A Critical Review of Software Defined Networks Enabled Vehicular Ad Hoc Network

Moawiah El-Dalahmeh*, Adi El-Dalahmeh, and Usman Adeel

***Abstract*—Software-Defined Networking (SDN) enabled Vehicular Ad-hoc Networks (VANETs) are a new paradigm for vehicular communication that leverages the benefits of SDN to improve the efficiency, reliability, and security of VANETs. In an SDN-based VANET, the traditional centralized control plane architecture is replaced by a SDN controller that manages the network's routing decisions. The controller has a global view of the network topology and can dynamically adjust the routing paths based on changing traffic conditions, environmental factors. While SDN enabled VANETs offer many benefits, there are also several challenges. Security is a critical concern in SDN enabled VANET architectures must address such as authentication, access control, and data privacy. Therefore, the researcher presents authentication approach to solve the challenges. However, the authentication framework still has challenges in privacy, security, cost. Therefore, in this paper we summarize the existing authentication scheme to determine the limitation and the future direction.**

***Index Terms*—SDN (Software-defined networking), VANET (vehicular ad hoc network), security, authentication**

I. Introduction

VANETs have become a readily available technology to enhance road safety and transportation efficiency. With continuous advancements in VANET technologies, they are now being recognized as networks capable of offering a variety of services such as vehicular cloud computing, surveillance, IoT-based advertising, and safety traffic management [1]. However, due to the differing node densities and high mobility of VANETs, it is still challenging to coordinate them to provide efficient services with various QoS requirements. Therefore, programmable networking architectures have become essential for VANETs to support inter-operation among diverse networks, manage a large number of mobile nodes (or users) with smart devices, and allocate resources effectively [1, 2].

SDN-enabled VANET architectures have emerged as promising technologies in recent times, with significant potential for simplifying network management and promoting innovation through network programmability [2]. Both academia and industry have taken a keen interest in these technologies. SDN technology allows for the separation of control and data planes in SDN-enabled VANET, resulting in an abstraction for VANET applications to the underlying networking infrastructure, as well as logically centralized networking intelligence and network state [3]. The merging of SDN with VANET represents a crucial direction that can tackle most of the challenges encountered by VANETs, especially with the help of SDN's significant features like a current global topology that enables dynamic management of networking resources and efficient networking services, ultimately enhancing the user experience [4]. These SDN features can cater to the advanced demands of VANETs, such as high throughput, high mobility, low communication latency, heterogeneity, scalability, among others.

The complete conversion of current VANETs into SDN-enabled VANETs is still ambiguous until the security, scalability, and reliability of data communication issues regarding SDN are wholly resolved [1-6]. The centralization of network logic control (or intelligence) and the escalating rate of cyber-attacks render emerging SDN-enabled VANETs more susceptible to threats than current VANETs [6]. Furthermore, the latest entities and structural components used in the current SDN-enabled VANET are creating new attack surfaces and vulnerabilities that are currently unknown. Therefore, in this paper, we review the existing privacy-preserving schemes to determine the limitations and challenges in network security and privacy. Our contributions to this paper are highlighted as:

- The paper provided a detail about SDN enabled VANET, including its features, communications, applications, and challenges.
- The paper addressed multiple privacy preserving authentication scheme from different perspective like security, privacy, and scalability to determine the limitations and challenges.

II. Overview of SDN Enabled VANET

In this section we will discuss SDN enabled VANET features, communication, application, and attacks.

A. SDN Enabled VANET Features

SDN enabled VANET architecture provides several features that improve network management and facilitate innovation. Some of the significant features are [7]:

- Programmability: SDN enabled VANETs are highly programmable, allowing for the automation of network management tasks, such as network configuration, monitoring, and troubleshooting.
- Centralized Control: The centralized control plane of SDN enabled VANET architecture allows for efficient management of network resources, such as bandwidth and routing, resulting in better network performance and resource utilization.

Manuscript received May 1, 2023; revised July 2, 2023; accepted August 15, 2023.

Moawiah El-Dalahmeh, Adi El-Dalahmeh, and Usman Adeel are with the School of Computing, Engineering and Digital Technologies, Teesside University, United Kingdom.

*Correspondence: M.El-Dalahmeh@tees.ac.uk (M.E.D.)

- Global Network Visibility: SDN enabled VANETs provide global network visibility, enabling network administrators to monitor and manage network traffic in real-time.
- Scalability: SDN enabled VANETs are highly scalable, allowing for the deployment of new network services and applications without the need for extensive hardware upgrades.
- Flexibility: SDN enabled VANETs are highly flexible, enabling the creation of multiple virtual networks on the same physical infrastructure, reducing network deployment costs, and improving network flexibility.

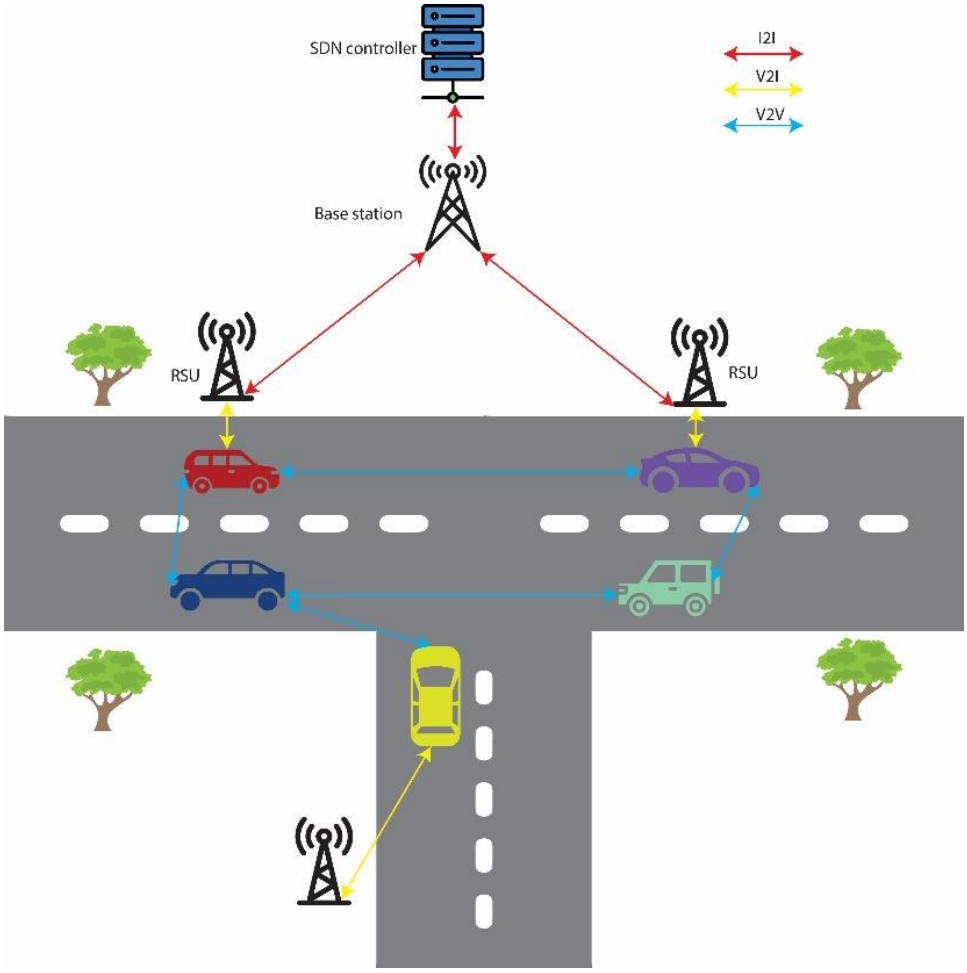

Fig. 1. SDN based VANET communication.

B. SDN Enabled VANET Communication

SDN-enabled VANET communication refers to the exchange of data between vehicles or between vehicles and roadside infrastructure (such as traffic lights or sensors) using wireless communication technologies. SDN enabled VANETs are designed to improve road safety and transportation efficiency by enabling vehicles to communicate with each other and with the surrounding environment in real time [8].

SDN enabled VANET communication can be categorized into three types: vehicle-to-vehicle (V2V) communication allows vehicles to communicate directly with other nearby vehicles, enabling them to share information about road conditions, traffic flow, and potential hazards. Communication enables vehicles to communicate with roadside infrastructure (V2I), providing information about traffic signals, roadwork, or other relevant data. V2X communication refers to the integration of V2V and V2I

communication, allowing vehicles to communicate with any available network resources, including other vehicles, infrastructure, or the cloud. Also, they enable infrastructure component to communicate each other (I2I). Fig. 1. presents SDN enabled VANET communication.

C. SDN Enabled VANET Applications

SDN enabled VANET applications are designed to enhance road safety and transportation efficiency by utilizing the communication capabilities of SDN enabled VANETs. Some of the applications are [9]:

- Safety applications: These applications are designed to prevent accidents and reduce fatalities by providing drivers with real-time information about traffic conditions, road hazards, and potential collisions. Some examples of safety applications are collision warning systems, intersection collision avoidance systems, and lane departure warning systems.
- Traffic management applications: These applications are designed to improve traffic flow and reduce congestion by providing real-time traffic data to drivers and traffic management authorities. Some examples of traffic management applications are real-time traffic congestion detection, intelligent traffic signal control,

and dynamic route guidance.

- Entertainment applications: These applications are designed to enhance the driving experience by providing entertainment content, such as music, video, and games. These applications are typically accessed through a vehicle's infotainment system.

D. Attacks in SDN Enabled VANET

SDN enabled VANETs are vulnerable to various attacks, including [10]:

- Sybil attacks: In a Sybil attack, an attacker creates multiple fake identities or nodes in the VANET to control and manipulate network behavior.
- Denial-of-Service (DoS) attacks: In a DoS attack, an attacker floods the network with a large amount of data or requests, causing network congestion and preventing legitimate communication.
- Message falsification attacks: In a message falsification attack, an attacker intercepts and alters legitimate messages exchanged between vehicles, causing false information to be propagated throughout the VANET.
- Physical attacks: Physical attacks involve the physical destruction or damage to network components, such as roadside units or vehicles, resulting in the disruption of VANET communication.

III. Literature Survey

This section deals with multifarious existing research on authentication framework for vehicle communications.

Adnan *et al*. [11] propounded a secured network model for supporting the VANET, aided by the SDN paradigm. The research considered vehicle-to-vehicle communication and vehicle-to-infrastructure to secure the transmitted data. For this, they proposed a public key-based digital signature scheme generated by the trusted advisor. The main entities of this research paper included master controllers, slave controllers, cloud servers, trusted advisor, RSU, base stations, and vehicles. Communication between every entity was secured through a digital signature scheme, i.e., vehicle to vehicle, vehicle to RSU, RSU to controller, and slave controller to master controller. Data transmitted between the network entities must be signed by the sender using a digital signature to ensure information integrity. In addition, communication between the controllers was ensured through a 3-way handshake method; distrusted controllers were removed from the network. Finally, the proposed scheme was evaluated through AVISPA simulation tool, and the authors mentioned that the work satisfied all the system security properties.

Wu *et al.* [12] introduced an authentication framework using a cryptographic key distribution system in a fog enabled VANET. The main objective of this research was to improve communication security between the fog paradigm and vehicular networks. The major entities included in this work were vehicles, access points, fog servers, and cloud servers, and the paper stated three essential progressions: the users registration stage, the fog server registration stage, and the login stage. The cloud server was accountable for the entities' registration. Here, the fog server acts as the coordinator between VANET users and cloud platform. To ensure high security between the users and fog server, a common session token was established to authenticate each one. During user (vehicle) registration, passwords, identity, and biometrics were acquired by the cloud server, which then offered the secret card. A random number and server ID were acquired from the fog servers and a pseudo-identity was returned to them by the cloud server. The registration phase can be formulated as:

$$\begin{aligned} Ve \rightarrow ID, BIO, \& PW \rightarrow CS \\ Fs \rightarrow ID \& RN \rightarrow CS \end{aligned} \quad (1)$$

where Ve represents vehicle, Fs stands for fog server, ID depicts identity, BIO stands for biometrics, PW stands for password, RN represents random number, and CS stands for cloud server. The proposed work analysed security through ProVerif and Burrows–Abadi–Needham (BAN) logic. This work secured the communication between the fog server and cloud server but the communication between the users and fog nodes used a public channel, and hence this affects security at the bottom layer.

Zhong *et al.* [13] worked on a condition-based secure and lightweight authentication scheme in fog computing-assisted VANET. To mitigate the conventional conditional privacy-based authentication schemes in terms of key escrow problems, this paper introduced an elliptic curve cryptographic-based lightweight authentication scheme. In addition, a hash-centred chain generated pseudonyms for the vehicles, which minimises storage-oriented problems. The work was composed of several progressions, namely initialisation, registration, cryptographic keys and pseudonym creation, and authentication. Initially, all the vehicles were registered with the trusted advisor and then each vehicle created cryptographic keys and pseudorandom numbers themselves. To do so, a token for securing the communication was requested by the vehicles from the trusted advisor or fog nodes. During message broadcasting, every vehicle had to sign their messages for verification purposes. Having the vehicles generate their own keys and pseudonyms mitigated the problem of key escrow problems in this work. As per the system evaluation, the proposed work offered better performance in terms of the time taken to generate credentials and the minimisation of computational and communication overhead. However, this research allowed the vehicles to generate pseudonyms and secret keys themselves, and so the presence of insider attacks cannot be diminished.

Zhang *et al.* [14] dealt with a lightweight protocol for the verification of batches in the VANET, which was supported by the fog computing paradigm. The main intention of the authors was to overcome the existing research problems of computation and communication overhead as well as security issues by proposing lightweight cryptographic means. Specifically, a public key-based scheme was presented, i.e., elliptic curve cryptography. Here, fog devices, trusted advisors, a cloud server, and vehicles were considered the main entities. The main responsibility of the trusted advisor was to handle the vehicles registration and track attacker nodes. Moreover, fog nodes were entirely managed by the trusted authority and its roles were allocated to process vehicle data. To minimise the time taken for verification,

bilinear operation was excluded from the cryptographic system. The authors concluded that their model preserved conditional privacy during the evaluation using random oracle. In addition, the experimental results showed that the work outperformed others on communication and computation overhead. However, the management of the system is complex due to poor network flexibility.

Mei *et al.* [15] presented a framework that combined agreement based on cryptographic keys and authentication in VANET, taking into account RSU cache memory. The network components in this work were RSU, vehicles, and the trusted authority, and the progressions included initialisation, entity registration, RSU cluster formation, and key modification. The main objectives were to establish secure communication during vehicle mobility. Authentication-based details were securely disseminated within the network to minimise the complexity of authentication. The main reason for adopting the RSU cache memory was to improvise the efficacy of agreement on cryptographic keys. Here, each RSU-situated location was headed by an RSU cluster leader; when a node entered the range of a cluster, other cluster members collected the authentication-oriented information and forwarded it to the cluster leader. The leader node distributed the authenticated vehicle information in the network. Further, a session key was used to reduce the number of authentications held when entering the regions of different RSU. In doing so, the number of authentications is reduced but system security can be lost.

Wang *et al.* [16] proposed in which intent-centred networking was given weight. The main aim of this research was to secure the location information of internet-stemmed vehicles. As location information has become basic information in most of internet-connected things, the authors of this research work proposed an intent forecasting technique. More specifically, this technique helped identify the intent of location admittance as well as reprimand illegitimate location queries. As the location information was critical, security for location was prioritised. The entities in the system model were internet-connected vehicles, an intent-based networking control unit, location privacy shielding unit, and other applications. A machine learning algorithm was embedded with an intent-based networking unit to predict the intent of location access. Further, virtual money was provided to the vehicles to obtain location admittance approval. Specifically, each vehicle was urged to spend that money to obtain location access. In doing so, the authors stated that they were able to limit illegitimate location access.

Kong *et al.* [17] performed secure seamless data acquisition in a fog-enabled cloud environment by the incorporation of prognostic preservation. They used a slide window-based approach to maintain and structure the data, sensed through vehicle sensors. Further, alpha geometric and homomorphic cryptographic schemes were used to secure the sensed data and realise differential privacy benefits. The proposed work was composed of three consecutive layers: the cloud, fog, and vehicles. In each layer, different entities were positioned. The cloud layer was embedded with the cloud server, the fog layer was positioned with storage devices, and the vehicles layer was filled with OBU-enabled vehicles. Further, the information from the vehicles was verified by their signatures. Finally, the proposed work's security was analysed through privacy preservation, verifiable condition, and confidentiality. At the end of the discussion, the authors concluded that the proposed work had better computational performance and communication overhead. Apart from these factors mean squared error was also taken into account to demonstrate the work's efficacy. However, the research work used different privacy mechanisms to ensure security and the intended receiving node also handled noisy information.

Wei *et al*. [18] proposed a lightweight security mechanism in the VANET by introducing a tree-centred cryptographic security agreement. The communication standard considered in this work was vehicle-to-vehicle communication and vehicle-to-infrastructure and the basic entities were a trusted authority, RSU, and vehicles. More than five processes were performed, including system initialisation, registration of vehicles, and registration of RSU, authentication of the vehicle and RSU, responses, and key restoration. ID and a random number were acquired from the vehicles and RSU during registration. Initially, the sensed data were aggregated by the fog storage devices and cyclically updated the cloud server. Tripartite authentication was used for registration, in which a public session-based key was given to the vehicles and RSU by the trusted authority. The experimental results showed that the proposed work outperformed other research work in terms of computation and communication overhead, and key establishment latency. However, this research offered a public key for all authenticated vehicles and thus insider attackers can take advantage, resulting in security issues.

Soleymani *et al.* [19] attempted to secure a fog assisted VANET by proposing a security framework in which nodes and their information were authenticated. A pretending node was used to spread untrusted information in the network to obtain the most reliable benefits. The main objective of this study was to achieve high security by introducing three progressions as node authentication, message verification, and trust method to deal with illegitimate nodes. The authors embedded several entities into their model, namely: a cloud server, the trusted authority, access points (treated as edge fog entities), and vehicles. The first stage was system initialisation, in which the trusted authority loaded essential information into the fog entities and vehicles. Then, entities were registered to allow network participation. Further, the integrity of data was ensured by message authentication; when an entity communicated with other entities, the messages had to be signed. Further, two different trust values were considered in this work to enhance security. An issue with this work, however, is that authentication of the messages only on the basis of trust is poor compared to cryptographic schemes.

Zhong *et al.* [20] proposed a security framework based on authentication in the SDN-based VANET. The main objective of this research paper was to enhance security and increase the flexibility of the VANET by anonymous authentication techniques and SDN, respectively. The work was composed of several network entities: a base station, access point, software unit, and transport leader, and global and multiple local SDN controllers. First, weight values were

estimated to the vehicles based on different factors such as the condition of the roads, the number of messages sent by the vehicles, energy, distance, speed of traffic, and so on. Then, the messages sent by the vehicles were signed by the sender to ensure legitimacy, with the intention of securing the communication between the vehicles and minimising malicious vehicle participation. However, this research was limited in terms of the distant controller placement, which increases communication latency and energy consumption.

TABLE I: SUMMERY OF THE AUTHENTICATION SCHEMES

Ref.	Research Objective	Method/Algorithm	Limitations
Adnan *et al.* [11]	Secure and efficient design for safeguarding SDN-enabled VANET	PKI (Public Key Infrastructure) based signature technique	Poor security Huge processing cost
Wu *et al.* [12]	Secure the communication among FN (fog node), VN (vehicular node), and RSU	Improved authentication key exchange	Less intelligent
Zhong *et al.* [13]	Preserve the privacy of fog assisted VANET by using a lightweight authentication	Enhanced conditional-based privacy-preserving authentication	Poor security measures
Zhang *et al.* [14]	Ultra-lightweight protocol was designed to circumvent the security risk and increased communication cost burden	Public key-based scheme	Less system flexibility
Mei *et al.* [15]	RSU cache history utility to minimise the complexities inherited during authentication	Common session key-based approach	Low system security
Wang *et al.* [16]	To rescue the internet of connected vehicles in terms of limiting the illegitimate location access	Intent-based networking approach	Less informative
Kong *et al.* [17]	Increase the security during the collection of data in the cloud-fog-enabled vehicular network	Differential privacy mechanism and homomorphic-based technique	Impractical for real-time applications
Wei *et al.* [18]	Minimise the security vulnerabilities in V2I and V2V communications in VANET	Tree structure-based authenticated key agreement	Increased insider attackers' rate
Soleymani *et al.* [19]	Ensure the vehicular node and its data legitimacy	Data and nodes combined authentication scheme	Poor data integrity verification scheme
Zhong *et al.* [20]	Strengthen SDVANET security by excluding malicious nodes from the environment	Threshold- and conditional-based privacy-preserving authentication scheme	Ineffective vehicular node management
Wu *et al.* [21]	Reduce security threats and lower burden on cloud servers using fog computing paradigm	Improved and computation-friendly authentication protocol	Minimal protocol security
Wei *et al.* [22]	Improve security practices in VANET by concurrent secret key updating progression	Shamir's secret key-based technique	Huge key extraction time

Wu *et al.* [21] explored security in the social internet of vehicles, supplemented with a fog computing paradigm. The entities were the cloud server, fog servers, and internet connection-enabled vehicles. Further, an agreement-centred lightweight session-based security key was used to authenticate both fog entities and vehicles mutually. During mutual authentication, the cloud server established the consecutive processes of fog (random number and ID) and vehicle (password, random number, and ID) registration to generate a pseudo-identity and, based on this, authentication held. The authors noted that their proposed method had better performance than other works in terms of cost of communication as well as power required for computation. However, communication between the RSU and vehicles is prone to security vulnerabilities.

Wei *et al.* [22] considered the security-oriented problems arising from conventional condition-based authentication and the delay sensitivity of network traffic. The predominant entities in this work were vehicles and a trusted advisor, and elliptic curve cryptography was utilised. Two main issues were addressed: disk overhead and latency issues of emergency messages; and the lack of secret key updating in classical authentication schemes. To resolve these issues, a condition-centred authentication method was proposed by incorporating a discrete logarithm-based elliptic curve which secured as well as mitigated the overhead problem. Pseudo-random numbers and secret key updating techniques were based on the Shamir key-sharing method. The proposed work included different performance metrics such as transmission latency and resource utilisation (storage). Table I discuss the existing authentication scheme.

IV. OPEN RESEARCH ISSUES

In this section, we will discuss the potential research directions, future issues, and challenges. As evidenced by the numerous research studies we have reviewed in our survey, both the industry and academia are focusing on developing

authentication frameworks for SDN-enabled VANETs. This shift is due to the emergence of innovative applications such as 6G, Automated Transport Systems, and the Internet of Vehicles, which have strict requirements for robustness, flexibility, low latency for real-time decision making, security, and privacy.

- Security and privacy are essential requirements for SDN-enabled VANETs due to their use in mission-critical and life-sensitive applications. For example, an attacker could maliciously take control of vehicles in an Intelligent Transport System or driverless scenario, resulting in severe damage to infrastructure and human life. Additionally, the sensitive information of drivers and vehicles, such as location or travel route, could be leaked from a centralized controller. Therefore, the development of privacy-preserving schemes remains an important area for improving the network's security level.
- SDN-enabled VANETs face a challenging task of interworking with heterogeneous networks as their future is not limited to communication between vehicles only. As new technologies and devices with multiple features from different manufacturers are introduced, mutual exclusiveness can become a problem, resulting in communication failure between vehicles. To address this issue, technology standardization is necessary. Additionally, due to the large number of vehicles, common problems such as collisions, long delays, increased packet loss rates, interference, and noise can occur. Therefore, existing heterogeneous V2X networks require efficient interworking mechanisms to cope with real-world scenarios.

V. Conclusion

The SDN-based VANET architecture offers many benefits for vehicular communication and has the potential to revolutionize the way we design and deploy VANETs in the future. However, it is still having challenges such as: secure communication: SDN enabled VANET are susceptible to various attacks, such as eavesdropping, spoofing, and tampering. Also, privacy SDN enabled VANETs contain sensitive information about vehicles and their movements and preserving the privacy of this information is crucial.

To address these challenges, SDN-based VANETs can use various authentication mechanisms such as digital certificates, public-key infrastructure (PKI), and mutual authentication. Additionally, a combination of physical and cryptographic authentication methods can also be used to improve the security of the network. However, finding the right balance between security and efficiency is critical to ensuring the successful deployment of SDN-based VANETs.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Moawiah, the first author conducted an analysis of existing authentication research, summarizing its limitations and writing the paper. Adi, the second author, focused on highlighting the advantages of the existing work, creating figures and tables, and identifying open research issues. Dr. Usman, the third author, supervised the project and performed a thorough check of the paper; all authors had approved the final version.

References

[1] H. Trivedi, S. Tanwar, and P. Thakkar, "Software defined network-based vehicular ad hoc networks for intelligent transportation system: recent advances and future challenges," in *Proc. Futuristic Trends in Network and Communication Technologies: First International Conference*, pp. 325–333, 2018.

[2] R. Sultana, J. Grover, and M. Tripathi, "Security of SDN-based vehicular ad hoc networks: State-of-the-art and challenges," *Vehicular Communications*, vol. 27, p. 100284, 2021.

[3] A. A. Khan, M. Abolhasan, and W. Ni, "5G next generation VANETs using SDN and fog computing framework," in *Proc. 2018 15th IEEE Annual Consumer Communications and Networking Conference (CCNC)*, pp. 1–6, 2018.

[4] E. Qafzezi, K. Bylykbashi, E. Spaho, and L. Barolli, "An intelligent approach for resource management in SDN-VANETs using fuzzy logic," in *Proc. 14th International Conference on Broad-Band Wireless Computing, Communication and Applications (BWCCA-2019)*, Springer, pp. 747–756, 2020.

[5] M. Arif *et al*., "Sdn-based vanets, security attacks, applications, and challenges," *Applied Sciences*, vol. 10, no. 9, p. 3217, 2020.

[6] H. Shafiq, R. A. Rehman, and B. S. Kim, "Services and security threats in sdn based vanets: A survey," *Wireless Communications and Mobile Computing*, 2018.

[7] W. B. Jaballah, M. Conti, and C. Lal, "A survey on software-defined VANETs: benefits, challenges, and future directions," arXiv preprint arXiv:1904.04577, 2019.

[8] A. Hussein, I. H. Elhajj, A. Chehab, and A. Kayssi, "SDN VANETs in 5G: An architecture for resilient security services," in *Proc. 2017 Fourth International Conference on Software Defined Systems (SDS)*, pp. 67–74, 2017.

[9] H. Polat, M. Turkoglu, and O. Polat, "Deep network approach with stacked sparse autoencoders in detection of DDoS attacks on SDN-based VANET," *IET Communications*, vol. 14, no. 22, pp. 4089–4100, 2020.

[10] W. B. Jaballah, M. Conti, and C. Lal, "Security and design requirements for software-defined VANETs," *Computer Networks*, vol. 169, p. 107099, 2020.

[11] M. Adnan *et al*., "Towards the design of efficient and secure architecture for software-defined vehicular networks," *Sensors*, vol. 21, no. 11, p. 3902, 2021.

[12] T. Y. Wu, Z. Lee, L. Yang, J. N. Luo, and R. Tso, "Provably secure authentication key exchange scheme using fog nodes in vehicular ad hoc networks," *The Journal of Supercomputing*, vol. 77, pp. 6992–7020, 2021.

[13] H. Zhong, L. Chen, J. Cui, J. Zhang, I. Bolodurina, and L. Liu, "Secure and lightweight conditional privacy-preserving authentication for fog-based vehicular ad hoc networks," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8485–8497, 2021.

[14] X. Zhang, H. Zhong, J. Cui, I. Bolodurina, and L. Liu, "Lbvp: A lightweight batch verification protocol for fog-based vehicular networks using self-certified public key cryptography," I*EEE Transactions on Vehicular Technology*, vol. 71, no. 5, pp. 5519–5533, 2022.

[15] S. Mei, G. Yuyan, Z. Juan, and J. Mingming, "An authentication and key agreement scheme based on roadside unit cache for VANET," *Security and Communication Networks*, 2022.

[16] Y. Wang, Z. Tian, Y. Sun, X. Du, and N. Guizani, "LocJury: an IBN-based location privacy preserving scheme for IoCV," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5028–5037, 2020.

[17] Q. Kong, R. Lu, F. Yin, and S. Cui, "Privacy-preserving continuous data collection for predictive maintenance in vehicular fog-cloud," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5060–5070, 2020.

[18] L. Wei, J. Cui, H. Zhong, Y. Xu, and L. Liu, "Proven secure tree-based authenticated key agreement for securing V2V and V2I communications in VANETs," *IEEE Transactions on Mobile Computing*, vol. 21, no. 9, pp. 3280–3297, 2021.

[19] S. A. Soleymani, S. Goudarzi, M. H. Anisi, M. Zareei, A. H. Abdullah, and N. Kama, "A security and privacy scheme based on node and message authentication and trust in fog-enabled VANET," *Vehicular Communications*, vol. 29, p. 100335, 2021.

[20] H. Zhong, Y. Geng, J. Cui, Y. Xu, and L. Liu, "A weight-based conditional privacy-preserving authentication scheme in software-defined vehicular network," *Journal of Cloud Computing*, vol. 9, pp. 1–13, 2020.
[21] T. Y. Wu, X. Guo, L. Yang, Q. Meng, and C. M. Chen, "A lightweight authenticated key agreement protocol using fog nodes in social Internet of vehicles," *Mobile Information Systems*, vol. 2021, pp. 1–14, 2021.
[22] 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 Transactions on Information Forensics and Security*, vol. 16, pp. 1681–1695, 2020.