IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 12 October 2024, accepted 19 November 2024, date of publication 21 November 2024,
date of current version 9 December 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3504404

SURVEY

Integrating Cybersecurity in V2X: A Review of Simulation Environments

KEVIN HERMAN MURARO GULARTE [1],
JOÃO PAULO JAVIDI DA COSTA [1,2,3,4], **(Senior Member, IEEE),**
JOSÉ ALFREDO RUIZ VARGAS [5], **(Member, IEEE), ANTONIO SANTOS DA SILVA** [2,4,6,7],
GIOVANNI ALMEIDA SANTOS [2], **YUMING WANG** [2],
CHRISTIAN ALFONS MÜLLER [8], **CHRISTOPH LIPPS** [9], **(Member, IEEE),**
RAFAEL TIMÓTEO DE SOUSA JÚNIOR [3], **(Senior Member, IEEE),**
WALTER DE BRITTO VIDAL FILHO [10], **PHILIPP SLUSALLEK** [8,11],
AND HANS DIETER SCHOTTEN [9,12], **(Member, IEEE)**

[1] Graduate Program in Mechatronic Systems (PPMEC), University of Brasília (UnB), Brasília 70910-900, Brazil
[2] Hamm-Lippstadt University of Applied Sciences (HSHL), Lippstadt Campus, 59063 Hamm, Germany
[3] Professional Postgraduate Program in Electrical Engineering (PPEE), UnB, Brasília 70910-900, Brazil
[4] Graduate School for Applied Research in North Rhine-Westphalia (PK NRW), 44801 Bochum, Germany
[5] Department of Electrical Engineering, University of Brasília (UnB), Brasília 70910-900, Brazil
[6] Karlsruhe Institute of Technology (KIT), 76133 Karlsruhe, Germany
[7] Graduate Program in Computing (PPGC), Federal University of Rio Grande do Sul (UFRGS), Porto Alegre 91501-970, Brazil
[8] German Research Center for Artificial Intelligence (DFKI), 66123 Saarbrücken, Germany
[9] DFKI, 67663 Kaiserslautern, Germany
[10] Department of Mechanical Engineering, UnB, Brasília 70910-900, Brazil
[11] Saarland University, Saarland Informatics Campus, 66123 Saarbrücken, Germany
[12] 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 supported in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior-Brasil (CAPES) under Grant 001, in part by the University of Brasilia, and in part by the Bundesamt für Sicherheit in der Informationstechnik (BSI) through the Project Beyond 5G Virtuelle Umgebung für Cybersicherheitstests von V2X-Systemen under Grant B5GCyberTestV2X.

ABSTRACT The deployment and acceptance of Vehicle-to-Everything (V2X) technologies are essential for the advancement of intelligent transportation systems, requiring robust simulation tools for development and validation. This paper offers an overview of leading V2X simulation tools, emphasizing their role in communication and cybersecurity applications. Existing surveys are reviewed, identifying gaps such as the limited coverage of less known tools such as CARLA and CarSim and the absence of detailed market analyses. A thorough assessment of the market significance of V2X simulation tools is provided, highlighting annual trends and profiling leading companies. Publication trends across major scientific databases are also examined, reflecting the growing interest and research diversity in V2X simulations. The review includes an analysis of crucial simulation tools such as SUMO, NS3, OMNeT++, Veins, and CARLA, emphasizing their contributions to V2X communications. Regarding cybersecurity, the study explores simulation parameters for mitigating security threats such as jamming, spoofing, Denial of Service (DoS), and eavesdropping. Furthermore, the increasing integration of different simulation tools is highlighted to address their individual limitations. Finally, emerging research opportunities are identified, advocating for the integration of co-simulation frameworks and AI-driven (Artificial Intelligence) approaches to improve the accuracy and resilience of V2X systems. This survey aims to guide future research efforts in developing secure, efficient, and scalable V2X communication technologies.

INDEX TERMS Vehicle-to-everything, connected and automated vehicles, trends in V2X simulations, V2X simulation tools, V2X cybersecurity, radio jamming, spoofing, denial of service, eavesdropping.

I. INTRODUCTION

In the era of intelligent mobility, Vehicle-to-Everything (V2X) technologies are revolutionizing our transportation

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

systems. This shift is driven by the increasing recognition of V2X Information and Communication Technology (ICT) as a groundbreaking tool for improving road safety, optimizing transportation, and disrupting society through infotainment and Mobility as a Service (MaaS) initiatives [1]. Given its extensive capabilities, V2X has garnered considerable interest for its potential to enhance the safety of drivers, passengers and pedestrians, efficiently manage traffic flow, and introduce advanced services [2], [3], [4]. To understand these capabilities in detail, Table 1 [5] illustrates the range of communication types encompassed by V2X, categorized into specific groups [6], [7], [8], [9], [10], [11], [12], [13]. Specifically, this table defines the six types of V2X communications: Vehicle-to-Vehicle (V2V), Vehicle-to-Person/Pedestrian (V2P), Vehicle-to-Infrastructure (V2I), Vehicle-to-Network (V2N), Vehicle-to-Grid (V2G), and Vehicle-to-Cloud (V2C).

TABLE 1. Types of V2X communication: V2V, V2P, V2I, V2N, V2G, and V2C.

V2X Type	Details
Vehicle-to-Vehicle	Direct interaction among vehicles
Vehicle-to-Person/Pedestrian	Interaction with vulnerable road users such as pedestrians and cyclists
Vehicle-to-Infrastructure	Communication with infrastructure elements such as traffic lights
Vehicle-to-Network	Linking vehicles with network entities via mobile network stations
Vehicle-to-Grid	Enabling electric vehicles to connect and interact with the power grid
Vehicle-to-Cloud	Communication between vehicles and cloud servers for data exchange and updates on vehicle status and sensor information

V2X communication enables seamless interactions between vehicles and everything around them, from other vehicles and pedestrians to road infrastructures and traffic management systems. This interconnectedness significantly improves traffic efficiency, road safety, and environmental impact [14]. However, despite these advantages, realizing the full potential of V2X technologies requires overcoming substantial technical and security challenges [15]. For instance, as vehicles progress from assisted driving to full autonomy, the risk of cyber threats increases [16]. The extensive communication channels with external entities, such as networks, infrastructure, and the electric grid, heighten vulnerability to cyber attacks. The potential exploitation of remote control features in intelligent vehicles has raised substantial societal concern [17]. As vehicles become more sophisticated and interconnected, their security challenges grow, resembling those faced by smartphones [17]. Moreover, the Fifth-Generation (5G) network infrastructure, integral to V2X systems, is susceptible to cyber threats, potentially leading to data breaches and corruption [7].

In order to address these challenges, advanced simulation tools can allow developers and researchers to predict, analyze, and refine the complex behaviors of integrated transportation networks under safe, controlled conditions. Moreover, validation of automotive functionalities using simulation tools in millions of scenarios incurs a tiny cost compared to test field validation. Furthermore, simulation validation does not present safety issues compared to test field validation. As a result, simulation validation can dramatically reduce costs and is completely safe. Nevertheless, the complexity and cost of testing advanced vehicle technologies in real-world conditions necessitate using advanced simulations.

For this reason, developing simulation tools that lend themselves to designing, testing, and optimizing V2X communication systems has become a vital area of research [18]. For example, in Germany, the importance of simulators is highlighted by initiatives such as the collaboration between Technischer Überwachungsverein (TÜV) SÜD, the German vehicle licensing body, and Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI), the German Research Center for Artificial Intelligence. They are developing platforms to evaluate autonomous vehicle Artificial Intelligence (AI) modules, demonstrating the relevance of simulations in the modern automotive industry.

Specifically, V2X-related simulation frameworks combining tools such as Car Learning to Act (CARLA) [19], Objective Modular Network Testbed in C++ (OMNeT++) [20], SIMU5G [21], Simulation of Urban MObility (SUMO) [22], Network Simulator 3 (NS3) [23], Vehicles in Network Simulation (Veins) [24], and CarSim [25] offer diverse capabilities that are critical for the development of functionalities in V2X environments. Many of these simulation tools have been available for a considerable time, as seen in Table 2. These tools can simulate realistic urban, suburban, and rural traffic conditions and model the behavior of hundreds to thousands of individual static and dynamic nodes within milliseconds of real-time. For instance, CARLA provides high-fidelity visual simulation of urban environments, which is crucial for testing the perceptual algorithms of autonomous vehicles. In contrast, OMNeT++ excels in detailed network simulation, allowing for intricate modeling of communication protocols and network traffic. SIMU5G further extends these capabilities into the domain of 5G communications, introducing the 5G user plane into the simulation of mobile networks and their interactions with vehicular technologies.

TABLE 2. Released date of the main simulation tools in the context of V2X communication covered in Section II and the number of results in searches on Scopus based on the criteria "title, abstract or keyword".

Simulation Tool	Date	Reference	Results in the Scopus
Veins	2008	[26]	603654
NS3	2008	[27]	11643
SUMO	2001	[28]	10915
OMNeT++	1997	[20]	2824
CarSim	1996	[25]	2601
CARLA	2017	[19]	1789

Table 2 also shows the research results collected on January 1, 2024, in the Scopus database using the "title, abstract or keyword" criteria. The chosen simulation tools had the most relevance in Section II of this work. In the case of NS3, the search was performed using the tags

("NS3" OR "NS-3"). The term Veins is a common term in works unrelated to the V2X context, so it is safe to assume that most of the results are noisy; that is, they are not correlated to the Veins simulation tool. However, in the other simulation tools, it is clear that a considerable number of works in the literature show the historical relevance of these simulation tools.

Moreover, the robustness of V2X systems against cyber threats is another critical area where simulation tools demonstrate their value since millions of scenarios considering the impact of cyber-attacks can be tested and validated. These systems are potential targets for various cyber-attacks, including spoofing, jamming, and Denial of Service (DoS) attacks, each capable of disrupting vehicle communication and compromising safety. This paper shows simulation parameters for scenarios in the context of four cyber-attacks: jamming, spoofing, DoS, and eavesdropping. Jamming attacks disrupt communication by flooding the electromagnetic spectrum with high levels of noise or spurious interference signals, thereby impairing legitimate communications. Spoofing attacks involve falsifying the identity of a vehicle or infrastructure component to transmit deceptive messages, potentially leading to misdirected vehicles or incorrect traffic management decisions. DoS attacks overload the network with excessive requests, which can degrade the performance or completely halt the network services. Through V2X simulations, researchers can evaluate the resilience of network infrastructure under scaled DoS attacks, optimizing system design to ensure continuity of service and quick recovery. Lastly, eavesdropping involves unauthorized interception of communications, which threatens privacy and data security. Additionally, V2X simulation tools can help model the pathways and potential vulnerabilities that might be exploited for eavesdropping, aiding in the design of encrypted communication protocols and secure data transmission methods.

Understanding and mitigating cyberattacks through advanced simulations is crucial for the deployment of secure and reliable V2X systems. Moreover, simulation tools enable the modeling of these threats in a virtual environment, allowing researchers to evaluate the effectiveness of security protocols and countermeasures. For instance, effective simulation of spoofing scenarios helps in developing authentication protocols that can verify the integrity and origin of transmitted data. Simulators such as NS3 and Veins can model the impact of jamming on signal integrity and network throughput, facilitating the development of robust countermeasures such as spread spectrum techniques or adaptive frequency hopping.

By analyzing the drastic increase in patents in the area of V2X simulation, the industrial interest and investment in developing more sophisticated and accurate simulation environments are escalating. The next generation of V2X simulation tools must incorporate more sophisticated AI and machine learning algorithms, enabling them to predict and react to dynamic conditions of the vehicles and the communication systems more accurately in the presence of cybersecurity attacks.

The rise in cyberattacks brings a new dimension of risk, raising critical questions about how vehicles and their functionality respond in the presence of such threats. Projects such as B5GCyberTestV2X [29], an initiative focused on testing the resilience of vehicles against cyber attacks, are vital to this analysis. Another aspect that motivates this article is the emergence of new businesses and services based on V2X, including MaaS. V2X, primarily enabled by 5G and Sixth-Generation (6G) technologies, is critical to facilitating these innovations. Examples include receiving personalized offers in autonomous vehicles, such as discounts at nearby stores, and using neural and haptic interfaces to create immersive in-vehicle environments. V2X technology transforms the in-vehicle experience, as evidenced by innovations such as the Eight360 NOVA virtual reality simulator [30], [31], which illustrates the potential of creating dynamic virtual environments within vehicles. Therefore, this paper provides an overview to bridge the knowledge gap and foster a broader understanding of the dynamic interplay between V2X and simulations. Additionally, it proposes an integrated simulation framework designed to meet the demands of future V2X research in Section V.

For the sake of clarity, this section is divided into four subsections. In Subsection I-A, the main contributions of this paper are summarized, while in Subsection I-B, the organization of the survey is depicted. Finally, the scope and related surveys to V2X simulation tools are presented in Subsection I-C.

A. CONTRIBUTIONS

This work presents seven main contributions to the field of V2X simulations. The contributions are detailed below.

1) LITERATURE REVIEW OF SURVEYS

A review of existing survey papers on V2X simulation tools is provided in Subsection I-C, identifying potential gaps for future research, in contrast to [32] and [33]. This was accomplished by critically analyzing these surveys to assess their coverage of simulation tools and market relevance. Notable gaps were identified, such as the need for more discussion on less proeminent tools such as CARLA and CarSim and the absence of detailed market analyses. This analysis helped pinpoint specific gaps that this survey aims to address.

2) MARKET RELEVANCE ANALYSIS

A holistic view of the market significance of V2X simulation tools is presented in Subsection II-B, charting the annual trends and profiling the top 50 companies in the sector based on a meticulous patent search, in contrast to [32] and [33]. This analysis used targeted search parameters in both Google Patents and Scopus, ensuring a comprehensive overview of the patent landscape. The search strategy included filtering by publication date to track trends over time. Then, the results were cross-checked between both platforms to mitigate discrepancies and refine the conclusions.

3) SCIENTIFIC LANDSCAPE OVERVIEW

The publication trends of V2X simulation tools across several central scientific databases are analyzed in Subsection II-C, revealing the breadth of research and interest in this domain, in contrast to [32] and [33]. This analysis emphasizes the increasing focus on simulation tools within the V2X field, underlining how multiple databases have uncovered diverse research trajectories. These trends point to a rapidly evolving landscape, where simulation tools are becoming integral to advancing both academic research and practical applications in V2X communication systems.

4) V2X SIMULATORS RESEARCH EXPLORATION

A detailed examination of V2X simulator studies in Scopus is undertaken in Subsection II-D, offering insights into the diversity and intensity of research across different years, countries, and funding sponsors, in contrast to [32] and [33]. The analysis applied specific search filters to focus on relevant academic papers, ensuring the inclusion of high-quality studies. This exploration revealed vital trends in the temporal growth and geographic concentration of research, with China emerging as a dominant country. The systematic breakdown of results highlights regions and sponsors that have significantly contributed to the advancement of V2X simulation tools.

5) LITERATURE REVIEW AND EVOLUTION OF V2X SIMULATION TOOLS

The development and current state of leading V2X simulation tools, such as CARLA, OMNeT++, SUMO, NS3, and Veins, are thoroughly reviewed in Section III and Subsection II-C, highlighting their significant contributions to advancing V2X communications and simulation technologies, in contrast to [32]. The review is based on recent high-impact papers and those with significant citation counts, ensuring that the most influential studies are included. This literature review systematically examined studies focusing on various simulation tools and their integration with advanced sensor technologies. The tools explored offer robust environments for testing scenarios related to autonomous driving and Advanced Driver Assistance Systems (ADAS) functionalities, emphasizing their relevance in simulating real-world challenges such as cooperative perception and communication.

6) SECURITY ANALYSIS THROUGH SIMULATION PARAMETERS

The critical role of simulations and their respective parameters in analyzing and mitigating key security threats, including jamming, spoofing attacks, Denial of Service (DoS), and eavesdropping within the V2X domain, is emphasized in Section IV, showcasing how simulations enhance system security, in contrast to [32] and [33]. The detailed simulations replicate real-world conditions under controlled environments, enabling a comprehensive assessment of these cybersecurity threats. This section focuses on key simulation parameters that replicate specific attack scenarios. The simulations are structured to closely mirror the conditions under which these cyberattacks manifest, allowing researchers to evaluate potential vulnerabilities and countermeasures with precision. Through this structured simulation framework, researchers can better strategize to mitigate the impact of these threats on V2X communications, ensuring greater system resilience.

7) FUTURE RESEARCH DIRECTIONS

Emerging research opportunities in V2X simulation tools, as detailed in Section V, aim to direct future efforts towards co-simulation and integrating diverse simulation tools. This approach seeks to bridge current gaps and foster advancements in the field, contrasting with earlier studies [32], [33]. The focus is on enhancing the accuracy and interoperability of these tools, allowing for more complex and realistic simulations. There is also an analysis of future trends in simulation tools in the V2X cybersecurity context in Section VI. The exploration of integrating cybersecurity elements into these simulations aims to address increasing concerns about system vulnerabilities. This area of research suggests the need for further development in security-driven simulation frameworks to anticipate and counteract cyber threats in real-time V2X environments.

B. SURVEY ORGANIZATION AND SCOPE

In Figure 1, the organization of this review paper is presented, including all six sections and their respective subsections. According to Figure 1, Section II shows an overview of the V2X simulations area, showing statistics related to papers and patents. In Section III, a literature review is performed, where works related to simulations in the context of V2X are analyzed. In Section IV, simulation parameters associated with V2X security are commented on and analyzed. The future trends are analyzed and established in Section V, including a proposal for future work on an integrated simulation. Section VI is focused on future works related to the subject covered in this paper. Finally, the conclusions are drawn in Section VII.

As shown in this survey paper, V2X communication, particularly in the areas of V2X simulation tools, has received the attention of the academy and industry worldwide. This survey distinguishes itself from conventional V2X surveys by exploring V2X nuances, specifically emphasizing an in-depth insight into the main simulation tools found in scientific papers and patents, including an analysis of integrated simulations. Journal papers with a high impact factor were prioritized as reference sources.

C. RELATED SURVEYS TO V2X SIMULATION TOOLS

In V2X research, two surveys were found in the field of V2X simulation tools. The work [33] delves deeply into

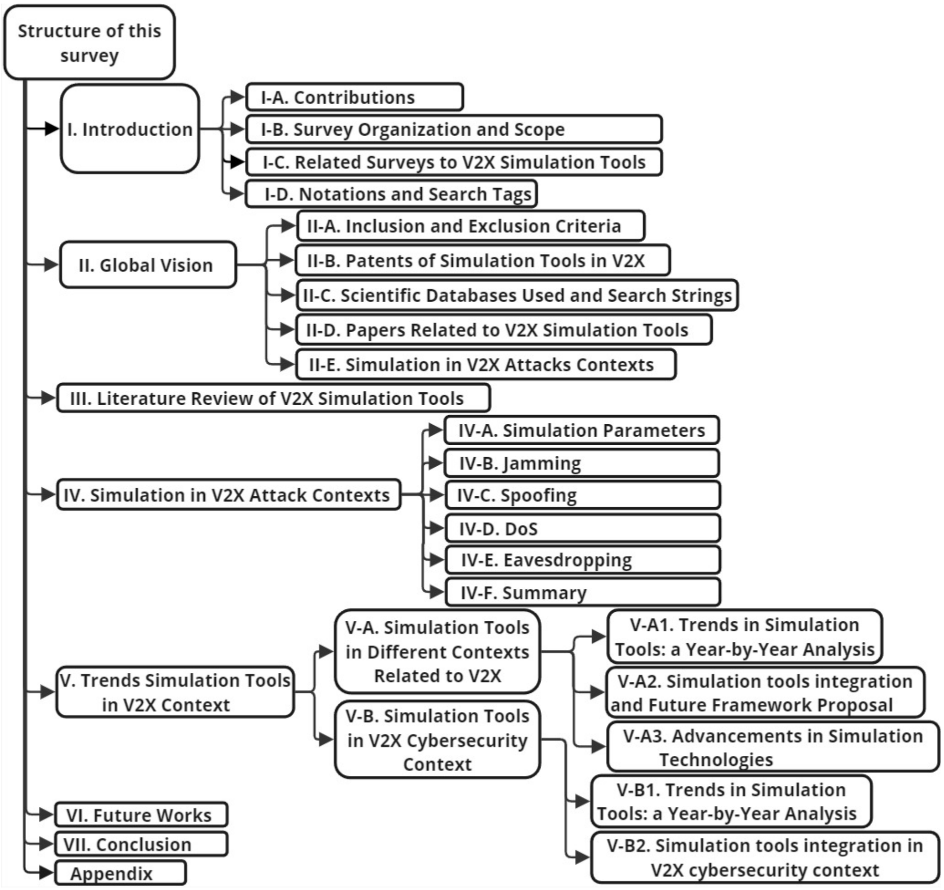

Structure of this survey
I. Introduction
I-A. Contributions
I-B. Survey Organization and Scope
I-C. Related Surveys to V2X Simulation Tools
I-D. Notations and Search Tags
II. Global Vision
II-A. Inclusion and Exclusion Criteria
II-B. Patents of Simulation Tools in V2X
II-C. Scientific Databases Used and Search Strings
II-D. Papers Related to V2X Simulation Tools
II-E. Simulation in V2X Attacks Contexts
III. Literature Review of V2X Simulation Tools
IV. Simulation in V2X Attack Contexts
IV-A. Simulation Parameters
IV-B. Jamming
IV-C. Spoofing
IV-D. DoS
IV-E. Eavesdropping
IV-F. Summary
V. Trends Simulation Tools in V2X Context
V-A. Simulation Tools in Different Contexts Related to V2X
V-B. Simulation Tools in V2X Cybersecurity Context
V-A1. Trends in Simulation Tools: a Year-by-Year Analysis
V-A2. Simulation tools integration and Future Framework Proposal
V-A3. Advancements in Simulation Technologies
V-B1. Trends in Simulation Tools: a Year-by-Year Analysis
V-B2. Simulation tools integration in V2X cybersecurity context
VI. Future Works
VII. Conclusion
Appendix

FIGURE 1. **Organization of the survey. Section II provides an overview of the V2X simulations area with relevant statistics on papers and patents. Section III presents a literature review analyzing related simulation works in the V2X context. Section IV examines and analyzes simulation parameters associated with V2X security. Section V discusses future trends and proposes future work on integrated simulations. Section VI focuses on future works related to the topics covered in this paper. Conclusions are drawn in Section VII.**

the convergence of Software-Defined Networking (SDN) and blockchain technology in Vehicular Networks (VNs), especially the potential challenges and security concerns posed by the centralized nature of SDN controllers. The work emphasizes the utility of adopting decentralized blockchain technology for improved security in SDN-Based Vehicular Networks (SDVNs), offering an overview of the state-of-the-art blockchain-based schemes and the relevant security requirements. However, it lacks a comprehensive analysis of V2X simulation tools themselves and needs to provide a detailed market relevance analysis.

On the other hand, [32] underscores the imperative nature of realistic simulation for the design and assessment of Intelligent Transport Systems (ITS). This survey comprehensively reviews significant simulation models for wireless signal propagation, dedicated short-range communication technologies, and vehicular mobility. The work [32] provides valuable insights into the best practices for simulation, aiming to ensure the accuracy and reliability of results while also discussing the support different simulation tools offer. The work [32] covers famous simulators such as SUMO, OMNET++, NS3, and Veins. However, it does not address other famous simulation tools such as CARLA and CarSim. Furthermore, this work does not analyze the publication trends or provide a market relevance analysis, which is critical for understanding the broader impact and adoption of these tools.

These surveys offer a holistic perspective on the intertwined relationship between V2X communication and the simulation tools that aid in its research and development. However, they did not cover the diversity of current simulation tools or provide a detailed market analysis, which are significant gaps that this survey aims to address.

D. NOTATIONS AND SEARCH TAGS

Areas related to V2X, including simulation tools, tend to have technical terms found in several works in the literature. Hence, the abbreviations used in the V2X areas of simulations are presented in the Appendix Section in Table 37. In addition, in Table 3, we show the notations to represent different tags used in the search part. The following tags are adopted throughout the paper:

TABLE 3. Utilized notation and correspondent tag.

Notation	Tag
V2X[a]	("vehicle-to-everything" OR "vehicle-to-anything" OR "V2X" OR "vehicle-to-vehicle" OR "V2V" OR "vehicle-to-pedestrian" OR "V2P" OR "vehicle-to-infrastructure" OR "V2I" OR "vehicle-to-network" OR "V2N" OR "vehicle-to-grid" OR "V2G" OR "vehicle-to-cloud" OR "V2C")
SIM[b]	("simulated" OR "simulator" OR "simulators" OR "simulation" OR "emulated" OR "emulator" OR "emulators" OR "emulation")
SEC[c]	("security" OR "cybersecurity")
ATK[d]	("attack" OR "attacks" OR "cyberattack" OR "cyberattacks" OR "threat" OR "threats")

II. GLOBAL VISION OF V2X CYBERSECURITY

The goal of this section is to enhance our understanding and extend our insight into the domain of V2X simulators. It delves into an analysis of research papers indexed in the Scopus database, categorizing them based on publication year, country of origin, and funding sources. Additionally, this section conducts a review of patents listed in Scopus and Google Patents. Moreover, it encompasses examining research from leading academic databases and sorting them by specific keywords and search phrases used.

This section is organized into four subsections. In Subsection II-A, we explore the criteria used for selecting relevant papers and patents in the field of V2X simulators, providing a foundation for our analysis. Then, in Subsection II-B, we unpack the rationale, research methodologies, and insights gained from the patent landscape in V2X simulation tools. Subsection II-C presents a series of tables that compile and contrast the volume of results associated with various tags across key scientific databases, providing a quantitative snapshot of the field. Lastly, Subsection II-D compiles an array of findings from scientific papers, categorizing them by year, geographical origin, and sponsoring entities, thus painting a diverse and multi-dimensional picture of the research activity in V2X simulation tools.

A. INCLUSION AND EXCLUSION CRITERIA

The selection of works is usually based on a criteria delineated in Table 4.

a) Since the core of this study is on V2X and simulation tools, the main criterion for selection is its pertinence to the simulators V2X field. The tags V2X[a] AND SIM[b] are generally used, where the logical AND operator indicates whether both operands are present. simultaneously.

b) The search used tags in “title, summary or keyword” as it produced fewer off-topic results than the “all fields” option.

c) Duplicates are omitted, as they typically represent echoes of original material encountered in less prominent databases. This method was mainly utilized during the Google Scholar search, bypassing the “include citations” option.

TABLE 4. Inclusion and exclusion criteria used in the papers selection procedure.

	Inclusion criteria	Exclusion criteria
1	Review articles related to the subject of V2X simulation tools	Duplicate studies
2	Papers by titles, abstracts or keywords tags	-

B. PATENTS OF SIMULATION TOOLS IN V2X

In the evolving landscape of V2X communication, the role of patents in the domain of simulation tools is essential, embodying the nexus of innovation and industrial advancement. Patents secure novel methodologies and technological advancements and provide a tangible metric for assessing the trajectory of research and development (R&D) efforts within this sector. Through a comprehensive evaluation of patent repositories, notably Google Patents and Scopus, our January 1, 2024 analysis unveils a growth in patent filings related to V2X simulation technologies. This surge highlights the escalating interest and investment in developing more sophisticated and accurate simulation environments. The intricate balance between academic explorations and their industrial applications is further evidenced through patents, which bridge the gap between theoretical research and its practical, commercial realization.

In Google Patents, the search is guided by the publication search parameter, signifying that the results were compiled when a patent application for an invention was published or made available to the public. The search tags were V2X[a] AND SIM[b]. Table 5 categorizes patents annually for detailed analysis, and Figure 2 provides a graphical representation of this data. Table 5 and Figure 2 illustrate a significant increase in the volume of patents related to V2X simulation tools, indicating a robust and expanding market. Table 6 shows the number of patents by different companies, and Table 38 in the Appendix Section shows the companies with their full names compared to the tags used in Table 6. The reason for using shorter tags is that several related patents would not be found if long tags were used.

Table 5 shows that, according to Google Patents, over 50% and, according to Scopus, more than 60% of registered patents belong to the last four years. However, there exists a difference in the number of patents between Scopus and Google Patents, potentially due to Scopus employing a more stringent vetting process. This difference, however, serves as a minor hurdle in achieving our primary objective of delineating broad trends. The relevance of each corporation in Table 6 is maintained consistently across both platforms, guiding us to similar conclusions. Note that the limitation within the Scopus database regarding the capability to search patents by title, abstract, or keyword, which contrasts with the method for scientific papers, thus necessitating the application of the “all fields” search criterion. This

TABLE 5. Detailed data on simulation tools suitable for V2X found in Google Patents and Scopus separated by year and amount of patents.

Year	Google Patents	% Google Patents	Scopus	% Scopus
2023	9835	17.48	3013	21.12
2022	8474	15.06	2350	16.47
2021	6689	11.89	2049	14.36
2020	5242	09.31	1520	10.65
2019	5634	10.01	1212	08.50
2018	3977	07.07	822	05.76
2017	2802	04.98	522	03.66
2016	1984	03.53	332	02.33
2015	1776	03.16	309	02.17
2014	1209	02.15	284	01.99
Pre-2014	8656	15.38	1853	12.99
Total	**56278**	**100.00**	**14266**	**100.00**

TABLE 6. Detailed data on the number of patents from different companies in the Google Patents and Scopus databases in the V2X simulations area.

	Companies	Country	Google	% Google	Scopus	% Scopus
			Patents	Patents		
1	Qualcomm	United States	4711	22.61	1712	14.26
2	Toyota	Japan	2732	13.11	905	07.54
3	Intel	United States	2227	10.69	986	08.21
4	Ford	United States	1556	07.47	664	05.53
5	Apple	United States	1223	05.87	768	06.40
6	NVIDIA	United States	1019	04.89	898	07.48
7	LG	South Korea	556	02.67	523	04.36
8	Huawei	China	503	02.41	459	03.82
9	GM	United States	409	01.96	124	01.03
10	Nissan	Japan	408	01.96	29	00.24
11	Honda	Japan	331	01.59	324	02.70
12	Sony	Japan	317	01.52	395	03.29
13	Denso	Japan	297	01.43	241	02.01
14	AMD	United States	269	01.29	238	01.98
15	Bosch	Germany	266	01.28	76	00.63
16	Ericsson	Sweden	249	01.20	242	02.02
17	Hitachi	Japan	227	01.09	1	00.01
18	Texas	United States	211	01.01	346	02.88
19	Samsung	South Korea	208	01.00	209	01.74
20	Tesla	United States	206	00.99	388	03.23
21	InterDigital	United States	203	00.97	184	01.53
22	Mitsubishi	Japan	189	00.91	79	00.66
23	Spoke	United States	166	00.80	29	00.24
24	Hyundai	South Korea	164	00.79	76	00.63
25	Siemens	Germany	149	00.72	73	00.61
26	Mercedes	Germany	149	00.72	41	00.34
27	Audi	Germany	148	00.71	36	00.30
28	Volkswagen	Germany	144	00.69	93	00.77
29	Ofinno	United States	142	00.68	313	02.61
30	Micron	United States	136	00.65	21	00.17
31	Nokia	Finland	125	00.60	57	00.47
32	Analog	United States	122	00.59	228	01.90
33	Panasonic	Japan	106	00.51	150	01.25
34	BMW	Germany	102	00.49	112	00.93
35	Philips	Netherlands	96	00.46	60	00.50
36	Alphabet	United States	92	00.44	198	01.65
37	Geely	China	86	00.41	0	00.00
38	BYD	China	80	00.38	7	00.06
39	Motional	United States	79	00.38	124	01.03
40	DOCOMO	Japan	74	00.36	76	00.63
41	ZTE	China	48	00.23	53	00.44
42	Autoliv	Sweden	42	00.20	18	00.15
43	Oppo	China	41	00.20	22	00.18
44	Comcast	United States	40	00.19	230	01.92
45	DSpace	Germany	40	00.19	16	00.13
46	Skyworks	United States	36	00.17	153	01.27
47	Aptiv	Ireland	29	00.14	26	00.22
48	Faurecia	France	29	00.14	0	00.00
49	ZF	Germany	28	00.13	2	00.02
50	Blackberry	Canada	24	00.12	1	00.01
-	**Total**	**-**	**20834**	**100.00**	**12006**	**100.00**

approach might lead to the retrieval of a multitude of results that, despite mentioning V2X simulators, do not concentrate specifically on the topic, introducing the potential for irrelevant data.

On the other hand, according to Table 6, Qualcomm is accountable for nearly a quarter (22.61%) of the patents discovered among the top 50 ranked companies. The top five companies with the most patents are Qualcomm, Toyota, Intel, and Ford, collectively responsible for over 50% of the patents. It is also noteworthy that the top 10 companies account for more than 70% of patents in this top 50 category. Another observation is that only companies in the top 8 hold more than 2% of the total number of patents. While the authors have made extensive efforts to identify leading companies in the field, it is acknowledged that the dynamic and rapidly evolving nature of V2X simulation tools means that some relevant companies may not have been included in the initial dataset. Consequently, the ranking presented in Table 6 may not be exhaustive and should be interpreted with this limitation in mind. The total value results from Table 5 compared to Table 6 are different for a few reasons. The first is that there are other companies besides those that appear in Table 6. The second reason is that some tags may not be directly attributable to a specific company and can be identified by a broader tag search across multiple companies.

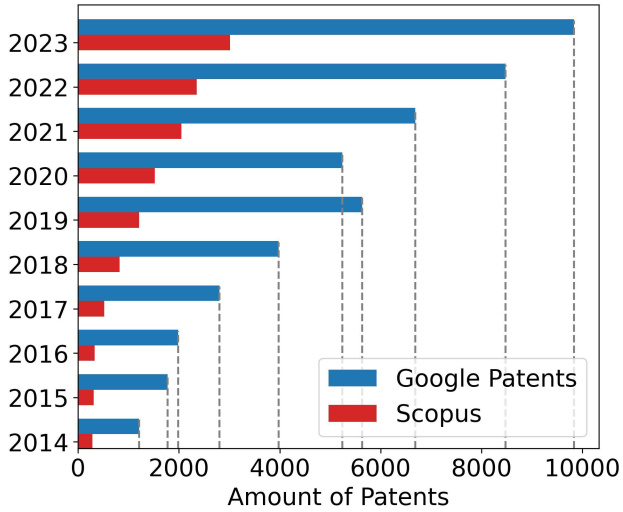


FIGURE 2. Simulation tools suitable for V2X found in Google Patents and Scopus separated by year and amount of patents.

C. SCIENTIFIC DATABASES USED AND SEARCH STRINGS

Table 7 is a starting point for searches based on tags. The scientific base is the Scopus academic database. Considering the reputation of Scopus as a leading platform for comprehensive academic research, it naturally emerged as the primary resource for the work. The approach varied, sometimes scanning all content fields and narrowing the search to just the "title, abstract, or keyword". The research was done on January 1, 2024, and can be viewed in Table 7. Most of the results of this work are English-language entries, with Chinese works being the next most frequent. Note that the far-right column in Table 7 displays the ratio of V2X simulator works to total V2X works, offering an indicator that resembles the percentage of simulator-related works compared to the overall body of work. Note that approximately 40% works in the V2X area related to simulations using the "title, abstract, or keyword" criteria.

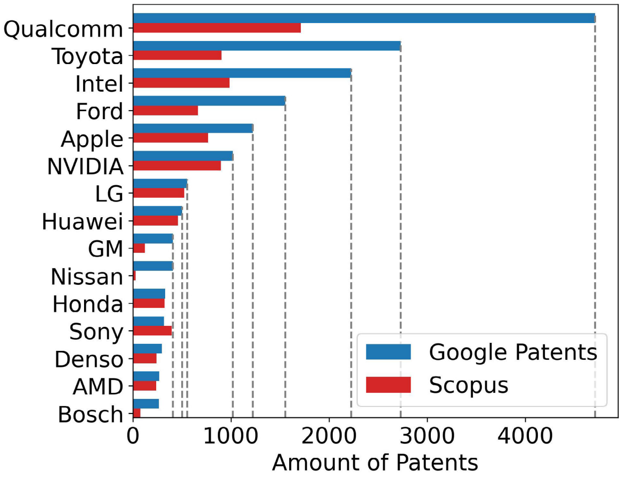


FIGURE 3. Number of patents from leading companies in the Google Patents and Scopus databases in the V2X simulations area.

Furthermore, Table 8 shows a survey with results from the main simulation tools in the V2X context on several different scientific bases. Table 9 shows different combinations of tags in these same scientific bases to find results in cases where more than one simulation tool is used simultaneously in the same work. This may indicate an integration between different simulation tools. All data collection is timestamped to January 1, 2024. In this work, Section V addresses the issue of simulation tool integration, which is relevant to point out some future trends. This section discusses several works and the cases of integration of different simulation tools in the context of V2X that were found. Several of the tag combinations used in Table 9 were chosen based on these works. Thus, the results shown in Table 9 are relevant to finding the most relevant integrations of different simulation tools, and this information is essential for the conclusions made in Section V.

In Table 10, important characteristics of V2X simulation tools are presented. We utilize widely recognized databases, including Google Scholar and Scopus, alongside four specialized academic resources that are deemed highly relevant. Searches from Elsevier are conducted through the Science Direct platform, whereas searches from the Institute of Electrical and Electronic Engineers (IEEE) are performed using IEEE Xplore. An important consideration is that on the Science Direct platform, it is not possible to use more than eight Boolean operators per search, therefore, in this specific case, a much shorter tag is used for V2X^{a}. The tag used is ("vehicle-to-everything" OR "vehicle-to-anything" OR "V2X" OR "vehicle-to-vehicle" OR "V2V"). For this reason, there may be fewer references than there would be if there were no such limitation.

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

Search Withing	Language	Tags	Number of References	Tags	Number of References	%
All Fields	All	V2X^{a} AND SIM^{b}	50784	V2X^{a}	94525	53.73
All Fields	English	V2X^{a} AND SIM^{b}	48862	V2X^{a}	91365	53.48
TITLE-ABS-KEY	All	V2X^{a} AND SIM^{b}	14697	V2X^{a}	36762	39.98
TITLE-ABS-KEY	English	V2X^{a} AND SIM^{b}	14182	V2X^{a}	35682	39.75
TITLE	All	V2X^{a} AND SIM^{b}	221	V2X^{a}	8564	02.58
TITLE	English	V2X^{a} AND SIM^{b}	219	V2X^{a}	8302	02.64

TABLE 8. Number of results in searches for simulation tools in V2X context on different scientific bases in the criteria "title, abstract or keyword" and "all fields".

Scientific basis	In Title, Abstract or Keyword				All Fields	
Tags	Scopus	IEEE	MDPI	Elsevier	Google Scholar	Springer
V2X^{a} AND "SUMO"	468	260	103	36	14500	867
V2X^{a} AND ("NS3" OR "NS-3")	307	167	616	8	9430	438
V2X^{a} AND "OMNeT++"	201	115	24	15	5610	366
V2X^{a} AND "Veins"	148	85	302	12	12400	295
V2X^{a} AND "CarSim"	60	18	169	3	1310	66
V2X^{a} AND "CARLA"	57	63	26	1	20800	83
V2X^{a} AND "PreScan"	46	17	121	3	918	38
V2X^{a} AND "OPNET"	46	15	4	2	1680	128
V2X^{a} AND "Artery"	30	13	609	10	22900	135
V2X^{a} AND ("Virtual Test Drive" OR "VTD")	26	17	323	0	962	44
V2X^{a} AND "CarMaker"	25	7	70	4	2690	71
V2X^{a} AND "iTetris"	16	5	1	3	666	42
V2X^{a} AND "Simu5G"	15	11	2	0	161	5
V2X^{a} AND "PLEXE"	14	12	29	0	2220	114
V2X^{a} AND "VSimRTI"	13	5	0	1	403	27
V2X^{a} AND "INET"	12	6	1	1	1350	44
V2X^{a} AND "SimuLTE"	10	6	0	0	23200	18
V2X^{a} AND "TruckSim"	10	4	0	2	200	11
V2X^{a} AND "Mininet-WiFi"	9	5	2	1	227	17
V2X^{a} AND "OpenC2X"	7	5	77	0	87	3
V2X^{a} AND "MilliCar"	7	5	0	0	116	1
V2X^{a} AND "Ventos"	7	2	1	2	8860	9
V2X^{a} AND "Apollo"	7	1	12	0	2960	103
V2X^{a} AND "AirSim"	6	2	21	1	298	12
V2X^{a} AND "Eclipse MOSAIC"	5	3	0	0	66	6
V2X^{a} AND "GloMoSim"	5	2	0	0	743	52
V2X^{a} AND "GEMV"	4	3	1	0	62	7
V2X^{a} AND "MiXiM"	3	3	0	0	368	16
V2X^{a} AND "LTEV2Vsim"	3	3	0	0	136	2
V2X^{a} AND "OpenCV2X"	3	2	6	0	73	1
V2X^{a} AND "Vanetza"	3	2	0	0	147	4
V2X^{a} AND "CrowNet"	2	1	0	0	12	1
V2X^{a} AND "JiST/SWANS"	2	0	0	0	533	33
V2X^{a} AND "Flowsim"	1	2	0	0	587	2
V2X^{a} AND "MoReV2X"	1	1	11	0	94	0
V2X^{a} AND "HYDRO-3D"	1	1	9	0	49	0
V2X^{a} AND "LGSVL"	1	1	0	0	152	5
V2X^{a} AND "Containernet"	1	0	0	0	102	0
V2X^{a} AND "Altair WinProp"	1	0	0	0	37	0
V2X^{a} AND "Cognata"	0	0	0	0	352	2
V2X^{a} AND "rfpro"	0	0	0	0	65	0
V2X^{a} AND "NVIDIA DRIVE Constellation"	0	0	0	0	59	2
V2X^{a} AND "ANSYS VRXPERIENCE"	0	0	0	0	9	0

Our research predominantly targeted the "title, abstract, or keyword" tags rather than searching across "all fields". This strategy is instrumental in filtering the search results to those most pertinent. However, certain databases, such as Google Scholar and Springer, lacked this specific search functionality, necessitating our use of either "title" or "all fields" as search parameters. Consequently, our searches in Google Scholar and Springer were conducted using the "all fields" criteria. Despite these methodological differences, we remain assured of the pertinence of our findings.

Insights drawn from Tables 8 and 9 highlight several important observations:

a) Within specialized academic resources, IEEE stands out as the premier platform for topics concerning V2X

TABLE 9. Number of results in searches for different tag combinations on different scientific bases in the criteria "title, abstract or keyword" and "all fields".

Scientific basis Tags	In Title, Abstract or Keyword				All Fields	
	Scopus	IEEE	MDPI	Elsevier	Google Scholar	Springer
V2X[a] AND ("simulated" OR "simulator" OR "simulators" OR "simulation")	14594	6209	13524	695	51700	8888
V2X[a] AND ("emulated" OR "emulator" OR "emulators" OR "emulation")	193	97	170	11	21300	413
V2X[a] AND "SUMO" AND "OMNeT++"	94	61	8	9	3880	254
V2X[a] AND "SUMO" AND "Veins"	69	45	6	4	3310	193
V2X[a] AND "SUMO" AND "OMNeT++" AND "Veins"	51	37	3	4	2970	171
V2X[a] AND "SUMO" AND "MOVE"	16	6	0	0	-	-
V2X[a] AND "SUMO" AND "CARLA"	10	7	0	1	940	12
V2X[a] AND "SUMO" AND "OMNeT++" AND "Artery"	5	3	0	0	418	12
V2X[a] AND "SUMO" AND "OMNeT++" AND "INET"	3	3	0	0	674	20
V2X[a] AND "SUMO" AND "OMNeT++" AND "Veins" AND "INET"	3	3	0	0	602	18
V2X[a] AND "OMNeT++" AND "CARLA"	3	3	0	0	151	3
V2X[a] AND "SUMO" AND "OMNeT++" AND "Ventos"	3	2	0	2	112	7
V2X[a] AND "SUMO" AND "OMNeT++" AND "CARLA"	2	2	0	0	133	2
V2X[a] AND "OMNeT++" AND "Simu5G" AND "Artery"	2	0	0	0	26	2
V2X[a] AND "SUMO" AND "OMNeT++" AND "Veins" AND "MiXiM"	1	1	0	0	66	10
V2X[a] AND "SUMO" AND "GEMV"	1	1	0	0	44	3
V2X[a] AND "SUMO" AND "OMNeT++" AND "Artery" AND "simuLTE"	1	0	0	0	305	4
V2X[a] AND "OMNeT++" AND "CARLA" AND "Artery"	1	1	0	0	42	0
V2X[a] AND "SUMO" AND "CARLA" AND ("NS3" OR "NS-3")	0	2	0	0	127	5
V2X[a] AND "SUMO" AND "Containernet" AND "Mininet-WiFi"	0	2	0	0	12	0
V2X[a] AND "SUMO" AND "OMNeT++" AND "Veins" AND ("NS3" OR "NS-3")	0	1	0	0	806	42
V2X[a] AND "SUMO" AND "OMNeT++" AND "Veins" AND "PLexe"	0	0	0	0	513	7
V2X[a] AND "SUMO" AND "OMNeT++" AND "INET" AND "simuLTE"	0	0	0	0	465	8
V2X[a] AND "SUMO" AND ("NS3" OR "NS-3") AND "RACE"	0	0	0	0	287	0
V2X[a] AND "SUMO" AND "OMNeT++" AND "Veins" AND "INET" AND "Vanetza" AND "Artery"	0	0	0	0	63	2
V2X[a] AND "SUMO" AND "OMNeT++" AND "CARLA" AND "Artery"	0	0	0	0	35	0
V2X[a] AND "SUMO" AND "LTEV2Vsim"	0	0	0	0	26	1
V2X[a] AND "Containernet" AND "Mininet-WiFi"	0	0	0	0	14	0
V2X[a] AND "OMNeT++" AND "CARLA" AND "Simu5G"	0	0	0	0	8	0

and its security aspects, with MDPI, Elsevier, and Springer following closely in significance. The Springer database yielded more results due to the broader "all fields" search criteria.

b) Google Scholar revealed more results than Scopus for more complex queries. Although Google Scholar tends to produce more extensive results due to its broader search scope, it is essential to acknowledge that our Scopus search is confined to "titles, abstracts, and keywords", whereas Google Scholar encompassed "all fields".

c) The frequency of specific terms varies across works. Terms associated with simulation tools are more prevalent than those related to emulators.

Table 11 shows essential characteristics of V2X related programming languages. Markup languages such as HyperText Markup Language (HTML) and Cascading Style Sheets (CSS) are integral to developing user interfaces in V2X simulation tools such as OMNeT++ and potentially Eclipse MOSAIC. Extensible Markup Language (XML) is crucial for managing configuration and data exchange in tools such as SUMO and NS-3, streamlining simulation setup, and intermodule communication.

Table 12 shows searches in the Scopus database for different tags, showing the relevance of some programming languages found in the context of simulation tools related to V2X. Table 12 shows a considerable relevance of Matlab and Python. In the case of the C++ language, the number of results does not correspond to reality, so most of the results are noisy. This occurred because the Scopus database cannot accurately search the C++ tag.

Traffic simulation models, crucial in V2X studies, range from macroscopic to microscopic. Macroscopic models analyze aggregated traffic flow, whereas microscopic models such as SUMO focus on individual vehicle interactions. As a microscopic traffic simulator, SUMO adeptly models vehicle movements but lacks inherent V2X communication features, necessitating integration with network simulators for comprehensive V2X simulations [22], [34], [35]. In the realm of network simulation, NS3 and OMNeT++ stand out. Primarily functioning as network simulators, they require coupling with traffic simulators such as SUMO to capture the V2X environment. NS3, in particular, excels in simulating network communication aspects but needs this integration to to effectively simulate vehicle traffic [36].

Veins plays an indispensable role as an interface in V2X simulations. By bridging the traffic modeling of SUMO with the network simulation of OMNeT++, Veins emerges as a comprehensive tool for V2X simulations, marrying traffic dynamics with network communication. While Veins is not a standalone V2X simulator, its intermediary role is key in creating microscopic V2X scenarios [37], [38]. The addition of Simu5G to this ecosystem brings 5G network

TABLE 10. List of simulation tools and their description.

Tool Name	Tool Type
AirSim	Unreal Engine based 3D autonomous driving simulator
Altair WinProp	Advanced wave propagation modeling for network planning
ANSYS VRXPERIENCE	Unreal Engine based 3D autonomous driving simulator
Artery	Extension or framework based on ETSI ITS-G5 protocols
CARLA	Unreal Engine based 3D autonomous driving simulator
CarMaker	3D autonomous driving simulator
CarSim	Detailed vehicle dynamics simulator with real-world validation
Cognata	3D autonomous driving simulator
Containernet	Docker-based network emulator with virtual network capabilities
CrowNet	Network simulator with focus on V2X and crow communication
Eclipse Mosaic	Framework for multi-domain V2X co-simulation scenarios
Flowsim	Simulator for analyzing and visualizing traffic flow dynamics
GEMV	Geometric vehicular mobility and V2X communication simulator
GloMoSim	Discrete-event network simulator
HYDRO-3D	Simulator for hydrodynamic behaviors in 3D environments
iTetris	ITS co-simulation platform for V2X communication scenarios
LGSVL	Unity Engine based 3D autonomous driving simulator
LTEV2Vsim	Specialized simulator for vehicle-to-vehicle communication over Long-Term Evolution (LTE)
Mininet-WiFi	Emulator for software-defined wireless networking in V2X
MilliCar	Simulator for millimeter-wave vehicular communication analysis
MoReV2X	Modeling and simulation framework for V2X communication
MOSAIC	Co-simulation framework for connected and automated mobility
NS-3	Discrete-event network simulator
NVIDIA DRIVE Sim	3D autonomous driving simulator
OMNeT++	Discrete-event network simulator
OpenC2X	Open-source Car-to-X communication testing platform
OpenCV2X	Open-source platform for V2X communication and testing
OPNET	Discrete-event network simulator
PLEXE	Platooning extension for Veins
PreScan	Unreal Engine based 3D autonomous driving simulator
rfpro	3D autonomous driving simulator
Simu5G	Extension of OMNeT++ to simulate 5G NewRadio networks
SimuLTE	Simulator for LTE and LTE-Advanced vehicular networks
SUMO	Traffic simulator
TruckSim	Dynamic simulation for trucks and heavy-duty vehicle dynamics
Vanetza	Toolkit for V2X networking services and protocols
Ventos	Vehicular network simulator with traffic and network integration
VSimRTI	Integrative V2X network simulation coupling multiple simulators
VTD	3D autonomous driving simulator
Veins	Vehicular network simulator combining SUMO and OMNeT++

simulation capabilities into the fold, enhancing OMNeT++ for 5G-based V2X scenarios. This integration is critical for simulating the 5G user plane in vehicular communication, mainly when used alongside Veins [21], [39]. Artery, another significant framework in V2X simulations, built on OMNeT++, showcases specialized Middleware functionalities. Though its direct comparison with tools such as CARLA in V2X contexts requires further exploration, its standalone capabilities in simulating European V2X standards are noteworthy [39]. Also, the emergence of B5GCyberTestV2X is a notable advancement [29]. This recent addition incorporates 5G control plane functionalities into simulations based on Veins, thus enriching the simulation landscape for V2X scenarios utilizing 5G technology.

Our approach in this analysis has adopted a broader interpretation of V2X simulation tools, encompassing both standalone tools and integrative frameworks. This perspective is essential to accurately depict real-world scenarios in V2X simulations, where traffic dynamics and network communication are often indispensable. In reviewing Table 8, a notable observation is the prevalence of specific simulation tools in V2X research, as evidenced by the frequency of their mention across various academic databases. The most common simulation tool related to V2X is SUMO, followed by NS3 and OMNeT++. Also, note that there are a considerable number of different simulation tools found on different academic bases, with 39 simulation tools that have at least 1 result found in the Scopus database and 43 simulation tools that were found in any scientific base.

From Table 9, it is evident that scientific works that simultaneously deal with SUMO and OMNeT++ are the most common, followed by combinations involving simulation tools such as Veins, the Mobility Model Generator for Vehicular Networks (MOVE), and CARLA. A concern regarding MOVE is that, being a widespread word, it is likely that many of the data are noisy and do not necessarily refer to the simulation tool. This suggests that CARLA is probably the most used in simulator integrations after SUMO, OMNeT++, and Veins. Furthermore, regarding the "MOVE" tag, the searches were manually checked to remove possible noisy results. It was also determined that it was appropriate not to perform searches in "All Fields" because

TABLE 11. List of program languages and their usage for V2X simulation.

Programming Language Name	Description
C++	Employed in the core simulation engines of tools such as SUMO, NS-3, OMNeT++, Veins, and CARLA due to its high performance and system resource management capabilities.
Python	Used for scripting, data analysis, and automation within simulation tools such as NS-3 and CARLA to enhance usability and data handling.
Java	Utilized in OMNeT++ for plugin functionalities and user interface components, valued for its portability and robustness.
MATLAB	Integrated with tools such as CARLA for data analysis and algorithm development, predominantly used in academic and research settings for numerical computing.
JavaScript	Deployed in OMNeT++ or Eclipse MOSAIC to develop web-based user interfaces and visualization components.
Lua	Used in OMNeT++ for configuration and scenario scripting, offering flexibility and customization due to its ease of embedding.

most of the results would be noisy, i.e., disconnected from the MOVE simulation tool.

The results in Table 9 only show if more than one simulation tool was found in the same work, but most of these works involve integration between different simulation tools. Another important observation is that the results found for Artery tags are less than half of those found in the top five searches combining different simulation tools in most scientific databases. There are works simultaneously involving using the CARLA and OMNeT++ simulators, which indicates that combining different simulators can reduce their limitations.

Another example is the prominent usage of SUMO, predominantly featured in conjunction with OMNeT++ and Veins. While robust in simulating traffic and urban mobility, SUMO lacks native support for V2X functionalities. This gap is bridged by integrating SUMO with OMNeT++, a network simulator, and Veins, which acts as a mediator, facilitating the seamless interaction between the mobility patterns from SUMO and the network dynamics within OMNeT++. This trio of SUMO, OMNeT++, and Veins constitutes a comprehensive solution for V2X simulation, representing a synergy where each component complements the others to create a holistic simulation environment.

TABLE 12. Number of results in searches for different tags on Scopus base in the criteria "title, abstract or keyword".

Tags	Number of Results
V2X[a] AND SIM[b]	14704
V2X[a] AND SIM[b] AND "C++"	13619
V2X[a] AND SIM[b] AND "Matlab"	1164
V2X[a] AND SIM[b] AND "Python"	146
V2X[a] AND SIM[b] AND "Java"	53
V2X[a] AND SIM[b] AND "JavaScript"	5
V2X[a] AND SIM[b] AND "Lua"	4

In V2X simulation, integrating different simulation tools to compensate for individual limitations is not just common but necessary for comprehensive research. This is particularly evident in the case of simulation tools such as CARLA, PreScan, CarMaker, and Virtual Test Drive (VTD). While advanced in certain aspects of simulation, these tools notably lack built-in V2X capabilities. Their utilization in V2X research often involves innovative integration with other simulation tools that provide the missing V2X functionalities. For instance, CARLA, an open-source simulator for autonomous driving research, excels in creating realistic urban environments and vehicle dynamics but does not natively support network communication aspects of V2X. To overcome this, researchers have integrated CARLA with network simulators such as NS3 [40]. NS3 complements CARLA by simulating the wireless communication environment, which is essential for V2X. This integration allows for a more realistic assessment of how autonomous vehicles interact within a V2X framework, considering both the physical movements of vehicles and the underlying network communications.

Similarly, NS3, predominantly a network simulator, cannot simulate real-world traffic conditions. Its integration with traffic simulation tools such as SUMO enables a more holistic approach to V2X research, allowing for the simulation of both network performance and traffic dynamics. This combination is crucial for studying the impact of network latency, packet loss, and other network variables on the behavior of connected vehicles in realistic traffic scenarios. The necessity of such integrations points to a fundamental aspect of V2X simulation research: the requirement for multidisciplinary tools to capture the full spectrum of V2X interactions. More details about the integration of different simulation tools are covered in Section V.

D. PAPERS RELATED TO V2X SIMULATION TOOLS

In this subsection, we performed searches on the Scopus platform for number of academic papers results, separated year by year, by country of origin, and by funding sponsors. To refine our search and reduce the number of irrelevant findings, we focused on "title, abstract, and keywords". A unique criterion not applied in other sections of this study is to filter results to include only articles or conference papers. This method aids in pinpointing academic sources that offer greater relevance and depth for exploring new directions in scholarly research. The papers were carried out on January 1, 2024. An impressive 14354 papers were found tagged under V2X[a] AND SIM[b].

Tables 13-15 break down the results by year, originating country, and funding sponsors, respectively. The cumulative term represents the total values starting from pre-2009 and continuing through the subsequent years, as shown in Table 13. Figures 4-5 visually show the separation of results by years and by different countries. According to Table 13 and Figure 4, there is a consistent annual growth in the number of academic results in V2X simulators. Note that in the final four years (2020-2023), more than half of the results were found.

Regarding countries, Table 14 and Figure 5 show that China leads this area of research, followed by the United States, India, and Germany. Notably, the cumulative number of publications from the second to the fourth-ranked countries (United States, India, and Germany) does not match the total number of publications from China alone. This highlights the dominant position of China in the V2X simulations research field. There are 156 undefined results in the search carried out in relation to countries and 8468 in relation to funding sponsors. These elusive results came directly from the Scopus search. Note that the total results in Table 14 vary from those in Table 13 since there are publications with authors from multiple countries.

In line with the results of Table 14, Table 15 shows that the National Natural Science Foundation of China leads among funding sponsors, with a remarkable 2263 publications. This dominance underscores the significant investment and research output from China in the V2X simulation tools area. Notably, the number of publications supported by the National Natural Science Foundation of China is greater than the combined total of the second to the tenth-ranked sponsors, further highlighting its substantial influence. In addition to the leading Chinese sponsors, the National Science Foundation from the United States ranks fourth with 391 publications, demonstrating a notable contribution from the United States in this research field. European funding sources also appear prominently, with the Horizon 2020 Framework Programme, the European Commission, and the European Regional Development Fund collectively contributing 480 publications, reflecting strong support from European initiatives.

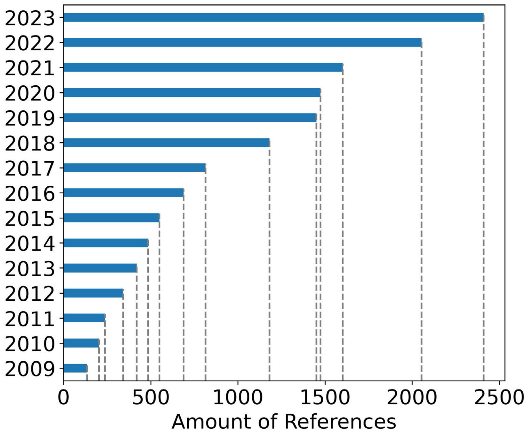


FIGURE 4. Number of references separated year by year in the V2X simulations area.

E. SIMULATION TOOLS IN CONTEXT OF V2X SECURITY

Simulations in the context of V2X communication serve myriad applications, from testing system performance under varied traffic scenarios to assessing the effectiveness of communication protocols and bolstering the safety mechanisms of automated vehicles. These simulations are crucial for grasping the complex dynamics within V2X ecosystems, enabling the creation of efficient and resilient systems against the diverse challenges encountered in real-world environments. Within this broad spectrum of applications, security is paramount, addressing essential facets directly influencing road safety, traffic management efficiency, and the dependability of automated vehicle navigation.

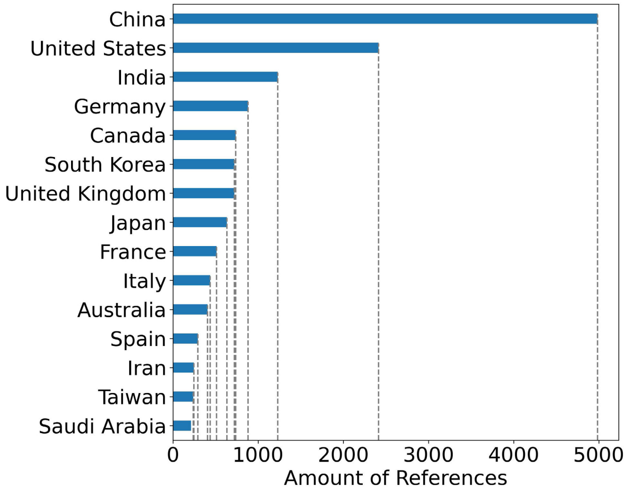


FIGURE 5. Number of references separated country by country in the V2X simulation tools area.

A variety of threats primarily dominates security concerns in V2X communications [5]. Examples of the most frequently referred attacks include jamming [41], spoofing [42], DoS [43], and eavesdropping [42]. Jamming attacks aim to disrupt communications by either inundating channels with noise or employing robust Radio Frequency (RF) signals to congest these channels with unauthorized traffic [41]. Spoofing involves impersonating legitimate sources and transmitting fabricated messages to compromise the integrity of vehicular communications [42]. A DoS attack disrupts network services by flooding the target with too many requests, blocking access for legitimate users [43]. Eavesdropping, the unauthorized interception of messages, breaches the confidentiality of vehicular communications [42]. These cybersecurity threats challenge the integrity and reliability of V2X systems, posing considerable risks to user privacy and the safety of Intelligent Transportation Systems (ITS).

Tables 16-17 show the correlation of results between simulation tools and cyberattacks in the context of V2X. From Table 16, note that according to the "title, abstract or keyword" criterion, around 8% of the works related to the context of V2X deal with the topic of cybersecurity. In Table 17, there are works on different scientific bases dealing with simulation tools and security and cyberattacks. Also, note that jamming has been a cyberattack widely discussed in scientific works. Although our work focuses

TABLE 13. The number of publications is separated year by year in the V2X simulation tools area in the Scopus database using the title, abstract, and keywords criteria.

Year	Amount of Publications	% Amount of Publications	Cumulative	% Cumulative
2023	2410	16.79	14354	100.00
2022	2053	14.30	11944	83.21
2021	1601	11.15	9891	68.91
2020	1474	10.27	8290	57.75
2019	1450	10.10	6816	47.49
2018	1181	08.23	5366	37.38
2017	814	05.67	4185	29.16
2016	689	04.80	3371	23.48
2015	550	03.83	2682	18.68
2014	485	03.38	2132	14.85
2013	419	02.92	1647	11.47
2012	342	02.38	1228	08.56
2011	238	01.66	886	06.17
2010	203	01.41	648	04.51
2009	135	00.94	445	03.10
Pre-2009	310	02.16	310	02.16
Total	**14354**	**100.00**	**-**	**-**

TABLE 14. Number of publications separated country by country in the V2X simulations area in the Scopus database using the title, abstract, and keywords criteria.

Country	Amount of Publications	% Amount of Publications
China	4984	26.49
United States	2414	12.83
India	1229	06.53
Germany	881	04.68
Canada	737	03.92
South Korea	721	03.83
United Kingdom	721	03.83
Japan	633	03.36
France	513	02.73
Italy	437	02.32
Australia	407	02.16
Spain	292	01.55
Iran	246	01.31
Taiwan	239	01.27
Saudi Arabia	211	01.12
Others	4153	22.07
Total	**18818**	**100.00**

TABLE 15. Number of publications in the different funding sponsors in the V2X simulation tools area in the Scopus database using the title, abstract, and keywords criteria.

Funding Sponsor	Amount of Publications
National Natural Science Foundation of China	2263
National Key Research and Development Program of China	430
Fundamental Research Funds for the Central Universities	403
National Science Foundation	391
Horizon 2020 Framework Programme	223
National Research Foundation of Korea	211
Ministry of Science, ICT and Future Planning	159
Natural Sciences and Engineering Research Council of Canada	144
European Commission	139
Engineering and Physical Sciences Research Council	124
European Regional Development Fund	117
China Postdoctoral Science Foundation	115
Japan Society for the Promotion of Science	114
Institute for Information and Communications Technology Promotion	113
Natural Science Foundation of Jiangsu Province	99

more attention on DoS attacks than Distributed Denial of Service (DDoS), we put DDoS-related tags in Table 17 because DDoS is a type of DoS and also because the DoS tag is small and can lead to a lot of noisy data which no relation to denial of service. Just note that there are a huge number of results on Google Scholar regarding DoS,

TABLE 16. Searches for cybersecurity-related tags in scientific publications in the Scopus database using different criteria.

Search Within	Language	Tags	Number of References	Tags	Number of References	%
All Fields	All	V2X[a] AND SIM[b] AND SEC[c]	12198	V2X[a] AND SIM[b]	50784	24.02
All Fields	English	V2X[a] AND SIM[b] AND SEC[c]	11832	V2X[a] AND SIM[b]	48862	24.22
TITLE-ABS-KEY	All	V2X[a] AND SIM[b] AND SEC[c]	1240	V2X[a] AND SIM[b]	14697	08.44
TITLE-ABS-KEY	English	V2X[a] AND SIM[b] AND SEC[c]	1200	V2X[a] AND SIM[b]	14182	08.46
TITLE	All	V2X[a] AND SIM[b] AND SEC[c]	2	V2X[a] AND SIM[b]	221	00.90
TITLE	English	V2X[a] AND SIM[b] AND SEC[c]	2	V2X[a] AND SIM[b]	219	00.91

TABLE 17. Number of results in searches for different tags related to cyberattacks and cybersecurity on different scientific bases.

Scientific basis	In Title, Abstract or Keyword				All Fields	
Tags	Scopus	IEEE	MDPI	Elsevier	Google Scholar	Springer
V2X[a] AND SIM[b] AND SEC[c]	1240	563	374	10	27500	3039
V2X[a] AND SIM[b] AND "jamming"	113	41	61	3	7870	294
V2X[a] AND SIM[b] AND ("Denial of Service" OR "DoS")	87	114	12	1	273000	580
V2X[a] AND SIM[b] AND "eavesdropping"	83	16	10	1	6270	291
V2X[a] AND SIM[b] AND "spoofing"	23	15	11	0	5890	217
V2X[a] AND SIM[b] AND ("Distributed Denial of Service" OR "DDoS")	21	22	5	0	4790	185

and the real number of works would probably be much smaller.

Table 18 and 19 were created to analyze the annual growth of the V2X cybersecurity subject on the Scopus database. In Table 18, results are observed in the most diverse contexts, while in Table 19, results related only to simulations are shown. From Table 18, note a growing number of papers related to security in the context of V2X in the Scopus database. In this way, simulations in the context of V2X have several interesting applications, one of which is the application in the area of cybersecurity. An important observation is that recent papers addressing cyberattacks have grown more than papers addressing cybersecurity. Table 19 shows considerable growth over the years, but it has grown at an even higher rate in the context of simulations. Note that, in Table 13, 42.24% of the works had been published in the last three years while, in Table 19, 56.06% of the total works were published in the same period. This suggests that in the area of simulation tools in the context of V2X, the area of cyberattacks has been growing faster than papers that do not address this topic. All searches found in Tables 16-19 were carried out on January 1, 2024.

III. LITERATURE REVIEW OF V2X SIMULATION TOOLS

In this section, we conduct a literature review based on various academic works on V2X and simulation tools. The criteria for selecting papers are: 1) based on recent studies (from 2020 to 2024) published in journals with high scientific relevance or exceptionally from scientific conferences; or 2) papers with over one hundred academic citations in the Scopus or Google Scholar databases. Journals were considered to have high scientific relevance if they had a Scopus percentile above 50% or an impact factor greater than 3. The tags employed in the search were V2X[a] and the names of each different simulation tool.

With the increase in demand for testing scenarios related to functionalities related to ADAS or autonomous vehicles simulation tools have emerged, such as SUMO [22], OMNeT++ [20], CARLA [19], and NS3 [23]. Also, some frameworks have surged such as Veins [24], Simu5G [21], and Artery [44], [45]. Also, the recent surge in V2X communication research has led to various approaches in integrating simulators, such as CARLA and OMNeT++, focusing mainly on cooperative perception, sensor data processing, and communication in autonomous driving systems. Several studies, including [46], [47], [48], explore the use of CARLA and OMNeT++ for simulating urban and suburban environments. These studies commonly employ advanced onboard sensors such as cameras, radar, and Light Detection and Ranging (LiDAR), but their data fusion methodologies differ. While [46] does not specify its fusion approach, [47] adopts early fusion of LiDAR point clouds, and [48] uses a nonlinear Kalman filter for probabilistic data fusion. These papers collectively underscore the potential of 5G networks, with [46] and [47] focusing on teleoperated driving and cooperative perception, respectively. However, they do not extensively address cybersecurity threats in communication systems.

The works of [49] and [50] further extend the application of CARLA in autonomous driving scenarios. Reference [49] highlights the vulnerability of cooperative perception to cyberattacks and proposes an encryption technique, whereas [50] focuses on cooperative LiDAR-based 3D object detection, emphasizing the challenges of communication in V2V systems. Both studies reflect the need for secure and reliable data exchange, although [50] delves more into the communication nuances, such as latency and reliability.

TABLE 18. The number of publications in V2X cybersecurity area separated year by year in the Scopus database using the title, abstract, and keywords criteria.

Year	V2X[a] AND SEC[c]		V2X[a] AND SEC[c] AND ATK[d]	
	Amount of Publications	% Amount of Publications	Amount of Publications	% Amount of Publications
2023	905	19.95	382	21.67
2022	769	16.95	336	19.06
2021	598	13.18	259	14.69
2020	450	09.92	180	10.21
2019	413	09.10	177	10.04
2018	335	07.39	141	08.00
2017	222	04.89	87	04.93
2016	172	03.79	54	03.06
2015	134	02.95	42	02.38
2014	104	02.29	22	01.25
2013	92	02.03	23	01.30
2012	78	01.72	18	01.02
2011	61	01.34	16	00.91
2010	42	00.93	4	00.23
2009	49	01.08	8	00.45
Pre-2009	112	02.47	14	00.79
Total	**4536**	**100.00**	**1763**	**100.00**

TABLE 19. The number of publications in the area of simulation tools and cybersecurity in the V2X context is separated year by year in the Scopus database using the title, abstract, and keywords criteria.

Year	V2X[a] AND SIM[b] AND SEC[c]		V2X[a] AND SIM[b] AND SEC[c] AND ATK[d]	
	Amount of Publications	% Amount of Publications	Amount of Publications	% Amount of Publications
2023	261	21.03	108	22.59
2022	244	19.66	100	20.92
2021	155	12.49	60	12.55
2020	128	10.31	46	09.62
2019	124	09.99	53	11.09
2018	96	07.74	41	08.58
2017	58	04.67	25	05.23
2016	39	03.14	9	01.88
2015	30	02.42	13	02.72
2014	17	01.37	5	01.05
2013	25	02.01	6	01.26
2012	12	00.97	2	00.42
2011	20	01.61	5	01.05
2010	7	00.56	0	00.00
2009	9	00.73	2	00.42
Pre-2009	16	01.89	3	00.63
Total	**1241**	**100.00**	**478**	**100.00**

In contrast, [51] and [52] leverage OpenCDA alongside CARLA and SUMO for creating and analyzing traffic scenarios. These studies highlight the integration of various sensors and fusion strategies, with [52] introducing the Attentive Intermediate Fusion pipeline. Both papers consider communication aspects such as bandwidth and latency but do not explicitly discuss cybersecurity threats.

The work of [53] and [54] presents a blend of simulation and communication technologies. The work [53] combines CARLA with SUMO, employing a high-level object fusion framework and addressing the necessity of misbehavior detection systems in shared perception V2X applications. The work [54] focuses on the implementation of a basic communication channel within the CARLA simulator to facilitate the exchange of sensor information between vehicles. To evaluate their framework, the authors conducted simulations using the Town01 3D road network in CARLA, highlighting the importance of high-throughput, low-latency networks such as 5G for effective data transmission in scenarios involving various types of vehicles, objects, and static elements. Lastly, the works [55] and [56] explore specific aspects of V2X communication. The work [55] concentrates on On-Board Unit (OBU) performance within Cellular Vehicle-to-Everything (C-V2X) scenarios using CARLA. In contrast, the work [56] discusses the integration of Simu5G with CARLA for cooperative perception, with a focus on secure and efficient communication networks.

In addition to the tools and frameworks discussed, alternative simulation tools employed in V2X communication research include Mininet-WiFi. Mininet-WiFi is an extension of the Mininet network emulator that adds wireless channel emulation and mobility support, making it suitable for simulating software-defined wireless networks in vehicular environments [57], [58], [59]. This tool enables the emulation of various wireless network topologies, allowing researchers to configure nodes with multiple wireless interfaces [58]. In the context of V2X, Mininet-WiFi can be integrated with SUMO to simulate realistic vehicular mobility scenarios where the movement of vehicles directly influences network behavior [59], [60]. This combination facilitates the reproduction of complex road environments by directly injecting real traffic data, making it particularly useful for evaluating the performance of adaptive SDN frameworks under different traffic conditions, such as congestion and interference [57], [58]. Studies utilizing this integrated approach have highlighted its effectiveness in assessing resource management strategies and exploring the potential of SDN in vehicular networks [57], thereby contributing to the advancement of V2X communication systems.

In summary, these studies collectively enhance the understanding of V2X communication in autonomous driving, emphasizing the integration of simulation tools, advanced sensor technologies, and the importance of secure and efficient data exchange. Despite their contributions, a common thread in these works is exploring the potential and challenges of 5G and beyond in V2X communication, highlighting the need for continuous innovation in this rapidly evolving field of knowledge.

IV. SIMULATION IN V2X ATTACK CONTEXTS

In the V2X cybersecurity context, simulations are invaluable for understanding and mitigating vulnerabilities. It allows for an in-depth examination of threat models and the assessment of countermeasures within a controlled setting. This section thus explores specific simulation parameters critical for precisely replicating the conditions under which cybersecurity threats manifest, underpinning the development of robust defenses and ensuring the resilience of V2X communications against these widespread challenges. This section highlights the importance of simulations within the V2X security landscape and sheds light on the methodologies employed in simulating cybersecurity threats. The adoption of extensive simulation practices aids researchers and practitioners in identifying vulnerabilities within V2X systems and strategizing effectively to bolster security measures. Detailed insights into the simulation parameters used to model these threats are provided in the following subsections, laying the groundwork for enhancing the security architecture of V2X communications.

This section is divided into six subsections. Subsection IV-A shows the abbreviations and meanings of the parameters analyzed in the simulations of four cyberattacks - jamming, spoofing, DoS, and eavesdropping. Furthermore, The subsection IV-A presents the simulation tools present in all works used in this section. In Subsections IV-B-IV-E, tables with simulation parameters for jamming, spoofing, DoS, and eavesdropping are presented, respectively. Finally, a summary with the conclusion is done in Subsection IV-F.

A. SIMULATION PARAMETERS

The Section IV uses several works in which simulations related to jamming, spoofing, DoS, and eavesdropping occur. The works used were [61], [62], [63], [64], [65], [66], [67], [68], [69], [70], [71], [72], [73], [74], [75], [76], [77], [78], [79], [80], [81], [82], [83], [84], [85], [86], [87]. Table 20 shows all the simulation tools found for these types of attacks in the context of V2X. Due to the simulation parameters extension, it was necessary to use some abbreviations placed both in Table 21 and in the Table 37 in the Appendix Section. Also, GEO is a type of satellite orbit often used in telecommunications; FHS is a method of transmitting radio signals by rapidly switching among many frequency channels; and USRP is a device used in wireless communication and Software-Defined Radio (SDR) research. Tables 22-25 aggregate the parameters and the respective values and some techniques and parameters used by some state-of-the-art works. Tables 22-25 refer, respectively, to jamming, spoofing, DoS, and eavesdropping.

TABLE 20. Simulation tools in V2X cyberattacks present in the works related to Section IV.

Work	Simulation Tools
[61]	SUMO
[62]–[64]	SUMO and OMNeT++
[65]	OMNeT++, Veins, SUMO, and Plexe-veins
[66]	NS-2.35 and SUMO
[67]	NS-3
[68]	NS-3 and SUMO
[69]	WiLabV2Xsim and VEINS

TABLE 21. Abbreviations used in Section IV and their full meanings.

Abbreviation	Full meaning
3GPP	Third Generation Partnership Project
AWGN	Additive White Gaussian Noise
FAP	Femtocells/Femto Access Points
FSPL	Free Space Path Loss
GEO	Geosynchronous Earth Orbit
LEO	Low Earth Orbit
MBS	Macro Base Stations
MIMO	Multiple Input, Multiple Output
RSUs	Road Side Units
SIRN	signal-to-interference-plus-noise ratio
SISO	Single Input, Single Output
SNR	Signal-to-noise ratio
UAV	Unmanned Aerial Vehicle
UE	User Equipment
URPA	Uniform Rectangular Planar Array Antenna
USRP	Universal Software Radio Peripheral
WAVE	Wireless Access in Vehicular Environments

B. JAMMING

As illustrated in Table 22, the simulation parameters for jamming in V2X contexts exhibit considerable variation, underscoring the complexity and diversity of this type of cyberattack. The carrier frequencies used in these simulations range from 2 GHz and 28 GHz, indicating the wide spectrum of operational scenarios that researchers need to consider. This variability is essential for developing robust

V2X systems that can function effectively across different frequency bands, especially as wireless communication technologies continue to evolve. The bandwidth utilized in these simulations also varies significantly, from as narrow as 1 MHz to as broad as 1 GHz. This range highlights the necessity to account for different communication channel conditions and the impact of bandwidth on the performance and resilience of V2X systems under jamming attacks. For instance, narrower bandwidths might be more susceptible to jamming, while broader bandwidths might offer more robustness but at the cost of increased complexity and resource requirements.

Vehicle speed is another critical parameter, with simulations considering speeds from 12 m/s to 120 km/h. This variation is crucial because the effectiveness of jamming attacks and the performance of V2X communications can be highly dependent on the relative speed of the vehicles. High-speed scenarios pose unique challenges for maintaining reliable communication links and ensuring timely delivery of safety-critical messages. Transmit power for both UE and V2V communications is also a significant factor. The transmit power for UE ranges from 0.1 W to 23 dBm, while V2V ranges from 16 dBm to 38 dBm. Higher transmit power can enhance communication range and signal strength but also increase the risk of detection and the potential impact of jamming attacks. On the other hand, jamming power levels range from 1 dBm to 40 dBm, demonstrating the varying intensities of jamming signals that can be simulated to assess the resilience of V2X systems.

The required SINR thresholds in these simulations range from -1000 dBm to 24.6 dB. This wide range reflects the different sensitivity levels of various communication systems to interference and how these thresholds can influence the success rate of jamming attacks and the performance of countermeasures. Pathloss models, such as the Free Space Path Loss model and Nakagami-m, are utilized to simulate different environmental conditions and their impact on signal propagation. The choice of pathloss model can significantly affect the accuracy of the simulation results and the understanding of how jamming attacks might propagate in real-world scenarios. Noise power and models, such as AWGN, are critical for accurately simulating the background interference that V2X systems must contend with. Accurate noise modeling helps in assessing the robustness of communication links under jamming conditions. Other parameters such as packet length, channel model, data rate, transmission rate, number of jammers, and antenna configurations are equally important. They provide a comprehensive view of the various factors that influence the effectiveness of jamming attacks and the resilience of V2X communication systems. For example, using different channel models (e.g., Rayleigh fading, log-normal shadowing) and antenna configurations (e.g., MIMO, SISO) helps understand the diverse operational environments and their impact on system performance.

In conclusion, the diversity of simulation parameters illustrated in Table 22 highlights the multifaceted nature of jamming attacks in V2X systems. It underscores the importance of considering a wide range of factors to develop robust and resilient V2X communication systems capable of withstanding various types of cyberattacks. These comprehensive simulations are crucial for advancing our understanding of V2X cybersecurity and for designing effective countermeasures to protect these critical communication networks. Note that d in $128.1 + 37.6\log_{10}(d)$ represents the space dimensionality.

C. SPOOFING

As illustrated in Table 23, the simulation parameters for spoofing in V2X contexts exhibit considerable variability, reflecting the complex and multifaceted nature of this type of cyberattack. The carrier frequencies used in these simulations span from 2 GHz to 60 GHz, covering a wide range of operational scenarios. This diversity is crucial for developing V2X systems that can securely operate across different frequency bands, addressing the evolving challenges of wireless communication technologies and potential spoofing threats. The bandwidth values in these simulations range from 1.4 MHz to 7.2 MHz. This variation highlights the need to consider different communication channel conditions and the impact of bandwidth on the susceptibility of V2X systems to spoofing attacks. Narrower bandwidths may be more vulnerable to spoofing, while wider bandwidths could offer more robust defenses but with increased system complexity and resource requirements.

Vehicle speed is another critical parameter, with simulations considering speeds from 40 km/h to 500 km/h. The variation in speed is crucial because the effectiveness of spoofing attacks and the performance of V2X communications can significantly depend on the relative speed of the vehicles. High-speed scenarios pose unique challenges for maintaining secure communication links and ensuring the integrity of transmitted data. Transmit power for both UE and V2I communications plays a significant role in spoofing simulations. The transmit power for UE ranges from 8 dBm to 23 dBm, while V2I transmit power is typically 23 dBm. Higher transmit power can enhance communication range and signal strength and increase the risk of interception and manipulation by spoofer devices. The attacking power levels, varying from 20 dBm to 40 dBm, illustrate the different intensities of spoofing attacks that can be simulated to assess the resilience of V2X systems. The pathloss models, such as the Free Space Path Loss model and the model defined as $128.1 + 37.6\log_{10}(d)$, are employed to simulate different environmental conditions and their impact on signal propagation. The choice of pathloss model significantly affects the accuracy of simulation results and the understanding of how spoofing attacks might occur in real-world scenarios.

Noise models, such as AWGN, are critical for accurately simulating the background interference that V2X systems must contend with. Accurate noise modeling helps assess the robustness of communication links against spoofing

TABLE 22. State of the art in simulation parameters for jamming simulation.

Parameters	Values	Papers
Carrier frequency	2 GHz 2.4 GHz 5.9 GHz 28 GHz	[63], [70], [71] [74] [65], [69], [72] [73]
Bandwidth	1 – 15 MHz 1.4 MHz 10 MHz 20 MHz 1 GHz	[74] [63], [70] [62], [65], [69], [72], [75] [76] [73]
Vehicle speed	12 m/s 30 – 70 km/h 40 km/h Until 100 km/h 120 km/h	[75] [72] [63], [70] [65] [73]
UE transmit power	0.1 W 20 dBm 23 dBm	[75] [62] [69]
V2V transmit power	16 – 38 dBm 100 mW	[72] [65]
V2I transmit power	23 dBm	[63], [70]
Attacking power	1 – 18 dBm 18 – 38 dBm 20 dBm 20 – 40 dBm 23 dBm 30 dBm	[76] [72] [62] [63] [73] [70]
The required SINR threshold	-1000 dBm -15 dB 3 dB 6 – 24.6 dB	[69] [62] [72] [76]
Pathloss model	Free-space path loss model $128.1 + 37.6\log_{10}(d)$, d represents the space dimensionality	[62], [65], [72], [73] [63], [70]
Noise power	-114 dBm -104 dBm -95 dBm -20 dB	[70] [62] [65] [71]
Noise model for system	AWGN	[74], [75]
Packet length	200 bits 756 bytes 1000 bits 1500 bytes	[65] [62] [75] [76]
Channel model	3GPP 5G Model Free Space Path Loss (FSPL) Rayleigh fading Log-normal shadowing Nakagami-m Shadowed Rician	[69] [65] [62], [70], [72], [73] [63] [75] [71]
Data rate (Physical Layer)	6 Mbps 6 – 54 Mbps 27 Mbps	[65] [76] [62]
Transmission rate	1 bps/Hz 10 Hz	[71] [65], [69]
Number of jammers	4	[72], [76]
Number of antennas	1 per vehicle 1 – 2 4 antennas on the UAV 64 SISO and MIMO	[65], [72] [69] [74] [73] [76]
Antenna configuration	64-element uniform linear array USRP B210s Monopole antennas Omnidirectional antennas	[73] [69] [65] [74], [75]
Antenna gain	4 dB 4 – 5 dBi 3 – 8 dBi	[71] [69] [70]
Types of satellite	GEO (Geosynchronous Earth Orbit) LEO (Low Earth Orbit)	[71] [74]
Maximum beam gain	30 dB 48 dB	[73] [71]
Node working mode	Full-duplex	[71], [74], [75]

TABLE 23. State of the art in simulation parameters for spoofing simulation.

Parameters	Values	Papers
Carrier frequency	2 GHz	[63]
	2.6 GHz	[77]
	5.9 GHz	[64]
	24 – 60 GHz	[78]
	28 GHz	[79]
Bandwidth	1.4 MHz	[63]
	7.2 MHz	[77]
Vehicle speed	40 km/h	[63]
	Until 500 km/h	[80]
UE transmit power	8 –23 dBm	[64]
V2I transmit power	23 dBm	[63]
Attacking power	20 – 40 dBm	[63]
Pathloss model	Free-space path loss model	[64], [79]
	$128.1 + 37.6\log_{10}(d)$, d represents the space dimensionality	[63]
Noise model for system	AWGN	[77], [80]
Channel model	5G 3GPP-like Channel Model	[64]
	Log-normal shadowing	[63]
	mmWave	[78], [79]
	Rayleigh	[80]
	AWGN	[77]
Number of antennas	4 × 4, 6 × 6, 16 × 16, 32 × 32	[78]
	16 × 16, 32 × 32, 64 × 64, 128 × 128	[79]
Antenna configuration	Massive MIMO	[79]
	Uniform Rectangular Planar Array Antenna (URPA)	[78]
	Omnidirectional antennas	[80]
Antenna gain	3-8 dBi	[63]
	8 dBi	
Distance to RSUs	500 m	[63]
Node working mode	Half-duplex	[80]

attempts. Other parameters such as channel model, number of antennas, antenna configuration, and antenna gain are equally important. They provide a comprehensive view of the various factors that influence the effectiveness of spoofing attacks and the resilience of V2X communication systems. For example, using different channel models (e.g., 5G 3GPP-like Channel Model, Log-normal shadowing, mmWave, Rayleigh, AWGN) helps understand the diverse operational environments and their impact on system performance. The number of antennas, ranging from 4 × 4 to 128 × 128, and configurations such as Massive MIMO and Uniform Rectangular Planar Array Antenna (URPA), are key in understanding how multiple input and output systems can enhance or mitigate the effects of spoofing. The distance to RSUs, typically set at 500 meters, and the node working mode, usually half-duplex, are also crucial parameters that affect the susceptibility and detection of spoofing attacks.

In conclusion, the diversity of simulation parameters illustrated in Table 23 highlights the intricate nature of spoofing attacks in V2X systems. It underscores the importance of considering various factors to develop robust and secure V2X communication systems capable of withstanding various types of cyberattacks. These comprehensive simulations are crucial for advancing our understanding of V2X cybersecurity and for designing effective countermeasures to protect these critical communication networks from spoofing threats.

D. DoS

As illustrated in Table 24, the simulation parameters for Denial of Service (DoS) attacks in V2X contexts reveal significant variability, reflecting the complexity and multifaceted nature of this type of cyberattack. The carrier frequencies used in these simulations span from 2.6 GHz to 5.9 GHz, covering critical operational scenarios relevant to V2X communications. This diversity is essential for developing V2X systems that can operate securely across different frequency bands, addressing the evolving challenges of wireless communication technologies and potential DoS threats. The bandwidth values in these simulations range from 7.2 MHz to 10 MHz. This variation highlights the necessity to account for different communication channel conditions and the impact of bandwidth on the susceptibility of V2X systems to DoS attacks. Narrower bandwidths may be more vulnerable to congestion and disruption, while wider bandwidths could offer more robustness but with increased system complexity and resource requirements.

Vehicle speed is another critical parameter, with simulations considering speeds from 30 km/h to 80 km/h. The variation in speed is crucial because the effectiveness of DoS attacks and the performance of V2X communications can significantly depend on the relative speed of the vehicles. High-speed scenarios pose unique challenges for maintaining reliable communication links and ensuring timely delivery of safety-critical messages. Transmit power for both UE and MBS communications plays a significant role in DoS simulations. The transmit power for UE ranges from 23 dBm to 60 dBm, while MBS transmit power is typically around 43 dBm. Higher transmit power can enhance communication range and signal strength but also increases the risk of interference and network congestion, making the system

TABLE 24. State of the art in simulation parameters for DoS simulation.

Parameters	Values	Papers
Carrier frequency	2.6 GHz	[77]
	5.9 GHz	[66]–[69]
Bandwidth	7.2 MHz	[77]
	10 MHz	[67]–[69]
Vehicle speed	30 – 80 km/h	[61]
	60 – 80 km/h	[68], [81]
UE transmit power	23 dBm	[69]
	33.8 – 60 dBm	[68]
MBS transmission power	43 dBm	[61]
FAP transmission power	23 dBm	[61]
Pathloss model	Path loss coefficient: FAP: 3.5, MBS: 2.5	[61]
	Signal attenuation model, considering obstacles	[68]
Noise model for system	AWGN	[77]
Packet length	160 bytes	[61]
	512 bytes	[66]
	1000 bytes	[67]
Packet generation rate (attack)	1 Packet/ms	[61]
Packet generation rate (legitimate vehicle)	200 Packets/s	[61]
Channel model	3GPP 5G Model	[69]
	AWGN	[77]
	IEEE 802.11p protocol stack	[68]
	IEEE 802.11p and 5G	[81]
	WAVE (Wireless Access in Vehicular Environments)	[67]
Transmission rate	10 Hz	[69]
	100 Mbps	[67]
Receiving rate	1.5 Mbps	[67]
Number of antennas	1 – 2	[69]
Antenna configuration	USRP B210s	[69]
	USRP X310	[77]
Antenna gain	4 – 5 dBi	[69]

more susceptible to DoS attacks. The pathloss models, such as those considering path loss coefficients (e.g., FAP: 3.5, MBS: 2.5) and signal attenuation models considering obstacles, are employed to simulate different environmental conditions and their impact on signal propagation. The choice of pathloss model significantly affects the accuracy of simulation results and the understanding of how DoS attacks might occur in real-world scenarios.

Noise models, such as AWGN, are critical for accurately simulating the background interference that V2X systems must contend with. Accurate noise modeling helps in assessing the robustness of communication links against DoS attempts. Other parameters such as packet length, packet generation rate, channel model, transmission rate, and number of antennas are equally important. They provide a comprehensive view of the various factors that influence the effectiveness of DoS attacks and the resilience of V2X communication systems. For instance, packet lengths in these simulations range from 160 to 1000 bytes, and packet generation rates for attacks can be as high as one packet/ms. These parameters are crucial for understanding the capacity of the network to handle legitimate traffic versus malicious traffic. Using different channel models (e.g., 3GPP 5G Model, IEEE 802.11p, WAVE) helps understand the diverse operational environments and their impact on system performance. The number of antennas, typically 1 to 2, and configurations such as USRP B210s and USRP X310 are vital in understanding how multiple input and output systems can enhance or mitigate the effects of DoS attacks. Antenna gain, usually around 4-5 dBi, is another critical factor influencing signal strength and network resilience.

In conclusion, the diversity of simulation parameters illustrated in Table 24 highlights the intricate nature of DoS attacks in V2X systems. It underscores the importance of considering a wide range of factors to develop robust and secure V2X communication systems capable of withstanding various types of cyberattacks. These comprehensive simulations are crucial for advancing our understanding of V2X cybersecurity and for designing effective countermeasures to protect these critical communication networks from DoS threats.

E. EAVESDROPPING

As illustrated in Table 25, the simulation parameters for eavesdropping in V2X contexts reveal substantial variability, reflecting the complexity and multifaceted nature of this type of cyberattack. The carrier frequencies used in these simulations span from 1 GHz to 28 GHz, covering a broad spectrum of operational scenarios. This diversity is essential for developing V2X systems that can operate securely across different frequency bands, addressing the evolving challenges of wireless communication technologies and potential eavesdropping threats. The bandwidth values in these simulations range from as narrow as 1 MHz to as wide as 1 GHz. This variation underscores the need to consider different communication channel conditions and

TABLE 25. State of the art in simulation parameters for eavesdropping simulation.

Parameters	Values	Papers
Carrier frequency	1 GHz	[82]
	2 GHz	[71]
	2.4 GHz	[74]
	5.9 GHz	[72]
	28 GHz	[73]
Bandwidth	1 – 15 MHz	[74]
	10 MHz	[62], [72], [75]
	1 GHz	[73]
Vehicle speed	12 m/s	[75]
	30 – 70 km/h	[72]
	120 km/h	[73]
UE transmit power	0.1 W	[75]
	20 dBm	[62]
V2V transmit power	16 – 38 dBm	[72]
Attacking power	0 – 0.4 W	[83]
	18 – 38 dBm	[72]
	20 dBm	[62]
	23 dBm	[73]
Pathloss model	Free-space path loss model	[62], [72], [73]
	Nakagami-m	[75], [82]–[84]
The required SINR threshold	3 dB	[72]
Noise power	-110 dBm	[83]
	-104 dBm	[62]
	-20 dB	[71]
Noise model for system	AWGN	[74], [75], [82]–[87]
Packet length	756 bytes	[62]
	1000 bits	[75]
Channel model	Double Rayleigh	[86]
	Rayleigh fading	[62], [72], [73], [85], [87]
	Nakagami-m	[75], [82], [84]
	line-of-sight probabilistic channel model	[83]
	Shadowed Rician	[71]
Data rate (Physical Layer)	27 Mbps	[62]
Transmission rate	1 bps/Hz	[71]
Number of antennas	1 per vehicle	[72]
	1 antenna per UAV	[82]
	2	[84]
	4	[85], [86]
	4 antennas on the UAV	[74]
	5	[87]
	64	[73]
Antenna configuration	64-element uniform linear array	[73]
	Multi-beam antennas on the satellite and transceiver antennas on the relay	[71], [84]
	Omnidirectional antennas	[74], [75], [82], [83], [85]–[87]
Antenna gain	4 dB	[71]
Types of satellite	GEO (Geosynchronous Earth Orbit)	[71]
	LEO (Low Earth Orbit)	[74]
Maximum beam gain	30 dB	[73]
	48 dB	[71]
Node working mode	Full-duplex	[71], [74], [75], [82]–[85]
	Half-duplex	[86], [87]
Number of eavesdroppers	1	[72], [73]
	1 – 4	[84]
Distance to RSUs	800 m	[84]
Signal-to-noise ratio (SNR)	-5 – 20 dBm	[84]

the impact of bandwidth on the susceptibility of V2X systems to eavesdropping. Narrower bandwidths may be more vulnerable to interception, while wider bandwidths could offer more robust defenses but with increased system complexity and resource requirements. Vehicle speed is another critical parameter, with simulations considering speeds from 12 m/s to 120 km/h. The variation in speed is crucial because the effectiveness of eavesdropping and the performance of V2X communications can significantly depend on the relative speed of the vehicles. High-speed scenarios pose unique challenges for maintaining secure communication links and ensuring the confidentiality of transmitted data.

Transmit power for both UE and V2V communications plays a significant role in eavesdropping simulations. The transmit power for UE ranges from 0.1 W to 20 dBm, while V2V transmit power ranges from 16 dBm to 38 dBm. Higher transmit power can enhance communication range and signal strength but also increase the risk of interception by eavesdroppers. The eavesdropping power levels, varying from 0 to 0.4 W and up to 38 dBm, illustrate the different intensities of eavesdropping attacks that can be simulated to assess the resilience of V2X systems. The required SINR thresholds in these simulations, typically set at 3 dB, reflect the sensitivity levels of various communication systems to interference and how these thresholds can influence the success rate of eavesdropping attempts. Pathloss models, such as the Free Space Path Loss model and Nakagami-m, are employed to simulate different environmental conditions and their impact on signal propagation. The choice of pathloss model significantly affects the accuracy of simulation results and the understanding of how eavesdropping attacks might occur in real-world scenarios.

Noise power and models, such as AWGN, are critical for accurately simulating the background interference that V2X systems must contend with. Accurate noise modeling helps in assessing the robustness of communication links against eavesdropping attempts. Other parameters such as packet length, channel model, data rate, transmission rate, number of eavesdroppers, and antenna configurations are equally important. They provide a comprehensive view of the various factors that influence the effectiveness of eavesdropping attacks and the resilience of V2X communication systems. For example, using different channel models (e.g., Double Rayleigh, Rayleigh fading, Nakagami-m) and antenna configurations (e.g., MIMO, SISO) helps understand the diverse operational environments and their impact on system performance. The number of eavesdroppers, ranging from 1 to 4, highlights the varying threat levels and the importance of simultaneously designing systems that can withstand multiple eavesdropping attempts.

In conclusion, the diversity of simulation parameters illustrated in Table 25 highlights the intricate nature of eavesdropping attacks in V2X systems. It underscores the importance of considering various factors to develop robust and secure V2X communication systems capable of withstanding various types of cyberattacks. These comprehensive simulations are crucial for advancing our understanding of V2X cybersecurity and for designing effective countermeasures to protect these critical communication networks from eavesdropping threats.

F. SUMMARY

In summary, the detailed simulation parameters outlined in Tables 22, 23, 24, and 25 provide a comprehensive overview of the current state-of-the-art in V2X security research. These parameters underscore the importance of considering a broad array of factors to ensure the robustness and reliability of V2X communication systems against various security threats, including jamming, spoofing, DoS, and eavesdropping. The variability in simulation setups highlights the inherent complexity of V2X systems and the necessity for extensive and diverse testing methodologies. Researchers can better anticipate potential vulnerabilities and devise more effective countermeasures by incorporating a broad spectrum of operational scenarios and conditions. This approach ultimately enhances the overall security posture of V2X communication networks, ensuring their effectiveness in real-world applications. The comprehensive nature of these simulations is crucial for advancing our understanding of V2X cybersecurity and for developing robust systems capable of withstanding a multitude of cyber threats.

V. TRENDS SIMULATION TOOLS IN V2X CONTEXT

This section analyzes future trends related to simulation tools related to V2X. Understanding these trends is crucial for anticipating advancements and challenges in V2X technology. It enables researchers and developers to proactively address emerging issues and innovate solutions that enhance the security, efficiency, and reliability of V2X communication systems. Moreover, aligning research efforts with industry developments is essential. It fosters collaboration and ensures the practical applicability of simulation tools in real-world scenarios.

This section contains two subsections. Subsection V-A deals with trends in simulation tools related to V2X in the most diverse contexts. Subsection V-A is divided into three subsubsections in which the first sub-subsection analyzes year-by-year simulation tools and, based on these analyses, identifies future trends. In the second subsubsection, research is carried out on works that have cases of integration of simulation tools in the context of V2X, and based on this information, a framework proposal is made that involves simulation tool integration. In the third subsubsection, other trends are presented. On the other hand, Subsection V-B deals with trends in simulation tools related to V2X in the context of cybersecurity. In a similar way to the previous subsection, Subsection V-B is divided into two subsubsections very similar to the first and second subsubsection of the previous subsection but with a focus on the V2X cybersecurity area.

A. SIMULATION TOOLS IN DIFFERENT CONTEXTS RELATED TO V2X

1) TRENDS IN SIMULATION TOOLS: A YEAR-BY-YEAR ANALYSIS

Table 26 and Figure 6 present research data on the leading simulation tools featured in scientific publications indexed by Scopus. This table compares total publication results from January 1, 2021, to December 31, 2023. Note from Table 26 that the SUMO, NS3, and OMNeT++ simulation tools are the most used. OMNeT++, CARLA, Minine-Wifi, VTD, Eclipse MOSAIC, and Simu5G have grown in the last three years, suggesting a more significant presence of these simulation tools in the coming years. It is easily seen from Figure 6 that SUMO, NS3, OMNeT++, Veins, and Carla have been more relevant in the last three years than the other simulation tools. For this reason, research was carried out year after year on these five simulation tools, shown in Tables 27-28 and Figures 7-8. All data was collected on January 1, 2024.

TABLE 26. Trends from the number of search results for simulation tools in V2X context on the Scopus database using the title, abstract, and keywords criteria.

Tags	Total History		Last 3 years	
	Scopus	%Scopus	Scopus	%Scopus
V2X[a] AND "SUMO"	468	29.62	243	31.40
V2X[a] AND ("NS3" OR "NS-3")	307	19.43	136	17.57
V2X[a] AND "OMNeT++"	201	12.72	103	13.31
V2X[a] AND "Veins"	148	09.37	60	07.75
V2X[a] AND "CARLA"	57	03.61	54	06.98
V2X[a] AND "CarSim"	60	03.80	24	03.10
V2X[a] AND "PreScan"	46	02.91	24	03.10
V2X[a] AND "Artery"	30	01.90	16	02.07
V2X[a] AND ("Virtual Test Drive" OR "VTD")	26	01.65	15	01.94
V2X[a] AND "Simu5G"	15	00.95	14	01.81
V2X[a] AND "CarMaker"	25	01.58	12	01.55
V2X[a] AND "OPNET"	46	02.91	7	00.90
V2X[a] AND "PLEXE"	14	00.89	7	00.90
V2X[a] AND "INET"	12	00.76	6	00.78
V2X[a] AND "iTetris"	16	01.01	5	00.65
V2X[a] AND "Mininet-WiFi"	9	00.57	5	00.65
V2X[a] AND "AirSim"	6	00.38	5	00.65
V2X[a] AND "Eclipse MOSAIC"	5	00.32	5	00.65
V2X[a] AND "TruckSim"	10	00.63	4	00.52
V2X[a] AND "MilliCar"	7	00.44	4	00.52
V2X[a] AND "Apollo"	7	00.44	3	00.39
V2X[a] AND "Ventos"	7	00.44	3	00.39
V2X[a] AND "GEMV"	4	00.25	3	00.39
V2X[a] AND "SimuLTE"	10	00.63	2	00.26
V2X[a] AND "GloMoSim"	5	00.32	2	00.26
V2X[a] AND "LTEV2Vsim"	3	00.19	2	00.26
V2X[a] AND "MiXiM"	3	00.19	2	00.26
V2X[a] AND "CrowNet"	2	00.13	2	00.26
V2X[a] AND "OpenC2X"	7	00.44	1	00.13
V2X[a] AND "Vanetza"	3	00.19	1	00.13
V2X[a] AND "Flowsim"	1	00.06	1	00.13
V2X[a] AND "HYDRO-3D"	1	00.06	1	00.13
V2X[a] AND "LGSVL"	1	00.06	1	00.13
V2X[a] AND "MoReV2X"	1	00.06	1	00.13
V2X[a] AND "VSimRTI"	13	00.82	0	00.00
V2X[a] AND "JiST/SWANS"	2	00.13	0	00.00
V2X[a] AND "Altair WinProp"	1	00.06	0	00.00
V2X[a] AND "Containernet"	1	00.06	0	00.00
Total	**1580**	**100.00**	**774**	**100.00**

TABLE 27. Total number of results in searches for leading simulation tools in the V2X context separated year by year in the Scopus database using "title, abstract or keyword" criteria.

Year	V2X[a] AND "SUMO"	V2X[a] AND ("NS3" OR "NS-3")	V2X[a] AND "OMNeT++"	V2X[a] AND "Veins"	V2X[a] AND "CARLA"
2023	104	46	46	24	21
2022	66	55	22	22	22
2021	73	35	35	14	11
2020	55	27	26	20	2
2019	52	26	19	27	1
2018	36	34	17	10	0
2017	22	26	13	11	0
2016	21	21	7	7	0
2015	13	8	3	5	0
2014	12	11	2	3	0
2013	6	5	9	4	0
2012	4	8	0	1	0
2011	2	2	2	0	0
2010	1	2	0	0	0
2009	1	0	0	0	0
Total	**468**	**306**	**201**	**148**	**57**

Table 27 and Figure 7 show the total results year-by-year in the Scopus database found for the main simulation tools, while Table 28 and Figure 8 show the percentage numbers annually in relation to the total. In Table 27, SUMO in

TABLE 28. Percentage numbers of results in searches for leading simulation tools in the V2X context separated year by year in the Scopus database using "title, abstract or keyword" criteria.

Year	V2X[a] AND "SUMO"	V2X[a] AND ("NS3" OR "NS-3")	V2X[a] AND "OMNeT++"	V2X[a] AND "Veins"	V2X[a] AND "CARLA"
2023	22.22	15.03	22.89	16.22	36.84
2022	14.10	17.97	10.95	14.86	38.60
2021	15.60	11.44	17.41	09.46	19.30
2020	11.75	08.82	12.94	13.51	03.51
2019	11.11	08.50	09.45	18.24	01.75
2018	07.69	11.11	08.46	06.76	00.00
2017	04.70	08.50	06.47	07.43	00.00
2016	04.49	06.86	03.48	04.73	00.00
2015	02.78	02.61	01.49	03.38	00.00
2014	02.56	03.59	01.00	02.03	00.00
2013	01.28	01.63	04.48	02.70	00.00
2012	00.85	02.61	00.00	00.68	00.00
2011	00.43	00.65	01.00	00.00	00.00
2010	00.21	00.65	00.00	00.00	00.00
2009	00.21	00.00	00.00	00.00	00.00
Total	**100.00**	**100.00**	**100.00**	**100.00**	**100.00**

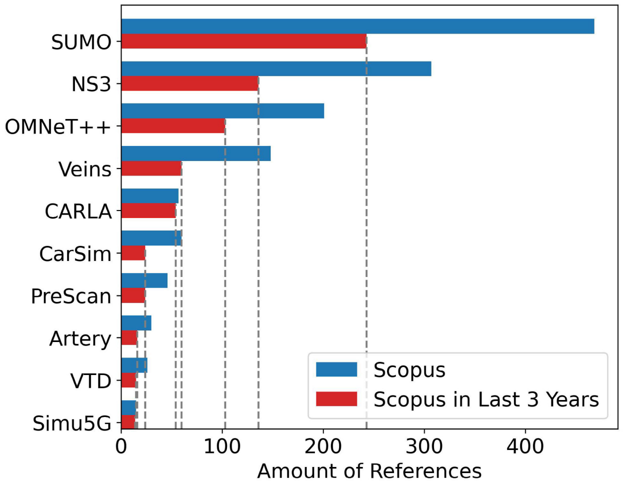


FIGURE 6. Reference numbers of the main simulation tools in V2X context found in the Scopus database using the title, abstract, and keywords criteria.

2023 has more than double the results compared to NS3 and OMNeT++, the ones with the most results in that year after SUMO. This suggests the great relevance of SUMO today, even though it does not have such a large percentage growth in Table 26 and Table 28. On the other hand, from Table 28, it is clear that NS3 and Veins have had less growth in 2023, while CARLA in the last two years has had the greatest growth among the simulation tools present in the V2X context., based on the information contained in Table 26-28 it is observed in academic works that:

1) there is a large presence of SUMO, so it will continue to be very relevant in simulation tool work;

2) there is a considerable presence of NS3 and Veins, but with a recent percentage decrease;

3) there is a significant presence of OMNeT++, maintaining this presence recently;

4) CARLA is small, but it has been the simulation tool that has grown the most in recent years.

The rapid growth of CARLA can be attributed to its advanced functionalities and the growing demand for more realistic and detailed simulations, which are particularly important in developing and testing autonomous vehicles and intelligent transportation systems.

2) SIMULATION TOOLS INTEGRATION AND FUTURE FRAMEWORK PROPOSAL

Another crucial aspect is the integration of different simulation tools in order to overcome their individual limitations. Integration is a natural path between simulators, as several simulators have advantages and disadvantages, and by integrating different simulators, it is possible to combine their advantages. Few works that relate to the subject of V2X and the integration of different simulation tools were found. Table 29 shows the works related to the V2X area and the integration between at least two simulation tools. Table 30 shows less common cases of integration of simulation tools in the context of V2X. Note that the abbreviations used in Table 30 include Rapid Cellular Network Simulation Framework (RACE), MOVE, and Geometry-based, Efficient Propagation Model for Vehicle-to-Vehicle (GEMV). Note in Table 29 that as Simu5G and Artery are frameworks extending the OMNeT++ network simulator, OMNeT++ will also be present whenever they are found. In work [39], there is integration between the Artery and Simu5G frameworks, although there is strictly only the independent simulator OMNeT++. Furthermore, the works [88], [89], [90] are recent, and all the remaining works mentioned in Table 29 were published from 2023 onwards. Based on this information from our research, it is possible to infer a significant increase in the topic of simulator integration in the context of V2X, revealing a likely future trend for future work in the area.

Table 29 shows that the integration between OMNeT++ and SUMO is the most common, being present in many works. However, the integration between OMNeT++ and

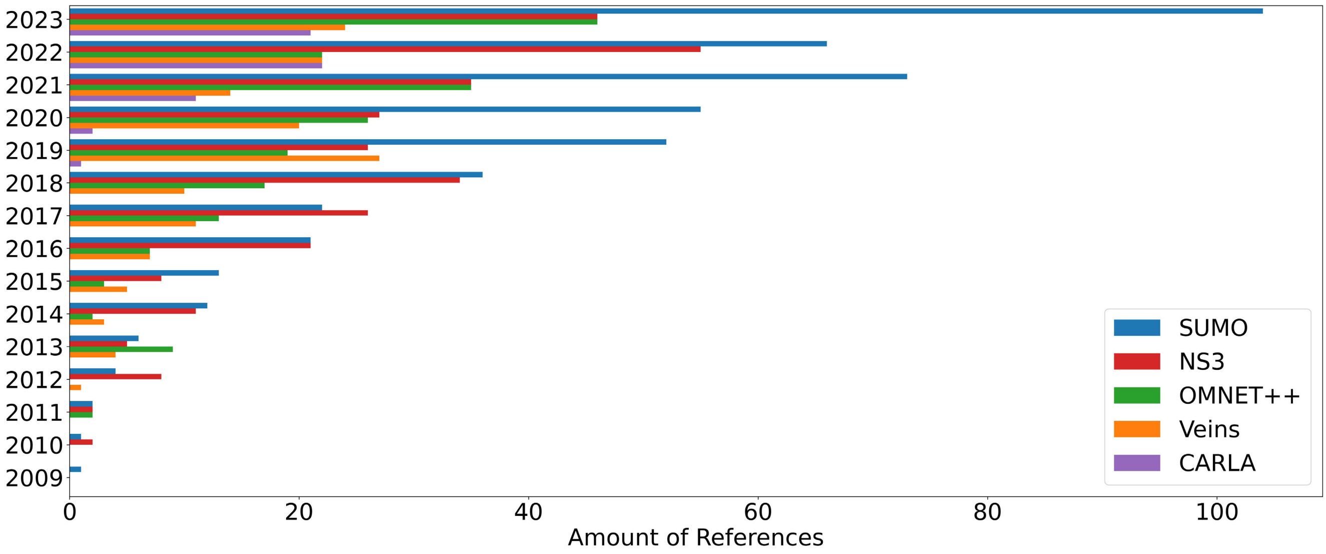


FIGURE 7. Total number of results in searches year by year for leading simulation tools in the V2X context in the Scopus database using "title, abstract or keyword" criteria.

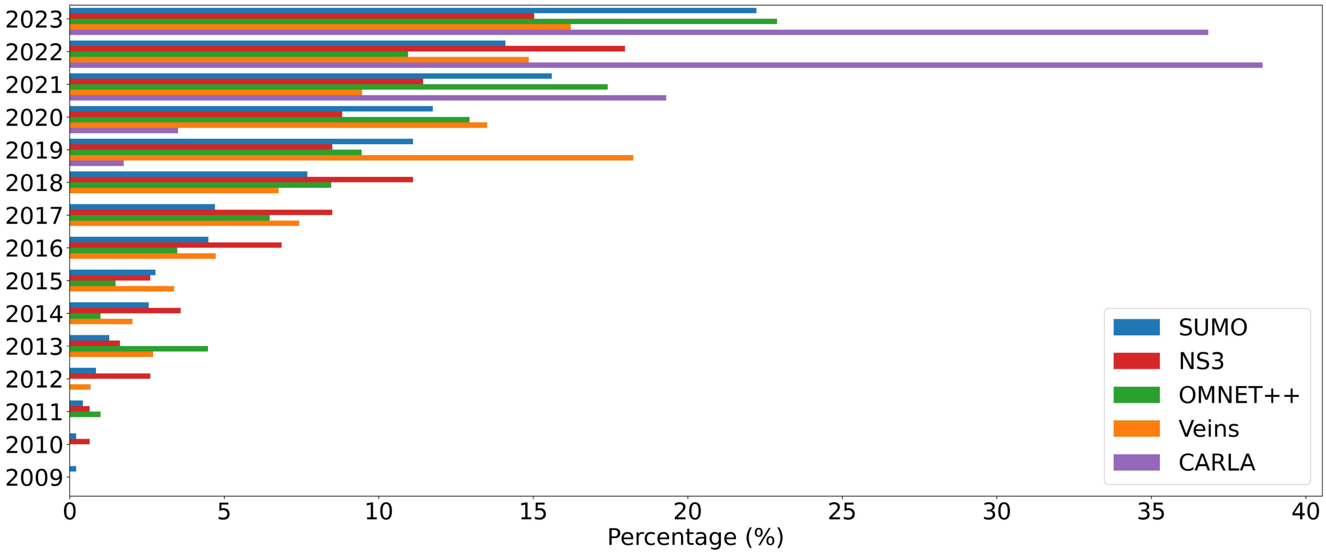


FIGURE 8. Percentage numbers of results in searches year by year for leading simulation tools in the V2X context in the Scopus database using "title, abstract or keyword" criteria.

CARLA is also considerable [46], [56], [88], [91], [92]. The integration between OMNeT++ and SUMO is suitable for large-scale traffic, as SUMO allows the user to simulate traffic behavior in detail, including vehicle movement patterns and V2X interactions. On the other hand, with the increasing relevance of autonomous vehicles, CARLA, which is designed specifically for autonomous driving simulations, offers robust support for modeling sensors and perception systems. For research focused on security against attacks on V2X systems, this combination offers a more comprehensive simulation environment adapted to the future needs of the automotive industry and traffic infrastructure, even more so with the growing search for V2X communication and its related security. Also, note from Table 26 that CARLA suggests a more significant growth trend than SUMO. Therefore, it is argued that although other integrations between simulators are relevant, the future trend will probably favor the integration of OMNeT++ with CARLA for advanced research in V2X security.

In the evolving field of simulator integration in the V2X context, recent studies [46] and [56] have both adopted message-oriented middleware to facilitate communication between CARLA and OMNeT++ simulators. Nevertheless, they exhibit notable distinctions in their implementation strategies. Alternatively to the scheme of these two works, one of the most interesting and valuable works found is [91],

TABLE 29. Cases of integration of simulation tools in V2X context.

Work	SUMO	OMNeT++	CARLA	Veins	NS3	Simu5G	Artery	INET	simuLTE	Containernet	Mininet-WiFi
[88], [91]	✓	✓	✓				✓				
[92]	✓	✓	✓								
[93]	✓	✓		✓	✓						
[94]–[97]	✓	✓		✓				✓			
[37], [98]–[105]	✓	✓		✓							
[106], [107]	✓	✓					✓		✓		
[44], [108], [109]	✓	✓					✓				
[110], [111]	✓	✓						✓			
[40]	✓		✓		✓						
[90], [112]–[116]	✓		✓								
[117]–[123]	✓				✓						
[124], [125]	✓									✓	✓
[56]		✓	✓			✓		✓			
[46]		✓	✓								
[39]		✓				✓	✓	✓			

TABLE 30. Other cases of integration of simulation tools in V2X context.

Work	Simulation Tools
[126]	SUMO and MOVE
[127]	SUMO and LTEV2Vsim
[128]	SUMO, OMNeT++, Veins, and PLexe
[129]	SUMO, OMNeT++, Veins, and MiXiM
[130]	SUMO, OMNeT++, Veins, INET, Vanetza, and Artery
[131]	SUMO, OMNeT++, and OpenCV2X
[132]	SUMO, and GEMV
[133]	SUMO, NS3, and RACE
[134]	SUMO, OMNeT++, and Ventos
[135]	SUMO, OMNeT++, INET, VeinsLTE, and SimuLTE
[89]	SUMO, OMNeT++, and Webots

as it integrates SUMO, OMNeT++, Artery, and CARLA. The Artery provides the middleware for sharing information among V2X services. While SUMO-CARLA-OMNeT++ integration of [91] offers benefits in network traffic optimization and environmental awareness, the methods proposed in the works [46] and [56] may be better suited to address the security challenges in V2X communications directly. This is because the choice of JavaScript Object Notation (JSON) and high-level libraries such as ZeroMQ allows for greater flexibility and extensibility.

The framework in [46] utilizes the ZeroMQ library for message dispatching, employing a JSON Application Programming Interface (API) for message format conversion. This approach contrasts with the conventional binary interface such as Traffic Control Interface (TraCI), primarily due to the design of TraCI for external program interaction with the physical world of SUMO. The decision to use JSON, as opposed to a binary interface, is driven by the need for a more versatile and extendable API, one that not only maintains vehicular position consistency across simulation tools but also maps the network application layer, implemented in OMNeT++ to the applications built upon the CARLA API.

Conversely, [56] also employs a message-oriented middleware with JSON formatted messages but emphasizes high-level messaging libraries such as ZeroMQ over basic Transmission Control Protocol (TCP) sockets. This choice allows for greater flexibility and extensibility in API customization for specific scenarios. It facilitates the development of the CARLA counterpart of the simulator interface using more adaptable programming languages such as Python. While both approaches aim to achieve seamless integration between CARLA and OMNeT++, they reflect different priorities: [46] focuses on maintaining consistency and mapping between layers, whereas [56] prioritizes flexibility and extensibility in the development environment.

Motivated by the trends identified in Table 26 and informed by previous works, we propose future research that entails developing an implementation scheme by simulating automated vehicles using V2X communication with CARLA and OMNeT++ simulators. This simulation aims to replicate automated vehicle behavior in crossroads scenarios, a critical aspect of urban traffic management. The integration between CARLA and OMNeT++ can be achieved through a message-oriented middleware responsible for dispatching JSON-formatted messages, with ZeroMQ serving as the chosen library for this purpose. This communication initially takes place between OMNeT++ and the CARLA Client.

The choice of C++ as the development language opens up access to many valuable libraries. Open Computer Vision Library (OpenCV), for instance, can be leveraged for processing image data, which is important in realistic simulation scenarios. Additionally, Open Cellular Vehicle To Everything (OpenCV2X), a library tailored explicitly for C-V2X, will be instrumental in enhancing the communication capabilities of the simulated vehicles. The primary goal of this integrated simulation is to harness the strengths of both CARLA, known for its realistic graphical simulation, and OMNeT++, renowned for its advanced V2X functionalities. Integrating these two platforms necessitates the translation of data formats from one language to another—Python in the case of CARLA and C++ for OMNeT++. The choice of JSON also reflects its growing popularity across various fields, attributed to its simplicity and flexibility in data representation. This format aligns with our objective to develop a simulation framework that is effective and adaptable to a wide range of V2X scenarios.

3) ADVANCEMENTS IN SIMULATION TECHNOLOGIES

Emerging trends in integrating simulation tools for V2X highlight the increasing use of Augmented Reality (AR) and Virtual Reality (VR) to enhance simulation environments. These technologies enable real-time visualization and interaction, creating more immersive and realistic testing scenarios. For instance, the Omniverse platform of NVIDIA allows users to experience high-fidelity virtual environments that mimic real-world conditions, facilitating the testing and development of V2X applications [136].

Additionally, the concept of metamobility, which connects future mobility systems with the metaverse, is gaining traction. This approach leverages technologies such as digital twins, edge AI, and immersive environments to provide comprehensive virtual testing grounds for V2X systems. Metamobility aims to create a frictionless, personalized mobility experience by integrating physical and digital spaces, which can significantly enhance the development and validation of V2X applications [137].

Moreover, the trend towards real-time data integration and multi-platform simulations is becoming more common. These trends enable simulation tools to utilize live data streams, creating dynamic and accurate simulations of current traffic conditions and operational scenarios. Integrating tools such as SUMO, OMNeT++, and Veins ensures the robust performance of V2X systems across different domains. The use of AI and machine learning in these simulations helps predict and respond to real-time conditions, enhancing the overall effectiveness of V2X applications.

B. SIMULATION TOOLS IN V2X CYBERSECURITY CONTEXT

1) TRENDS IN SIMULATION TOOLS: A YEAR-BY-YEAR ANALYSIS

Table 31 and Figure 9 show results combining tags for simulation tools and cybersecurity.

In this context, there are slight differences in the results, with a notable increase in the presence of CarMaker and Veins in the last three years in Table 31 compared to Table 26. It is also interesting that there is a decrease in SUMO usage and an increase in Veins and OMNeT++ in the last three years in Table 31 compared to Table 26. Observe that SUMO, NS3, OMNeT++, and Veins represent 75.9% of the total results in the last three years, indicating that they are the leading simulation tools in the context of V2X cybersecurity.Based on this previous information, the research was done year after year on these four simulation tools, shown in Tables 32-33 and Figures 10-11. All data was collected on January 1, 2024.

Table 32 and Figure 10 present the total results year-by-year in the Scopus database found for the leading simulation tools, while Table 33 and Figure 11 show the percentage numbers annually in relation to the total. Table 27 presents 1023 total results, adding the results in all years of all simulation tools. On the other hand, Table 32 shows 125 results for the same calculation; that is, 12.22% of simulation tool results in the context of V2X apply to the cybersecurity area. Regarding recent growth, Table 32 shows that in the last two years, NS3 has the highest percentage with 46.66% of the results in relation to its total, while Veins has the lowest with 31.82%.

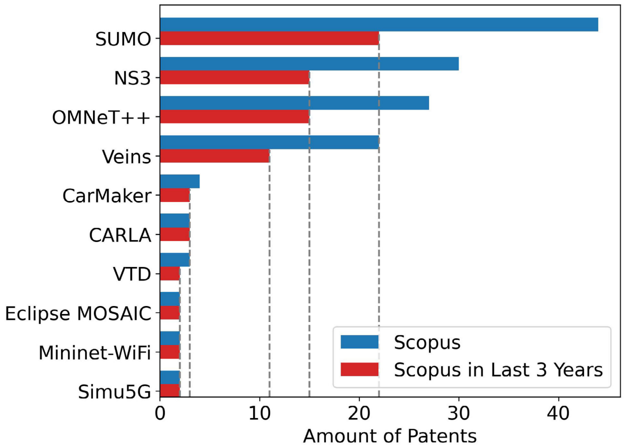


FIGURE 9. Reference numbers of the main V2X simulations found in security context in the Scopus database using the title, abstract, and keywords criteria.

To more comprehensively analyze trends in relation to cybersecurity in the V2X context, it is also interesting to analyze the case of the four most commonly encountered types of cyberattacks. To this end, research was carried out year after year on the attacks jamming, spoofing, DoS, and eavesdropping, presented in Tables 34-35 and Figures 12-13. All data was collected on January 1, 2024.

Table 34 shows that jamming is the most frequently found attack, while spoofing is the least found in papers that address simulation tools in the V2X context. Interestingly, although the total number of works on DoS is greater than eavesdropping, in recent years, more results have been found on eavesdropping than on DoS. This can be confirmed through Table 35 in which eavesdropping has 67.47% of the results in the last two years while DoS has only 47.13%. Note that spoofing also has the lowest percentage value of results in the last two years, with 39.13% results. On the other hand, jamming in the last two years had 51.79% of results, suggesting that jamming is and will most likely continue to be the most common attack to be found in scientific works on V2X cybersecurity.

2) SIMULATION TOOLS INTEGRATION IN V2X CYBERSECURITY CONTEXT

The integration of simulation tools in the context of V2X cybersecurity is a critical aspect of research and development, as it allows for comprehensive testing and validation of various security mechanisms in a controlled and reproducible

TABLE 31. Trends from the number of search results for simulation tools in V2X cybersecurity context on the Scopus database using the title, abstract, and keywords criteria.

Tags	Total History		Last 3 years	
	Scopus	%Scopus	Scopus	%Scopus
V2X[a] AND SEC[c] AND "SUMO"	44	27.50	22	26.51
V2X[a] AND SEC[c] AND ("NS3" OR "NS-3")	30	18.75	15	18.07
V2X[a] AND SEC[c] AND "OMNeT++"	27	16.88	15	18.07
V2X[a] AND SEC[c] AND "Veins"	22	13.75	11	13.25
V2X[a] AND SEC[c] AND "CarMaker"	4	02.50	3	03.61
V2X[a] AND SEC[c] AND "CARLA"	3	01.88	3	03.61
V2X[a] AND SEC[c] AND ("Virtual Test Drive" OR "VTD")	3	01.88	2	02.41
V2X[a] AND SEC[c] AND "Eclipse MOSAIC"	2	01.25	2	02.41
V2X[a] AND SEC[c] AND "Mininet-WiFi"	2	01.25	2	02.41
V2X[a] AND SEC[c] AND "Simu5G"	2	01.25	2	02.41
V2X[a] AND SEC[c] AND "CarSim"	4	02.50	1	01.20
V2X[a] AND SEC[c] AND "Ventos"	4	02.50	1	01.20
V2X[a] AND SEC[c] AND "PreScan"	3	01.88	1	01.20
V2X[a] AND SEC[c] AND "Artery"	1	00.63	1	01.20
V2X[a] AND SEC[c] AND "Flowsim"	1	00.63	1	01.20
V2X[a] AND SEC[c] AND "PLEXE"	1	00.63	1	01.20
V2X[a] AND SEC[c] AND "GloMoSim"	3	01.88	0	00.00
V2X[a] AND SEC[c] AND "Containernet"	1	00.63	0	00.00
V2X[a] AND SEC[c] AND "OPNET"	1	00.63	0	00.00
V2X[a] AND SEC[c] AND "Vanetza"	1	00.63	0	00.00
V2X[a] AND SEC[c] AND "VSimRTI"	1	00.63	0	00.00
Total	**160**	**100.00**	**83**	**100.00**

TABLE 32. Total number of results in searches for leading simulation tools in the V2X cybersecurity context separated year by year in the Scopus database using "title, abstract or keyword" criteria.

Year	V2X[a] AND SEC[c] AND "SUMO"	V2X[a] AND SEC[c] AND ("NS3" OR "NS-3")	V2X[a] AND SEC[c] AND "OMNeT++"	V2X[a] AND SEC[c] AND "Veins"
2023	9	7	8	0
2022	10	7	4	7
2021	3	1	3	4
2020	7	2	5	4
2019	6	5	3	4
2018	2	3	3	1
2017	3	3	1	1
2016	3	1	1	0
2015	0	0	0	1
2014	1	1	1	0
Total	**44**	**30**	**29**	**22**

TABLE 33. Percentage numbers of results in searches for leading simulation tools in the V2X cybersecurity context separated year by year in the Scopus database using "title, abstract or keyword" criteria.

Year	V2X[a] AND SEC[c] AND "SUMO"	V2X[a] AND SEC[c] AND ("NS3" OR "NS-3")	V2X[a] AND SEC[c] AND "OMNeT++"	V2X[a] AND SEC[c] AND "Veins"
2023	20.45	23.33	27.59	00.00
2022	22.73	23.33	13.79	31.82
2021	06.82	03.33	10.34	18.18
2020	15.91	06.67	17.24	18.18
2019	13.64	16.67	10.34	18.18
2018	04.55	10.00	10.34	04.55
2017	06.82	10.00	03.45	04.55
2016	06.82	03.33	03.45	00.00
2015	00.00	00.00	00.00	04.55
2014	02.27	03.33	03.45	00.00
Total	**100.00**	**100.00**	**100.00**	**100.00**

environment. Table 36 highlights several works that have employed integrated simulation tools to address cybersecurity challenges in V2X systems.

From the Table 36, it is evident that certain combinations of simulation tools are frequently used. The most common integration involves using SUMO, OMNeT++, and Veins.

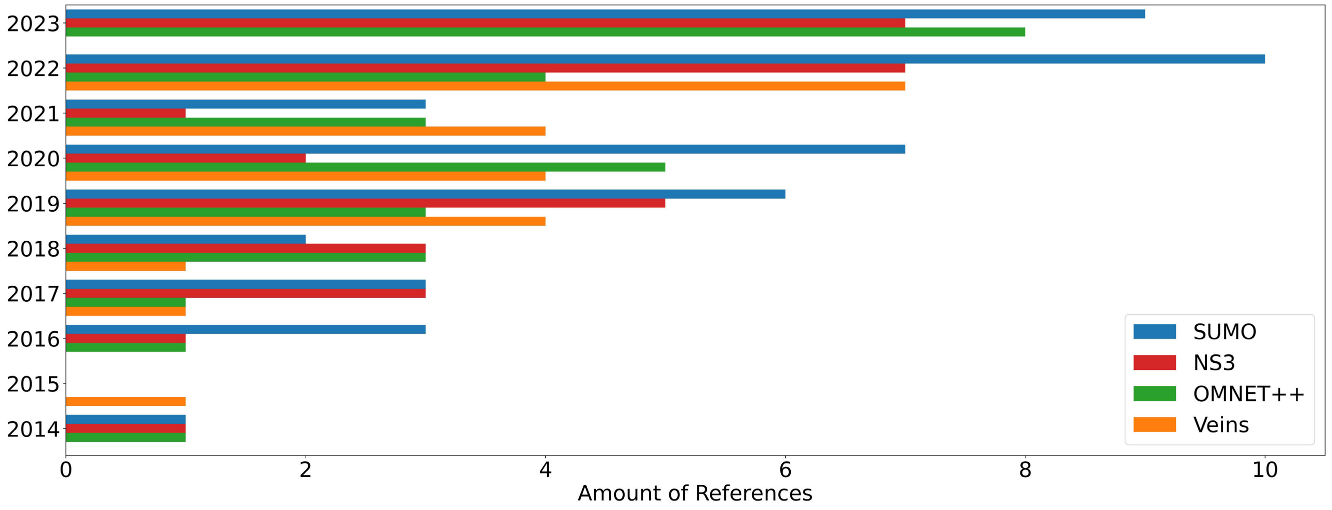


FIGURE 10. **Total number of results in searches year by year for leading simulation tools in the V2X cybersecurity context in the Scopus database using "title, abstract or keyword" criteria.**

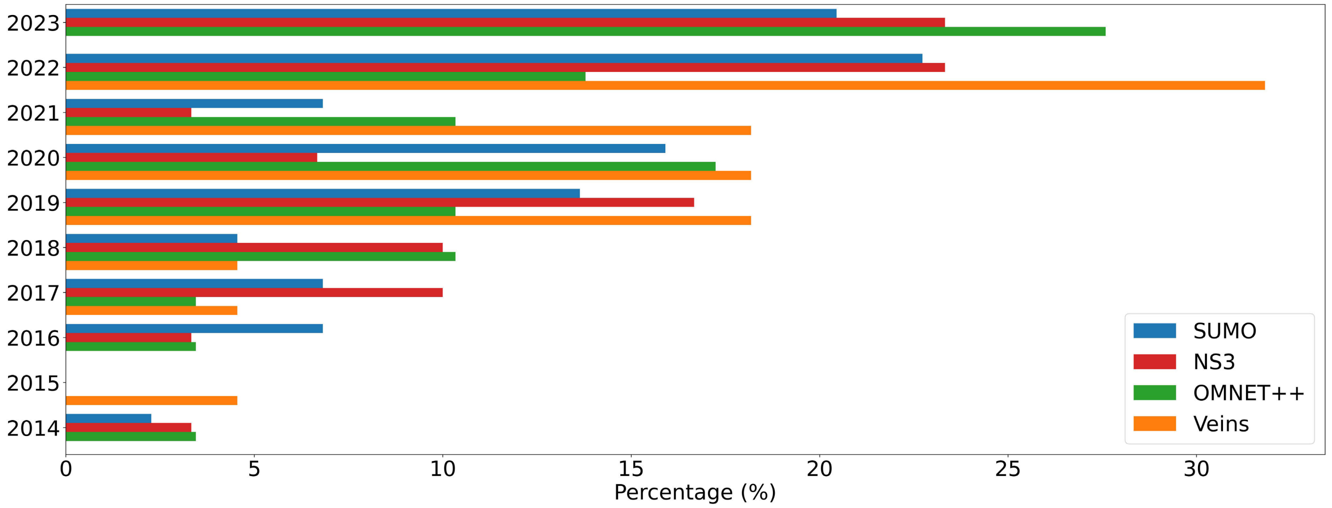


FIGURE 11. **Percentage numbers of results in searches year by year for leading simulation tools in the V2X cybersecurity context in the Scopus database using "title, abstract or keyword" criteria.**

This combination is prevalent because each tool offers complementary capabilities essential for V2X cybersecurity research:

1) SUMO: Provides realistic traffic scenarios and mobility models. In the context of cybersecurity, realistic traffic data is crucial for testing how cyber-attacks might impact the flow of vehicles and the overall traffic dynamics.

2) OMNeT++: Facilitates network simulation, allowing for the modeling of communication protocols. Cybersecurity in V2X relies heavily on the robustness of communication protocols. OMNeT++ allows researchers to simulate how these protocols behave under various attack scenarios, such as denial-of-service (DoS) attacks, spoofing, or eavesdropping. This is essential for developing and testing secure communication strategies.

3) Veins: Acts as a bridge between SUMO and OMNeT++, enabling the simulation of vehicular networks. It is designed specifically for vehicular network simulations, integrating the mobility models from SUMO with the communication models from OMNeT++. This integration is vital for cybersecurity research, as it allows for a detailed analysis of how cyber-attacks on the network layer can affect vehicular mobility and vice versa.

Additionally, tools such as CARLA and INET are also integrated into these simulations. CARLA offers high-fidelity simulation environments for autonomous driving. In the context of V2X cybersecurity, CARLA allows for the simulation of complex driving scenarios and the testing of autonomous vehicle responses to cyber-attacks. INET provides an extensive framework for wireless network simulation within

TABLE 34. Total number of results in searches for V2X cyberattacks in the simulations context separated year by year in the Scopus database using "title, abstract or keyword" criteria.

Year	V2X[a] AND SIM[b] AND "jamming"	V2X[a] AND SIM[b] AND ("Denial of Service" OR "DoS")	V2X[a] AND SIM[b] AND "eavesdropping"	V2X[a] AND SIM[b] AND "spoofing"
2023	31	24	31	6
2022	27	17	25	3
2021	11	9	10	3
2020	9	8	1	2
2019	10	7	6	2
2018	13	6	7	3
2017	3	5	1	1
2016	2	3	1	1
2015	2	2	0	1
2014	0	1	0	0
2013	1	2	1	0
2012	1	1	0	0
2011	0	0	0	1
2010	0	1	0	0
2008	1	1	0	0
2007	1	0	0	0
Total	**112**	**87**	**83**	**23**

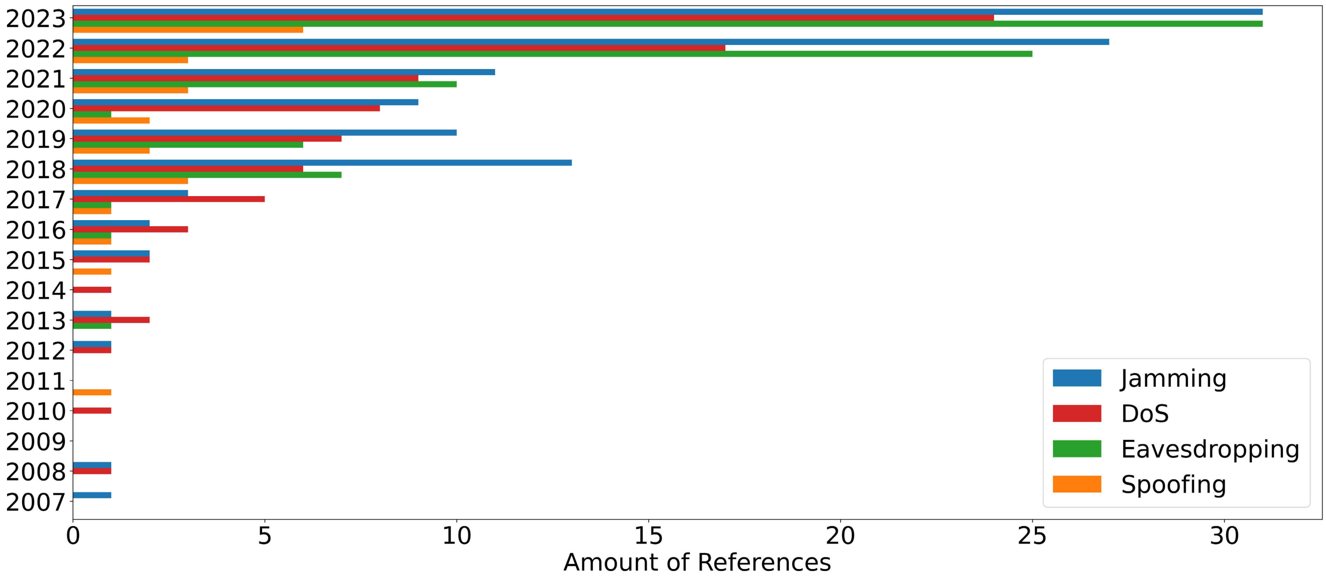


FIGURE 12. Total number of results in searches year by year for V2X cyberattacks in the simulations context in the Scopus database using "title, abstract or keyword" criteria.

OMNeT++. INET enhances OMNeT++ by adding models for various network protocols and technologies, including those used in V2X communications. This is crucial for cybersecurity research, as it enables the simulation of attacks on different layers of the communication stack and the development of countermeasures.

The integration of simulation tools such as SUMO, OMNeT++, Veins, CARLA, and INET in V2X cybersecurity research reflects the necessity for comprehensive, realistic, and flexible simulation environments. These integrations facilitate the development and validation of robust cybersecurity measures, ensuring the reliability and security of future V2X systems. As the field progresses, we can expect to see continued innovation and refinement in the use of these integrated tools, driven by the evolving and challenging requirements of V2X cybersecurity.

VI. FUTURE WORKS

Several areas for future research are proposed. Firstly, integrating diverse simulation tools is an essential area of study. Such integration aims to foster a rich, multifaceted environment capable of simulating complex scenarios with greater real-world accuracy, offering invaluable insights into developing and optimizing V2X systems.

Secondly, advancing AI within the V2X context opens a realm of opportunities. Future research should center on developing AI algorithms that enhance autonomous decision-making capabilities, traffic management, and accident prevention, exploiting the burgeoning potential of 6G technology [138]. Deep learning techniques, in particular, could revolutionize ITS systems by predicting and mitigating real-time security threats, optimizing routes, and managing traffic in densely populated urban settings.

TABLE 35. Percentage numbers of results in searches for V2X cyberattacks in the simulations context separated year by year in the Scopus database using "title, abstract or keyword" criteria.

Year	V2X[a] AND SIM[b] AND "jamming"	V2X[a] AND SIM[b] AND ("Denial of Service" OR "DoS")	V2X[a] AND SIM[b] AND "eavesdropping"	V2X[a] AND SIM[b] AND "spoofing"
2023	27.68	27.59	37.35	26.09
2022	24.11	19.54	30.12	13.04
2021	09.82	10.34	12.05	13.04
2020	08.04	09.20	01.20	08.70
2019	08.93	08.05	07.23	08.70
2018	11.61	06.90	08.43	13.04
2017	02.68	05.75	01.20	04.35
2016	01.79	03.45	01.20	04.35
2015	01.79	02.30	00.00	04.35
2014	00.00	01.15	00.00	00.00
2013	00.89	02.30	01.20	00.00
2012	00.89	01.15	00.00	00.00
2011	00.00	00.00	00.00	04.35
2010	00.00	01.15	00.00	00.00
2008	00.89	01.15	00.00	00.00
2007	00.89	00.00	00.00	00.00
Total	**100.00**	**100.00**	**100.00**	**100.00**

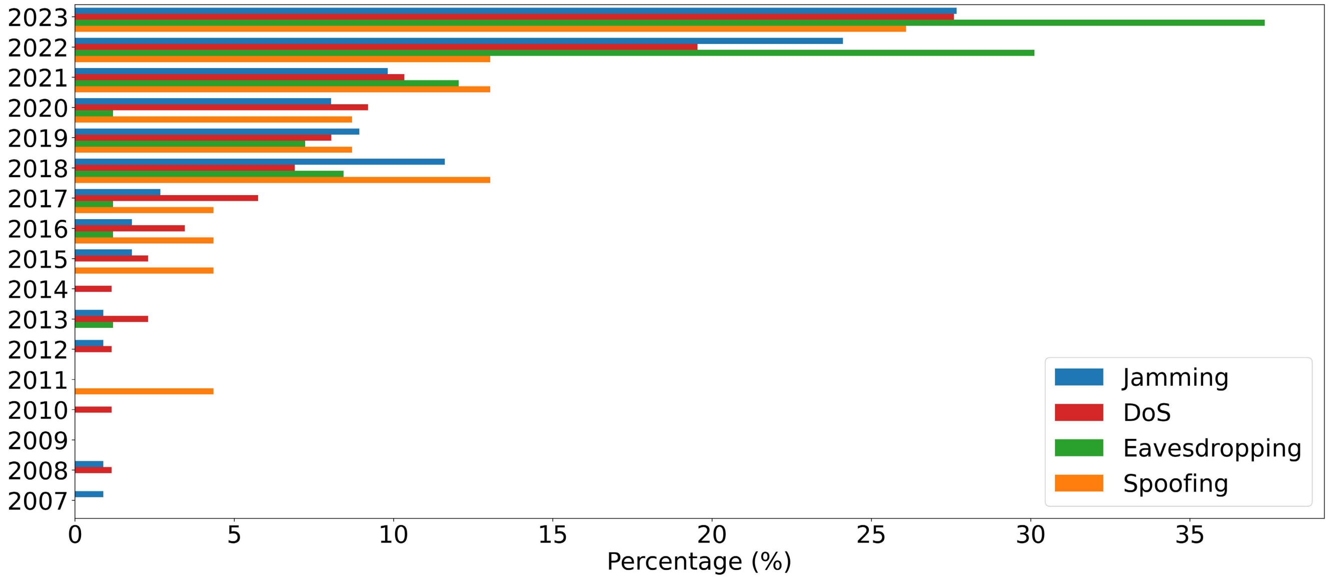


FIGURE 13. Percentage numbers of results in searches year by year for V2X cyberattacks in the simulations context in the Scopus database using "title, abstract or keyword" criteria.

TABLE 36. Cases of integration of simulation tools in V2X cybersecurity context.

Work	Simulation Tools
[92]	SUMO, OMNeT++, and CARLA
[94]	SUMO, OMNeT++, Veins, and INET
[95]	SUMO, OMNeT++, Veins, and INET
[101]	SUMO, OMNeT++, and Veins
[117]	SUMO and Veins
[134]	SUMO, OMNeT++, and Ventos

One promising direction is implementing and exploring Digital Twins in the V2X context. Digital Twins create dynamic, real-time digital replicas of physical entities, significantly enhancing the modeling, testing, and optimization of V2X systems. For example, a comprehensive Digital Twin framework that integrates connected vehicles and pedestrian interactions using co-simulation platforms such as Carla and Sumo has been proposed, allowing real-time replication of physical states and behaviors in a robust environment for testing V2X applications under varied and realistic conditions [139].

Furthermore, advancements in Digital Twin technology have been demonstrated to provide comprehensive virtual testing grounds for V2X systems. These advancements incorporate real-time data streams and AI-driven analytics to enhance the accuracy and reliability of these simulations. This is critical for developing accurate perception systems for autonomous vehicles, which play a crucial role in maintaining system integrity under cyber threats and adverse conditions [140].

For example, a proposed framework in Figure 14 for integrating simulation tools in the V2X context offers a comprehensive approach to enhancing V2X systems through the use of Digital Twins [141]. This framework, with its key components such as *traffic simulators*, *communication network simulators*, and *autonomous vehicle simulators*, all integrated with *local and global Digital Twins*, provides a robust and all-encompassing environment for testing V2X applications. The *Traffic Simulator* sets up realistic traffic scenarios, feeding data into the *Autonomous Vehicles Simulator* and *Local Digital Twin*, which model vehicle behaviors in real time. The *Communication Network Simulator*, divided into *User Plane* and *Control Plane*, ensures robust analysis of network interactions and protocol performance. The *Global Digital Twin* aggregates data from these simulations to provide a holistic system view, essential for comprehensive testing and optimization. Additionally, integrating the framework with *ITS Applications* and *FOG/MEC* infrastructures facilitates low latency, real-time data processing, and enhancing traffic management and safety.

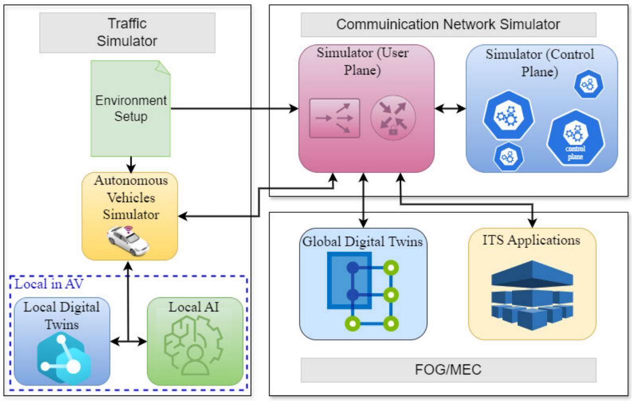


FIGURE 14. **Proposed framework for integrating simulation tools in the V2X context [141].**

Figure 15 illustrates a scenario where a vehicle receiver has two direct line-of-sight (LOS) connections. In these LOS connections, the communication between transmitted signals from the transmitters to the receiver is not significantly obstructed by obstacles. In contrast, with connections where obstacles block the line of sight, reflections occur due to these barriers, leading to more complex signal propagation. These received signals can be mapped into a power histogram, which displays the peak powers and directions of the reception angles. It is noted that there is direct communication between the vehicles, and the vehicle on the far right does not have a view of the jammer. However, with an appropriate mitigation method, vehicles can exchange information and identify the jammer, subsequently applying techniques to neutralize its effect.

Addressing cybersecurity, Figure 16 presents a generalized framework based on the invention, composed of three main blocks. The first block is responsible for monitoring the communication channel. In this context, various characteristics of the received signal are analyzed to identify anomalies, such as jammer or spoofer attacks. Various techniques and configurations can be employed in the process of signal characteristic analysis, including AI and Direction of Arrival (DoA) estimation to determine the physical position of the transmitter. The goal is to identify any abnormality in the received signal that may indicate the presence of an attacker. A decision module exists to identify the presence of anomalies in the received signal, analyze possible false positives, and, through mathematical techniques and models, decide on the presence of an attacker. If an anomaly is detected, the system proceeds to the next block.

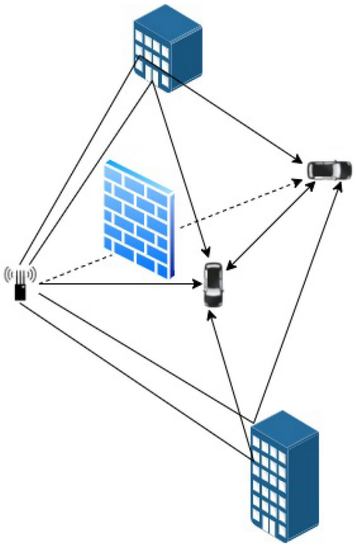


FIGURE 15. **The arrangement is with a jammer and two motor vehicles, both receiving different reflections of the signal transmitted by the jammer [141].**

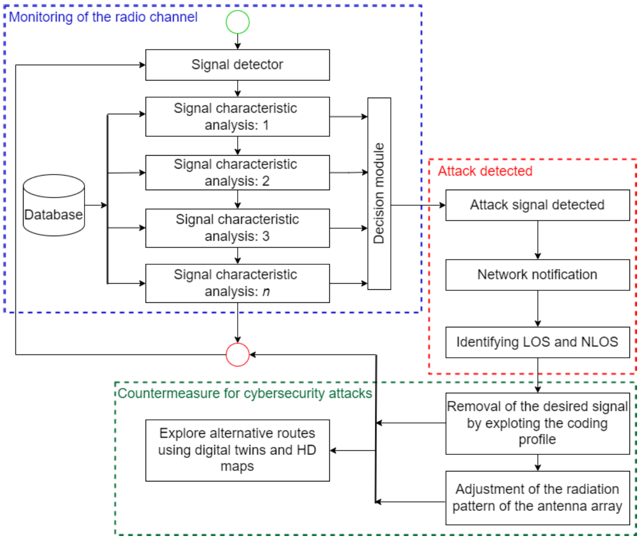

Monitoring of the radio channel
Signal detector
Signal characteristic analysis: 1
Signal characteristic analysis: 2
Signal characteristic analysis: 3
Signal characteristic analysis: n
Database
Decision module
Attack detected
Attack signal detected
Network notification
Identifying LOS and NLOS
Countermeasure for cybersecurity attacks
Explore alternative routes using digital twins and HD maps
Removal of the desired signal by exploiting the coding profile
Adjustment of the radiation pattern of the antenna array

FIGURE 16. **Generalized framework for detecting and mitigating cyber attacks in V2X communication, including monitoring, notification, and countermeasure blocks [141].**

The second block is responsible for notifying the network of the anomaly presence. A notification is sent to all network users informing them of the attack detection. Then, LOS and non-line-of-sight (NLOS) paths are identified using histograms or DoA methods. Tools such as histogram techniques and DoA methods can be used to identify LOS and NLOS paths.

The third block implements actions to mitigate the effects of the identified attack. First, exploiting the coding profile identified in the monitoring block removes the signal of the attacker. The radiation pattern can be adjusted to nullify the signal of the interferer using an antenna array. Additionally, executing Digital Twins is performed to identify paths or routes where the interferer is absent, ensuring secure communication even in changing conditions.

This setup underscores the potential of Digital Twins not only to improve the accuracy and reliability of V2X simulations significantly but also to drive future research directions. By leveraging the capabilities of Digital Twins, future research can develop more sophisticated simulation environments, ensuring V2X systems remain secure, efficient, and adaptive to changing conditions. This potential of Digital Twins to drive future research directions is a crucial aspect, as it will drive forward the capabilities of V2X systems, making them more robust, intelligent, and resilient to future challenges.

VII. CONCLUSION

This survey has highlighted the role of simulation tools in the development and security assurance of V2X systems. By examining various simulation tools, we have revealed the wide range of resources available for thorough modeling, testing, and enhancement of V2X networks.

A global analysis, grounded in recent publications and patents, has illuminated the growth in V2X research and innovation, with search string analytics underscoring the increasing scholarly interest in this field. This indicates an expanding community of researchers dedicated to advancing the technology, emphasizing the pressing need for advanced simulations capable of accurately modeling and mitigating threats such as jamming and spoofing attacks. These advancements are crucial for developing secure and trustworthy V2X systems. The introduction of an integrated simulation framework addresses these challenges, offering a comprehensive approach for future investigations in V2X technology. As the integration of 5G and Beyond 5G (B5G) technologies unfolds, the potential for V2X communication expands, necessitating ongoing research to leverage these advances while thoroughly ensuring system security.

For example, significant advances have been made in sensor integration techniques, notably in the fusion of raw data from LiDAR and camera sensors. As discussed in [142], these advancements play a crucial role in enhancing the accuracy and reliability of perception systems in autonomous vehicles. This is important for maintaining system integrity under cyber threats, as the enhanced sensor data fusion facilitates better detection and response capabilities under adverse conditions.

Overall, this paper has also identified several emerging trends in the integration of simulation tools, highlighting the increasing use of AR and VR to enhance simulation environments. These trends reflect the importance of innovative

TABLE 37. List of abbreviations.

Abbreviations	Definition
3GPP	Third Generation Partnership Project
5G	Fifth-Generation
6G	Sixth-Generation
ADAS	Advanced Driver Assistance Systems
AI	Artificial Intelligence
AR	Augmented Reality
AWGN	Additive White Gaussian Noise
B5G	Beyond 5G
C-V2X	Cellular Vehicle-to-Everything
CARLA	Car Learning to Act
CSS	Cascading Style Sheets
DDoS	Distributed Denial of Service
DFKI	Deutsches Forschungszentrum für Künstliche Intelligenz
DoA	Direction of Arrival
DoS	Denial of Service
FAP	Femtocells/Femto Access Points
FSPL	Free Space Path Loss
GEO	Geosynchronous Earth Orbit
HTML	HyperText Markup Language
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronic Engineers
ITS	Intelligent Transportation Systems
JSON	JavaScript Object Notation
LEO	Low Earth Orbit
LiDAR	Light Detection and Ranging
LOS	line-of-sight
LTE	Long-Term Evolution
MBS	Macro Base Stations
MIMO	Multiple Input, Multiple Output
NLOS	Non-Line-of-Sight
NS3	Network Simulator 3
OBUs	On-Board Units
OMNeT++	Objective Modular Network Testbed in C++
R&D	Research and Development
RF	Radio Frequency
RSUs	Road Side Units
SDN	Software-Defined Networking
SIRN	signal-to-interference-plus-noise ratio
SISO	Single Input, Single Output
SNR	Signal-to-noise ratio
SUMO	Simulation of Urban MObility
TÜV	Technischer Uberwachungsverein
UAV	Unmanned Aerial Vehicle
UE	User Equipment
URPA	Uniform Rectangular Planar Array Antenna
USRP	Universal Software Radio Peripheral
V2C	Vehicle-to-Cloud
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
Veins	Vehicles in Network Simulation
VR	Virtual Reality
VRU	Vulnerable Road Users
WAVE	Wireless Access in Vehicular Environments
XML	Extensible Markup Language

approaches to simulation and security in advancing V2X technology.

APPENDIX

See Tables 37, 38.

TABLE 38. Tag used in the search and full name of company.

	Tag	Company Name
1	Qualcomm	Qualcomm Incorporated
2	Toyota	Toyota Motor Corporation
3	Intel	Intel Corporation
4	Ford	Ford Motor Company
5	Apple	Apple Inc.
6	NVIDIA	NVIDIA Corporation
7	LG	LG Electronics Inc.
7	Huawei	Huawei Technologies Co., Ltd.
9	GM	General Motors Company
10	Nissan	Nissan Motor Co., Ltd.
11	Honda	Honda Motor Co., Ltd.
12	Sony	Sony Corporation
13	Denso	Denso Corporation
14	AMD	Advanced Micro Devices, Inc.
15	Bosch	Robert Bosch GmbH
16	Ericsson	Telefonaktiebolaget LM Ericsson
17	Hitachi	Hitachi, Ltd.
18	Texas	Texas Instruments Incorporated
19	Samsung	Samsung Electronics Co., Ltd.
20	Tesla	Tesla, Inc.
21	InterDigital	InterDigital, Inc.
22	Mitsubishi	Mitsubishi Electric Corporation
23	Spoke	Spoke Safety
24	Hyundai	Hyundai Motor Company
25	Siemens	Siemens AG
26	Mercedes	Mercedes-Benz Group AG
27	Audi	Audi AG
28	Volkswagen	Volkswagen AG
29	Ofinno	Ofinno, LLC
30	Micron	Micron Technology, Inc.
31	Nokia	Nokia Corporation
32	Analog	Analog Devices, Inc.
33	Panasonic	Panasonic Corporation
34	BMW	Bayerische Motoren Werke AG
35	Philips	Koninklijke Philips N.V.
36	Alphabet	Alphabet Inc.
37	Geely	Geely Automobile Holdings Limited
38	BYD	BYD Company Limited
39	Motional	Motional AD Inc.
40	DOCOMO	NTT DOCOMO, Inc.
41	ZTE	ZTE Corporation
42	Autoliv	Autoliv Inc.
43	Oppo	Guangdong Oppo Mobile Telecommunications Corp., Ltd.
44	Comcast	Comcast Corporation
45	DSpace	dSPACE GmbH
46	Skyworks	Skyworks Solutions, Inc.
47	Aptiv	Aptiv PLC
48	Faurecia	Faurecia S.A.
49	ZF	ZF Friedrichshafen AG
50	Blackberry	BlackBerry Limited

ACKNOWLEDGMENT

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

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

REFERENCES

[1] 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.

[2] 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.

[3] M. 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.

[4] 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.

[5] K. H. M. Gularte, J. A. R. Vargas, J. P. J. da Costa, A. S. D. Silva, G. A. Santos, Y. Wang, C. A. Müller, C. Lipps, R. T. de Sousa Júnior, W. de Britto Vidal Filho, P. Slusallek, and H. D. Schotten, "Safeguarding the V2X pathways: Exploring the cybersecurity landscape through systematic review," *IEEE Access*, vol. 12, pp. 72871–72895, 2024, doi: 10.1109/ACCESS.2024.3402946.

[6] 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.

[7] 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.

[8] 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. Surveys*, vol. 55, no. 9, pp. 1–36, Jan. 2023, doi: 10.1145/3558052.

[9] 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.

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

[11] 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.

[12] L. M. Maller, P. Suskovics, and L. Bokor, "Edge computing in the loop simulation framework for automotive use cases evaluation," *Wireless Netw.*, vol. 29, no. 8, pp. 3717–3735, Jul. 2023, doi: 10.1007/s11276-023-03432-3.

[13] R. Teng and K. Sato, "A fundamental study of reliable vehicle-to-cloud communication using multiple paths with redundancy mitigation," *Appl. Sci.*, vol. 14, no. 7, p. 2841, Mar. 2024, doi: 10.3390/app14072841.

[14] T. Petrov, P. Pocta, and T. Kovacikova, "Benchmarking 4G and 5G-based cellular-V2X for vehicle-to-infrastructure communication and urban scenarios in cooperative intelligent transportation systems," *Appl. Sci.*, vol. 12, no. 19, p. 9677, Sep. 2022, doi: 10.3390/app12199677.

[15] 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.

[16] 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.

[17] 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.

[18] J. J. Jaime-Rodríguez, C. A. Gómez-Vega, C. A. Gutiérrez, J. M. Luna-Rivera, D. U. Campos-Delgado, and R. Velázquez, "A non-WSSUS channel simulator for V2X communication systems," *Electronics*, vol. 9, no. 8, p. 1190, Jul. 2020, doi: 10.3390/electronics9081190.

[19] A. Dosovitskiy, G. Ros, F. Codevilla, A. Lopez, and V. Koltun, "CARLA: An open urban driving simulator," in *Proc. 1st Annu. Conf. Robot Learn.* Mountain View, CA, USA: PMLR, Oct. 2017, pp. 1–16. [Online]. Available: https://proceedings.mlr.press/v78/dosovitskiy17a.html

[20] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," in *Proc. 1st Int. ICST Conf. Simulation Tools Techn. Commun., Netw. Syst.*, Rio de Janeiro, Brazil, Mar. 2008, pp. 1–10. Accessed: Aug. 2024. [Online]. Available: https://dl.acm.org/doi/abs/10.5555/1416222.1416290

[21] G. Nardini, D. Sabella, G. Stea, P. Thakkar, and A. Virdis, "Simu5G—An OMNeT++ library for end-to-end performance evaluation of 5G networks," *IEEE Access*, vol. 8, pp. 181176–181191, 2020, doi: 10.1109/ACCESS.2020.3028550.

[22] P. A. Lopez, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y.-P. Flötteröd, R. Hilbrich, L. Lücken, J. Rummel, P. Wagner, and E. Wießner, "Microscopic traffic simulation using sumo," in *Proc. 21st Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2018, pp. 2575–2582, doi: 10.1109/ITSC.2018.8569938.

[23] C. Storck and F. Duarte-Figueiredo, "A 5G V2X ecosystem providing Internet of Vehicles," *Sensors*, vol. 19, no. 3, p. 550, Jan. 2019, doi: 10.3390/s19030550.

[24] R. Riebl, H.-J. Günther, C. Facchi, and L. Wolf, "Artery: Extending veins for VANET applications," in *Proc. Int. Conf. Models Technol. Intell. Transp. Syst. (MT-ITS)*. Budapest, Hungary: IEEE, Jun. 2015, pp. 450–456, doi: 10.1109/MTITS.2015.7223293.

[25] Mechanical Simulation Corporation. (2023). *Carsim*. Accessed: Jun. 2024. [Online]. Available: https://www.carsim.com/

[26] C. Sommer, Z. Yao, R. German, and F. Dressler, "On the need for bidirectional coupling of road traffic microsimulation and network simulation," in *Proc. 1st ACM SIGMOBILE workshop Mobility models*, May 2008, pp. 41–48, doi: 10.1145/1374688.1374697.

[27] NS-3 Consortium. (2023). *Ns-3*. Accessed: Jun. 2024. [Online]. Available: https://www.nsnam.org/releases/older/

[28] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO–simulation of urban mobility: An overview," in *Proc. 3rd Int. Conf. Adv. Syst. Simulation (SIMUL)*, Oct. 2011, pp. 1–6. Accessed: Aug. 2024. [Online]. Available: https://elib.dlr.de/71460/

[29] G. A. Santos, J. P. J. da Costa, and A. A. S. da Silva, "Towards to beyond 5G virtual environment for cybersecurity testing in V2X systems," in *Proc. Workshop Commun. Netw. Power Syst. (WCNPS)*. Brasília, Brazil: IEEE, 2023, pp. 1–7, doi: 10.1109/WCNPS60622.2023.10344440.

[30] Eight360. *Eight360—NOVA Untethered Motion Simulator*. Accessed: Jun. 2024. [Online]. Available: https://www.eight360.com/

[31] M. Ghafarian, M. Watson, N. Mohajer, D. Nahavandi, P. M. Kebria, and S. Mohamed, "A review of dynamic vehicular motion simulators: Systems and algorithms," *IEEE Access*, vol. 11, pp. 36331–36348, 2023, doi: 10.1109/ACCESS.2023.3265999.

[32] F. J. Ros, J. A. Martinez, and P. M. Ruiz, "A survey on modeling and simulation of vehicular networks: Communications, mobility, and tools," *Comput. Commun.*, vol. 43, pp. 1–15, May 2014, doi: 10.1016/j.comcom.2014.01.010.

[33] 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.

[34] H. Mosavat-Jahromi, Y. Li, L. Cai, and L. Lu, "NC–MAC: A distributed MAC protocol for reliable beacon broadcasting in V2X," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 6044–6057, Jun. 2021, doi: 10.1109/TVT.2021.3077877.

[35] J. J. Gonzalez-Delicado, J. Gozalvez, J. Mena-Oreja, M. Sepulcre, and B. Coll-Perales, "Alicante-Murcia freeway scenario: A high-accuracy and large-scale traffic simulation scenario generated using a novel traffic demand calibration method in SUMO," *IEEE Access*, vol. 9, pp. 154423–154434, 2021, doi: 10.1109/ACCESS.2021.3126269.

[36] L. Campanile, M. Gribaudo, M. Iacono, F. Marulli, and M. Mastroianni, "Computer network simulation with ns-3: A systematic literature review," *Electronics*, vol. 9, no. 2, p. 272, Feb. 2020, doi: 10.3390/electronics9020272.

[37] M. S. Bahbahani, E. Alsusa, and A. Hammadi, "A directional TDMA protocol for high throughput URLLC in mmWave vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 3, pp. 3584–3599, Mar. 2023, doi: 10.1109/TVT.2022.3219771.

[38] J. S. Weber, M. Neves, and T. Ferreto, "VANET simulators: An updated review," *J. Brazilian Comput. Soc.*, vol. 27, no. 1, pp. 1–31, May 2021, doi: 10.1186/s13173-021-00113-x.

[39] G. A. Kovács and L. Bokor, "Implementation of MEC-assisted collective perception in an integrated Artery/Simu5G simulation framework," *Sensors*, vol. 23, no. 18, p. 7968, Sep. 2023, doi: 10.3390/s23187968.

[40] G. Luo, C. Shao, N. Cheng, H. Zhou, H. Zhang, Q. Yuan, and J. Li, "EdgeCooper: Network-aware cooperative LiDAR perception for enhanced vehicular awareness," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 1, pp. 207–222, Jan. 2024, doi: 10.1109/JSAC.2023.3322764.

[41] 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.

[42] 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.

[43] 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.

[44] A. Wippelhauser, A. Edelmayer, and L. Bokor, "A declarative application framework for evaluating advanced V2X-based ADAS solutions," *Appl. Sci.*, vol. 13, no. 3, p. 1392, Jan. 2023, doi: 10.3390/app13031392.

[45] O. Váczi and L. Bokor, "Modeling and evaluation of a dynamic channel selection framework for multi-channel operation in ITS-G5," *Telecom*, vol. 4, no. 2, pp. 313–333, Jun. 2023, doi: 10.3390/telecom4020019.

[46] V. Cislaghi, C. Quadri, V. Mancuso, and M. A. Marsan, "Simulation of tele-operated driving over 5G using CARLA and OMNeT++," in *Proc. IEEE Veh. Netw. Conf. (VNC)*. Istanbul, Turkiye: IEEE, Apr. 2023, pp. 81–88, doi: 10.1109/vnc57357.2023.10136340.

[47] A. N. Ahmed, I. Ravijts, J. de Hoog, A. Anwar, S. Mercelis, and P. Hellinckx, "A joint perception scheme for connected vehicles," in *Proc. IEEE Sensors*. Dallas, TX, USA: IEEE, Oct./Nov. 2022, pp. 1–4, doi: 10.1109/SENSORS52175.2022.9967271.

[48] M. Shan, K. Narula, S. Worrall, Y. F. Wong, J. S. B. Perez, P. Gray, and E. Nebot, "A novel probabilistic V2X data fusion framework for cooperative perception," in *Proc. IEEE 25th Int. Conf. Intell. Transp. Syst. (ITSC)*. Macau, China: IEEE, Oct. 2022, pp. 2013–2020, doi: 10.1109/ITSC55140.2022.9922251.

[49] M. Hussain and J.-E. Hong, "Enforcing safety in cooperative perception of autonomous driving systems through logistic chaos map-based end-to-end encryption," in *Proc. 16th Int. Conf. Open Source Syst. Technol. (ICOSST)*, Dec. 2022, pp. 1–6, doi: 10.1109/ICOSST57195.2022.10016879.

[50] J. Li, R. Xu, X. Liu, J. Ma, Z. Chi, J. Ma, and H. Yu, "Learning for vehicle-to-vehicle cooperative perception under lossy communication," *IEEE Trans. Intell. Vehicles*, vol. 8, no. 4, pp. 2650–2660, Apr. 2023, doi: 10.1109/TIV.2023.3260040.

[51] R. Xu, Y. Guo, X. Han, X. Xia, H. Xiang, and J. Ma, "OpenCDA: An open cooperative driving automation framework integrated with co-simulation," in *Proc. IEEE Int. Intell. Transp. Syst. Conf. (ITSC)*. Indianapolis, IN, USA: IEEE, Sep. 2021, pp. 1155–1162, doi: 10.1109/ITSC48978.2021.9564825.

[52] R. Xu, H. Xiang, X. Xia, X. Han, J. Li, and J. Ma, "Opv2v: An open benchmark dataset and fusion pipeline for perception with vehicle-to-vehicle communication," in *Proc. Int. Conf. Robot. Autom. (ICRA)*, May 2022, pp. 2583–2589, doi: 10.1109/ICRA46639.2022.9812038.

[53] M. Shan, K. Narula, Y. F. Wong, S. Worrall, M. Khan, P. Alexander, and E. Nebot, "Demonstrations of cooperative perception: Safety and robustness in connected and automated vehicle operations," *Sensors*, vol. 21, no. 1, p. 200, Dec. 2020, doi: 10.3390/s21010200.

[54] F. Hawlader and R. Frank, "Towards a framework to evaluate cooperative perception for connected vehicles," in *Proc. IEEE Veh. Netw. Conf. (VNC)*. Ulm, Germany: IEEE, Nov. 2021, pp. 36–39, doi: 10.1109/VNC52810.2021.9644667.

[55] W. Yi, F. Ma, B. Rao, X. Yu, G. Tan, and S. Zhou, "A HIL platform for evaluating OBU performance in C-V2X scenarios," in *Proc. Int. Conf. Intell. Traffic Syst. Smart City (ITSSC)*. Zhengzhou, China: SPIE, Mar. 2022, p. 17, doi: 10.1117/12.2627784.

[56] C. Ayimba, V. Cislaghi, C. Quadri, P. Casari, and V. Mancuso, "Copy-CAV: V2X-enabled wireless towing for emergency transport," *Comput. Commun.*, vol. 205, pp. 87–96, May 2023, doi: 10.1016/j.comcom.2023.04.009.

[57] R. Dos Reis Fontes, C. Campolo, C. Esteve Rothenberg, and A. Molinaro, "From theory to experimental evaluation: Resource management in software-defined vehicular networks," *IEEE Access*, vol. 5, pp. 3069–3076, 2017, doi: 10.1109/ACCESS.2017.2671030.

[58] R. Singh, L. Mendiboure, J. Soler, M. S. Berger, T. Sylla, M. Berbineau, and L. Dittmann, "SDN-based secure common emergency service for railway and road co-existence scenarios," *Future Internet*, vol. 16, no. 4, p. 122, Apr. 2024, doi: 10.3390/fi16040122.

[59] L. Nkenyereye, L. Nkenyereye, B. A. Tama, A. Reddy, and J. Song, "Software-defined vehicular cloud networks: Architecture, applications and virtual machine migration," *Sensors*, vol. 20, no. 4, p. 1092, Feb. 2020, doi: 10.3390/s20041092.

[60] S. N. Saleh and C. Fathy, "A novel deep-learning model for remote driver monitoring in SDN-based Internet of autonomous vehicles using 5G technologies," *Appl. Sci.*, vol. 13, no. 2, p. 875, Jan. 2023, doi: 10.3390/app13020875.

[61] 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.

[62] F. Ayaz, Z. Sheng, I. W. Ho, D. Tiany, and Z. Ding, "Blockchain-enabled FD-NOMA based vehicular network with physical layer security," in *Proc. IEEE 95th Veh. Technol. Conf. (VTC-Spring)*. Helsinki, Finland: IEEE, Jun. 2022, pp. 1–6, doi: 10.1109/VTC2022-Spring54318.2022.9860421.

[63] 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.: IEEE, Mar. 2023, pp. 1–7, doi: 10.1109/WCNC55385.2023.10118852.

[64] 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.

[65] 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: IEEE, Dec. 2022, pp. 12–23, doi: 10.1109/PRDC55274.2022.00016.

[66] M. Alawieh, W. Fahs, J. Haydar, F. Chbib, and A. Fadlallah, "A secure scheme for vehicle-to-vehicle (v2v) routing protocol," in *Proc. 5th Conf. Cloud Internet Things (CIoT)*. Marrakech, Morocco: IEEE, Mar. 2022, pp. 1–8, doi: 10.1109/CIoT53061.2022.9766544.

[67] 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.

[68] E. P. Valentini, G. P. R. Filho, R. E. D. Grande, C. M. Ranieri, L. A. P. Junior, 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.

[69] 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.

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

[71] 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.

[72] 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.

[73] 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. IEEE Global Commun. Conf.* Brazil: IEEE, Jan. 2022, pp. 2686–2691, doi: 10.1109/GLOBECOM48099.2022.10001684.

[74] 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.

[75] J. Qin and J. Liu, "Physical layer security assisted multi-access edge task offloading in C-V2X system," in *Proc. IEEE Int. Conf. Commun. (ICC)*. Seoul, Republic of Korea: IEEE, May 2022, pp. 3328–3333, doi: 10.1109/ICC45855.2022.9838785.

[76] 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.

[77] 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: ACM, Jun. 2021, pp. 250–260, doi: 10.1145/3448300.3467817.

[78] 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, 2022, doi: 10.1109/TIFS.2022.3170276.

[79] 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: IEEE, Jun. 2019, pp. 1–5, doi: 10.1109/CNS.2019.8802768.

[80] 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.

[81] 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. Automat. Sinica*, vol. 10, no. 5, pp. 1234–1251, May 2023, doi: 10.1109/JAS.2022.105845.

[82] 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.

[83] 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.

[84] 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.

[85] M. Li, X. Yang, F. Khan, M. A. Jan, W. Chen, and Z. Han, "Improving physical layer security in vehicles and pedestrians networks with ambient backscatter communication," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 9380–9390, Jul. 2022, doi: 10.1109/TITS.2021.3117887.

[86] 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.

[87] 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: IEEE, Jul. 2023, pp. 392–397, doi: 10.1109/icufn57995.2023.10200146.

[88] C. Anagnostopoulos, C. Koulamas, A. Lalos, and C. Stylios, "Open-source integrated simulation framework for cooperative autonomous vehicles," in *Proc. 11th Medit. Conf. Embedded Comput. (MECO)*. Budva, Montenegro: IEEE, Jun. 2022, pp. 1–4, doi: 10.1109/MECO55406.2022.9797115.

[89] D. Jia, J. Sun, A. Sharma, Z. Zheng, and B. Liu, "Integrated simulation platform for conventional, connected and automated driving: A design from cyber–physical systems perspective," *Transp. Res. C, Emerg. Technol.*, vol. 124, Mar. 2021, Art. no. 102984, doi: 10.1016/j.trc.2021.102984.

[90] S. Aoki, T. Higuchi, and O. Altintas, "Cooperative perception with deep reinforcement learning for connected vehicles," in *Proc. IEEE Intell. Vehicles Symp. (IV)*. Las Vegas, NV, USA: IEEE, Oct. 2020, pp. 328–334, doi: 10.1109/IV47402.2020.9304570.

[91] H. Masuda, O. E. Marai, M. Tsukada, T. Taleb, and H. Esaki, "Feature-based vehicle identification framework for optimization of collective perception messages in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 2, pp. 2120–2129, Feb. 2023, doi: 10.1109/TVT.2022.3211852.

[92] A. Finkenzeller, A. Mathur, J. Lauinger, M. Hamad, and S. Steinhorst, "Simutack—An attack simulation framework for connected and autonomous vehicles," in *Proc. IEEE 97th Veh. Technol. Conf. (VTC-Spring)*. Florence, Italy: IEEE, Jun. 2023, pp. 1–7, doi: 10.1109/VTC2023-Spring57618.2023.10200555.

[93] B. Ribeiro, M. J. Nicolau, and A. Santos, "Using machine learning on V2X communications data for VRU collision prediction," *Sensors*, vol. 23, no. 3, p. 1260, Jan. 2023, doi: 10.3390/s23031260.

[94] T. Ormándi and B. Varga, "The importance of V2X simulation: An in-depth comparison of intersection control algorithms using a high-fidelity communication simulation," *Veh. Commun.*, vol. 44, Dec. 2023, Art. no. 100676, doi: 10.1016/j.vehcom.2023.100676.

[95] M. Benguenane, A. Korichi, B. Brik, and N. Azzaoui, ''Towards mitigating jellyfish attacks based on honesty metrics in V2X autonomous networks,'' *Appl. Sci.*, vol. 13, no. 7, p. 4591, Apr. 2023, doi: 10.3390/app13074591.

[96] T. Wágner, T. Ormándi, T. Tettamanti, and I. Varga, ''SPaT/MAP V2X communication between traffic light and vehicles and a realization with digital twin,'' *Comput. Electr. Eng.*, vol. 106, Mar. 2023, Art. no. 108560, doi: 10.1016/j.compeleceng.2022.108560.

[97] N. F. Abdullah, T. E. Shen, A. A. Samah, and R. Nordin, ''Internet of Vehicles based on cellular-vehicle-to-everything (C-V2X),'' *Int. J. Integr. Eng.*, vol. 15, no. 5, pp. 244–252, Oct. 2023. Accessed: Aug. 2024. [Online]. Available: https://publisher.uthm.edu.my/ojs/index.php/ijie/article/view/15076

[98] X. Zhao, Y. Gao, S. Jin, Z. Xu, Z. Liu, W. Fan, and P. Liu, ''Development of a cyber-physical-system perspective based simulation platform for optimizing connected automated vehicles dedicated lanes,'' *Expert Syst. Appl.*, vol. 213, Mar. 2023, Art. no. 118972, doi: 10.1016/j.eswa.2022.118972.

[99] Y. Shi, L. Lv, H. Yu, L. Yu, and Z. Zhang, ''A center-rule-based neighborhood search algorithm for roadside units deployment in emergency scenarios,'' *Mathematics*, vol. 8, no. 10, p. 1734, Oct. 2020, doi: 10.3390/math8101734.

[100] M. Gonzalez-Martín, M. Sepulcre, R. Molina-Masegosa, and J. Gozalvez, ''Analytical models of the performance of C-V2X mode 4 vehicular communications,'' *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1155–1166, Feb. 2019, doi: 10.1109/TVT.2018.2888704.

[101] H. Xiao, W. Zhang, W. Li, A. T. Chronopoulos, and Z. Zhang, ''Joint clustering and blockchain for real-time information security transmission at the crossroads in C-V2X networks,'' *IEEE Internet Things J.*, vol. 8, no. 18, pp. 13926–13938, Sep. 2021, doi: 10.1109/JIOT.2021.3068175.

[102] Z. Pei, W. Chen, C. Li, L. Du, H. Liu, and X. Wang, ''Analysis and optimization of multihop broadcast communication in the Internet of Vehicles based on C-V2X mode 4,'' *IEEE Sensors J.*, vol. 22, no. 12, pp. 12428–12443, Jun. 2022, doi: 10.1109/JSEN.2022.3175158.

[103] A. Brummer, R. German, and A. Djanatliev, ''Methodology and performance assessment of three-dimensional vehicular ad-hoc network simulation,'' *IEEE Access*, vol. 11, pp. 36349–36364, 2023, doi: 10.1109/ACCESS.2023.3264668.

[104] D. Bischoff, F. A. Schiegg, D. Schuller, J. Lemke, B. Becker, and T. Meuser, ''Prioritizing relevant information: Decentralized V2X resource allocation for cooperative driving,'' *IEEE Access*, vol. 9, pp. 135630–135656, 2021, doi: 10.1109/ACCESS.2021.3116317.

[105] M. E. L. A. Ameur, H. Drias, and B. Brik, ''Cooperative parking search strategy through V2X communications: An agent-based decision,'' *Wireless Netw.*, pp. 1–22, Nov. 2023, doi: 10.1007/s11276-023-03568-2.

[106] B. Y. Yacheur, T. Ahmed, and M. Mosbah, ''Efficient DRL-based selection strategy in hybrid vehicular networks,'' *IEEE Trans. Netw. Service Manage.*, vol. 20, no. 3, pp. 2400–2411, Sep. 2023, doi: 10.1109/TNSM.2023.3300653.

[107] T. Renzler, M. Stolz, and D. Watzenig, ''Feudalistic platooning: Subdivide platoons, unite networks, and conquer efficiency and reliability,'' *Sensors*, vol. 22, no. 12, p. 4484, Jun. 2022, doi: 10.3390/s22124484.

[108] A. Hegde, R. Song, and A. Festag, ''Radio resource allocation in 5G-NR V2X: A multi-agent actor-critic based approach,'' *IEEE Access*, vol. 11, pp. 87225–87244, 2023, doi: 10.1109/ACCESS.2023.3305267.

[109] Q. Delooz, A. Willecke, K. Garlichs, A.-C. Hagau, L. Wolf, A. Vinel, and A. Festag, ''Analysis and evaluation of information redundancy mitigation for V2X collective perception,'' *IEEE Access*, vol. 10, pp. 47076–47093, 2022, doi: 10.1109/ACCESS.2022.3170029.

[110] F. M. Malik, H. A. Khattak, A. Almogren, O. Bouachir, I. U. Din, and A. Altameem, ''Performance evaluation of data dissemination protocols for connected autonomous vehicles,'' *IEEE Access*, vol. 8, pp. 126896–126906, 2020, doi: 10.1109/ACCESS.2020.3006040.

[111] S. A. Alghamdi, ''Cellular V2X with D2D communications for emergency message dissemination and QoS assured routing in 5G environment,'' *IEEE Access*, vol. 9, pp. 56049–56065, 2021, doi: 10.1109/ACCESS.2021.3071349.

[112] H. Zainudin, K. Koufos, G. Lee, L. Jiang, and M. Dianati, ''Impact analysis of cooperative perception on the performance of automated driving in unsignalized roundabouts,'' *Frontiers Robot. AI*, vol. 10, Aug. 2023, Art. no. 1164950, doi: 10.3389/frobt.2023.1164950.

[113] S. Fu, W. Zhang, and Z. Jiang, ''A network-level connected autonomous driving evaluation platform implementing C-V2X technology,'' *China Commun.*, vol. 18, no. 6, pp. 77–88, Jun. 2021, doi: 10.23919/JCC.2021.06.007.

[114] H. Yin, D. Tian, C. Lin, X. Duan, J. Zhou, D. Zhao, and D. Cao, ''V2VFormer++: Multi-modal vehicle-to-vehicle cooperative perception via global-local transformer,'' *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 2, pp. 2153–2166, Feb. 2024, doi: 10.1109/TITS.2023.3314919.

[115] W. Xu, F. Gao, X. Tao, J. Zhang, and A. Alkhateeb, ''Computer vision aided mmWave beam alignment in V2X communications,'' *IEEE Trans. Wireless Commun.*, vol. 22, no. 4, pp. 2699–2714, Apr. 2023, doi: 10.1109/TWC.2022.3213541.

[116] H. Li, H. Liu, H. Lu, B. Cheng, M. Gruteser, and T. Shimizu, ''Bridging the gap between point cloud registration and connected vehicles,'' *IEEE Open J. Veh. Technol.*, vol. 3, pp. 178–192, 2022, doi: 10.1109/OJVT.2022.3165930.

[117] H. Mun, M. Seo, and D. H. Lee, ''Secure privacy-preserving V2V communication in 5G-V2X supporting network slicing,'' *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 14439–14455, Sep. 2022, doi: 10.1109/TITS.2021.3129484.

[118] C. B. Math, H. Li, S. H. de Groot, and I. G. Niemegeers, ''V2X application-reliability analysis of data-rate and message-rate congestion control algorithms,'' *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1285–1288, Jun. 2017, doi: 10.1109/LCOMM.2017.2675899.

[119] J. Heo, B. Kang, J. M. Yang, J. Paek, and S. Bahk, ''Performance-cost tradeoff of using mobile roadside units for V2X communication,'' *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 9049–9059, Sep. 2019, doi: 10.1109/TVT.2019.2925849.

[120] M. Zhang, Y. Dou, P. H. J. Chong, H. C. B. Chan, and B.-C. Seet, ''Fuzzy logic-based resource allocation algorithm for V2X communications in 5G cellular networks,'' *IEEE J. Sel. Areas Commun.*, vol. 39, no. 8, pp. 2501–2513, Aug. 2021, doi: 10.1109/JSAC.2021.3087244.

[121] H. Kaja, J. M. Stoehr, and C. Beard, ''V2X-assisted emergency vehicle transit in VANETs,'' *Simulation*, vol. 100, no. 3, pp. 229–244, Mar. 2024, doi: 10.1177/00375497231209774.

[122] R. Chhabra, C. R. Krishna, and S. Verma, ''Augmenting driver's situational awareness using smartphones in VANETs,'' *Arabian J. Sci. Eng.*, vol. 47, no. 2, pp. 2271–2288, Feb. 2022, doi: 10.1007/s13369-021-06159-5.

[123] M. Ali, H. Hwang, and Y.-T. Kim, ''Enhanced C-V2X mode-4 with virtual cell, resource usage bitmap, and smart roaming,'' *IEEE Access*, vol. 11, pp. 142628–142642, 2023, doi: 10.1109/ACCESS.2023.3341915.

[124] S. D. A. Shah, M. A. Gregory, S. Li, R. d. R. Fontes, and L. Hou, ''SDN-based service mobility management in MEC-enabled 5G and beyond vehicular networks,'' *IEEE Internet Things J.*, vol. 9, no. 15, pp. 13425–13442, Aug. 2022, doi: 10.1109/JIOT.2022.3142157.

[125] S. D. A. Shah, M. A. Gregory, and S. Li, ''Toward network slicing enabled edge computing: A cloud-native approach for slice mobility,'' *IEEE Internet Things J.*, vol. 11, no. 2, pp. 2684–2700, Jul. 2023, doi: 10.1109/JIOT.2023.3292520.

[126] Z. Khan, P. Fan, F. Abbas, H. Chen, and S. Fang, ''Two-level cluster based routing scheme for 5G V2X communication,'' *IEEE Access*, vol. 7, pp. 16194–16205, 2019, doi: 10.1109/ACCESS.2019.2892180.

[127] K. Z. Ghafoor, M. Guizani, L. Kong, H. S. Maghdid, and K. F. Jasim, ''Enabling efficient coexistence of DSRC and C-V2X in vehicular networks,'' *IEEE Wireless Commun.*, vol. 27, no. 2, pp. 134–140, Apr. 2020, doi: 10.1109/MWC.001.1900219.

[128] M. Won, ''L-platooning: A protocol for managing a long platoon with DSRC,'' *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 6, pp. 5777–5790, Jun. 2022, doi: 10.1109/TITS.2021.3057956.

[129] S. Chavhan, S. Kumar, D. Gupta, A. Alkhayyat, A. Khanna, and R. Manikandan, ''Edge-empowered communication-based vehicle and pedestrian trajectory perception system for smart cities,'' *IEEE Internet Things J.*, vol. 10, no. 21, pp. 18951–18960, Nov. 2023, doi: 10.1109/JIOT.2023.3254647.

[130] A. Wippelhauser, T. A. Tomaschek, M. Verdes, and L. Bokor, ''Real-life traffic data based ITS-G5 channel load simulations of a major Hungarian C-ITS deployment site,'' *Appl. Sci.*, vol. 13, no. 14, p. 8419, Jul. 2023, doi: 10.3390/app13148419.

[131] B. Wang, J. Zheng, N. Mitton, and C. Li, ''InP-CRS: An intra-platoon cooperative resource selection scheme for C-V2X networks,'' *IEEE Commun. Lett.*, vol. 27, no. 11, pp. 3118–3122, Nov. 2023, doi: 10.1109/LCOMM.2023.3315010.

[132] F. Linsalata, S. Mura, M. Mizmizi, M. Magarini, P. Wang, M. N. Khormuji, A. Perotti, and U. Spagnolini, ''LoS-map construction for proactive relay of opportunity selection in 6G V2X systems,'' *IEEE Trans. Veh. Technol.*, vol. 72, no. 3, pp. 3864–3878, Mar. 2023, doi: 10.1109/TVT.2022.3217966.

[133] V. K. Gautam and B. R. Tamma, "RETALIN: A queue aware uplink scheduling scheme for reducing scheduling signaling overhead in 5G NR," *IEEE Access*, vol. 12, pp. 16632–16651, 2024, doi: 10.1109/ACCESS.2024.3359028.

[134] B. Ching, M. Amoozadeh, C.-N. Chuah, H. M. Zhang, and D. Ghosal, "Enabling performance and security simulation studies of intelligent traffic signal light control with VENTOS-HIL," *Veh. Commun.*, vol. 24, Aug. 2020, Art. no. 100230, doi: 10.1016/j.vehcom.2020.100230.

[135] L. Nkenyereye, L. Nkenyereye, S. M. R. Islam, C. A. Kerrache, M. Abdullah-Al-Wadud, and A. Alamri, "Software defined network-based multi-access edge framework for vehicular networks," *IEEE Access*, vol. 8, pp. 4220–4234, 2020, doi: 10.1109/ACCESS.2019.2962903.

[136] A. M. Aslam, R. Chaudhary, A. Bhardwaj, I. Budhiraja, N. Kumar, and S. Zeadally, "Metaverse for 6G and beyond: The next revolution and deployment challenges," *IEEE Internet Things Mag.*, vol. 6, no. 1, pp. 32–39, Mar. 2023, doi: 10.1109/IOTM.001.2200248.

[137] H. Wang, Z. Wang, D. Chen, Q. Liu, H. Ke, and K. K. Han, "Metamobility: Connecting future mobility with the metaverse," *IEEE Veh. Technol. Mag.*, vol. 18, no. 3, pp. 69–79, Apr. 2023, doi: 10.1109/MVT.2023.3263330.

[138] H. Pennanen, T. Hänninen, O. Tervo, A. Tölli, and M. Latva-Aho, "6G: The intelligent network of everything—A comprehensive vision, survey, and tutorial," 2024, *arXiv:2407.09398*.

[139] Z. Wang, O. Zheng, L. Li, M. Abdel-Aty, C. Cruz-Neira, and Z. Islam, "Towards next generation of pedestrian and connected vehicle in-the-loop research: A digital twin co-simulation framework," *IEEE Trans. Intell. Vehicles*, vol. 8, no. 4, pp. 2674–2683, Mar. 2023, doi: 10.1109/TIV.2023.3250353.

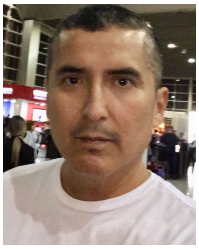
[140] K. Wang, Z. Li, K. Nonomura, T. Yu, K. Sakaguchi, O. Hashash, and W. Saad, "Smart mobility digital twin based automated vehicle navigation system: A proof of concept," *IEEE Trans. Intell. Vehicles*, vol. 9, no. 3, pp. 4348–4361, Mar. 2024, doi: 10.1109/TIV.2024.3368109.

[141] J. P. J. da Costa, A. A. S. da Silva, G. A. Santos, E. P. de Freitas, and A. Vinel, "Vorrichtung und verfahren zur erkennung und entschärfung von jamming-attacken in mobilen anwendungen," Germany Patent application (DE) 2024 021 309 180 000 DE, Deutsches Patent- und Markenamt, Munich, Germany, Feb. 13, 2024.

[142] G. Danapal, G. A. Santos, J. P. C. da Costa, B. J. Praciano, and G. P. Pinheiro, "Sensor fusion of camera and lidar raw data for vehicle detection," in *Proc. Workshop Commun. Netw. Power Syst. (WCNPS)*. Brasilia, Brazil: IEEE, Nov. 2020, pp. 1–6, doi: 10.1109/WCNPS50723.2020.9263724.

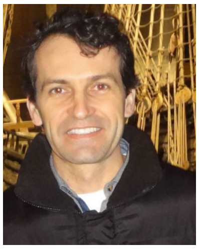
KEVIN HERMAN MURARO GULARTE received the Bachelor of Science degree in mechatronics engineering, the Master of Science degree in mechatronic systems, and the Doctor of Science degree in electronic systems and automation from the University of Brasília (UnB), in 2013, 2018, and 2021, respectively. His research interests include autonomous vehicles, synchronization systems, chaotic systems, adaptive control, neural networks, Lyapunov stability theory, and system identification.

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, where he became a Research Professor, in March 2022. He is currently a Professor Member with the Graduate School for Applied Research in North Rhine-Westphalia (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 has obtained seven best paper awards in international conferences.



JOSÉ ALFREDO RUIZ VARGAS 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. Since 2023, he has been engaged as a Researcher with Hamm-Lippstadt University of Applied Sciences, Lippstadt, Germany. He is currently a Professor of control systems with the Department of Electrical Engineering, University of Brasília. His current research interests include chaos-based communication, V2X communication, nonlinear and adaptive control, neural networks, and online machine learning.

ANTONIO SANTOS DA SILVA received the B.Sc. 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, in 2021. He is currently pursuing the dual Ph.D. degree with the Graduate School for Applied Research in North Rhine-Westphalia (PK NRW), Karlsruhe Institute of Technology (KIT), Germany, and the Federal University of Rio Grande do Sul (UFRGS), Brazil. 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 of computer science with the Catholic University of Brasilia (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.

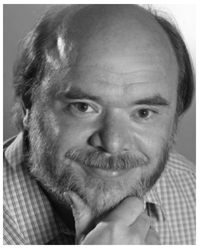
YUMING WANG is currently pursuing the bachelor's degree in electronic engineering with Hamm-Lippstadt University of Applied Sciences (HSHL). He is also a Research Student on the project B5GCyberTestV2X funded by BSI. His research interests include autonomous systems, embedded systems, and cybersecurity.

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. He is currently a Senior Researcher with Germany Research Center for Artificial Intelligence (DFKI), 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.

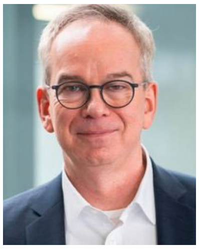
CHRISTOPH LIPPS (Member, IEEE) is currently a Researcher with the Intelligent Networks Department, German Research Center for Artificial Intelligence, Kaiserslautern. He is the Team Leader of the Cyber Resilience and Security, Intelligent Networks Department, German Research Center for Artificial Intelligence. 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 master's/D.E.A. degree in information systems and computing from the Ecole Supérieure d'Electricité—Supélec, 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 Supérieure d'Electricité—Supélec, from 2006 to 2007. He worked in the 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 a 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 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 São Paulo (USP), in 2003. He is currently 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 Diploma degree in physics in Frankfurt, the M.Sc. degree in physics in Tübingen, and the Ph.D. degree in computer science from Erlangen University. He is currently the Scientific Director of German Research Center 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 at the ''Intel Visual Computing Institute,'' a central research institute at 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 the Principle Investigator of 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 3D-internet technology and integrating research in areas, such as real-time realistic graphics, artificial intelligence, high-performance computing as well as security by design for creating distributed, immersive, 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 the Research and Development Group, Research Coordinator for 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 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 articles and participated more than 40 European and national collaborative research projects. Since 2018, he has been the Chairman of German Society for Information Technology and a member of the Supervisory Board of the VDE.