IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 14 April 2023, accepted 8 May 2023, date of publication 10 May 2023, date of current version 17 May 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3274774

SURVEY

A Systematic Literature Review on Security of Vehicular Ad-Hoc Network (VANET) Based on VEINS Framework

MAHMOOD A. AL-SHAREEDA AND SELVAKUMAR MANICKAM
National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM), George Town, Penang 11800, Malaysia
Corresponding authors: Mahmood A. Al-Shareeda (alshareeda022@usm.my) and Selvakumar Manickam (selva@usm.my)

ABSTRACT Innovative framework on Vehicles in Network Simulation (VEINS) for Vehicular Ad-hoc Network (VANET) that use security aspect is mainly limited and dispersed. In order to offer valuable visions for technical settings and researchers, the study looked into the trends and gaps that were currently present. As a result, this systematic literature review was carried out to develop a comprehensive taxonomy of the research landscape. A thorough study was done for papers about (a) VANET, (b) VEINS, and (C) security aspects. This research used three databases, namely IEEE Xplore, ScienceDirect, and Scopus. These databases included in-depth research focused on VANET based on the VEINS framework. Then, on the basis of the security aspect, filtering was accomplished. The first class includes threats and vulnerabilities that evaluate the effects of threats and vulnerabilities on VANETs by using the VEINS framework and suggest ways to mitigate or lessen their effects. The second category includes articles on the solution technology that uses blockchain, machine learning, and Software-Defined Networking (SDN) techniques in VEINS-based VANET applications. The third class comprises the requirements that satisfy privacy, authentication, trust management, reliability, and revocation of the VANET security-based VEINS framework. Finally, this paper reviews the architecture and bidirectional coupling of the VEINS framework.

INDEX TERMS Vehicular ad-hoc network, SLR VEINS, VANET security, OMNeT++, VEINS framework.

I. INTRODUCTION

The majority of the industry's research laboratories began studying Vehicular Ad-hoc Networks (VANETs) in about 2000 [1], [2], [3]. Initially, VANET is utilized to enhance road traffic safety and reduce road accident's and jam [4], [5], [6]. It now has a considerably wider reach, encompassing integrated services using various technologies in addition to the fundamental functionalities offered by VANET architecture [7].

Typically, the main components in VANETs include, namely, Trusted Authority (TA), Roadside Units (RSUs) and Onboard Units (OBUs), as presented in Figure 1. TA is a fully trusted component in VANET and is in charge of managing the whole system and updating the parameters to the rest components in VANETs. While, RSU is deployed on the roadside as wireless infrastructure to connect vehicles with TA. OBU is a wireless device equipped on each vehicle to process, send and receive messages (e.g. road status, road condition and etc.) among vehicles.

The difficult aspect of VANET is that the topology of the network is always vulnerable to security attacks. Due to the high cost and heavy effort involved in deploying VANET, researchers typically use simulators in their research. Additionally, testing VANETs under these conditions may produce unreliable findings. Studies already conducted indicate that the mobility models have a considerable impact on how accurately the simulation outputs should be approximated to true values. Many simulators for vehicular networks, which are extended from three categories: a) mobility simulators (e.g, straw, netstream, sumo); b) network generators (e.g. OMNeT++, ns2, ns3) Integrated framework (e.g. mobireal, trans, VEINS). Sadly, there isn't a standard VANET simulator. Typically, scholars integrated current network simulators

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

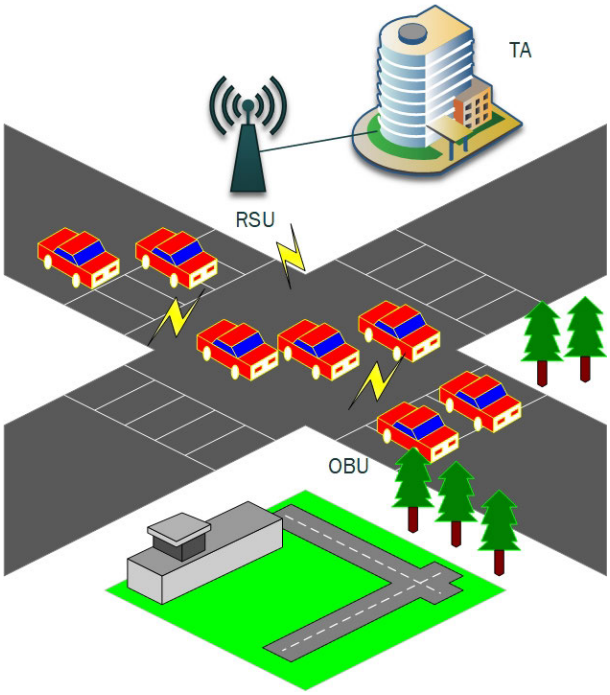

FIGURE 1. Structure of VANET.

with current mobility simulators. VEINS [8] is one of these integrated systems that is becoming more and more common. Veins combines the well-known SUMO [9] network simulator with OMNET++ [10].

In the literature review, there are several researches in VANET. As a new paradigm for TM design, management, and evaluation across settings and with hostile vehicles present, Ahmad et al. [11] investigated forth the Trust Evaluation and Management (TEAM) framework. Noori et al. [12] investigated the Veins framework, which simultaneously executes the SUMO traffic simulator and the OMNET++ network simulator, and run an ad hoc simulation of the traffic patterns in the German city of Cologne. [13] suggested the use of PREXT, a location privacy add-on for the Veins framework. Seven alternative privacy techniques, such as silent periods, context-based, and cryptographic mix-zone, are currently supported by PREXT. Riebl et al. [14] introduced a new feature for the V2X simulation framework ''Vehicles in Network Simulation'' (Veins) that separates network concerns from application concerns. Because of distinctively modelled Facilities and Application layers, this approach enables the concurrent combination of multiple VANET application sets as well as the evaluation of their interdependencies. Martinez et al. [15] provided a detailed analysis and comparison of existing VANET simulation tools and their constituent parts. In this comparison, Martinez et al. [15] focus on the software itself, contrasting its features, GUI, popularity, ease of use, input requirements, output visualisation capability, simulation accuracy, etc. A brief overview of some widely-used simulators with potential VANET applications is presented in Aljabry et al. [16]. Since such platforms can save both time and money while also improving the realism of the simulation, OMNeT++ and SUMO are combined to study the VANET environment by means of a simulated road traffic scenario.

One of the most effective network simulators, OMNeT++ enjoys widespread support in the scientific community. The extremely portable SUMO road traffic simulator takes into account specific vehicle behaviours including velocity, acceleration, location relative to the route and road descriptions on the map, such as arrival and departure timings, etc. In general, simulator of VEINS appears to be much more advantageous, especially in light of the network's stability, portability, and mobility model.

Current research publications have focused on the constraints and difficulties that prevent the full use of the security of VANET based on the VEINS framework, and proposals have been made to address these problems. Research on the security aspect of VANET for use in the VEINS framework is ongoing and diverse. The main contribution of this paper are as follows.

- Providing insightful analyses of technological settings and research by examining the present gaps in this area;
- Accentuating the efforts involving modern technology;
- Describing this fantastic strategy to research the security of VANET based on VEINS framework and depict the landscape of research towards a consistent taxonomy.

This review is organized into six sections as follows: Section I presents the security of VANET technology for the VEINS framework. Section II describes the method of our study in terms of the research scope, database source, and scanning steps. A solid taxonomy from the study landscape is also listed. Section III outlines the findings of this paper in the form of results and statistical analysis for the complete collection of publications that were subjected to the review. Section IV introduces the distribution results for the number of included articles in different subcategories according to database source and number of published journals. Section V review VEINS framework in details. Finally, Section VI concludes of this paper.

II. METHOD

In this section, the basic keyword in the research based database was 'VEINS framework and its utilization in VANET'. The search excluded any related article on the security of the VANET-based VEINS framework. Moreover, the research scope was restricted to English papers that take into account the utilization of the VEINS framework in VANET.

A. INFORMATION SOURCES

This work uses three source databases to extract and collect related studies from the literature, namely (1) IEEE ®Digital Library, which is a research database that offers a massive number range of papers in computer science and electrical and electronic engineering; and (2) ScienceDirect, that is a massive number scientific, and (3) Scopus, which offers a

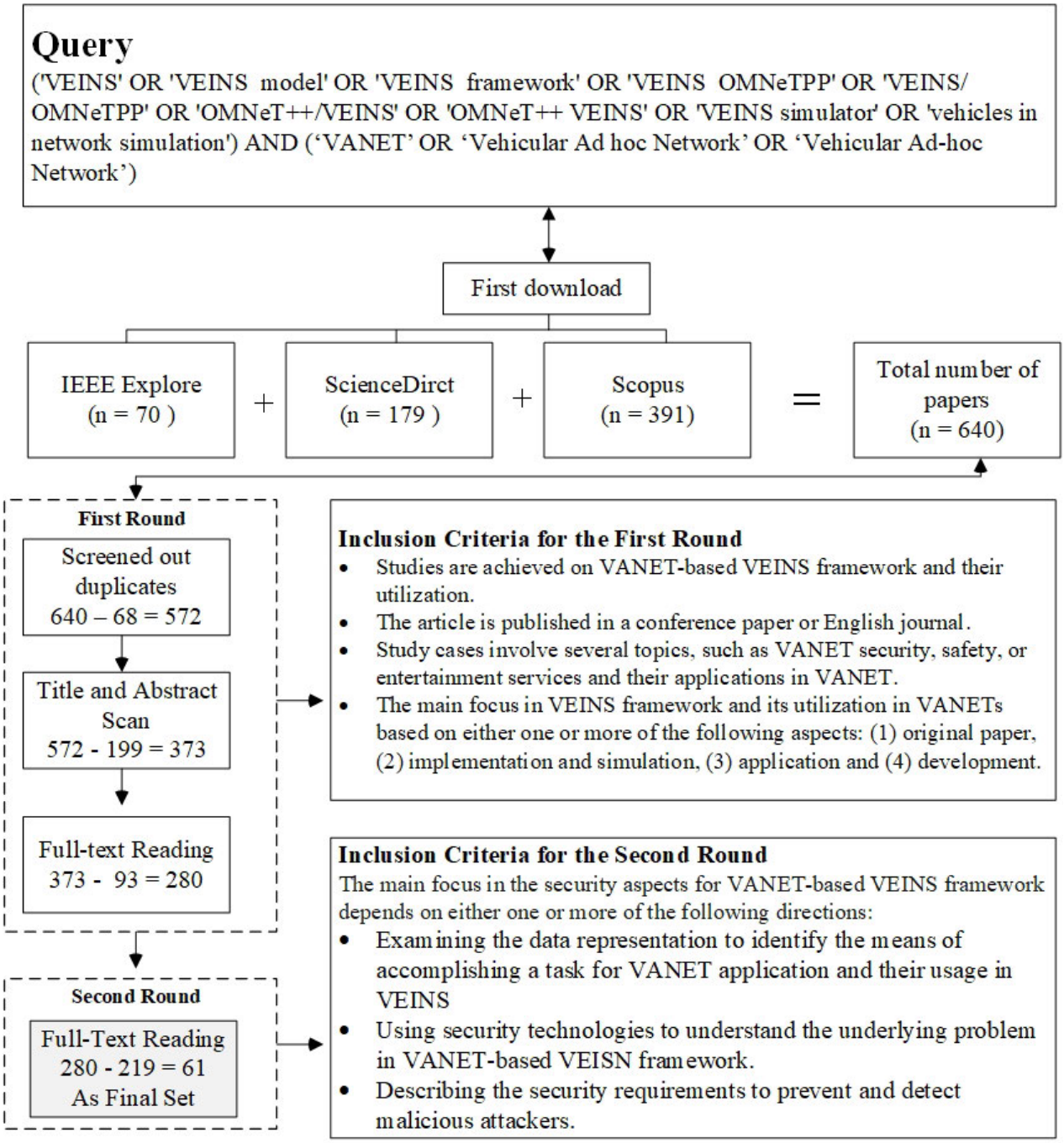

FIGURE 2. Flowchart of Our Method.

large scientific technique in various fields, including humanities and arts, sciences and social sciences, electronics and electrical methods. These three databases cover the security of the VANET-based VEINS framework and investigate a wide range of related schemes. The electronic link for databases searched are as follows:

- IEEE Xplore®Digital Library (http://ieeexplore.ieee.org; accessed on: 5 MAY 2022).
- ScienceDirect (http://www.sciencedirect.com; accessed on: 5 MAY 2022).
- Scopus Database (http://www.scopus.com; accessed on: 5 MAY 2022).

B. PROCEDURE OF STUDY SELECTION

Study selection consisted of a search for relevant studies sources and was categorized into two rounds. In the first round, this paper performs three iterations of filtering and screening to identify articles according to the security of the VANET-based VEINS framework. In the first screening and filtering iteration, all duplicates and irrelevant papers to the

VANET-based VEINS framework were removed. In the second iteration, unrelated articles were excluded by checking the abstracts and titles. Lastly, an intensive survey of the full-text articles was carefully screened and investigated. All iteration steps used similar properties of eligibility followed by authors. In the second round, this paper performs a single iteration of filtering and screening according to the security aspect or all articles get from the first round iteration. Therefore, the final selected set was according to the VANET-based VEINS framework via various topics.

C. SEARCH

The search was conducted in March 2022 utilizing the search boxes of IEEE Xplore, ScienceDirect, and Scopus. To identify the studies related to VANET, such as 'Vehicular Ad-hoc Networks', a set of keywords was used, including 'VEINS', 'VEINS model', 'VEINS framework', 'VEINS OMNeTPP', 'VEINS/OMNeTPP', 'OMNeT++/VEINS', 'OMNeT++ VEINS', 'VEINS simulator', and 'vehicles in network simulation' in different combinations and merged with operators of 'AND' and 'OR', followed by 'Vehicular Ad-hoc Network', 'Vehicular Ad hoc Network' OR 'VANET'. Figure 2 displays the query text. The options of advanced study in the source database engines were used to exclude short communication, letters, correspondence, and book chapters. The modern scientific research associated with the article on the tremendous direction in VEINS/OMNeT++ framework utilization in VANET was also accessed.

D. ELIGIBILITY CRITERIA

The articles that achieved our criteria shown in Figure 2 were included. An initial target was set to identify the research aspect of the VEINS-based studies for VANET in a generic and coarse-grained taxonomy of three categories. It was derived without constraint from the literature pre-survey. The result of the first round, which includes three iterations of screening and filtering, is to exclude ineligible papers according to the needed criteria. The exclusion criteria included (a) non-security of VANET-based studies for VEINS, (b) articles on safety and service, and (c) non-English articles. Thus, when articles did not satisfy the VEINS utilization criteria, they were excluded.

E. DATA COLLECTION PROCESS

In order to simplify the process of screening and filtering, all selected papers were reviewed, analyzed, and reviewed depending on their corresponding initial categories and were stored as Excel and Microsoft PowerPoint files. The full-text reading of all papers was performed carefully by the authors. Thus, based on massive comments and highlights on the related articles, the proposed taxonomy runs a classification of all the articles. Besides, taxonomy was used to categorize the articles with massive highlight and note collections. The taxonomy suggested different categories and subcategories, comprising three main categories: Threats and vulnerabilities, solutions, and requirements. Texts were classified based on the authors' preferred style. All the articles from different databases were read and analyzed in depth to provide researchers with the comprehensive emergence of diverse investigation and utilization.

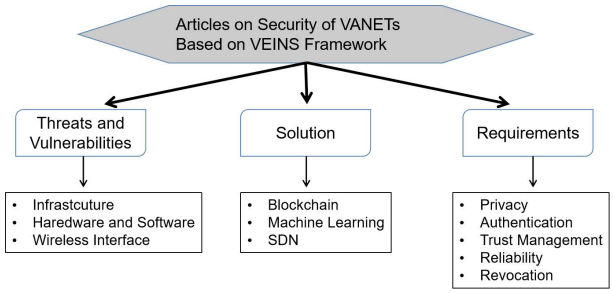

FIGURE 3. Taxonomy of Literature on Security of VANET-based VEINS Framework.

III. RESULTS AND STATISTICAL INFORMATION OF ARTICLES

The following result of the first query search of 640 papers is: 70 from the IEEE Explore database, 179 from ScienceDirect, and 391 from Scopus. The filtered papers published from 2011 to 2022 were adopted in this research and categorized into three groups in the first round. In the three chosen databases, 68 out of 640 articles were duplicates. After investigating the titles and abstracts, 199 articles were excluded further, for a total of 373 articles. Finally, in the first round, the full-text scan excluded 93 articles, for a total of 280 articles on the VANET-based VEINS framework. In the second step, the last full-text survey excluded 219 of the 280 papers, leaving 61 papers for the final set. All of these were associated with the security of VEINS framework-based VANET technology via various topics. The taxonomy displayed in Figure 3 was utilized to show the main research streams focusing on the security of the VEINS framework and their general utilization in VANET. This taxonomy reviews the comprehensive overview of the subject. The taxonomy suggests different categories and subcategories. The first category comprises threats and vulnerabilities aspect related to the VANET-based VEINS framework (16/61 articles). The second category includes articles on the solution aspect (19/61 articles). The Final category comprises articles on the requirements aspect (26/61 articles). For statistical analysis, the observed classes are reviewed as follows.

A. THREATS AND VULNERABILITIES

Numerous research assesses the effects of threats and vulnerabilities on VANETs by using the VEINS framework and suggest ways to mitigate or lessen their effects. These researches are categorized as follows.

- Infrastructure: In order to improve operational efficiency and provide better traffic management, a Sybil attack in vehicular platoons was modeled and evaluated their impact on performance in vehicular network [17]. Under platoon maneuver attacks, jamming, channel overhearing, and data packet injection, a hybrid security and

IEEE 802.11p based on visible light communication (VLC) protocol was proposed to offer securing platoon maneuvers and platoon stability [18]. An efficient approach was suggested to detect Sybil attacks by dividing the vehicles into different clusters with their filter, the Sybil nodes, certificate, and location information [19]. Static/dynamic selfishness was investigated and defined to permit intermediate nodes to forward tasks to others [20]. According to the adaptive detection threshold, a new solution was proposed to detect behaviors of intelligent malicious [21].

- Hardware and Software: A Machine Learning (ML) technique based on a probabilistic cross-layer Intrusion Detection System (IDS) was introduced to be able to detect spoofing attacks with more than top accuracy [22]. A new speed-based attacker placement algorithm was proposed to investigate an intelligent attacker placement scheme for a Pseudonym Change Strategy (PCS) by matching several pseudonyms to the same source [23]. To identify betray attacks in vehicular network, an invariant-based distributed collaborative intrusion detection system was proposed by [24].
- Wireless Interface: The impact on network performance of Man-in-the-middle attacks was studied on different strategies such as random or fleet strategies [25]. Distributed Denial of Service (DDOS) Flood attacks based on a lightweight anomaly was investigated by [26]. To achieve high level of privacy for drivers, existing pseudonymous schemes were identified with feasible attacking capabilities in vehicular communication [27]. For misbehaving vehicular, an analytical model was proposed to accurately evaluate the optimal value of threshold to launch the mechanism of fail-safe [28]. The effect of the adversary's eavesdropping was investigated by proposing a privacy scheme on the overall system functioning [29]. Two adversary placement strategies were proposed by using different Pseudonym Management Techniques (PMTs) to track success [30]. For secure VANET applications, threat source and security requirements were analyzed to provide a general testing framework [31]. The effects of unintentional misbehavior of vehicles were investigated by extending the weighted persistence broadcast mitigation technique to be utilized for the scenario of dense suburban [32].

B. SOLUTION

- Blockchain: A trust management model and blockchain-based authentication scheme was proposed to prevent inside attackers from injecting false emergency messages in VANET system [33]. A blockchain-based decentralized pseudonym management scheme was suggested to enable the vehicles to provide conditional anonymity [34]. A smart contract feature-based permissioned consortium blockchain system was proposed for facilitating pseudonym issuance and management of privacy preservation, and security [35]. A Biometrics Blockchain (BBC) framework was presented to retain statuary data sharing among vehicles [36]. A decentralized authentication approach based on a new blockchain was proposed to create strengthen the integrity of the data, maintain an immutable record, and distribute the framework of the system [37]. A secure distributed message-passing framework was proposed to rate the message source credibility utilizing blockchain technology [38]. A futuristic blockchain that consists of all main components like a priority, reputation system, and incentive mechanism for cost-effective and scalable 5G vehicular network architecture [39].
- Machine Learning: By using entropy and machine learning frameworks, a novel classification approach was introduced to detect protocol misbehavior [40]. Reinforcement Learning based cluster-enabled cooperative scheduling was proposed to improve the vehicular networks' reliability and communication efficiency, with the target of maximizing the information capacity [41]. The message clustering intuitively was understood by collecting awareness and safety information messages [42]. Artificial Intelligence (AI) was applied to lead to self-driving cars and avoiding collision [43].
- Software Defined Network (SDN): A misbehavior detection in software-defined vehicular networks (TFMD-SDVN) framework was proposed for detecting the valid events issued by the legal or illegal nodes in the VANET system [44]. In order to build an architecture of hierarchical hybrid trust management, an efficient flow forwarding mechanism was proposed by [45]. A Trust-Based Distributed DoS Misbehave Detection Approach (TBDDoSA-MD) was suggested to secure the Software-Defined Vehicular Network (SDVN) for detecting the DDoS misbehavior by utilizing the vehicles trust values [46]. A Trust-Based Event Detection Algorithm (TB-EDA) was suggested for detecting false events by comparing the trust values of node's neighbor vehicles with the measured threshold trust value [47]. The utilization of a central controller to schedule traffic light causes higher efficiency because of the higher knowledge of intersection conditions and street traffic [48]. SDN controller was used to alleviate congestion among vehicles while routing data on segments of road [49]. SDN planes based VANET was exploited to ensure road safety on highways [50]. A data offloading based on smart ranking algorithm was proposed to choose an RSU and to enhance the quality of service [51].

C. REQUIREMENTS

- Privacy: A safety-aware location privacy-preserving scheme was proposed to adjust the vehicle's communication area to prevent continuous location monitoring [52]. A security protocol according to a pseudonym dynamic change for anonymity and privacy to ensure

privacy for the driver and his/her vehicle whether he/she is the sender or receiver of the message [53]. A set enhancement of schemes to allow vehicles to adjust their beacon communication area to conditionally avert tracking [54]. A location privacy mechanism with an adaptive beaconing approach preserved the Quality of Service (QoS) of the applications of road safety [55]. A dynamic change of pseudonyms-based security protocol was proposed to ensure privacy for the driver to handle all possible cases of changes in vehicle behavior during traffic [56]. A Vehicular Location Privacy Zone (VLPZ) based pseudonym changing and management scheme was proposed by [57]. Mix-zones-based location privacy was improved by [58] and [59]. An anonymization approach according to generalization and differential privacy was proposed for ensuring the privacy of the sensitive vehicular trajectories [60]. A Cooperative Pseudonym Exchange and Scheme Permutation (CPESP) scheme were proposed to preserve the privacy of users [61].

- Authentication: In order to secure traffic emergency messages in VANETs, an elliptic curve cryptography-based signature scheme was proposed by [62] and [63]. To ensure node identity security with a non-duplicated physical information identity authentication mechanism, the hash chain based on a cross-regional node identity management architecture was proposed and combined with Radio Frequency (RF) fingerprint theory [64]. The Hashchain based on an identity authentication and privacy protection scheme was proposed to simplify the blockchain in the Space-Air-Ground Integrated Network (SAGIN) [65]. In order to enhance the efficiency of authentication and decrease the communication overhead, an efficient message authentication scheme was proposed to include both signature aggregation and batch message verification [66]. To preclude respective drawbacks for privacy-preserving authentication, the hybrid approach was proposed to combine both the group signature-based approaches and the pseudonym-based approaches in VANETs [67]. A security schema was proposed to use Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Diffie-Hellman (ECDH) algorithm for ensuring RSU identification and the vehicle authenticates the message beforehand signing, respectively [68], [69]. By modeling on two public key cryptosystems: CL-PKC and PKI, a privacy-preserving localized hybrid authentication scheme (PLHAS) were proposed to ensure role separation and minimize centralized dependency [70], [71]. By combining Tamper Proof Device Based (TPDB) schemes and Road Side Unit Based (RSUB) schemes, an authentication scheme was proposed to address the overhead of the system [72], [73]. In a generalized framework utilizing the logic of subjective, two position verification mechanisms were enhanced for considering misbehavior detection [74]. Anonymous authentication and Sybil attack detection protocol were proposed to offer robustness against Sybil attacks for VANETs [75].
- Trust Management: By using a hybrid approach: Entity-based and data-based, a novel trust management scheme was proposed for self-organized VANETs [76]. To achieve trust management mechanism in VANETs, a centralized reputation system was presented to record the behavior of the vehicles in the opportunistic messages of message forwarding, and messages creation [77], [78]. For improving the trustworthiness of shared location information, a Vouch+ scheme was proposed by using mobility awareness, and cryptographic primitives in high-speed scenarios [79].
- Reliability: In order to ensure messages' reliability according to the credit of nodes, a novel self-reliant trust management was proposed by [80]. To satisfy top reliability for data dissemination while achieving delay requirements, Bayesian networks and unipolar orthogonal Code based Reliable multi-hop Broadcast (BCRB) was proposed for various channel conditions [81], [82].
- Revocation: A Smart Certificate Revocation List Exchange (SCRLE) was proposed to distribute Certificate Revocation List (CRL) pieces among the vehicles [83]. A revocation and authentication framework based on blockchain was proposed to speedily update the status of revocated vehicles in the shared blockchain ledger [84].

IV. DISTRIBUTION RESULTS

In this section, the articles distribution in diverse classes is shown based on database sources and subcategories in the taxonomy.

A. DISTRIBUTION BY DATABASE SOURCE

Figure 4 reveals that the three databases source contain a large number of research articles. The articles classify into three taxonomies, namely, threats and vulnerabilities, solutions, and requirements.

The number of studied articles from IEEE Explore is 10 for security aspects. Eleven of the studied articles were published in ScienceDirect. The number of studied articles from Scopus is 40. As shown in Figure 4, the total result of studied articles from Scopus is 40, which decreases by $\frac{40-10}{40} \approx 75\%$ and $\frac{40-11}{40} \approx 73\%$ receptively, against IEEE Explore and ScienceDirect database sources.

B. DISTRIBUTION BY SUBCATEGORIES IN THE TAXONOMY

This subsection shows a ratio of different articles selected in this work via titles sections in the taxonomy. Figure 5 displays the distribution of subcategories in the taxonomy according to the searched database sources. The title in the taxonomy consists of three basic aspects: Threats and vulnerabilities, solutions, and requirements. Each aspect has several subcategories. These subcategories indicate the direction for many

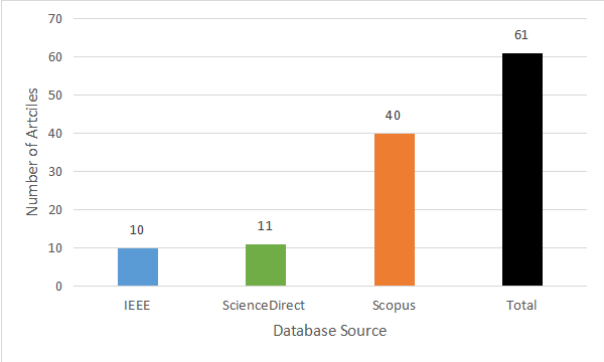

FIGURE 4. Number of Studied Articles in The Taxonomy Based on Database Source.

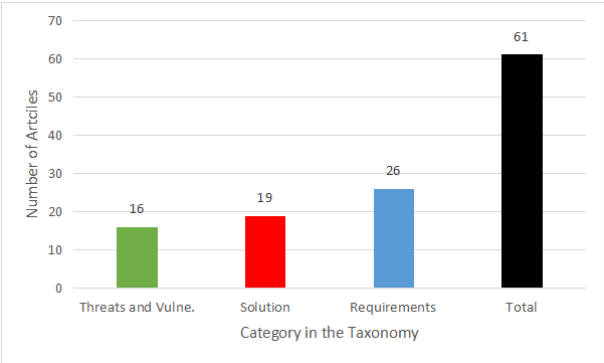

FIGURE 5. Distribution of Categories in the Taxonomy.

future studies in this field. As a result, many scholars may use these studies as a starting point for future studies.

In the security aspect, the number of studied articles on threats and vulnerabilities is 16, including five articles for infrastructure, 3 for hardware and software, and 8 for the wireless interface. The number of studied articles from solution is 19, consisting 4 articles for machine learning, and 7 for blockchain, 8 for SDN. The number of studied articles from requirements is 26, comprising nine articles for privacy, 10 for authentication, 3 for trust management, 2 for reliability, and 2 for revocation.

V. VEINS

The model library VEINS [85] for OMNeT++ enables researchers to run simulations, including communicating road vehicles, either as the primary subject of the investigation (e.g. VANETs) or as a component (e.g. in ITS). Since it is distributed as open-source software, downloading, modifying, and using it are all free.

As of VEINS 5.2, the model library contains a entire stack of simulators for analyzing connecting infrastructure and vehicles, namely trucks and cars, utilizing the technology of Wireless Local Area Network (WLAN). In order to accomplish this, VEINS incorporates a advanced model of the IEEE 802.11 MAC layer entities [86], [87] that are utilized by standards like IEEE Wireless Access in Vehicular Environments (WAVE). Due to the modular nature of Veins, it can be used to model a variety of mobile nodes, including Unmanned Aerial

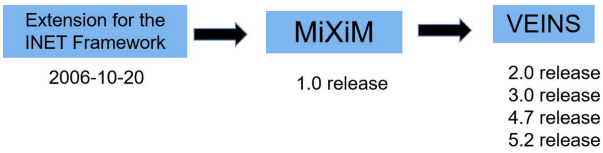

FIGURE 6. Release VEINS.

Vehicles (UAVs), bicycles, trains, and pedestrians, as well as other communication technologies like mobile broadband of Long Term Evolution (LTE) [88], [89] and Visible Light Communication (VLC) [90].

A. HISTORY OF VEINS

As shown in Figure 6, the initial public release of VEINS, an extension for the INET Framework version 20-10-2006, was made in early 2006. VEINS were converted to be an extension of MiXiM for its 1.0 release due to constraints in the quality of wireless channel modeling at the time. VEINS was then gradually enhanced with new paradigms, such as WAVE, IEEE 1609.4 and IEEE 802.11p for the 2.0 version, these paradigms were rebuild all the way down to the physical layer. VEINS 3.0, which was kept compatible with mixed simulations using paradigms from the INET framework, evolved into a legitimate fork of MiXiM as further rebuilding and rewriting occurred in the channel models. VEINS was gradually streamlining and adding more of the above paradigms related to contacting street cars up until the current 6.0 edition. This version is compatible with SUMO 1.8.0 and OMNeT++ 6 (up to the most recent 6.0 pre15 version). There is an online list of all compatible devices in http://veins.car2x.org/.

B. ARCHITECTURE AND BIDIRECTIONAL COUPLING

VEINS does not feature customized mobility models of road cars, despite what would be anticipated. Instead, as shown in Figure 7, it has simulations connected to a specific road traffic simulator that is active as a separate process. In this manner, Veins can gain from the years of study and development by subject matter specialists who have produced fully functional tools for simulating road traffic. VEINS was created to work with the Simulation of Urban MObility (SUMO) road traffic simulator [91], [92]. SUMO is capable of simulating medium-sized to massive road networks in urban areas, cities, and freeways. On them, it is possible to replicate the motion of trains, bicycles, scooters, and other types of street vehicles such as trucks and cars. A variety of mobility models, a selection of intersection controllers, and a variety of road network input formats are all supported by SUMO.

The well-tested road traffic simulations that have lately been made available are a better option. For the SUMO road traffic simulator, some examples are:

- The Bologna ‘‘Pasubia’’ and ‘‘Acosta’’ scenarios [93], Figure 8a shows two regions with a distance of 2 km by 1 km each and a total of 9k trips per area. 3 Featuring traffic driving in a limited area of Bologna’s city center, they can be performed alone or together

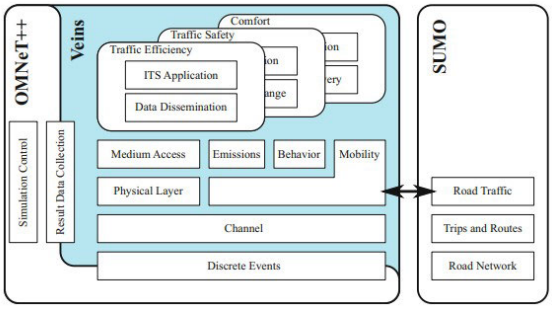

FIGURE 7. High-Level Architecture of VEINS.

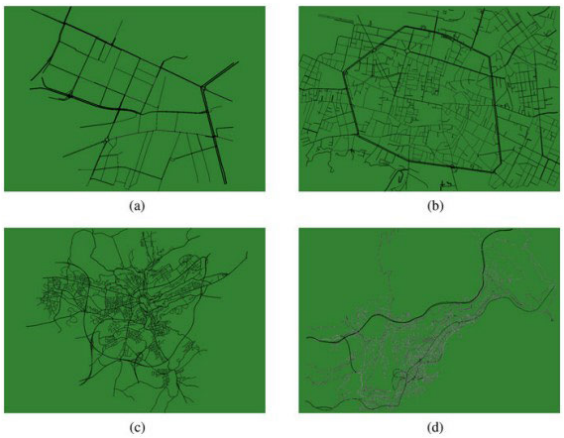

FIGURE 8. Chosen of current openly available maps. (a) Bologna: Pasubia and Acosta. (b) Bologna: Ringway. (c) Luxembourg: LuST. (d) Monaco: MoST [97].

as one larger road traffic scenario. However, caution is advised because no building placements are depicted in the scenario.

- The Bologna "Ringway" scenario [94], Figure 8.b shows the 22k trips over a 4 km by 3 km rectangle. It focuses on the traffic on a major thoroughfare that circles a city. The scenario does not include any building positions, just like the Pasubia and Acosta situations.
- The Luxembourg "LuST" scenario [95], Figure 8.c shows the 288k trips on a 14 km by 11 km rectangle. It contains a whole day's worth of mobility data for an entire city, together with the locations of buildings and parking lots. It is the most and largest comprehensive scenario to date.
- The Monaco "MoST" scenario [96], 18k trips are represented in Figure 8.d over a 10 km by 7 km area. It is still under development and concentrates on multi-modal traffic with additional data on pedestrians, bicycles, and public transportation.

C. THE MAC AND PHY LAYER

VEINS' intricate modeling of the lower levels of inter-vehicle communication is one of its key components (IVC). Most IVC applications and networks need to be reviewed; hence a thorough packet-level simulation employing precise models of the evaluated technology is necessary [98], [99]. The technology in question is frequently IEEE WAVE

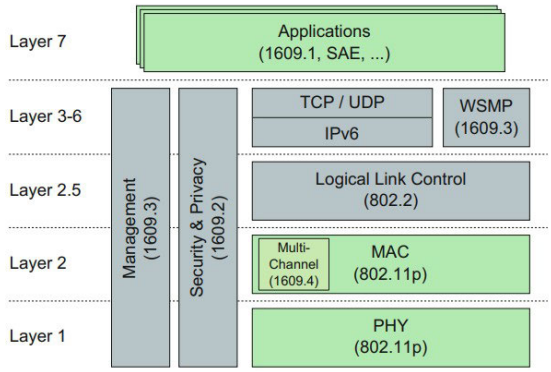

FIGURE 9. The IEEE WAVE family of Standards. PHY, MAC, and Application Layers are Represented in VEINS. (b) Layer Explanation in OMNeT++.

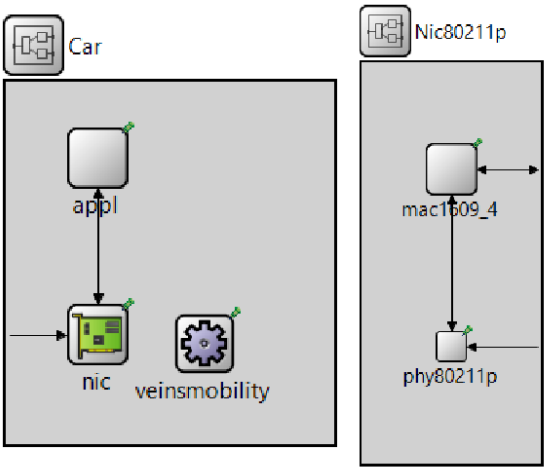

FIGURE 10. Layer representation in OMNeT++.

(or ETSI ITS-G5 in Europe) for vehicular networks. This set of standards' fundamental component is the IEEE 1609ȧ multi-channel operations are utilizing the IEEE 802.11p protocol Medium Access Control (MAC) and Physical Layer (PHY). Figure 9 depicts the stack's overall layout. Although any of these layers and standards can be implemented and integrated, Veins focuses on the bottom layers because they are crucial for the actual channel access and packet transfer [100], [101]. If more protocol levels of the various protocol stacks of ITS protocols around the world are to be represented, other simulators (not included with VEINS, but publically available, such as ARIB T-109 [102]) can be built upon this base.

The explanation of the stack within Veins is shown in Figure 10. To be able to connect with other devices, any node—whether it is a car, a roadside gadget, or even a pedestrian or bicycle using wireless communications—must have at least a Network Interface Card (NIC) based 802.11p. This NIC, which is a compound model made up of the PHY and MAC levels, is directly connected to higher layers. As a result, each node in Veins has a straightforward APP-MAC-PHY architecture. The *veinsmobility* module is in charge of updating the vehicle's position. The mobility in the case of a roadside unit would be a constant *BaseMobility*. Each module in OMNeT++ has the ability to communicate

with other modules if they are connected. These messages can be of any kind descended from cMessage*, including plain text messages and (encapsulated) packets of any particular message format (such as Wave Service Advertisements or Wave Short Messages, for example). Messages within a node can either be ''regular'' messages that are passed to levels below or above or control messages that cause the receiving layer to take a specific action. The receiving layer will execute a separate function depending on the type. The PHY layer is solely connected to the MAC layer and to the outside world, as illustrated in Figures 9 and 10.

VI. CONCLUSION

Recently, using the security aspect for VANET in the VEINS framework has become a key development. Although the research is ongoing, the limits and accompanying descriptions are still unclear. The purpose of current paper is to provide a taxonomized survey of existing research that will contribute to such visions. Particular patterns can be derived from diverse research on security aspects for VANET in the VEINS framework, including infrastructure, hardware and software, and wireless interface to evaluate the effect of attackers. In addition, some security aspects involve modern technologies such as blockchain, machine learning, and SDN in order to provide security in VANET. Other security aspect is also considered in this paper, including privacy, authentication, trust management, reliability, and revocation of the VANET security-based VEINS framework. The works are divided into the following categories: Threats and vulnerabilities, solution technology, and security requirements. The current perspective acknowledged the findings, and published studies on the VANET security procedure in the VEINS framework were given. For upcoming research, this work is important. The community of research will continue to study on and concentrate on this strategy. Therefore, scholars should investigate the changing trends and clever advancements for the security of VANET in the VEINS framework.

REFERENCES

[1] M. J. Haidari and Z. Yetgin, ''Veins based studies for vehicular ad hoc networks,'' in *Proc. Int. Artif. Intell. Data Process. Symp. (IDAP)*, 2019, pp. 1–7.
[2] M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, Z. G. Al-Mekhlafi, A. Qtaish, A. J. Alzahrani, G. Alshammari, A. A. Sallam, and K. Almekhlafi, ''Chebyshev polynomial-based scheme for resisting side-channel attacks in 5G-enabled vehicular networks,'' *Appl. Sci.*, vol. 12, no. 12, p. 5939, Jun. 2022.
[3] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, ''VANet security challenges and solutions: A survey,'' *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017.
[4] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, ''Survey of authentication and privacy schemes in vehicular ad hoc networks,'' *IEEE Sensors J.*, vol. 21, no. 2, pp. 2422–2433, Jan. 2021.
[5] S. S. Manvi and S. Tangade, ''A survey on authentication schemes in VANETs for secured communication,'' *Veh. Commun.*, vol. 9, pp. 19–30, Jul. 2017.
[6] M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, Z. G. Al-Mekhlafi, A. Qtaish, A. J. Alzahrani, G. Alshammari, A. A. Sallam, and K. Almekhlafi, ''CM-CPPA: Chaotic map-based conditional privacy-preserving authentication scheme in 5G-enabled vehicular networks,'' *Sensors*, vol. 22, no. 13, p. 5026, Jul. 2022.
[7] K. L. K. Sudheera, M. Ma, G. M. N. Ali, and P. H. J. Chong, ''Delay efficient software defined networking based architecture for vehicular networks,'' in *Proc. IEEE Int. Conf. Commun. Syst. (ICCS)*, Dec. 2016, pp. 1–6.
[8] C. Sommer. (2020). *Documentation-Veins*. Accessed: Jul. 30, 2022. [Online]. Available: https://veins.car2x.org/documentation/
[9] P. A. Lopez, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y.-P. Flotterod, R. Hilbrich, L. Lucken, J. Rummel, P. Wagner, and E. Wießner, ''Microscopic traffic simulation using SUMO,'' in *Proc. 21st Int. Conf. Intell. Transp. Syst. (ITSC)*, 2018, pp. 2575–2582.
[10] (2020). *OMNet++-Simulation Manual*. Accessed: Jul. 30, 2022. [Online]. Available: https://doc.omnetpp.org/omnetpp/manual/#sec:introduction:what-is-omnetpp
[11] F. Ahmad, V. N. L. Franqueira, and A. Adnane, ''TEAM: A trust evaluation and management framework in context-enabled vehicular ad-hoc networks,'' *IEEE Access*, vol. 6, pp. 28643–28660, 2018.
[12] H. Noori, ''Realistic urban traffic simulation as vehicular ad-hoc network (VANET) via veins framework,'' in *Proc. 12th Conf. Open Innov. Assoc. (FRUCT)*, Nov. 2012, pp. 1–7.
[13] K. Emara, ''Poster: PREXT: Privacy extension for veins VANET simulator,'' in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2016, pp. 1–2.
[14] R. Riebl, H.-J. Gunther, C. Facchi, and L. Wolf, ''Artery: Extending veins for VANET applications,'' in *Proc. Int. Conf. Models Technol. Intell. Transp. Syst. (MT-ITS)*, Jun. 2015, pp. 450–456.
[15] F. J. Martinez, C. K. Toh, J.-C. Cano, C. T. Calafate, and P. Manzoni, ''A survey and comparative study of simulators for vehicular ad hoc networks (VANETs),'' *Wireless Commun. Mobile Comput.*, vol. 11, no. 7, pp. 813–828, 2011.
[16] I. A. Aljabry and G. A. Al-Suhail, ''A survey on network simulators for vehicular ad-hoc networks (VANETS),'' *Int. J. Comput. Appl.*, vol. 174, no. 11, pp. 1–9, Jan. 2021.
[17] J. Santhosh and S. Sankaran, ''Defending against Sybil attacks in vehicular platoons,'' in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Dec. 2019, pp. 1–6.
[18] S. Ucar, S. C. Ergen, and O. Ozkasap, ''IEEE 802.11p and visible light hybrid communication based secure autonomous platoon,'' *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8667–8681, Sep. 2018.
[19] S. Kanumalli, A. Ch, and P. Murty, ''An efficient method for detection of Sybil attackers in IOV,'' *Adv. Model. Anal. B*, vol. 61, no. 1, pp. 5–8, Mar. 2018.
[20] A. Shan, X. Fan, C. Wu, and X. Zhang, ''Quantitative study on impact of static/dynamic selfishness on network performance in VANETs,'' *IEEE Access*, vol. 9, pp. 13186–13197, 2021.
[21] C. A. Kerrache, A. Lakas, and N. Lagraa, ''Detection of intelligent malicious and selfish nodes in VANET using threshold adaptive control,'' in *Proc. 5th Int. Conf. Electron. Devices, Syst. Appl. (ICEDSA)*, Dec. 2016, pp. 1–4.
[22] D. Kosmanos, A. Pappas, L. Maglaras, S. Moschoyiannis, F. J. Aparicio-Navarro, A. Argyriou, and H. Janicke, ''A novel intrusion detection system against spoofing attacks in connected electric vehicles,'' *Array*, vol. 5, Mar. 2020, Art. no. 100013.
[23] I. Saini, S. Saad, and A. Jaekel, ''Speed based attacker placement for evaluating location privacy in VANET,'' in *Proc. Int. Conf. Ad Hoc Netw.* Cham, Switzerland: Springer, 2018, pp. 215–224.
[24] M. Zhou, L. Han, H. Lu, and C. Fu, ''Distributed collaborative intrusion detection system for vehicular ad hoc networks based on invariant,'' *Comput. Netw.*, vol. 172, May 2020, Art. no. 107174.
[25] F. Ahmad, A. Adnane, V. N. Franqueira, F. Kurugollu, and L. Liu, ''Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies,'' *Sensors*, vol. 18, no. 11, p. 4040, 2018.
[26] K. M. Sai, B. B. Gupta, F. Colace, and K. T. Chui, ''A lightweight anomaly based DDoS flood attack detection for Internet of Vehicles,'' M.S. thesis, Dept. Comput. Sci., Fall 2020. [Online]. Available: https://bearworks.missouristate.edu/theses/3580/?utm_source=bearworks.missouristate.edu%2Ftheses%2F3580&utm_medium=PDF&utm_campaign=PDFCoverPages
[27] I. Saini, S. Saad, and A. Jaekel, ''Identifying vulnerabilities and attacking capabilities against pseudonym changing schemes in VANET,'' in *Proc. Int. Conf. Intell., Secure, Dependable Syst. Distrib. Cloud Environ.* Cham, Switzerland: Springer, 2018, pp. 1–15.
[28] K. Sharshembiev, S.-M. Yoo, Y.-K. Kim, and G.-H. Jeong, ''Optimal threshold analysis for triggering fail-safe mechanism in vehicular ad hoc networks,'' in *Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2019, pp. 344–350.

[29] M. Babaghayou, N. Labraoui, A. A. A. Ari, M. A. Ferrag, and L. Maglaras, "The impact of the adversary's eavesdropping stations on the location privacy level in Internet of Vehicles," in *Proc. 5th South-East Eur. Design Autom., Comput. Eng., Comput. Netw. Social Media Conf. (SEEDA-CECNSM)*, Sep. 2020, pp. 1–6.

[30] I. Saini, B. St. Amour, and A. Jaekel, "Intelligent adversary placements for privacy evaluation in VANET," *Information*, vol. 11, no. 9, p. 443, Sep. 2020.

[31] L. Ming, G. Zhao, M. Huang, X. Kuang, J. Zhang, H. Cao, and F. Xu, "A general testing framework based on veins for securing VANET applications," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Oct. 2018, pp. 2068–2073.

[32] K. Sharshembiev, S.-M. Yoo, and E. Elmahdi, "Broadcast storm mitigation from unintentional misbehavior in vehicular ad hoc networks," in *Proc. IEEE 8th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2018, pp. 925–930.

[33] W. Ahmed, W. Di, and D. Mukathe, "Privacy-preserving blockchain-based authentication and trust management in VANETs," *IET Netw.*, vol. 11, nos. 3–4, pp. 89–111, May 2022.

[34] S. A. George, S. M. Stephen, and A. Jaekel, "Blockchain-based pseudonym management scheme for vehicular communication," *Electronics*, vol. 10, no. 13, p. 1584, Jun. 2021.

[35] D. Chulerttiyawong and A. Jamalipour, "A blockchain assisted vehicular pseudonym issuance and management system for conditional privacy enhancement," *IEEE Access*, vol. 9, pp. 127305–127319, 2021.

[36] A. Alharthi, Q. Ni, and R. Jiang, "A privacy-preservation framework based on biometrics blockchain (BBC) to prevent attacks in VANET," *IEEE Access*, vol. 9, pp. 87299–87309, 2021.

[37] S. A. George, A. Jaekel, and I. Saini, "Secure identity management framework for vehicular ad-hoc network using blockchain," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2020, pp. 1–6.

[38] M. A. Hassan, U. Habiba, U. Ghani, and M. Shoaib, "A secure message-passing framework for inter-vehicular communication using blockchain," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 2, Feb. 2019, Art. no. 155014771982967.

[39] U. Arshad, M. Ali Shah, and N. Javaid, "Futuristic blockchain based scalable and cost-effective 5G vehicular network architecture," *Veh. Commun.*, vol. 31, Oct. 2021, Art. no. 100386.

[40] K. Sharshembiev, S.-M. Yoo, and E. Elmahdi, "Protocol misbehavior detection framework using machine learning classification in vehicular ad hoc networks," *Wireless Netw.*, vol. 27, no. 3, pp. 2103–2118, Apr. 2021.

[41] Y. Xia, L. Wu, Z. Wang, X. Zheng, and J. Jin, "Cluster-enabled cooperative scheduling based on reinforcement learning for high-mobility vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 12664–12678, Nov. 2020.

[42] G. R. Reddy and R. Ramanathan, "Performance analysis of clustering for message classification and congestion control in DSRC/WAVE-based vehicular ad-hoc networks," *Int. J. Vehicle Inf. Commun. Syst.*, vol. 4, no. 1, pp. 55–77, 2019.

[43] P. Sharma, H. Liu, H. Wang, and S. Zhang, "Securing wireless communications of connected vehicles with artificial intelligence," in *Proc. IEEE Int. Symp. Technol. Homeland Secur. (HST)*, Apr. 2017, pp. 1–7.

[44] R. P. Nayak, S. Sethi, S. K. Bhoi, D. Mohapatra, R. R. Sahoo, P. K. Sharma, and D. Puthal, "TFMD-SDVN: A trust framework for misbehavior detection in the edge of software-defined vehicular network," *J. Supercomput.*, vol. 78, pp. 7948–7981, Jan. 2022.

[45] M. Mao, P. Yi, T. Hu, Z. Zhang, X. Lu, and J. Lei, "Hierarchical hybrid trust management scheme in SDN-enabled VANETs," *Mobile Inf. Syst.*, vol. 2021, pp. 1–16, Aug. 2021.

[46] R. Prasad Nayak, S. Sethi, S. K. Bhoi, K. S. Sahoo, N. Jhanjhi, T. A. Tabbakh, and Z. A. Almusaylim, "TBDDoSA-MD: Trust-based DDoS misbehave detection approach in Software-Defined Vehicular Network (SDVN)," *Comput., Mater. Continua*, vol. 69, no. 3, pp. 3513–3529, 2021.

[47] R. P. Nayak, S. Sethi, and S. K. Bhoi, "TB-EDA: A trust-based event detection algorithm to detect false events in software-defined vehicular network," in *Intelligent Systems*. Berlin, Germany: Springer, 2021, pp. 413–424.

[48] N. Bagheri, S. Yousefi, and G. Ferrari, "Software-defined control of emergency vehicles in smart cities," in *Proc. 10th Int. Conf. Comput. Knowl. Eng. (ICCKE)*, Oct. 2020, pp. 519–524.

[49] M. S. Rayeni and A. Hafid, "Routing in heterogeneous vehicular networks using an adapted software defined networking approach," in *Proc. 5th Int. Conf. Softw. Defined Syst. (SDS)*, Apr. 2018, pp. 25–31.

[50] A. Kazmi, M. A. Khan, and M. U. Akram, "DeVANET: Decentralized software-defined VANET architecture," in *Proc. IEEE Int. Conf. Cloud Eng. Workshop (ICEW)*, Apr. 2016, pp. 42–47.

[51] S. Guntuka, E. M. Shakshuki, A. Yasar, and H. Gharrad, "Vehicular data offloading by road-side units using intelligent software defined network," *Proc. Comput. Sci.*, vol. 177, pp. 151–161, Jan. 2020.

[52] M. Babaghayou, N. Labraoui, A. A. A. Ari, M. A. Ferrag, L. Maglaras, and H. Janicke, "WHISPER: A location privacy-preserving scheme using transmission range changing for Internet of Vehicles," *Sensors*, vol. 21, no. 7, p. 2443, Apr. 2021.

[53] W. Bouksani and B. A. Bensaber, "RIN: A dynamic pseudonym change system for privacy in VANET," *Concurrency Comput., Pract. Exper.*, vol. 31, no. 24, p. e4719, Dec. 2019.

[54] M. Babaghayou and N. Labraoui, "Transmission range adjustment influence on location privacy-preserving schemes in VANETs," in *Proc. Int. Conf. Netw. Adv. Syst. (ICNAS)*, Jun. 2019, pp. 1–6.

[55] F. Zidani, F. Semchedine, and M. Ayaida, "Estimation of neighbors position privacy scheme with an adaptive beaconing approach for location privacy in VANETs," *Comput. Electr. Eng.*, vol. 71, pp. 359–371, Oct. 2018.

[56] W. Bouksani and B. A. Bensaber, "An efficient and dynamic pseudonyms change system for privacy in VANET," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2017, pp. 59–63.

[57] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "Towards an efficient pseudonym management and changing scheme for vehicular ad-hoc networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–7.

[58] A. M. Carianha, L. P. Barreto, and G. Lima, "Improving location privacy in mix-zones for VANETs," in *Proc. 30th IEEE Int. Perform. Comput. Commun. Conf.*, Nov. 2011, pp. 1–6.

[59] S. U. A. Laghari, S. Manickam, A. K. Al-Ani, M. A. Al-Shareeda, and S. Karuppayah, "ES-SECS/GEM: An efficient security mechanism for SECS/GEM communications," *IEEE Access*, vol. 11, pp. 31813–31828, 2023.

[60] M. Arif, J. Chen, G. Wang, O. Geman, and V. E. Balas, "Privacy preserving and data publication for vehicular trajectories with differential privacy," *Measurement*, vol. 173, Mar. 2021, Art. no. 108675.

[61] P. K. Singh, S. N. Gowtham, and S. Nandi, "CPESP: Cooperative pseudonym exchange and scheme permutation to preserve location privacy in VANETs," *Veh. Commun.*, vol. 20, Dec. 2019, Art. no. 100183.

[62] L. Wei, J. Cui, Y. Xu, J. Cheng, and H. Zhong, "Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1681–1695, 2021.

[63] M. A. Al-Shareeda and S. Manickam, "MSR-DoS: Modular square root-based scheme to resist denial of service (DoS) attacks in 5G-enabled vehicular networks," *IEEE Access*, vol. 10, pp. 120606–120615, 2022.

[64] G. Luo, M. Shi, C. Zhao, and Z. Shi, "Hash-chain-based cross-regional safety authentication for space-air-ground integrated VANETs," *Appl. Sci.*, vol. 10, no. 12, p. 4206, Jun. 2020.

[65] C. Zhao, M. Shi, M. Huang, and X. Du, "Authentication scheme based on hashchain for space-air-ground integrated network," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.

[66] Y. Xie, F. Xu, D. Li, and Y. Nie, "Efficient message authentication scheme with conditional privacy-preserving and signature aggregation for vehicular cloud network," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–12, Sep. 2018.

[67] U. Rajput, F. Abbas, H. Eun, and H. Oh, "A hybrid approach for efficient privacy-preserving authentication in VANET," *IEEE Access*, vol. 5, pp. 12014–12030, 2017.

[68] A. Bendouma and B. A. Bensaber, "RSU authentication by aggregation in VANET using an interaction zone," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[69] Z. G. Al-Mekhlafi, M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, A. Alreshidi, M. Alazmi, J. S. Alshudukhi, M. Alsaffar, and A. Alsewari, "Chebyshev polynomial-based fog computing scheme supporting pseudonym revocation for 5G-enabled vehicular networks," *Electronics*, vol. 12, no. 4, p. 872, Feb. 2023.

[70] F. Altaf and S. Maity, "PLHAS: Privacy-preserving localized hybrid authentication scheme for large scale vehicular ad hoc networks," *Veh. Commun.*, vol. 30, Aug. 2021, Art. no. 100347.

[71] Z. G. Al-Mekhlafi, M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, and A. Qtaish, "Lattice-based lightweight quantum resistant scheme in 5G-enabled vehicular networks," *Mathematics*, vol. 11, no. 2, p. 399, Jan. 2023.
[72] S. M. Pournaghi, B. Zahednejad, M. Bayat, and Y. Farjami, "NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET," *Comput. Netw.*, vol. 134, pp. 78–92, Apr. 2018.
[73] M. A. Al-Shareeda and S. Manickam, "COVID-19 vehicle based on an efficient mutual authentication scheme for 5G-enabled vehicular fog computing," *Int. J. Environ. Res. Public Health*, vol. 19, no. 23, p. 15618, Nov. 2022.
[74] R. W. Van Der Heijden, A. Al-Momani, F. Kargl, and O. M. F. Abu-Sharkh, "Enhanced position verification for VANETs using subjective logic," in *Proc. IEEE 84th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2016, pp. 1–7.
[75] T. B. M. de Sales, A. Perkusich, L. M. de Sales, H. O. de Almeida, G. Soares, and M. de Sales, "ASAP-V: A privacy-preserving authentication and Sybil detection protocol for VANETs," *Inf. Sci.*, vol. 372, pp. 208–224, Dec. 2016.
[76] I. A. Rai, R. A. Shaikh, and S. R. Hassan, "A hybrid dual-mode trust management scheme for vehicular networks," *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 7, Jul. 2020, Art. no. 155014772093937.
[77] L. M. Santos J. and E. Moreira, "An evaluation of reputation with regard to the opportunistic forwarding of messages in VANETs," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, pp. 1–14, Dec. 2019.
[78] B. A. Mohammed, M. A. Al-Shareeda, S. Manickam, Z. G. Al-Mekhlafi, A. Alreshidi, M. Alazmi, J. S. Alshudukhi, and M. Alsaffar, "FC-PA: Fog computing-based pseudonym authentication scheme in 5G-enabled vehicular networks," *IEEE Access*, vol. 11, pp. 18571–18581, 2023.
[79] F. Boeira, M. Asplund, and M. Barcellos, "Decentralized proof of location in vehicular ad hoc networks," *Comput. Commun.*, vol. 147, pp. 98–110, Nov. 2019.
[80] I. Souissi, N. B. Azzouna, and T. Berradia, "Towards a self-adaptive trust management model for VANETs," in *Proc. 14th Int. Joint Conf. E-Business Telecommun.*, 2017, pp. 738–748.
[81] W. Benrhaiem and A. S. Hafid, "Bayesian networks based reliable broadcast in vehicular networks," *Veh. Commun.*, vol. 21, Jan. 2020, Art. no. 100181.
[82] M. A. Al-Shareeda, M. Anbar, S. Manickam, I. H. Hasbullah, A. Khalil, M. A. Alazzawi, and A. S. Al-Hiti, "Proposed efficient conditional privacy-preserving authentication scheme for V2V and V2I communications based on elliptic curve cryptography in vehicular ad hoc networks," in *Proc. Int. Conf. Adv. Cyber Secur.* Penang, Malaysia: Springer, 2021, pp. 588–603.
[83] H. Kumar and D. Singh, "Smart certificate revocation list exchange in VANET," in *Proc. 12th Int. Conf. Comput. Intell. Commun. Netw. (CICN)*, Sep. 2020, pp. 210–214.
[84] N. Malik, P. Nanda, A. Arora, X. He, and D. Puthal, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 674–679.
[85] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved IVC analysis," *IEEE Trans. Mobile Comput.*, vol. 10, no. 1, pp. 3–15, Jan. 2010.
[86] D. Eckhoff and C. Sommer, "A multi-channel IEEE 1609.4 and 802.11p EDCA model for the veins framework," in *Proc. 5th ACM/ICST Int. Conf. Simul. Tools Techn. Commun.*, Desenzano, Italy, Mar. 2012.
[87] M. A. Al-shareeda, M. Anbar, S. Manickam, I. H. Hasbullah, N. Abdullah, M. M. Hamdi, and A. S. Al-Hiti, "NE-CPPA: A new and efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks (VANETs)," *Appl. Math.*, vol. 14, no. 6, pp. 1–10, 2020.
[88] F. Hagenauer, F. Dressler, and C. Sommer, "Poster: A simulator for heterogeneous vehicular networks," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2014, pp. 185–186.
[89] M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, Z. G. Al-Mekhlafi, A. Qtaish, A. J. Alzahrani, G. Alshammari, A. A. Sallam, and K. Almekhlafi, "Provably secure with efficient data sharing scheme for fifth-generation (5G)-enabled vehicular networks without road-side unit (RSU)," *Sustainability*, vol. 14, no. 16, p. 9961, Aug. 2022.
[90] A. Memedi, H.-M. Tsai, and F. Dressler, "Impact of realistic light radiation pattern on vehicular visible light communication," in *Proc. IEEE Global Commun. Conf.*, Dec. 2017, pp. 1–6.
[91] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO—Simulation of urban mobility," in *Proc. 3rd Int. Conf. Adv. Syst. Simul.*, 2011, pp. 1–6.
[92] M. A. Al-Shareeda and S. Manickam, "Man-in-the-middle attacks in mobile ad hoc networks (MANETs): Analysis and evaluation," *Symmetry*, vol. 14, no. 8, p. 1543, Jul. 2022.
[93] L. Bieker, D. Krajzewicz, A. Morra, C. Michelacci, and F. Cartolano, "Traffic simulation for all: A real world traffic scenario from the city of Bologna," in *Modeling Mobility With Open Data*. Berlin, Germany: Springer, 2015, pp. 47–60.
[94] L. Bedogni, M. Gramaglia, A. Vesco, M. Fiore, J. Härri, and F. Ferrero, "The Bologna ringway dataset: Improving road network conversion in SUMO and validating urban mobility via navigation services," *IEEE Trans. Veh. Technol.*, vol. 64, no. 12, pp. 5464–5476, Dec. 2015.
[95] L. Codeca, R. Frank, and T. Engel, "Luxembourg SUMO traffic (LuST) scenario: 24 hours of mobility for vehicular networking research," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2015, pp. 1–8.
[96] L. Codeca and J. Harri, "Towards multimodal mobility simulation of C-ITS: The Monaco SUMO traffic scenario," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Nov. 2017, pp. 97–100.
[97] C. Sommer, D. Eckhoff, A. Brummer, D. S. Buse, F. Hagenauer, S. Joerer, and M. Segata, "Veins: The open source vehicular network simulation framework," in *Recent Advances in Network Simulation*. Berlin, Germany: Springer, 2019, pp. 215–252.
[98] D. Eckhoff, C. Sommer, and F. Dressler, "On the necessity of accurate IEEE 802.11p models for IVC protocol simulation," in *Proc. IEEE 75th Veh. Technol. Conf. (VTC Spring)*, May 2012, pp. 1–5.
[99] Z. G. Al-Mekhlafi, M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, A. Alreshidi, M. Alazmi, J. S. Alshudukhi, M. Alsaffar, and T. H. Rassem, "Efficient authentication scheme for 5G-enabled vehicular networks using fog computing," *Sensors*, vol. 23, no. 7, p. 3543, Mar. 2023.
[100] D. Eckhoff, N. Sofra, and R. German, "A performance study of cooperative awareness in ETSI ITS G5 and IEEE WAVE," in *Proc. 10th Annu. Conf. Wireless Demand Netw. Syst. Services (WONS)*, Mar. 2013, pp. 196–200.
[101] B. A. Mohammed, M. A. Al-Shareeda, S. Manickam, Z. G. Al-Mekhlafi, A. M. Alayba, and A. A. Sallam, "ANAA-Fog: A novel anonymous authentication scheme for 5G-enabled vehicular fog computing," *Mathematics*, vol. 11, no. 6, p. 1446, Mar. 2023.
[102] J. Heinovski, F. Klingler, F. Dressler, and C. Sommer, "A simulative analysis of the performance of IEEE 802.11p and ARIB STD-T109," *Comput. Commun.*, vol. 122, pp. 84–92, Jun. 2018.

MAHMOOD A. AL-SHAREEDA received the B.S. degree in communication engineering from Iraq University College and the M.Sc. degree in information technology from the Islamic University of Lebanon (IUL), in 2018. He is currently a Postdoctoral Fellow with the National Advance IPv6 Center (NAv6), Universiti Sains Malaysia (USM). His research interests include security and privacy issues in vehicular ad hoc networks (VANETs) and network optimization.

SELVAKUMAR MANICKAM is currently the Director of the National Advanced IPv6 Centre and an Associate Professor specializing in cybersecurity, the Internet of Things, Industry 4.0, cloud computing, big data, and machine learning. He has experience building the IoT, embedded, server, mobile, and web-based applications. He has given several keynote speeches and dozens of invited lectures and workshops at conferences, international universities, and industry. He also lectures in various computer science and IT courses, including developing new courseware in tandem with current technology trends. He has authored or coauthored more than 220 articles in journals, conference proceedings, and book reviews, and graduated 18 Ph.D. students in addition to master's and bachelor's students.