Indonesian Journal of Electrical Engineering and Computer Science
Vol. 21, No. 1, January 2021, pp. 479~488
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v21.i1.pp479-488

Security schemes based on conditional privacy-preserving vehicular ad hoc networks

Mahmood A. Al-shareeda[1], Mohammed Anbar[2], Murtadha A. Alazzawi[3], Selvakumar Manickam[4], Iznan H. Hasbullah[5]
[1,2,4,5]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM), Penang, Malaysia
[3]Department of Computer Techniques Engineering, Imam Al-Kadhum College (IKC), Iraq

Article Info

Article history:

Received Mar 11, 2020
Revised Jul 8, 2020
Accepted Aug 2, 2020

Keywords:

Authentication
Privacy-preserving
Security
Vehicular ad hoc networks

ABSTRACT

Recently, vehicular ad hoc networks (VANETs) have been garnering significant inter-est from the people involved in transportation field. Nowadays automotive manufactur-ers have already supplying vehicles with multitude of road sensors that provides many useful characteristics. VANET communication not only offers the drivers and passen-gers with the various safety related services but also provides a wide range of valuable applications. However, the inherent openness of the wireless communication medium used by VANETs exposes vehicles to various security and privacy issues. Researchers have proposed many security schemes to solve the issues mentioned above for the widespread deployment of VANETs. However, these schemes failed to fulfill all as-pects of security and privacy requirements. Besides, these schemes have not provided the performance parameters such as computation and communication costs. The pri-mary emphasis of this paper is on the taxonomy of security schemes based conditional privacy-preserving with respect to strengths and limitations. Besides, a comparison be-tween these schemes related to the model of security and privacy requirements, attacks, and performance parameters is provided. Finally, this paper critically reviews the re-lated works by taking into consideration the design and development of all VANETs security and privacy schemes, this paper could serve as a guide and reference.

Corresponding Author:

Mohammed Anbar
National Advanced IPv6 Centre (NAv6)
Universiti Sains Malaysia
11800 USM, Penang, Malaysia
Email: anbar@nav6.usm.my

1. INTRODUCTION

With the fast expansion of mobile communication and wireless access technologies [1-4], the vehicular ad hoc networks (VANETs) is becoming very active and interesting research area in recent years. VANETs offer techniques for collecting self-motivated traffic data and observing other material amounts used in traffic data communication and aims to provide to the intelligent transportation systems [5-7]. VANET is very sim-ilar to the mobile ad-hoc network (MANET) [8-11] in the way it refers to vehicles as mobile nodes. In the deployment of VANETs [12], each vehicle is fitted with an on-board unit (OBU) that provides vehicles with the ability to communicate with other vehicles via vehicle-to-vehicle (V2V) communication or with a roadside unit (RSU) via vehicle-to-infrastructure (V2I) communication [13-15].

The dedicated short-range communication (DSRC) protocol is a short-range wireless protocol that plays a significant role in VANETs [16-18]. By utilizing the DSRC technology, each VANETs node periodically transmits traffic-related messages including the status information, such as traffic events, location, and velocity [19]. The mobile vehicles and fixed RSU make decisions in VANETs communication based on the information that they received. When the information are from illegal nodes, it can lead to serious implications with the decisions made based on false information [20]. For example, an attacker might call an ambulance to ask for traffic control to make their pass green [21].

To the open-access nature of the VANETs network allows attackers to launch malicious operations to create discord among the vehicles and also with the system [22, 23]. Therefore, VANETs become susceptible to security and privacy threats during broadcasting of the traffic-related message. Mismanagement on these messages may lead to traffic accidents and pedestrian fatality. Security and privacy are one of the challenges that hinders the progress of VANETs. Thus, to ensure widespread deployment of VANETs, the technology must be relatively free from such issues. To address these issues [24, 25], many researchers have proposed several security schemes based on conditional privacy preserving for VANETs. Even though many surveys about VANETs had been written, not many of them provide a comprehensive study of the security requirements and resistance to attacks in VANETs. Moreover, none provides the performance parameters for each scheme.

Riley et al. [26] surveyed many existing security schemes and classified them according to specific criteria. Moreover, they also compared the schemes with respect to the advantages and disadvantage. Petit et al. [27] proposed an abstract pseudonym lifecycle to discuss the issues and criteria for the pseudonym schemes. In their work, they classified the related schemes based on public-key cryptography (PKC) and identity-based public-key cryptography (ID-PKC), symmetric authentication and group signatures. Boualouache et al. [28] classified pseudonym changing strategies to provide a comprehensive survey in VANETs.

Unlike these surveys, the primary emphasis of this paper is on the taxonomy of security schemes based on conditional privacy-preserving with respect to their strengths and limitations. Besides, a comparison between these schemes in relation to the model of security requirements, attack resistance, and performance parameters is also provided. Finally, this work provides critical reviews of the related works.

The rest of the paper is organized as follows. Section 2 briefly introduces the background of VANETs, while Section 3 explains the security and privacy issues in VANETs. Section 4 presents the classification of security schemes based on conditional privacy-preserving. Section 5 is the critical review of the related works, and Section 6 concludes this paper.

2. VEHICLE AD HOC NETWORK

2.1. VANET architecture

In the literature [29], there are three major components of VANETs: trusted authority (TA), road-side units (RSUs), and on-board units (OBUs).

a) (TA) is fully trusted by all components in the system. It has huge computation and storage capabilities. It is responsible to maintain the whole VANET systems and for the RSUs and vehicle registration. Moreover, TA generated the public parameter and preloaded them in OBU during the registration process.
b) (RSUs) is the base station deployed on the roadside. It can communicate with other vehicles inside its range and broadcast the information using DSRC protocol. Moreover, it also communicates with other TA over a secure channel via a wired network.
c) (OBUs) is fitted in each vehicle which enables the vehicle to communicate with other vehicles or a nearby RSU over wireless communication. Each OBU has a tamper-proof device (TPD) that prevents unauthorized disclosure of the information stored in VANETs.

2.2. VANET communication

In general, the communication of VANETs can be organized into two modes [30]: vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication.

a) Vehicle-to-vehicle (V2V) communication: Any vehicles within the wireless range of each other can communicate via V2V communication channel, such as to broadcast messages about the road status. For example, the nodes in VANETs could broadcast messages to other nodes in the vicinity immediately after encountering a vehicle collision location and also send suggestion to avoid the area.
b) Vehicle-to-infrastructure (V2I) communication: The vehicle can broadcast the message to the nearby RSUs in V2I communication. V2I communication helps vehicles to avoid crashes and severe incidents on the road.

2.3. VANET characteristics

The VANETs have the following characteristic:

a) High mobility: In contrast with the MANETs, the main feature of VANETs is high mobility, which plays an extremely critical function in VANETs. Each VANET nodes typically moves very fast and this movement of nodes minimizes the communication window for vehicles on VANETs.

b) Driver safety: The main advantage of VANETs is providing comfort applications and improve the traffic flow for the driver as well as passengers. It can communicate among RSUs and OBUs with several applications.

c) Dynamic network topology: The VANET system varies quickly due to the rapid and high mobility of the vehicles. Because of the fast changes in VANETs topology, the vehicles are more exposed to attacks and at the same time making it difficult to detect and identify malicious vehicles or users.

d) Frequent network disconnection: VANETs connections are often intermittent due to high-speed travel between vehicles and other constraints such as the weather. Also, the repeated disconnection could be the result of too few numbers of vehicles on the road.

e) Driver safety: The main advantage of VANETs is providing comfort applications and improve the traffic flow for the driver as well as passengers. It can communicate among RSUs and OBUs with several applications.

f) Dynamic network topology: The VANET system varies quickly with respect to the rapidly and high mobility of the vehicle. Because of the fast alters in VANETs, the vehicles are more suffer from attacks and are not easy to identify malicious vehicles.

g) Frequent network disconnection: VANETs are often disconnected due to high-speed travel between vehicles and other problems such as the weather. Also, the repeated disconnection may result from a number of vehicles on the road.

2.4. Application

VANETs are aimed mainly at facilitating and coordinating with other vehicles. The applications of VANETs can be classified [31] as follows:

a) Driver Application: The application provides the driver with information about the status of driving environment such as traffic accidents, congestion, and collision. Moreover, it also helps the driver with guided parking and locating nearby base station.

b) Safety Application: The application improves the safety of the traveling party by avoiding any untoward incidents by providing warning on blind spots for a safe lane change or overtaking and left-turn assistance.

c) Comfort Application: The application offers various entertainment services for the drivers as well as passengers.

d) Vehicle Application: The application provides information to enhance vehicle safety on the road for the driver.

3. SECURITY AND PRIVACY IN VANET

In this section, various types of challenges confronting VANETs are analyzed and discussed. All security and privacy issues require careful consideration [32]. First and foremost, security is critical in VANET. Due to open nature of the wireless medium in VANETs, an attacker can easily replay, modify or impersonate other vehicles to take control of the commu-nication channel. For example, the attacker can send false information to deceive the nodes in VANETs that lead to wrong decisions and cause traffic jams or accidents. Therefore, it is important for the recipients to authenticate the source and verify the integrity of every message before accepting them [5]. Secondly, the vehicle privacy an important aspect in VANETs' authentication schemes [33]. To determine the real identity or the location of the vehicle, the attackers could disclose information collected from the transmitted messages. Therefore, the anonymity of the vehicle identity is needed to guarantee privacy and unlinkability of the user. When the TA received the report about the malicious vehicle, it retrieves the vehicle's original identity and revokes it from the system. For clarity, the major requirements and well-known attacks for a VANETs security are described is the following subsections.

3.1. Security and privacy requirements

To secure the communication in VANETs, the following security and privacy requirement should be fulfilled [34].

a) Entity & Message Authentication: Receivers should always verify the authenticity of the sender and the integrity of traffic related message.

b) Privacy preservation: Attackers should not be able to disclose the vehicles' original identity.
c) Unlinkability: Attackers should not be able to link received messages back to the same sender.
d) Traceability: The TA should be able to trace malicious nodes in VANETs by disclosing the original identity of the nodes.
e) Revocation: The TA should be able to revoke the malicious node.

3.2. Types of attacks in VANETs

It is necessary to understand VANET attacks better. There are various attacks in VANETs as follows:

a) Modification attack: The attacker updates/alters the traffic-related messages and then re-broadcast to other nodes in VANETs.
b) Impersonation attack: The attacker impersonates the traffic-related messages and then broadcast to other nodes in VANETs.
c) Replay attack: The attacker replays the previous traffic-related messages and then re-broadcast to other nodes in VANETs.

4. CLASSIFICATION OF SECURITY SCHEMES BASED CONDITIONAL PRIVACY PRESERVING

The existence of security and privacy requirements for VANETs would raise the confidence and trust of users towards V2V and V2I communications. Thus, many studies have proposed conditional privacy-preserving security schemes to secure the communication channel from malicious nodes, replayed messages, and withstand various types of attacks; and at the same time protect the privacy of users. Even though these schemes cope with security and privacy issues, none of them address the performance parameters, such as the efficiency, adequately. In this paper, these schemes are classified according to the location where the master key of the system is stored, such as OBU-based security schemes based conditional privacy preserving (OBU-SSCPP), RSU-based security schemes based conditional privacy-preserving (RSU-SSCPP) and TA-based se-curity schemes based conditional privacy-preserving (TA-SSCPP). This paper provides a comparison between these schemes in terms of the security and privacy requirements, attacks, and performance parameters. The two performance variables selected for analysis are computation cost and communication cost. We have given a linguistic representation for the measure of each parameters as high, medium or low. We accomplished this through a literary survey involving correlations of the outcomes of different schemes in the literature [34]. The spectrum of high, medium and low values for overheads in terms of computation and communication costs is shown in Table 1.

Table 1. Performance parameter values

	Range of Values		
Performance Measure	Low	Medium	High
Communication cost (bytes)	1 to 50	51 to 100	101 to 140
Computation cost (milliseconds)	1 to 3	3.1 to 6	6.1 to 10

4.1. OBU-based security schemes based conditional privacy-preserving (OBU-SSCPP)

Many hardware modules of on-board vehicle devices are required to ensure that the captured information was not altered during broadcasting in VANETs [35, 36]. Usually, each OBU of the vehicle has two modules in VANETs, the event data recorder (EDR) and the tamper-proof device (TPD). The main purpose of EDR is to provide a tamper-proof storage not unlike an airplane's black box. In case of any emergency situation or an incident, the EDR is responsible to record the vehicle's personal data (such as location, velocity, etc.). This information will be useful in the event that the reconstruction of the accident and the attribution of liability are required. These recorded messages could be extracted and used as evidence if some investigation is carried out later. The function of TPD is to provided storage and cryptographic processing capability. During the broadcasting process, TPD allows the vehicle to sign and verify traffic-related messages. TPD provides the hardware protection to store the master key of the system compared with general CPUs.

Zhang et al. [37] proposed a security scheme with conditional privacy-preserving based on bilinear pairing for V2V and V2I communication. This scheme supports the batch verification process, which allows significant traffic-related messages to be verified simultaneously. In their scheme, they eliminated the use of certificate management and certificate revocation list (CRL) which reduced the amount of storage needed, as well as the overhead of the system.

Lee and Lai [38] highlighted two shortcomings of the Zhang et al. scheme [37]. First, a vehicle can utilize a fake identity to remove the requirement of traceability. Second, their scheme is not able to prevent replay and impersonation attacks. So, Lee and Lai [38] introduced an improved authentication of the batch verification process based on bilinear pairing for secure communication in VANET.

Jianhong et al. [39] proposed an enhanced security scheme based conditional privacy-preserving to cope with the flaws in Lee and Lai [38] scheme. In their scheme, the batch verification process with group testing is provided. To guarantee the security and efficiency of VANETs, Tzeng et al. [40] introduced an Identity-based Batch Verification (IBV) scheme that utilized bilinear pairing-based cryptography. The vehicle uses framework master secrets to create its anonymous keys (pseudo-IDs) in their scheme. In other words, a significant portion of the security depends on the protection of deceptive devices.

He et al. [41] proposed a security scheme based on conditional privacy-preserving using Elliptic Curve Cryptography (ECC) instead of bilinear pair for both V2V and V2I communications in VANETs. In their scheme, the batch verification process is supported. This scheme reduces the overhead of the system in terms of computation cost. Thus, it is efficient and also fast in signing and verifying the traffic-related messages. Zhong et al. [42] improved the scheme by He et al. [41] by proposing a security scheme based on conditional privacy-preserving for secure service provision in VANET. In their scheme, the signature generation process is reduced, and efficiency is improved without compromising the security requirement.

Table 2 and 3 present the summary of security and privacy requirements and security attack resistance that are satisfied by OBU-SSCPP schemes and the results of performance parameter analysis in terms of computation and communication cost, respectively.

Table 2. The summary of security and privacy requirement and security attack resistance satisfied by OBU-SSCPP

Scheme	Modification	Impersonation	Replay	Entity & Message	Privacy	Unlinkability	Traceability	Revokecation
[37]	3	7	7	3	7	3	7	7
[38]	3	7	3	3	7	3	3	7
[39]	3	3	3	3	3	3	3	7
[40]	3	3	3	3	3	3	3	7
[41]	3	3	3	3	3	3	3	7
[42]	3	3	3	3	3	3	3	7

Table 3. OBU-SSCPP cost for computation and communication

Scheme	Computation Cost	Communication Cost
[37]	High	High
[38]	High	High
[39]	High	High
[40]	Medium	High
[41]	Medium	High
[42]	Medium	Medium

4.2. RSU-based security schemes based conditional privacy-preserving (RSU-SSCPP)

RSUs consist of high capacities, a high transmission rate, and sufficient processing power. Storage capacity and computing power of RSU are higher than those of OBUs, and those in RSU are lower than those in TA. RSUs located on every intersection in a city [43, 44]. Many researches of RSU-SSCPP schemes stores the master key of the system on each RSUs in VANETs. This method helps the vehicle during the mutual authentication and checks the validity of the signature for requested joining in VANETs system.

To cope with the issue of conditional privacy-preserving, Xue and Ding [45] proposed a Location based privacy-preserving authentication (LPA) scheme for V2V and V2I communication. This scheme depends on the top-down security system in which the top authority (TA) permits the RSUs to generate group certificates and then sends them to OBUs within its coverage area. Besides, they introduced a set of RSU neighbors to provide security in a more efficient manner.

Bayat et al. [46] introduced a new and efficient RSU based authentication (NERA) approach based on conditional privacy-preserving using bilinear pair to update the system’s master key during the period of keeping it inside the RSUs in VANETs. In their scheme, each RSU is fitted with a TPD. Pournaghi et al. [47] proposed a novel and efficient conditional privacy-preserving authentication (NECPPA) approach using bilinear pair in VANETs. In their scheme, the system’s master key and the public parameters are saved in the TPD of RSU. This is because the communication link between TA and RSU is secure and fast. Therefore, the RSU generate the sub-master key of it to send to all vehicle within the coverage area. Table 4 and 5 present the summary of security and privacy requirements and security attack resistance that are satisfied by OBU-SSCPP schemes and the results of performance parameter analysis in terms of computation and communication cost, respectively.

Table 4. The summary of security and privacy requirement and security attack resistance satisfied by RSU-SSCPP

Scheme	Modification	Impersonation	Replay	Entity & Message	Privacy	Unlinkability	Traceability	Revokecation
[45]	3	3	3	7	3	3	7	3
[46]	3	3	7	3	3	3	3	3
[47]	3	3	7	3	3	3	3	3

Table 5. RSU-SSCPP cost for computation and communication

Scheme	Computation Cost	Communication Cost
[45]	High	High
[46]	High	High
[47]	High	High

4.3. TA-based security schemes based conditional privacy-preserving (TA-SSCPP)

This classification, unlike RSU-APS or OBU-APS, which the authors keep the master key for the whole system in TA without sending it during RSU or OBU registration phase, the common characteristics of these schemes are as follows:

To provide secure communication and privacy of driver for vehicles in VANETs, Lo, and Tsai [48] proposed a security scheme based on conditional privacy-preserving using ECC. This scheme ensures the secure authentication of message transmission between vehicles and RSUs. Moreover, both operation of bilinear pairing and function of Map-To-Point are not utilized in their scheme. Therefore, they support the batch verifi-cation process to enhance the processing throughput of RSUs.

Zhong et al. [49] proposed a security scheme based on conditional privacy-preserving using the regis-tration list rather than the revocation list. Their scheme utilizes the cuckoo filter and binary search in VANET environments. By using these two methods, the batch verification process concerning other related current schemes is improved successfully. Before the deployment of applications in VANETs, security and privacy issues should be addressed. Wu et al. [50] introduced an efficient scheme-based location using ECC without the bilinear pairing and any special equipment (i.e., TPD) which could fulfill respect the security and privacy requirements.

J Cui et al. [51] introduced a security scheme based conditional privacy-preserving based on semiTA for V2V and V2I communication. This scheme utilizes two methods, self-healing key distribution and a cer-tificateless signature to combine them in a semi-TA environment. In their scheme, the vehicles do not save the CRLs during VANET's communication. Therefore, they save storage capacity and communication resources. Cui et al. [52] introduced an efficient conditional privacy-preserving security scheme based on ECC instead of bilinear pair for signing and verifying traffic-related messages. Besides, they also use a general one-way hash rather than a Map-To-Point function during batch verification process, which allows verification of multiple messages at the same time. Table 6 and 7 present the summary of security and privacy requirements and security attack resistance that are satisfied by the TA-SSCPP schemes; and the results of performance parameter analysis in terms of computation and communication costs, respectively.

Table 6. The summary of security and privacy requirement and security attack resistance satisfied by TA-SSCPP

Scheme	Modification	Impersonation	Replay	Entity & Message	Privacy	Unlinkability	Traceability	Revokecation
[48]	3	3	7	3	3	7	3	7
[49]	3	3	3	3	3	3	3	7
[50]	3	3	3	3	3	7	3	7
[51]	3	3	3	3	3	3	7	3
[52]	7	7	3	7	3	3	3	3

Table 7. TA-SSCPP cost for computation and communication

Scheme	Computation Cost	Communication Cost
[48]	High	High
[49]	Medium	Low
[50]	High	High
[51]	Low	Medium
[52]	Medium	High

5. CRITICAL REVIEW ON RELATED WORKS

Security and privacy issues are equally critical in V2V and V2I communication. Many researchers proposed security schemes based on conditional privacy-preserving to cope with these issues. These schemes are usually classified by type: OBU-SSCPP, RSU-SSCPP, and TA-SSCPP schemes.

In OBU-SSCPP schemes, there are two common limitations, side-channel attack, and revocation pro-cess. Based on the literature review of OBU-SSCPP scheme, the authors assumed that attackers are not able to disclose the personal information stored in TPD on the OBU of the vehicle. But on contrary, attackers could access the TPD physically by side-channel attack [53]. Since the possibility of their personal information to be exposed to others are high, the drivers are reluctant to utilize the technology of VANETs. Thus, the informa-tion stored be easier to disclose to dispute the VANETs system. Besides this, when one vehicle is controlled or compromised, the TA has no ability to revoke it. Therefore, the system of VANETs remains vulnerable to these type of attack. As shown in Table 2, none of the schemes [37-42] can satisfy the security and privacy requirement, especially in revocation process. This is because the master key of the system is stored in each vehicle, as mentioned above. However, the scheme [39-42] are better than other OBU-SSCPP schemes in satisfying most of the security and privacy requirements as well as having a decent security attack resistance. Moreover, as shown in Table 3, the scheme [42] has the best computation and communication costs compared to the rest of the OBU-SSCPP schemes studied. The main limitation of RSU-SSCPP schemes is related to key escrow issue. Each vehicle needs the key of the system to generate the signature of traffic-related message. This allows recipient to easily authenticate the validity of the message source by using the signature. Whenever the RSU transmits the key to an authenticated vehicle via VANETs environment which uses open-access wireless communication medium, the attacker will attempt to extract the key from the message captured. As shown in Table 4, the [46, 47] schemes are better than other RSU-SSCPP schemes in fulfilling most of the security and privacy requirement as well as having a better resistance to security attacks. Moreover, as shown in Table 5, none of schemes [45-47] has low overhead in terms of computation and communication costs. This is due to the use of the bilinear pair operation and Map-To-Point function for signing and verifying information in VANETs.

The limitation of TA-SSCPP schemes is the communication bottleneck. There is only one TA in the system model of TA-SSCPP schemes that is responsible for authentication and distribution of the key to all vehicles. The TA is required to authenticate and respond to all traffic-related messages received, even with multiple nodes in VANETs, the [49, 51] schemes areschemes performed better than other TA-SSCPP schemes in fulfilling most of the security and privacy requirements as well as resisting security attacks, as shown in Table 6. Also, none of the schemes other than [49, 51] has low overhead in either computation or communication costs, as shown in Table 7.

6. CONCLUSION

The VANETs contribute to improving the driver’s safety and road traffic reliability by broadcasting traffic-related information. However, the VANETs face some serious challenges and problems because of the open-access nature of the wireless medium that is used for communication. Attackers may compromise the data transmitted over this open wireless communication medium. The primary emphasis of this paper is on the taxonomy of conditional privacy-preserving based security schemes concerning their strengths and limitations. This paper classified these schemes into three categories, OBU-SSCPP, RSU-SSCPP, and TA-SSCPP, according to the location where the master key of the system is stored. A comparison between these schemes in terms of the security and privacy requirements, attack resistance, and performance parameters is presented. Finally, this work critically reviewed the related works.

REFERENCES

[1] S. Wang, et al., “Hybrid conditional privacy-preserving authentication scheme for VANETs,” *Peer-to-Peer Networking and Applications*, pp. 1-16, 2020.

[2] M. S. Sheikh, et al., “A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs),” *Sensors*, vol. 19, no. 16, p. 3589, 2019.

[3] M. Al Shareeda, et al., “Realistic Heterogeneous Genetic-based RSU Placement So-lution For V2I Networks,” *International Arab Journal of Information Technology*, vol. 16, no. 3A, pp. 540-547, 2019.

[4] WHO, “Global Status Report on Road Safety 2018: Summary,” World Health Organization, 2018.

[5] M. Wazid, et al., “Authentication in cloud-driven IoT-based big data environment: Survey and outlook,” *Journal of Systems Architecture*, vol. 97, pp. 185-196, 2019.

[6] X. Zhang, et al., “An Efficient Anonymous Authentication Scheme with Secure Communication in Intelligent Vehicular Ad-hoc Networks,” *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 13, no. 6, pp. 3280-3298, 2019.

[7] S. A. Alfadhli, et al., “ELCPH: An Efficient Lightweight Con-ditional Privacy-Preserving Authentication Scheme Based on Hash Function and Local Group Secrete Key for VANET,” in *Proceedings of the 2019 The World Symposium on Software Engineering*, pp. 32-36, 2019.

[8] S. S. Manivannan, et al., “Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs),” *Vehicular Communications*, p. 100247, 2020.

[9] M. Al Shareeda, et al., “Towards the Optimization of Road Side Unit Placement Using Genetic Algorithm,” in *2018 International Arab Conference on Information Technology (ACIT)*, pp. 1-5, 2018.

[10] O. A. Hammood, et al., “An effective transmit packet coding with trust-based relay nodes in vanets,” *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 2, pp. 685-697, 2020.

[11] B. H. Khudayer, et al., “Efficient route discovery and link failure detection mechanisms for source routing protocol in mobile ad-hoc networks,” *IEEE Access*, vol. 8, pp. 24019-24032, 2020.

[12] S. P. Godse and P. N. Mahalle, “A computational analysis of ecc based novel authentication scheme in vanet,” *International Journal of Electrical & Computer Engineering*, vol. 8, no. 6, pp. 5268-5277, 2018.

[13] J. Noh, et al., “Distributed Blockchain-Based Message Authentication Scheme for Con-nected Vehicles,” *Electronics*, vol. 9, no. 1, p. 74, 2020.

[14] I. Ali, et al., “Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey,” *Vehicular Communications*, vol. 16, pp. 45-61, 2019.

[15] M. I. Habelalmateen, et al., “Dynamic multiagent method to avoid dupli-cated information at intersections in vanets,” *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 18, no. 2, pp. 613-621, 2020.

[16] J. Kenney, “Dedicated Short-range Communications (DSRC) Standards in the United States,” *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162-1182, 2011.

[17] A. Chehri, et al., “Realistic 5.9 GHz DSRC vehicle-to-vehicle wireless communication protocols for cooperative collision warning in underground mining,” in *Smart Transportation Systems 2020*, pp. 133-141, 2020.

[18] M. A. Alazzawi, et al., “Robust Conditional Privacy-Preserving Authenti-cation based on Pseudonym Root with Cuckoo Filter in Vehicular Ad Hoc Networks,” *KSII Transactions on Internet and Information Systems*, vol. 13, no. 12, p. 6121-6144, 2019.

[19] M. Alazzawi, et al., “Efficient Conditional Anonymity with Message Integrity and Authentication in a Vehicular Ad hoc Network,” *IEEE Access*, vol. 7, pp. 71424-71435, 2019.

[20] S. S. Manvi and S. Tangade, “A survey on authentication schemes in VANETs for secured communication,” *Vehicular Communications*, vol. 9, pp. 19-30, 2017.

[21] R. Boussada, et al., “A Survey on Privacy: Terminology, Mechanisms and Attacks,” in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, pp. 1-7, 2016.

[22] S. E. Shladover, “Connected and automated vehicle systems: Introduction and overview,” *Journal of Intelligent Transportation Systems*, vol. 22, no. 3, pp. 190-200, 2018.

[23] Z. Lu, et al., “A survey on recent advances in vehicular network security, trust, and privacy,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2, pp. 760-776, 2018.

[24] X. Yang, et al., “A lightweight authentication scheme for vehicular ad hoc networks based on MSR,” *Vehicular communications*, vol. 15, pp. 16-27, 2019.

[25] M. A. Alazzawi, et al., “Authentication and revocation scheme for VANETs based on Chinese remainder theorem,” in *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pp. 1541-1547, 2019.

[26] M. Riley, et al., “A survey of authentication schemes for vehicular ad hoc networks,” *Security and Communication Networks*, vol. 4, no. 10, pp. 1137-1152, 2011.

[27] J. Petit, et al., “Pseudonym schemes in vehicular networks: A survey,” *IEEE communications surveys & tutorials*, vol. 17, no. 1, pp. 228-255, 2014.

[28] A. Boualouache, et al., “A survey on pseudonym changing strategies for vehicular ad-hoc networks,” *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 770-790, 2017.

[29] Z. Afzal and M. Kumar, “Security of Vehicular Ad-Hoc networks (vanet): A survey,” in *Journal of Physics: Conference Series*, vol. 1427, no. 1, p. 012015, 2020.

[30] I. A. Abbasi and A. S. Khan, “A review of vehicle to vehicle communication protocols for VANETs in the urban environment,” *Future Internet*, vol. 10, no. 2, p. 14, 2018.

[31] M. S. Sheikh, et al., “Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A survey,” *Wireless Communications and Mobile Computing*, vol. 2020, pp. 1-25, 2020.

[32] I. Ali, et al., “A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs,” *Journal of Systems Architecture*, vol. 99, p. 101636, 2019.

[33] F. Qu, et al., “A security and privacy review of VANETs,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985-2996, 2015.
[34] M. Raya and J. P. Hubaux, “The Security of Vehicular Ad hoc Networks,” in *Proceedings of the 3rd ACM Workshop on Security of Ad hoc and Sensor Networks*, pp. 11-21, 2005.
[35] J. Domingo-Ferrer and Q. Wu, “Safety and Privacy in Vehicular Communications,” in *Privacy in Location-Based Applications*, pp. 173-189, 2009.
[36] M. Bayat, et al., “A Secure Authentication Scheme for VANETs with Batch Verification,” *Wireless Networks*, vol. 21, no. 5, pp. 1733-1743, 2015.
[37] C. Zhang, et al., “On Batch Verification with Group Testing For Vehicular Commu-nications,” *Wireless Networks*, vol. 17, no. 8, pp. 1851-1865, 2011.
[38] C. C. Lee and Y. M. Lai, “Toward a Secure Batch Verification with Group Testing for VANET,” *Wireless Networks*, vol. 19, no. 6, pp. 1441-1449, 2013.
[39] Z. Jianhong, et al., “On the Security of a Secure Batch Verification with Group Testing for VANET,” *International Journal of Network Security*, vol. 16, no. 5, pp. 351-358, 2014.
[40] S. F. Tzeng, et al., “Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANETs,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3235-3248, 2015.
[41] D. He, et al., “An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681-2691, 2015.
[42] H. Zhong, et al., “Efficient Conditional Privacy-preserving and Authentication Scheme for Secure Service Provision in VANET,” *Tsinghua Science and Technology*, vol. 21, no. 6, pp. 620-629, 2016.
[43] A. Alganas, “Social-based Trustworthy Data Forwarding in Vehicular Delay Tolerant Networks,” Ph.D. dissertation, UOIT, 2011.
[44] H. W. Hu, et al., “Effects of Climate Warming and Elevated CO2 on Autotrophic Nitrification and Nitrifiers in Dryland Ecosystems,” *Soil Biology and Biochemistry*, vol. 92, pp. 1-15, 2016.
[45] X. Xue and J. Ding, “LPA: A New Location-based Privacy-preserving Authentication Protocol in VANET,” *Security and Communication Networks*, vol. 5, no. 1, pp. 69-78, 2012.
[46] M. Bayat, et al., “NERA: A New and Efficient RSU Based Authentication Scheme for VANETs,” *Wireless Networks*, vol. 26, pp. 3083-3098, 2020.
[47] S. M. Pournaghi, et al., “NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET,” *Computer Networks*, vol. 134, pp. 78-92, 2018.
[48] N. W. Lo and J. L. Tsai, “An Efficient Conditional Privacy-preserving Authentication Scheme for Ve-hicular Sensor Networks Without Pairings,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 5, pp. 1319-1328, 2015.
[49] H. Zhong, et al., “Conditional privacy-preserving authentication using registration list in vehicular ad hoc networks,” *IEEE Access*, vol. 6, pp. 2241-2250, 2017.
[50] L. Wu, et al., “Efficient Location-based Conditional Privacy-preserving Authentication Scheme for Vehicle Ad hoc Networks,” *International Journal of Distributed Sensor Networks*, vol. 13, no. 3, pp. 1-13, 2017.
[51] J. Cui, et al., “An efficient authentication scheme based on semi-trusted authority in VANETs,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2972-2986, 2019.
[52] J. Cui, et al., “Secure mutual authentication with privacy preservation in vehicular ad hoc networks,” *Vehicular Communications*, vol. 21, p. 100200, 2020.
[53] Y. Nozaki, et al., “Tamper resistance of iot devices against electromagnetic analysis,” in *2016 IEEE International Meeting for Future of Electron Devices, Kansai (IMFEDK)*, pp. 1-2, 2016.

BIOGRAPHIES OF AUTHORS

Mahmood Arif Al-shareeda received his B.S degree in from Communication Engineering in Iraq University College and MSc in Information Technology from Islamic University of Lebanon (IUL) in 2018. Currently, he is a Ph.D. candidate at National Advance IPv6 Center (NAv6), Universiti Sains Malaysia (USM). His research interests are security and privacy issues in Vehicular Ad hoc Network (VANET) and Network optimization.
E-mail: m.alshareeda@nav6.usm.my

Mohammed Anbar obtained his Ph.D. in Advanced Computer Network from University Sains Malaysia (USM). He is currently a senior lecturer at National Advanced IPv6 Centre (NAv6), Univer-siti Sains Malaysia. His current research interests include malware detection, web security, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), network monitoring, Internet of Things (IoT), Vehicular Ad hoc Network (VANET) security and IPv6 security. E-mail: anbar@nav6.usm.my

Murtadha A. Alazzawi received the bachelor's degree and master's degree in Computer Science from Science College, University of Basrah, Iraq, in 2010, 2013 respectively, and his Ph.D. from Huazhong University of Science and Technology, Wuhan, Hubei, China, in 2020. He is currently working with department of Computer Techniques Engineering, Imam Al-Kadhum College (IKC). His research interests are security and privacy issues in VANETs and WSNs. E-mail: murtadhaali@alkadhum-col.edu.iq

Selvakumar Manickam is an associate professor working in Cybersecurity, Internet of Things, In-dustry 4.0 and Machine Learning. He has authored and co-authored more than 160 articles in journals, conference proceedings and book reviews and graduated 13 PhDs. He has 10 years of industrial expe-rience prior to joining the academia. He is a member of technical forums at national and international levels. He also has experience building IoT, embedded, server, mobile and web-based applications. E-mail: selva@usm.my

Iznan Husainy Hasbullah holds a Bachelor of Science degree in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA. He is currently pursuing his M.Sc. in advanced network security. He has experience working as software developer, R&D consultant, and network security auditor prior to joining National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia in 2010 as Research Officer. His research interest includes unified communication, telematics, network security, network protocols and next generation network.
E-mail: iznan@nav6.usm.my