999885.

[35] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing vehicle-to-everything (V2X) communication platforms," *IEEE Trans. Intell. Vehicles*, vol. 5, no. 4, pp. 693–713, Dec. 2020, doi: 10.1109/TIV.2020.2987430.

[36] M. Dibaei, X. Zheng, K. Jiang, R. Abbas, S. Liu, Y. Zhang, Y. Xiang, and S. Yu, "Attacks and defences on intelligent connected vehicles: A survey," *Digit. Commun. Netw.*, vol. 6, no. 4, pp. 399–421, Nov. 2020, doi: 10.1016/j.dcan.2020.04.007.

[37] O. Y. Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby, and A. Mouzakitis, "Intrusion detection systems for intra-vehicle networks: A review," *IEEE Access*, vol. 7, pp. 21266–21289, 2019, doi: 10.1109/ACCESS.2019.2894183.

[38] 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, doi: 10.1109/COMST.2014.2345420.

[39] J. Jeong, Y. Shen, T. Oh, S. Céspedes, N. Benamar, M. Wetterwald, and J. Härri, "A comprehensive survey on vehicular networks for smart roads: A focus on IP-based approaches," *Veh. Commun.*, vol. 29, Jun. 2021, Art. no. 100334, doi: 10.1016/j.vehcom.2021.100334.

[40] B. Wang, Y. Han, S. Wang, D. Tian, M. Cai, M. Liu, and L. Wang, "A review of intelligent connected vehicle cooperative driving development," *Mathematics*, vol. 10, no. 19, p. 3635, Oct. 2022, doi: 10.3390/math10193635.

[41] J. Wang, Y. Shao, Y. Ge, and R. Yu, "A survey of vehicle to everything (V2X) testing," *Sensors*, vol. 19, no. 2, p. 334, Jan. 2019, doi: 10.3390/s19020334.

[42] W. Ji, S. Yu, Z. Shen, M. Wang, G. Cheng, T. Yang, and Q. Yuan, "Knowledge mapping with CiteSpace, VOSviewer, and SciMAT on intelligent connected vehicles: Road safety issue," *Sustainability*, vol. 15, no. 15, p. 12003, Aug. 2023, doi: 10.3390/su151512003.

[43] A. Biswas, M. A. O. Reon, P. Das, Z. Tasneem, S. M. Muyeen, S. K. Das, F. R. Badal, S. K. Sarker, M. M. Hassan, S. H. Abhi, M. R. Islam, M. F. Ali, M. H. Ahamed, and M. M. Islam, "State-of-the-art review on recent advancements on lateral control of autonomous vehicles," *IEEE Access*, vol. 10, pp. 114759–114786, 2022, doi: 10.1109/ACCESS.2022.3217213.

[44] L. Miao, S.-F. Chen, Y.-L. Hsu, and K.-L. Hua, "How does C-V2X help autonomous driving to avoid accidents?" *Sensors*, vol. 22, no. 2, p. 686, Jan. 2022, doi: 10.3390/s22020686.

[45] A. Biswas and H.-C. Wang, "Autonomous vehicles enabled by the integration of IoT, edge intelligence, 5G, and blockchain," *Sensors*, vol. 23, no. 4, p. 1963, Feb. 2023, doi: 10.3390/s23041963.

[46] F. Salahdine, T. Han, and N. Zhang, "5G, 6G, and beyond: Recent advances and future challenges," *Ann. Telecommun.*, vol. 78, nos. 9–10, pp. 525–549, Jan. 2023, doi: 10.1007/s12243-022-00938-3.

[47] S. Hacohen, O. Medina, and S. Shoval, "Autonomous driving: A survey of technological gaps using Google scholar and Web of science trend analysis," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 11, pp. 21241–21258, Nov. 2022, doi: 10.1109/TITS.2022.3172442.

[48] 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, doi: 10.1109/TITS.2017.2749459.

[49] V. S. R. Tappeta, B. Appasani, S. Patnaik, and T. S. Ustun, "A review on emerging communication and computational technologies for increased use of plug-in electric vehicles," *Energies*, vol. 15, no. 18, p. 6580, Sep. 2022, doi: 10.3390/en15186580.

[50] M. A. Altahrawi, N. F. Abdullah, R. Nordin, and M. Ismail, "Multi-radio access software-defined vehicular network," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 10030–10048, Aug. 2022, doi: 10.1109/TITS.2021.3115155.

[51] S. Islam, A. Iqbal, M. Marzband, I. Khan, and A. M. A. B. Al-Wahedi, "State-of-the-art vehicle-to-everything mode of operation of electric vehicles and its future perspectives," *Renew. Sustain. Energy Rev.*, vol. 166, Sep. 2022, Art. no. 112574, doi: 10.1016/j.rser.2022.112574.

[52] M. J. K. Abood and G. H. Abdul-Majeed, "Classification of network slicing threats based on slicing enablers: A survey," *Int. J. Intell. Netw.*, vol. 4, pp. 103–112, Apr. 2023, doi: 10.1016/j.ijin.2023.04.002.

[53] (2023). *Statista Database*. Accessed: Feb. 12, 2024. [Online]. Available: https://www.statista.com/

[54] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 767–809, 2nd Quart., 2022, doi: 10.1109/COMST.2022.3159185.

[55] S. Vadlamani, B. Eksioglu, H. Medal, and A. Nandi, "Jamming attacks on wireless networks: A taxonomic survey," *Int. J. Prod. Econ.*, vol. 172, pp. 76–94, Feb. 2016, doi: 10.1016/j.ijpe.2015.11.008.

[56] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," in *Proc. IEEE INFOCOM 26th IEEE Int. Conf. Comput. Commun.*, Anchorage, AK, USA, May 2007, pp. 1307–1315, doi: 10.1109/INFCOM.2007.155.

[57] Z. Lu, W. Wang, and C. Wang, "Modeling, evaluation and detection of jamming attacks in time-critical wireless applications," *IEEE Trans. Mobile Comput.*, vol. 13, no. 8, pp. 1746–1759, Aug. 2014, doi: 10.1109/TMC.2013.146.

[58] T. Erpek, Y. E. Sagduyu, and Y. Shi, "Deep learning for launching and mitigating wireless jamming attacks," *IEEE Trans. Cognit. Commun. Netw.*, vol. 5, no. 1, pp. 2–14, Mar. 2019, doi: 10.1109/TCCN.2018.2884910.

[59] D. J. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11 b and other networks," in *Proc. IEEE Conf. Military Commun.*, Oct. 2006, pp. 1075–1081, doi: 10.5555/1896579.1896741.

[60] S. Sodagari and T. C. Clancy, "On singularity attacks in MIMO channels," *Trans. Emerg. Telecommun. Technol.*, vol. 26, no. 3, pp. 482–490, May 2013, doi: 10.1002/ett.2657.

[61] Y. Yao, J. Zhao, Z. Li, X. Cheng, and L. Wu, "Jamming and eavesdropping defense scheme based on deep reinforcement learning in autonomous vehicle networks," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 1211–1224, 2023, doi: 10.1109/TIFS.2023.3236788.

[62] K. Pelechrinis, I. Broustis, S. V. Krishnamurthy, and C. Gkantsidis, "A measurement-driven anti-jamming system for 802.11 networks," *IEEE/ACM Trans. Netw.*, vol. 19, no. 4, pp. 1208–1222, Aug. 2011, doi: 10.1109/TNET.2011.2106139.

[63] A. Krayani, N. J. William, L. Marcenaro, and C. Regazzoni, "Jammer detection in vehicular V2X networks," in *Proc. Microw. Medit. Symp. (MMS)*, May 2022, pp. 1–5, doi: 10.1109/MMS55062.2022.9825566.

[64] G. Twardokus and H. Rahbari, "Towards protecting 5G sidelink scheduling in C-V2X against intelligent DoS attacks," *IEEE Trans. Wireless Commun.*, vol. 22, no. 11, pp. 7273–7286, Mar. 2023, doi: 10.1109/TWC.2023.3249665.

[65] M. Yang, Y. Ju, L. Liu, Q. Pei, K. Yu, and J. J. P. C. Rodrigues, "Secure mmWave C-V2X communications using cooperative jamming," in *Proc. GLOBECOM IEEE Global Commun. Conf.*, Rio de Janeiro, Brazil, Jan. 2022, pp. 2686–2691, doi: 10.1109/GLOBECOM48099.2022.10001684.

[66] M. Maleki, M. Malik, P. Folkesson, B. Sangchoolie, and J. Karlsson, "Modeling and evaluating the effects of jamming attacks on connected automated road vehicles," in *Proc. IEEE 27th Pacific Rim Int. Symp. Dependable Comput. (PRDC)*, Beijing, China, 2022, pp. 12–23, doi: 10.1109/PRDC55274.2022.00016.

[67] K. N. Vaishnavi, S. D. Khorvi, R. Kishore, and S. Gurugopinath, "A survey on jamming techniques in physical layer security and anti-jamming strategies for 6G," in *Proc. 28th Int. Conf. Telecommun. (ICT)*, London, U.K., Jun. 2021, pp. 174–179, doi: 10.1109/ICT52184.2021.9511465.

[68] I. Maskulainen, P. Luoto, P. Pirinen, M. Bennis, K. Horneman, and M. Latva-Aho, "Performance evaluation of adaptive beamforming in 5G-V2X networks," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Oulu, Finland, Jun. 2017, pp. 1–5, doi: 10.1109/EuCNC.2017.7980728.

[69] J. C. Sprott, *Elegant Chaos: Algebraically Simple Chaotic Flows*. Singapore: World Scientific, 2010, doi: 10.1142/7183.

[70] B. Vaseghi, M. A. Pourmina, and S. Mobayen, "Secure communication in wireless sensor networks based on chaos synchronization using adaptive sliding mode control," *Nonlinear Dyn.*, vol. 89, no. 3, pp. 1689–1704, May 2017, doi: 10.1007/s11071-017-3543-9.

[71] B. Jovic, *Synchronization Techniques for Chaotic Communication Systems*. Cham, Switzerland: Springer, 2011, doi: 10.1007/978-3-642-21849-1.

[72] C. Tse and F. Lau, *Chaos-Based Digital Communication Systems*. Cham, Switzerland: Springer, 2003, doi: 10.1007/978-3-662-05183-2.

[73] K. H. M. Gularte, J. C. G. Gómez, H. D. S. Rabelo, and J. A. R. Vargas, "Minimal underactuated synchronization with applications to secure communication," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 125, Oct. 2023, Art. no. 107376, doi: 10.1016/j.cnsns.2023.107376.

[74] J. C. G. Gómez, R. R. dos Santos, K. H. M. Gularte, J. A. R. Vargas, and J. A. R. Hernández, "A robust underactuated synchronizer for a five-dimensional hyperchaotic system: Applications for secure communication," *Int. J. Control, Autom. Syst.*, vol. 21, no. 9, pp. 2891–2903, Aug. 2023, doi: 10.1007/s12555-022-0909-7.

[75] K. H. M. Gularte, L. M. Alves, J. A. R. Vargas, S. C. A. Alfaro, G. C. De Carvalho, and J. F. A. Romero, "Secure communication based on hyperchaotic underactuated projective synchronization," *IEEE Access*, vol. 9, pp. 166117–166128, 2021, doi: 10.1109/ACCESS.2021.3134829.

[76] J. Yu and Y.-D. Yao, "Detection performance of chaotic spreading LPI waveforms," *IEEE Trans. Wireless Commun.*, vol. 4, no. 2, pp. 390–396, Mar. 2005, doi: 10.1109/TWC.2004.842948.

[77] B. V. Nguyen, M. T. Nguyen, H. Jung, and K. Kim, "Designing anti-jamming receivers for NR-DCSK systems utilizing ICA, WPD, and VMD methods," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 66, no. 9, pp. 1522–1526, Sep. 2019, doi: 10.1109/TCSII.2019.2891254.

[78] J.-J. E. Slotine and W. Li, *Applied Nonlinear Control*, vol. 199. Englewood Cliffs, NJ, USA: Prentice-Hall, 1991.

[79] K. H. M. Gularte, J. C. G. Gómez, J. A. R. Vargas, and R. R. Dos Santos, "Projective synchronization and antisynchronization of underactuated systems," in *Proc. 14th IEEE Int. Conf. Ind. Appl. (INDUSCON)*, Aug. 2021, pp. 1317–1322, doi: 10.1109/INDUSCON51756.2021.9529719.

[80] K. H. M. Gularte, J. C. G. Gómez, J. A. R. Vargas, and R. R. Dos Santos, "Chaos-based cryptography using an underactuated synchronizer," in *Proc. 14th IEEE Int. Conf. Ind. Appl. (INDUSCON)*, Aug. 2021, pp. 1303–1308, doi: 10.1109/INDUSCON51756.2021.9529455.

[81] K. H. M. Gularte, J. C. G. Gómez, M. E. V. Melgar, and J. A. R. Vargas, "Chaos synchronization and its application in parallel cryptography," in *Proc. IEEE 5th Colombian Conf. Autom. Control (CCAC)*, Oct. 2021, pp. 198–203, doi: 10.1109/CCAC51819.2021.9633306.

[82] K. H. M. Gularte, J. C. G. Gómez, M. E. V. Melgar, and J. A. R. Vargas, "Underactuated 4D-hyperchaotic system for secure communication in the presence of disturbances," in *Proc. IEEE 5th Colombian Conf. Autom. Control (CCAC)*, Ibague, Colombia, Oct. 2021, pp. 210–215, doi: 10.1109/CCAC51819.2021.9633276.

[83] K. H. M. Gularte, F. O. Hara, J. A. R. Vargas, and F. O. Guimaraes, "Hyperchaos-based secure communication using Lyapunov theory," in *Proc. 15th IEEE Int. Conf. Ind. Appl. (INDUSCON)*, Brazil, Nov. 2023, pp. 747–751, doi: 10.1109/INDUSCON58041.2023.10374589.

[84] K. H. M. Gularte, F. O. Hara, J. A. R. Vargas, and F. O. Guimarães, "Secure communications in the presence of disturbances based on Lyapunov theory," in *Proc. 15th IEEE Int. Conf. Ind. Appl. (INDUSCON)*, Nov. 2023, pp. 512–517, doi: 10.1109/induscon58041.2023.10374895.

[85] A. M. Wyglinski, T. Wickramarathne, D. Chen, N. J. Kirsch, K. S. Gill, T. Jain, V. Garg, T. Li, S. Paul, and Z. Xi, "Phantom car attack detection via passive opportunistic RF localization," *IEEE Access*, vol. 11, pp. 27676–27692, 2023, doi: 10.1109/ACCESS.2023.3257281.

[86] A. Krayani, G. Barabino, L. Marcenaro, and C. Regazzoni, "Integrated sensing and communication for joint GPS spoofing and jamming detection in vehicular V2X networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Glasgow, U.K., Mar. 2023, pp. 1–7, doi: 10.1109/WCNC55385.2023.10118852.

[87] Y. Feng, S. E. Huang, W. Wong, Q. A. Chen, Z. M. Mao, and H. X. Liu, "On the cybersecurity of traffic signal control system with connected vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 16267–16279, Sep. 2022, doi: 10.1109/TITS.2022.3149449.

[88] J. Shen, Z. Wan, Y. Luo, Y. Feng, Z. M. Mao, and Q. A. Chen, "Detecting data spoofing in connected vehicle based intelligent traffic signal control using infrastructure-side sensors and traffic invariants," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2023, pp. 1–8, doi: 10.1109/IV55152.2023.10186689.

[89] Z. Yang, J. Ying, J. Shen, Y. Feng, Q. A. Chen, Z. M. Mao, and H. X. Liu, "Anomaly detection against GPS spoofing attacks on connected and autonomous vehicles using learning from demonstration," *IEEE Trans. Intell. Transp. Syst.*, early access, Apr. 26, 2023, doi: 10.1109/TITS.2023.3269029.

[90] N. Wang, J. Tang, and K. Zeng, "Spoofing attack detection in mm-wave and massive MIMO 5G communication," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Washington, DC, USA, Jun. 2019, pp. 1–5, doi: 10.1109/CNS.2019.8802768.

[91] K. Gao, H. Wang, H. Lv, and P. Gao, "Your locations may be lies: Selective-PRS-Spoofing attacks and defence on 5G NR positioning systems," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, New York City, NY, USA, May 2023, pp. 1–10, doi: 10.1109/infocom53939.2023.10228877.

[92] M. R. Nosouhi, K. Sood, M. Grobler, and R. Doss, "Towards spoofing resistant next generation IoT networks," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 1669–1683, Apr. 2022, doi: 10.1109/TIFS.2022.3170276.

[93] N. Wang, L. Jiao, P. Wang, W. Li, and K. Zeng, "Machine learning-based spoofing attack detection in mmWave 60GHz IEEE 802.11ad networks," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, Toronto, ON, Canada, Jul. 2020, pp. 2579–2588, doi: 10.1109/INFOCOM41043.2020.9155382.

[94] D. Orlando, S. Bartoletti, I. Palamà, G. Bianchi, and N. B. Melazzi, "Innovative attack detection solutions for wireless networks with application to location security," *IEEE Trans. Wireless Commun.*, vol. 22, no. 1, pp. 205–219, Jan. 2023, doi: 10.1109/TWC.2022.3192225.

[95] K. Zheng, L. Zhao, J. Mei, B. Shao, W. Xiang, and L. Hanzo, "Survey of large-scale MIMO systems," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1738–1760, 3rd Quart., 2015, doi: 10.1109/COMST.2015.2425294.

[96] S. Kutty and D. Sen, "Beamforming for millimeter wave communications: An inclusive survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 949–973, 2nd Quart., 2016, doi: 10.1109/COMST.2015.2504600.

[97] G. Chopra, R. K. Jha, and S. Jain, "TPA: Prediction of spoofing attack using thermal pattern analysis in ultra dense network for high speed handover scenario," *IEEE Access*, vol. 6, pp. 66268–66284, 2018, doi: 10.1109/ACCESS.2018.2875921.

[98] 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, doi: 10.1109/MNET.2017.1600257.

[99] T. P. B. Vieira, D. F. Tenório, J. P. C. L. da Costa, E. P. de Freitas, G. D. Galdo, and R. T. de Sousa Júnior, "Model order selection and eigen similarity based framework for detection and identification of network attacks," *J. Netw. Comput. Appl.*, vol. 90, pp. 26–41, Jul. 2017, doi: 10.1016/j.jnca.2017.04.012.

[100] J. P. A. Maranhão, J. P. C. L. da Costa, E. P. de Freitas, E. Javidi, and R. T. de Sousa Júnior, "Error-robust distributed denial of service attack detection based on an average common feature extraction technique," *Sensors*, vol. 20, no. 20, p. 5845, Oct. 2020, doi: 10.3390/s20205845.

[101] J. P. A. Maranhão, J. P. C. L. da Costa, E. Javidi, C. A. B. de Andrade, and R. T. de Sousa, "Tensor based framework for distributed denial of service attack detection," *J. Netw. Comput. Appl.*, vol. 174, Jan. 2021, Art. no. 102894, doi: 10.1016/j.jnca.2020.102894.

[102] J. P. A. Maranhão, J. P. C. L. d. Costa, E. P. de Freitas, E. Javidi, and R. T. de Sousa, "Noise-robust multilayer perceptron architecture for distributed denial of service attack detection," *IEEE Commun. Lett.*, vol. 25, no. 2, pp. 402–406, Feb. 2021, doi: 10.1109/LCOMM.2020.3032170.

[103] M. R. Dey, M. Patra, and P. Mishra, "Efficient detection and localization of DoS attacks in heterogeneous vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 5, pp. 5597–5611, May 2023, doi: 10.1109/TVT.2022.3233624.

[104] X. Ge, Q.-L. Han, Q. Wu, and X.-M. Zhang, "Resilient and safe platooning control of connected automated vehicles against intermittent denial-of-service attacks," *IEEE/CAA J. Autom. Sinica*, vol. 10, no. 5, pp. 1234–1251, May 2023, doi: 10.1109/JAS.2022.105845.

[105] S. Ahmad, I. Raza, M. H. Jamal, S. Djuraev, S. Hur, and I. Ashraf, "Central aggregator intrusion detection system for denial of service attacks," *Comput., Mater. Continua*, vol. 74, no. 2, pp. 2363–2377, Oct. 2023, doi: 10.32604/cmc.2023.032694.

[106] E. P. Valentini, G. P. R. Filho, R. E. De Grande, C. M. Ranieri, L. A. P. Júnior, and R. I. Meneguette, "A novel mechanism for misbehavior detection in vehicular networks," *IEEE Access*, vol. 11, pp. 68113–68126, 2023, doi: 10.1109/ACCESS.2023.3292055.

[107] A. Haydari and Y. Yilmaz, "RSU-based online intrusion detection and mitigation for VANET," *Sensors*, vol. 22, no. 19, p. 7612, Oct. 2022, doi: 10.3390/s22197612.

[108] N. Ludant and G. Noubir, "SigUnder: A stealthy 5G low power attack and defenses," in *Proc. 14th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Abu Dhabi, United Arab Emirates, Jun. 2021, pp. 250–260, doi: 10.1145/3448300.3467817.

[109] B. Mokhtar and M. Azab, "Survey on security issues in vehicular ad hoc networks," *Alexandria Eng. J.*, vol. 54, no. 4, pp. 1115–1126, Dec. 2015, doi: 10.1016/j.aej.2015.07.011.

[110] F. Xu, S. Ahmad, M. N. Khan, M. Ahmed, S. Raza, F. Khan, Y. Ma, and W. U. Khan, "Beyond encryption: Exploring the potential of physical layer security in UAV networks," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 35, no. 8, Sep. 2023, Art. no. 101717, doi: 10.1016/j.jksuci.2023.101717.

[111] Y. Yao, F. Shu, Z. Li, X. Cheng, and L. Wu, "Secure transmission scheme based on joint radar and communication in mobile vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 9, pp. 10027–10037, May 2023, doi: 10.1109/TITS.2023.3271452.

[112] H. Ayaz, G. Abbas, M. Waqas, Z. H. Abbas, M. Bilal, A. Nauman, and M. A. Jamshed, "Physical layer security analysis using radio frequency-fingerprinting in cellular-V2X for 6G communication," *IET Signal Process.*, vol. 17, no. 5, May 2023, Art. no. e12225, doi: 10.1049/sil2.12225.

[113] N. Jaiswal, A. Pandey, S. Yadav, and N. Purohit, "Physical layer security performance of NOMA-assisted vehicular communication systems over double-Rayleigh fading channels," *Phys. Commun.*, vol. 57, Apr. 2023, Art. no. 101968, doi: 10.1016/j.phycom.2022.101968.

[114] A. Shen, J. Luo, J. Ning, Y. Li, Z. Wang, and B. Duo, "Safeguarding UAV networks against active eavesdropping: An elevation angle-distance trade-off for secrecy enhancement," *Drones*, vol. 7, no. 2, p. 109, Feb. 2023, doi: 10.3390/drones7020109.

[115] Z. Wu, K. Guo, and S. Zhu, "Covert communication for integrated satellite–terrestrial relay networks with cooperative jamming," *Electronics*, vol. 12, no. 4, p. 999, Feb. 2023, doi: 10.3390/electronics12040999.

[116] M. Li, H. Yuan, C. Maple, W. Cheng, and G. Epiphaniou, "Physical layer security analysis of cognitive NOMA Internet of Things networks," *IEEE Syst. J.*, vol. 17, no. 1, pp. 1045–1055, Mar. 2023, doi: 10.1109/JSYST.2022.3190297.

[117] K. Shim and B. An, "Exploiting impact of eavesdropping attacks on secrecy performance in WPT-based secure multi-hop transmission," in *Proc. 14th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Paris, France, Jul. 2023, pp. 392–397, doi: 10.1109/icufn57995.2023.10200146.

[118] H. Jung, I.-H. Lee, and J. Joung, "Security energy efficiency analysis of analog collaborative beamforming with stochastic virtual antenna array of UAV swarm," *IEEE Trans. Veh. Technol.*, vol. 71, no. 8, pp. 8381–8397, Aug. 2022, doi: 10.1109/TVT.2022.3171313.

[119] C. Han, L. Bai, T. Bai, and J. Choi, "Joint UAV deployment and power allocation for secure space-air-ground communications," *IEEE Trans. Commun.*, vol. 70, no. 10, pp. 6804–6818, Oct. 2022, doi: 10.1109/TCOMM.2022.3203471.

[120] K. Yu, L. Tan, S. Mumtaz, S. Al-Rubaye, A. Al-Dulaimi, A. K. Bashir, and F. A. Khan, "Securing critical infrastructures: Deep-learning-based threat detection in IIoT," *IEEE Commun. Mag.*, vol. 59, no. 10, pp. 76–82, Oct. 2021, doi: 10.1109/MCOM.101.2001126.

[121] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1851–1877, 2nd Quart., 2019, doi: 10.1109/COMST.2019.2891891.

[122] A. Roy, J. Kokila, N. Ramasubramanian, and B. S. Begum, "Device-specific security challenges and solution in IoT edge computing: A review," *J. Supercomput.*, vol. 79, no. 18, pp. 20790–20825, Jun. 2023, doi: 10.1007/s11227-023-05450-6.

[123] H. Hu, R. Lu, Z. Zhang, and J. Shao, "REPLACE: A reliable trust-based platoon service recommendation scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1786–1797, Feb. 2017, doi: 10.1109/TVT.2016.2565001.

[124] G. Usha, S. Kannimuthu, P. D. Mahendiran, A. K. Shanker, and D. Venugopal, "Static analysis method for detecting cross site scripting vulnerabilities," *Int. J. Inf. Comput. Secur.*, vol. 13, no. 1, p. 32, Apr. 2020, doi: 10.1504/ijics.2020.108123.

[125] S. Gupta, C. Maple, and R. Passerone, "An investigation of cyber-attacks and security mechanisms for connected and autonomous vehicles," *IEEE Access*, vol. 11, pp. 90641–90669, 2023, doi: 10.1109/ACCESS.2023.3307473.

[126] M. N. Al-Mhiqani, R. Ahmad, Z. Z. Abidin, W. Yassin, A. Hassan, K. H. Abdulkareem, N. S. Ali, and Z. Yunos, "A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations," *Appl. Sci.*, vol. 10, no. 15, p. 5208, Jul. 2020, doi: 10.3390/app10155208.

[127] S. G. Abbas, I. Vaccari, F. Hussain, S. Zahid, U. U. Fayyaz, G. A. Shah, T. Bakhshi, and E. Cambiaso, "Identifying and mitigating phishing attack threats in IoT use cases using a threat modelling approach," *Sensors*, vol. 21, no. 14, p. 4816, Jul. 2021, doi: 10.3390/s21144816.

[128] G. Sharma, S. Vidalis, N. Anand, C. Menon, and S. Kumar, "A survey on layer-wise security attacks in IoT: Attacks, countermeasures, and open-issues," *Electronics*, vol. 10, no. 19, p. 2365, Sep. 2021, doi: 10.3390/electronics10192365.

[129] M. A. Amanullah, R. A. A. Habeeb, F. H. Nasaruddin, A. Gani, E. Ahmed, A. S. M. Nainar, N. M. Akim, and M. Imran, "Deep learning and big data technologies for IoT security," *Comput. Commun.*, vol. 151, pp. 495–517, Feb. 2020, doi: 10.1016/j.comcom.2020.01.016.

[130] Y. Lee, S. Woo, Y. Song, J. Lee, and D. H. Lee, "Practical vulnerability-information-sharing architecture for automotive security-risk analysis," *IEEE Access*, vol. 8, pp. 120009–120018, 2020, doi: 10.1109/ACCESS.2020.3004661.

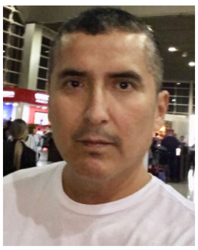
[131] W. G. Halfond, J. Viegas, and A. Orso, "A classification of SQL injection attacks and countermeasures," in *Proc. IEEE Int. Symp. Secure Softw. Eng.*, vol. 1, Mar. 2006, pp. 13–15.

[132] A. Boukerche and Q. Zhang, "Countermeasures against worm spreading: A new challenge for vehicular networks," *ACM Comput. Surv.*, vol. 52, no. 2, pp. 1–25, May 2019, doi: 10.1145/3284748.

[133] S. A. Bhosale and S. S. Sonavane, "Wormhole attack detection system for IoT network: A hybrid approach," *Wireless Pers. Commun.*, vol. 124, no. 2, pp. 1081–1108, Nov. 2021, doi: 10.1007/s11277-021-09395-y.

[134] Y. Roumani, "Patching zero-day vulnerabilities: An empirical analysis," *J. Cybersecurity*, vol. 7, no. 1, Nov. 2021, Art. no. tyab023, doi: 10.1093/cybsec/tyab023.

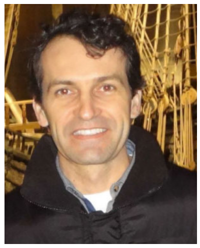
KEVIN HERMAN MURARO GULARTE received the B.S. degree in mechatronics engineering, the master's degree in mechatronic systems, and the Dr.Sc. degree in electronic systems and automation from the University of Brasília (UnB), in 2013, 2018, and 2021, respectively. His research interests include synchronization systems, chaotic systems, adaptive control, neural networks, Lyapunov stability theory, and system identification.



JOSÉ ALFREDO RUIZ VARGAS (Member, IEEE) received the Dr.Sc. degree in electronics and computer engineering from the Aeronautics Institute of Technology, São Paulo, Brazil, in 2003. From 2016 to 2017, he was a Visiting Professor with the University of Alberta, Edmonton, AB, Canada. He is a Professor of control systems with the Department of Electrical Engineering, University of Brasília. Since 2023, he has been engaged as a Researcher with Hamm-Lippstadt University of Applied Sciences, Lippstadt, Germany. His current research interests include chaos-based communication, V2X communication, nonlinear and adaptive control, neural networks, and online machine learning.

JOÃO PAULO JAVIDI DA COSTA (Senior Member, IEEE) received the Diploma degree in electronic engineering from the Military Institute of Engineering (IME), Rio de Janeiro, Brazil, in 2003, the M.Sc. degree in telecommunications from the University of Brasília (UnB), Brazil, in 2006, and the Ph.D. degree in electrical engineering from Ilmenau University of Technology (TU Ilmenau), Germany, in 2010. Since August 2020, he has been a Professor of applied electrical engineering with Hamm-Lippstadt University of Applied Sciences, Germany. He became a Research Professor with HSHL, in March 2022. He is a Professor Member of the Promotionskolleg NRW (PK NRW) in order to supervise Ph.D. students. He has published more than 195 scientific publications and patents. His research interests include autonomous vehicles, 6G, GNSS, and adaptive and array signal processing. He received seven best paper awards in international conferences.

ANTONIO SANTOS DA SILVA received the B.S. degree in software engineering from the Federal University of Goiás, in 2019, and the M.Sc. degree in computer science from the Federal University of Rio Grande do Sul (UFRGS), Brazil, in 2021, where he is currently pursuing the Ph.D. degree with the Graduate School for Applied Research in North Rhine-Westphalia (PK NRW), Karlsruhe Institute of Technology (KIT), Germany. He is also a Research Assistant with Hamm-Lippstadt University of Applied Sciences, Germany. His research interests include ICN, SDN, fog computing, 5G, beyond 5G, and V2X communication.



GIOVANNI ALMEIDA SANTOS received the bachelor's and master's degrees in computer science from the Federal University of Paraíba (UFPB), Campina Grande, Brazil, in 1998 and 2001, respectively, and the Ph.D. degree in electrical engineering from the University of Brasília (UnB), Brazil, in 2022. From 2003 to 2010, he was a Lecturer in computer science with the Catholic University of Brasília (UCB). Since 2010, he has been a Professor of software engineering with UnB. Since 2023, he has been engaged as a Researcher with Hamm-Lippstadt University of Applied Sciences, Lippstadt, Germany. His research interests include autonomous vehicles and informatics in education.

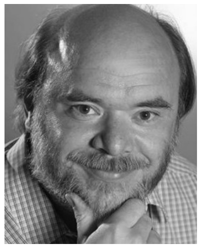
YUMING WANG is currently pursuing the bachelor's degree in electronic engineering with Hamm-Lippstadt University of Applied Sciences (HSHL). He is also a Research Student on the project B5GCyberTestV2X funded by the BSI. His research interests include autonomous systems, embedded systems, and cybersecurity.

CHRISTIAN ALFONS MÜLLER received the degree (Hons.) in computational linguistics and the Ph.D. degree in computer science from Saarland University, Saarbrücken, Germany, in 1994 and January 2006, respectively. His dissertation "Zweistufige kontextsensitive Sprecherklassifikation am Beispiel von Alter und Geschlecht" (Two-Layered Context-Sensitive Speaker Classification on the Example of Age and Gender) was supervised by Prof. W. Wahlster. He possesses more than a decade of professional experience in the field of speech technology. Currently, he is a Senior Researcher with Germany Research Center for Artificial Intelligence (DKFI), Saarbrücken. From 2006 to 2008, he was a Visiting Researcher with the International Computer Science Institute (ICSI), Berkeley, CA, USA. This work was conducted while he was with ICSI.

CHRISTOPH LIPPS (Member, IEEE) is a Researcher with the Intelligent Networks Department, German Research Center for Artificial Intelligence, Kaiserslautern. There, he is a Team Leader of the cyber resilience and security. His research interests include cyber-security, artificial intelligence, physical layer security, and security in the sixth generation (6G) wireless systems.

RAFAEL TIMÓTEO DE SOUSA JÚNIOR (Senior Member, IEEE) received the bachelor's degree in electrical engineering from the Federal University of Paraíba (UFPB), Campina Grande, Brazil, in 1984, the combined master's/D.E.A. degree in information systems and computing from the Ecole Superieure d'Electricite—Supelec, Rennes, France, in 1985, and the Ph.D. degree in telecommunications and signal processing from the University of Rennes 1, Rennes, in 1988. He was a Visiting Researcher with the Network Security and Information Systems Group (SSIR), Ecole Superieure d'Electricite—Supelec, from 2006 to 2007. He was with private sector, from 1988 to 1996. Since 1996, he has been an Associate Professor of engineering of communication networks with the Department of Electrical Engineering, University of Brasília, Brazil, where he is currently the Coordinator of the Professional Graduate Program in Electrical Engineering (PPEE) and supervises the Decision Technologies Laboratory (LATITUDE). He is also a Researcher with level 2 (PQ-2) productivity fellowship with the National Council for Scientific and Technological Development (CNPq). His professional experience includes research projects with Dell Computers, HP, IBM, Cisco, and Siemens. He is also the Coordinator of research, development, and technology transfer projects with the Ministries of Planning, Economy, and Justice of Brazil; the Institutional Security Cabinet of the Presidency of Brazil; the Administrative Council for Economic Defense; the Federal Attorney General; and the Federal Public Defender's Office. He has received research grants from Brazilian research and innovation agencies, such as CNPq, CAPES, FINEP, RNP, and FAPDF. He conducts research in cyber, information, and network security; distributed data services; machine learning for intrusion and fraud detection; signal processing; energy harvesting; and physical layer security.

WALTER DE BRITTO VIDAL FILHO received the B.S. degree in mechanical engineering from the Federal University of Pernambuco (UFPE), in 1995, the M.Sc. degree in mechanical engineering from the Pontifical Catholic University of Rio de Janeiro (PUC-Rio), in 1998, and the D.Sc. degree in mechanical engineering from the University of Sao Paulo (USP), in 2003. Currently, he is an Associate Professor with the University of Brasília (UnB). His research interests include mechatronics, robotic inspection, unmanned aerial vehicles, intelligent control systems, medical robotics, and assistive technologies.



PHILIPP SLUSALLEK received the combined Diploma/M.Sc. degree in physics from Frankfurt and Tbingen and the Ph.D. degree in computer science from Erlangen University. He is the Scientific Director with the German Research Centre for Artificial Intelligence (DFKI), where he has been heading the research area "Agents and Simulated Reality," since 2008. He is also the Director for Research with the Intel Visual Computing Institute (a central research institute), Saarland University, founded in 2009, in collaboration with Intel, DFKI, and the two local Max-Planck-institutes. At Saarland University, he has been a Professor of computer graphics, since 1999, and a Principle Investigator with the German Excellence-Cluster on "Multimodal Computing and Interaction," since 2007. Before coming to Saarland University, he was a Visiting Assistant Professor with Stanford University, USA. His research interests include novel service-oriented architectures for 3-D internet technology; integrating research in areas, such as real-time realistic graphics, artificial intelligence, high-performance computing; and security by design for creating distributed, immersive, and collaborative environments for simulation, analysis, visualization, and training.

HANS DIETER SCHOTTEN (Member, IEEE) received the Ph.D. degree from RWTH Aachen University, Aachen, Germany, in 1997. From 1999 to 2003, he was with Ericsson. From 2003 to 2007, he was with Qualcomm. He became the Manager of Research and Development Group, a Research Coordinator of Qualcomm Europe, and the Director of Technical Standards. In 2007, he accepted the offer to become a Full Professor with the Technical University of Kaiserslautern, Kaiserslautern, Germany. In 2012, he became the Scientific Director of the German Research Center for Artificial Intelligence (DFKI) and the Head of the Department for Intelligent Networks. From 2013 to 2017, he was the Dean of the Department of Electrical Engineering, Technical University of Kaiserslautern. He has authored more than 200 papers and participated more than 40 European and national collaborative research projects. Since 2018, he has been the Chairman of the German Society for Information Technology and a member of the Supervisory Board of VDE.