A review on various security attacks in vehicular ad hoc networks

Mustafa Maad Hamdi[1], Lukman Audah[2], Mohammed Salah Abood[3], Sami Abduljabbar Rashid[4], Ahmed Shamil Mustafa[5], Hussain Mahdi[6], Ahmed Shakir Al-Hiti[7]
[1,2,4]Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia, Batu Pahat Johor, Malaysia
[3]School of Information and Electronics Engineering, Beijing Institute of Technology, Beijing, China
[5]Department of Computer Engineering Techniques, Al-Maarif University College, Al-Anbar, Iraq
[1,6]Computer Engineering Department, Faculty of Engineering, University of Diyala, Baquba, Diyala Province, Iraq
[7]Department of Electrical Engineering, Faculty of Engineering, University of Malaya, Kuala Lumpur, Malaysia

Article Info

Article history:

Received Oct 27, 2020
Revised Dec 20, 2020
Accepted Jul 14, 2021

Keywords:

Attacks
Threats
V2I
V2V
VANET

ABSTRACT

Ad hoc vehicle networks (VANET) are being established as a primary form of mobile ad hoc networks (MANET) and a critical infrastructure to provide vehicle passengers with a wide range of safety applications. VANETs are increasingly common nowadays because it is connecting to a wide range of invisible services. The security of VANETs is paramount as their future use must not jeopardize their users' safety and privacy. The security of these VANETs is essential for the benefit of secure and effective security solutions and facilities, and uncertainty remains, and research in this field remains fast increasing. We discussed the challenges in VANET in this survey. Were vehicles and communication in VANET are efficient to ensure communication between vehicles to vehicles (V2V), vehicles to infrastructures (V2I). Clarified security concerns have been discussed, including confidentiality, authentication, integrity, availableness, and non-repudiation. We have also discussed the potential attacks on security services. According to analysis and performance evaluations, this paper shows that the ACPN is both feasible and appropriate for effective authentication in the VANET. Finally, the article found that in VANETs, encryption and authentication are critical.

Corresponding Author:

Lukman Audah
Faculty of Electrical and Electronic Engineering
Universiti Tun Hussein Onn Malaysia
86400 Parit Raja, Batu Pahat, Johor, Malaysia
Email: hanif@uthm.edu.my

1. INTRODUCTION

Rapid wireless technology should be used to enhance the driving environment to enable road safety, infotainment, and effective transport. Deaths worldwide are growing dramatically, with over 1 2.2 million fatalities killing on roads globally per year, with over 50 million being wounding. Over the next five years, such estimates would rise by nearly 60% if no measures are implementing in addition to other harm such as loss of time generated by road delays.

VANET is a mobile ad hoc (MANET) route network designed to enhance travel security, traffic flow, and driving experience. This consists of the registration/administration of transportation on-board units (OBUs) and roadside units (RSUs) [1]-[3]. An OBU is constructed as a communication transmitter with other vehicles on the road in every vehicle, while an RSU with networked equipment is installed along the road.

RSUs are used to connect to the networks and include dedicated short-range communication (DSRCs) [4], [5]. Two categories are describing as VANET as:

a. Vehicle-to-vehicle (V2V)

Only vehicles in the V2V communication domain share some features, such as vehicles with the same model or vehicles that share the exact location during the same time interval that share in this communication [6].

b. Vehicle to infrastructure (V2I) communications [7]

Warning messages are transmitted from infrastructure through RSUs to every vehicle within the road to improve traffic flow and safety. Their location, especially on curve roads, intersections, or on narrow roads, shall be detecting where possible. As shown in Figure 1, the VANET security protocols will provide security against unauthorized individuals being obtaining, detected, and profiled by non-authorized entities and against driver privacy (e.g. identity and location privacy). Otherwise, it would be challenging to convince drivers to become members of the driver. User profiling is necessary when the designated organization needs to share essential information, such as in cases of crime) [8], [9]. One instance of this is that malicious action identifies at VANET, which involves detection and distinction between malicious activities by legal and privileged users (network outsiders), which is a significant challenge [10]. A requirement to meet safety and privacy concerns, design a set of mechanisms to ensure protection and privacy in realistic VANET designs [11] to secure them effectively against significant security threats, including but not limited to, rendition, black hole, tunnelling, timing attack, and Sybil [12]. The VANET huge opportunity and scalability can have catastrophic consequences and an effective attack by an adversary [13], [14]. However, VANETs have some crucial differences with the MANETs (e.g. very high dynamic networks, capital limitations, large data supply application requirements, access to infrastructures, central identification, technical analysis, and identification of liability, more importantly, confidentiality in certain instances). Therefore the majority of MANET security research cannot be application [15], [16].

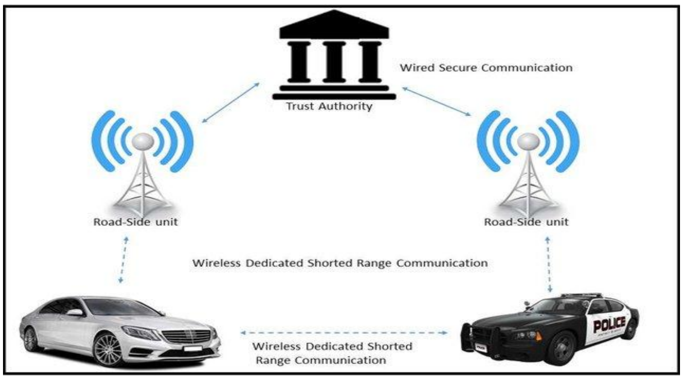
Wired Secure Communication
Trust Authority
Road-Side unit
Road-Side unit
Wireless Dedicated Shorted Range Communication
POLICE
Wireless Dedicated Shorted Range Communication

Figure 1. The structure of VANET [8]

It should be noted that most previous works focused only on a few aspects of various security attacks in vehicular ad hoc networks, such as vehicular communication [17], security attacks [18], green communication networks [19], and security issues [20]. So in this paper summarizes the main contributions as:

a. In this survey, the challenges in VANET were discussed, particularly in V2V and V2I and clarified security concerns, including confidentiality, authentication, integrity, availableness, and non-repudiation. With a literature survey for each case and made a comparison with previous studies as in Table 1. As well, security services have also has been discussed as a possible attack on the capabilities.
b. Some researchers have been working to provide VANET authentication. However, confidentiality and availability are almost non-existent in most studies, such as in privacy and safety and so on, especially in [16], [21], [22]. To fill this gap, this article comprehensively surveys the latest advances, focuses on requirements, and then describes the various attack and threats examples. Furthermore, we discovered that encryption and authentication are crucial in VANETs. This paper's novelty shows that the proposed ACPN is feasible and adequate to UVC in the VANET for efficient privacy-preserving authentication with non-repudiation, according to analysis and performance evaluations.

This paper's organization follows section 1, explaining the VANET and types of communication in VANET. Section 2, presenting the most challenges in VANETs. Section 3, explaining all kinds of security service in VANETs, section 4, show the discussion and conclusion.

Table 1. Summary of security service in VANETs

Author/year	Description	Security standards	Attacks	Applications	Security	Simulation Tools	Architectures	Parameters	Communications Paradigm	Strength
[7]/2020	Issues and challenges in VANET	-	x	x	x	x	x	-	V2V, V2I	Design of cost-effective VANET protocols and applications (ITS)
[23]/2020	Existing replay attack prevention schemes in VANETs	-	x	x	x	-	-	-	V2V, V2I	Discussed existing replay attack
[24]/2018	Challenges, security requirements and attacks in VANET	-	x	-	x	-	x	-	V2V, V2I, I2I	Taxonomy of Security Concept
[17]/2019	Design and implementation	x	x	x	x	-	x	-	V2V, V2I, V2X, V2P, V2C,	Security solutions in 5G
[1]/2017	security challenges and solutions	x	x	-	x	-	x	-	V2V, V2I	Security architectures, security standards, attacks and solutions,
[25]/2020	Security Attacks and Challenges	x	x	-	x	-	-	-	V2V, V2I, V2R	General analysis of possible challenges is mention
[18]/2017	Security Attacks and Challenges	-	x		x	-	x	-	V2V, V2I	Mobility and propose a new protocol
[19]/2019	Security Services, Attacks, and Applications	x	x	x	x	x	x	-	V2V, V2I, V2X, V2P, V2R,	Open research problems and future directions have been identified
[20]/2017	Mechanisms, advantages, disadvantages, and performance. Also, security issues in VANET authentication	x	x	-	x	-	x	x	V2V, V2I	Taxonomy and open security issues
[26]/2019	Authentication and privacy schemes have been classifying, discussed	-	x	-	x	-	-	x	V2V, V2I	Security requirements, Security attacks and Performance parameters
[27]/2020	Different issues in Man-In-The-Middle (MITM) attacks	-	x	-	x	-	x	-	V2V, V2I	Prevent MITM attacks in VANET.
[28]/2019	Safety will be maintained and the various protective technologies crashed in the VANETs	-	x	-	x	-	-	-	V2X, V2V	The relationship between literature algorithms and the various safety factors
[29]/2019	Current AV safety problems and security attacks research overview	-	x	-	x	-	-	-	V2X	The available safety and security countermeasures
Our Survey	Challenges in VANET, security concerns, including confidentiality, authentication, integrity, availableness, and non-repudiation	-	x	x	x	-	-	-	V2V, V2I	The proposed ACPN in the VANET setting is feasible for a UVC for effective non-repudiation confidentiality authentication

x	considers	-	non-considers

2. CHALLENGES OF VANETS

There are several issues challenges in VANETs:

a. Congestion and collision control; the unlimited size of the network is also a challenge. In rural areas, the traffic load is low, and in urban areas, even at night. It also happens while in a rush with network partitions. The traffic load is hefty hours, which causes network congestion and a network collision.

b. Real-time system; developing a real-time system is difficulty because it is challenging to send a warning message in an increasingly mobile environment before the deadline is the correct time.

c. Authentication; all messages sent from one vehicle to another must be authenticating. The central authority will authenticate each vehicle in the network [30].

d. Security and trust; security issues are sometimes dealt with in travel applications, especially in the comfort of the traveller, and the reason is that cooperation exists between all. If security and security are not ensuring, customers will not accept the warning systems they have received. Trust and trustworthy

software are one of the most critical protection issues in VANET. Implementing security maps for VANET implementations can also delay the message's delivery [25].
e. Environmental impact; for communication, VANETs are using electromagnetic waves. These waves are environmentally affected. Therefore, to deploy VANET should be considered for the environmental impact [31].
f. MAC design; VANET typically uses the common medium to notify the design of the MAC. Several approaches, such as TDMA, SDMA, CSMA, are taken. The CSMA based Mac for VANET was adopted by IEEE 802.11 [18].
g. Location-based services; through beaconing, we know where other cars are situated. However, we know the correct vehicle location by using GPS, sensors, cameras, radar.
h. Mobility; the VANET vehicles are highly dynamic, as they are free to travel and connect with other vehicles throughout their movement, which can never be approached before. Vehicles stay attached for so long, and then each vehicle loses its connection when it moves in a path that makes it challenging to secure VANET [32].

3. SECURITY SERVICE IN VANETS

MANETs has recently created security problem that researchers consider to be an important security issue, including fewer central points, insufficient mobility Wireless, and driver connectivity problems. For VANETs, the messages' security transferred to assured that the attackers cannot inject or change them. In fact, within a specific timeline, the driver will reliably inform traffic conditions. The VANET is more vulnerable to attacks due to its distinguishing characteristics. Also, safety issues would now be properly discussed. If not, certain obstacles would be generated to protect communication within VANETs. The system's requirements should be in line with the related network service that needs to be specified in VANET security. Such conditions could not be dealt with with possible VANET threats or attacks. This section discusses the security services in VANET. The primary safety Requirements are divide into five main domains, such as VANET [33]:

3.1. Availability attack

Units the availability includes bandwidth and connectivity for all node network services. A group signature system has been implementing to prevent and detect technology [19]. The program focuses on the availability of messages between vehicles and RSUs. If the attack causes network unavailability, the technical solution proposed is to survive through interconnections between RSUs and the vehicles using public and private keys [21]. At the same time, attack on availability, in the case of lack of availability functionality which may contribute to a decrease in the efficiency of the VANETs information accessibility, is a vital part of the VANET system. The following are its description and types:
a. Denial of service (DOS) attacks; DOS is one of the most common VANET attacks. The attacks in the VANET network internally or externally vehicles [34]. The attacker blocks vehicle communication and effectively prevents any possible means of behavior. Many attackers can simultaneously perform this attack on a distributed basis, known as a distributed denial of service (DDoS) [35].
b. Jamming attack; the VANET communication channel is disrupted by a strongly driven signal of an equivalent frequency. It is the riskiest security application attack because the valid security warning has not been following. If a successful jamming attack has been carried out, the jammer will disrupt the useful signal at the same time as an event [36].
c. Malware attack; malware is malicious software whose objective is to interrupt normal functioning. The attacker is responsible for this attack. This attack is introduced to the networks by VANET systems and roadside stations as software updates are received.
d. Black hole attack; it is one of VANET 's safety attacks. The assailant node refuses to participate in this attack or even drop the data packet [37]. This type of attack, therefore, affects the vehicle network more severely.
e. Gray hole attack; the black hole attack variant. It happens if unsustainable vehicles want to forward some data packets and remove the other packet without being tracked [19].
f. Greedy behavior attack; this attack mainly affects the MAC functionality when a malicious vehicle misuses the MAC protocol to maximize the costly bandwidth for many applications. This contributed to a traffic congestion and a collision in the broadcast channel that could delay the legitimate services of the registered user [20].
g. Broadcast tampering; attackers include false safety messages on the network in this attack. This message covers traffic alerts at times. The situation is critical, for example, accidents and traffic delays [38].
h. Spamming; spam attacks target bandwidth consumption and transmission latency. Spam attacks such messages, like advertising messaging, are not of interest to users [39].

3.2. Authentication attacks

VANET plays an essential function in authentication. It prevents VANET from attacking suspected network entities. Based type information, including user identity and sender address, is vital. It is necessary. Authentication can control vehicles' authorization levels and can, by allocating specific identification for each vehicle, often prevent Sybil attacks [40]. While attack on authentication, authentication is vital in the VANET network used to protect the system from attack due to malicious nodes. Authentication shall be responsible for Protecting internal and external connections from VANETs. The following are its description and types:

a. Sybil attack; this attack consists of sending more than one copy of messages to other vehicles, and every message includes a manufactured identity, i.e. The attacker appears hundreds of vehicles with specific IDs to other vehicles, informing them jam ahead and forcing them to take another path.
b. Tunnelling attack; this attack is like the wormhole attack. Initiating a personal chat and on a channel called the tunnel using the same network. The attacker joined the VANETs at two distant positions. Thus, nodes far apart can connect as neighbors [37].
c. GPS spoofing; a powerful signal transmitting an attacker, more significant than the GPS signal, causes VANET to be jamming, and the vehicle receiver gets the wrong position.
d. Node impersonation attack; this attack occurs when an attacker determines the VANET's user ID [19].
e. Free-riding attack; this attack is viral and performed by false authentication attempts and cooperative message authentication by an effective malicious user. During this attack, the malicious app is going to use other users' security efforts without their own. This form of action is considered free rein. This attack could severely threaten to authenticate the message of the cooperative.

3.3. Integrity attacks

Data integrity ensures that data obtained from nodes, RSUs, and AS areas created while exchanging messages. The integrated digital signature with app access guarantees the validity of the message [40]. While attack on integrity, invalid data measurements and the transmission of messages affected by managing vehicle sensors or altering the data transmitted will compromise data integrity. This influences the network's reliability. Therefore, some mechanisms have to be established in practice to protect the vehicle network from these attacks [41]. The following are its description and types:

a. Masquerading; in this attack, one attacker is defined by false identification and visibility as a legitimate node by another vehicle. The attacker behaves like a man in the central middle and spoofs them as the second vehicle as all vehicles interact in the process. That is also a deliberate attack to change the results [23].
b. Replay attack; the attacker aims to repeat or delay fraudulent transmission by continuously providing valid data and injecting beacon and responses received by the VANET network. In the case of an incident, traffic authorities can find it challenging to identify vehicles [42].
c. Message tampering attack; the attack is usually carrying out when an attacker modifies or changes recently transmitted messages as the name of the attack indicates. When the road is congested, the attacker changes the data to clear the path and may modify the path.
d. Illusion attack; in this attack, the attacker communicates alerts based on the road conditions, which give the vehicles an impression leading to delays, accidents, and lower overall VANET results. Unfortunately, because of the essential control of the sensors (of his vehicle) directly and technological them for producing and transmitting the bad traffic info, there is no authentication protocol against such an attack.

3.4. Confidentiality attacks

Confidentiality requires guarantees that unknown entities will never disclose classified information in the network [43]. It also prevents unauthorized access to private information, including name, plate, and location. Pseudonyms are used as the most popular technique in-vehicle networks to maintain privacy. That node of the vehicle will be encoded with many significant pairs. Messages are authenticated or signed with different psychographs, so this pseudo has not been connected to the vehicle's node; however, it is fixed by the qualified authority [44]. While attack on confidentiality, confidentiality is a vital safety requirement in-vehicle communications, guaranteeing that only authorized parties can be receiving the message [17]. In group communications, this type of security requirement is generally present in which only group members can read this information.

The remainder of the VANET. General information is transmitted through the remaining VANET settings. Because VANET mobility is more important than MANET, it is more complicated than Ad hoc to routing to guarantee security in VANET. Confidentiality of messages exchanged between vehicle network nodes is particularly vulnerable with techniques such as illegal messaging by eavesdropping and collecting local information available through broadcasting messages. The intruder will collect information from existing users around them in the condition of Eavesdropping. Allow using information while the user is unaware of the set. Security and confidentiality of the location are issues for vehicle drivers [45]. The following are its description and types:

a. Eavesdropping attack; eavesdropping is widely used in wireless networking technologies such as MANETs and VANETs. The aim is to obtain confidential information from the safe data. Therefore, unrequested users can know of the hidden specifications, including user identity theft and data location that can be used to identify vehicles.
b. Traffic analysis; an attacker analyses the traffic (collection of information/transactions) in this attack. By involve processing the vehicle network, the attacker collects all the information. The attacker can attack through a strategy by gathering information such as email addresses, requests, and responses from all vehicles communicating. It is also a passive attack in which the attacker does not make the data modifications.
c. Man-in-the-middle attack; this attack is taken from the v2v communication to tightly track and change communications. The attacker can access and control all V2V traffic, but communications companies believe they can communicate directly in private [46].
d. Social attack; the social attack is used to distract the focus of the driver. The attacker gives out immoral and immorality messages to the passengers. The attackers want the drivers to accept such unethical messages. VANET system often influences the driving actions and efficiency of the vehicle [47].

3.5. Non-repudiation attacks

The attacker may attempt to prevent the delivery of a message to escape liability after transmitting a message. Failure to repudiate allows attackers to be detected and prevents them from denying their crimes. All information is registered and stored on TPD to collect details from a formally authorized side [48]. While attack on non-repudiation, unless the user has the same key, two or three repudiations are not taken out. Therefore, two users are not differentiated and should not refuse to act. Reliable processing in different vehicles will avoid the same key. The following description and type as; repudiation attack: this attack happens if the attacker refuses to take action with sent messages [49].

4. DISCUSSION AND SUMMARY

Some researchers have been working to provide VANET authentication. However, confidentiality and availability in most studies are negligent. Also, double and related studies have been conducting. The need for more work on VANET security lies, therefore. Although no risk of immune from VANET can be assuring. As we know, secure strategies to enhance VANET privacy security must not be introduced with confidence. The exchange of information between the receiver and the sender must be protected from changes to improve efficiency. Several have addressed the challenges, but we aim to highlight the most important ones, including most small-and medium-sized networks and few significant networks. Through the use of surveys and studies. we are showing as; a) found out that encryption and authentication play a vital role in VANETS, b) analysis and performance evaluation showed that the proposed ACPN is feasible and adequate to UVC in the VANET environment for efficient privacy-preserving authentication with non-repudiation.

Due to the above information and challenges, we suggest in the future, work on; a) they are focusing on efforts and research on developing algorithms to work with extreme accuracy on large networks and test them on a huge data set, b) researchers must pay attention to these issues (that availability attacks have a more significant threat level compared to integrity and authentication) before using the blockchain as a tool to solve the rest of the problems, c) need new scenarios and simulations of hybrid cryptographic schemes to enhance the authentication process at low costs and be decentralized before VANET is practically implementing.

In summary, availability uses a group signature technique and interruption for security attacks. Authentication use certificate authority technique and fabrication for security attacks. Integrity uses a digital signature with a password technique and modification for security attacks. Confidentiality use encryption and decryption technique and interception for security attacks. At the same time, non-repudiation use sequence number and digital signature technique. Finally, confidentiality and authentication more secure than others.

5. CONCLUSION

In an open-access system, security messages are broadcasting VANETs are vulnerable to attack. Considerations related to VANET are covered, particularly in V2V and V2I. However, confidentiality and availability are almost non-existent in most studies. The article reviews the latest advancements to fill this gap and goes in-depth on the reasons and numerous dangers and risks. Furthermore, we discovered that encryption and authentication are crucial in VANETs. This paper's effectiveness shows that the ACPN is both feasible and appropriate for effective authentication to UVC in the VANET, according to analysis and performance evaluations. Also, we discussed security services and threats and attacks toward them. As future work, we suggest improving security and privacy by including artificial intelligence algorithms.

ACKNOWLEDGEMENTS

"Communication of this research is made possible through monetary assistance by Universiti Tun Hussein Onn Malaysia and the UTHM Publisher's Office via Publication Fund E15216"

REFERENCES

[1] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications,* vol. 7, pp. 7-20, 2017, doi: https://doi.org/10.1016/j.vehcom.2017.01.002.

[2] H. F. Mahdi, M. S. Abood, and M. M. Hamdi, "Performance evaluation for vehicular ad-hoc networks based routing protocols," *Bulletin of Electrical Engineering and Informatics (BEEI),* vol. 10, no. 2, pp. 1080-1091, 2021, doi: 10.11591/eei.v10i2.2943.

[3] A. S. Mustafa, M. M. Hamdi, H. F. Mahdi, and M. S. Abood, "VANET: Towards Security Issues Review," in *2020 IEEE 5th International Symposium on Telecommunication Technologies (ISTT),* 2020, pp. 151-156, doi: 10.1109/ISTT50966.2020.9279375.

[4] S. N. Pathak and U. Shrawankar, "Secured communication in real time VANET," *2009 Second International Conference on Emerging Trends in Engineering & Technology*, 2009, pp. 1151-1155, doi: 10.1109/ICETET.2009.198.

[5] M. S. Abood, A. S. Mustafa, H. F. Mahdi, A.-F. A. Mohammed, M. M. Hamdi, and N. A. Hussein, "The analysis of Teletraffic and Handover Performance in Cellular System," in *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 2021, pp. 1-5, doi: 10.1109/HORA52670.2021.9461300.

[6] M. A. Al-shareeda, M. Anbar, I. H. Hasbullah, S. Manickam, N. Abdullah, and M. M. Hamdi, "Review of Prevention schemes for Replay Attack in Vehicular Ad hoc Networks (VANETs)," in *2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP),* 2020, pp. 394-398, doi: 10.1109/ICICSP50920.2020.9232047.

[7] M. Hamdi, L. Audah, S. Rashid, A. Mustafa, and M. Abood, "A survey on data dissemination and routing protocol in VANET: Types challenges opportunistic and future role," *International Journal of Advanced Science and Technology,* vol. 29, no. 5, pp. 6473-6482, 2020.

[8] M. A. Al-Shareeda *et al.*, "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, doi: 10.18576/amis/140602.

[9] M. Noori, R. Sahbudin, M. S. Abood, and M. Hamdi, "A Performance Evaluation of Voice over IP Protocols (SIP and H. 323) in Wireless Network," EasyChair2516-2314, 2021.

[10] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Transactions on Parallel and Distributed Systems,* vol. 21, no. 9, pp. 1227-1239, Sept. 2010, doi: 10.1109/TPDS.2010.14.

[11] A. Wasef, R. Lu, X. Lin, and X. Shen, "Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]," *IEEE Wireless Communications,* vol. 17, no. 5, pp. 22-28, October 2010, doi: 10.1109/MWC.2010.5601954.

[12] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi, "Vehicular security through reputation and plausibility checks," *IEEE Systems Journal,* vol. 8, no. 2, pp. 384-394, June 2014, doi: 10.1109/JSYST.2013.2245971.

[13] 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 Journal,* 15 Jan.15, 2021, doi: 10.1109/JSEN.2020.3021731.

[14] M. S. Abood, M. M. Hamdi, A. S. Mustafa, Y. A. Najem, S. A. Rashid, and I. J. Saeed, "Analysis and Simulation for Mobile Ad Hoc Network Using QualNet Simulator," in *International Conference on Intelligent Systems Design and Applications,* 2020, pp. 689-700: Springer, doi: 10.1007/978-3-030-71187-0_63.

[15] S. A. Rashid, L. Audah, M. M. Hamdi, M. S. Abood, and S. Alani, "Reliable and efficient data dissemination scheme in VANET: a review," *International Journal of Electrical and Computer Engineering (IJECE),* vol. 10, no. 6, pp. 6423-6434, 2020, doi: 10.11591/ijece.v10i6.pp6423-6434.

[16] M. M. Hamdi, O. A. R. Al-Dosary, O. A. S. Alrawi, A. S. Mustafa, M. S. Abood, and M. S. Noori, "An overview of challenges for data dissemination and routing protocols in VANETs," in *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 2021, pp. 1-6, doi: 10.1109/HORA52670.2021.9461396.

[17] R. Hussain, F. Hussain, and S. Zeadally, "Integration of VANET and 5G Security: A review of design and implementation issues," *Future Generation Computer Systems,* vol. 101, pp. 843-864, 2019, doi: 10.1016/j.future.2019.07.006.

[18] G. Samara and Y. Al-Raba'nah, "Security issues in vehicular ad hoc networks (VANET): a survey," *arXiv preprint arXiv:1712.04263,* 2017.

[19] M. S. Sheikh, J. Liang, and W. Wang, "A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets)," *Sensors,* vol. 19, no. 16, p. 3589, 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, doi: 10.1016/j.vehcom.2017.02.001.

[21] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications,* vol. 44, pp. 1-13, 2014, doi: 10.1016/j.comcom.2014.02.020.

[22] M. M. Hamdi, Y. A. Yussen, and A. S. Mustafa, "Integrity and Authentications for service security in vehicular ad hoc networks (VANETs): A Review," *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA),* 2021, pp. 1-7, doi: 10.1109/HORA52670.2021.9461327.

[23] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Review of prevention schemes for modification attack in vehicular ad hoc networks," *International Journal of Engineering and Management Research,* vol. 10, 2020, doi: 10.2139/ssrn.3662927.

[24] M. A. H. Al Junaid, A. Syed, M. N. M. Warip, K. N. F. K. Azir, and N. H. Romli, "Classification of security attacks in VANET: A review of requirements and perspectives," in *MATEC Web of Conferences,* 2018, vol. 150, doi: 10.2139/ssrn.3662927.

[25] A. Quyoom, A. A. Mir, and A. Sarwar, "Security Attacks and Challenges of VANETs: A Literature Survey," *Journal of Multimedia Information System,* vol. 7, no. 1, pp. 45-54, 2020, doi: 10.33851/JMIS.2020.7.1.45.

[26] K.-M. Kouame and H. Mcheick, "Architectural QoS pattern to guarantee the expected quality of services at runtime for context-aware adaptation application," *SN Applied Sciences,* vol. 1, no. 5, p. 405, 2019, doi: 10.1007/s42452-019-0415-6.

[27] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, S. Manickam, and S. M. Hanshi, "Efficient conditional privacy preservation with mutual authentication in vehicular ad hoc networks," *IEEE Access,* 2020.

[28] E. Talavera, A. D. Álvarez, and J. E. Naranjo, "A review of security aspects in vehicular ad-hoc networks," in *IEEE Access,* vol. 8, pp. 144957-144968, 2020, doi: 10.1109/ACCESS.2020.3014678.

[29] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles," *Ad Hoc Networks,* vol. 90, p. 101823, 2019, doi: 10.1016/j.adhoc.2018.12.006.

[30] S. K. Bhoi and P. M. Khilar, "Vehicular communication: a survey," *IET networks,* vol. 3, no. 3, pp. 204-217, 2013, doi: 10.1049/iet-net.2013.0065.

[31] M. M. Hamdi, L. Audah, S. A. Rashid, and S. Alani, "VANET-based traffic monitoring and incident detection system: A review," *International Journal of Electrical & Computer Engineering (2088-8708),* vol. 11, no. 4, 2021, doi: 10.11591/ijece.v11i4.pp3193-3200.

[32] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *Journal of Network and Computer applications,* vol. 40, pp. 325-344, 2014, doi: 10.1016/j.jnca.2013.08.004.

[33] J. Cui, L. Wei, J. Zhang, Y. Xu, and H. Zhong, "An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems,* vol. 20, no. 5, pp. 1621-1632, 2018, May 2019, doi: 10.1109/TITS.2018.2827460.

[34] A. Daeinabi and A. G. Rahbar, "Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks," *Multimedia tools and applications,* vol. 66, no. 2, pp. 325-338, 2013, doi: 10.1007/s11042-011-0789-y.

[35] A. F. Femi, "Perception of performance appraisal and workers' performance in Wema Bank Headquarters, Lagos," *Global Journal of Arts, Humanities and Social Sciences,* vol. 1, no. 4, pp. 89-101, 2013.

[36] A. Y. Dak, S. Yahya, and M. Kassim, "A literature survey on security challenges in VANETs," *International Journal of Computer Theory and Engineering,* vol. 4, no. 6, p. 1007, 2012.

[37] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommunication Systems,* vol. 50, no. 4, pp. 217-241, 2012, doi: 10.1007/s11235-010-9400-5.

[38] S. Benkerdagh and C. Duvallet, "Cluster- based emergency message dissemination strategy for VANET using V2V communication," *International Journal of Communication Systems,* vol. 32, no. 5, p. e3897, 2019, doi: 10.1002/dac.3897.

[39] C. Sun, J. Liu, X. Xu, and J. Ma, "A privacy-preserving mutual authentication resisting DoS attacks in VANETs," *IEEE Access,* vol. 5, pp. 24012-24022, 2017, doi: 10.1109/ACCESS.2017.2768499.

[40] T. Karimireddy and A. G. A. Bakshi, "A hybrid security framework for the vehicular communications in VANET," in *2016 international conference on wireless communications, signal processing and networking (WiSPNET),* 2016, pp. 1929-1934, doi: 10.1109/WiSPNET.2016.7566479.

[41] A. Festag, "Cooperative intelligent transport systems standards in Europe," in *IEEE communications magazine,* vol. 52, no. 12, pp. 166-172, December 2014, doi: 10.1109/MCOM.2014.6979970.

[42] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Workshop on hot topics in networks (HotNets-IV),* 2005, pp. 1-6: Maryland, USA.

[43] I. A. Sumra, I. Ahmad, and H. Hasbullah, "Classes of attacks in VANET," in *2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC),* 2011, pp. 1-5, doi: 10.1109/SIECPC.2011.5876939..

[44] M. Abu Talib, S. Abbas, Q. Nasir, and M. F. Mowakeh, "Systematic literature review on Internet-of-Vehicles communication security," *International Journal of Distributed Sensor Networks,* vol. 14, no. 12, 2018, doi: 10.1177/1550147718815054.

[45] J.-C. Xi, Q.-Q. Kong, and X.-G. Wang, "Spatial polarization of villages in tourist destinations: A case study from Yesanpo, China," *Journal of Mountain Science,* vol. 12, no. 4, pp. 1038-1050, 2015, doi: 10.1007/s11629-014-3358-9.

[46] M. L. Das, A. Saxena, V. P. Gulati, and D. B. Phatak, "A novel remote user authentication scheme using bilinear pairings," *Computers & Security,* vol. 25, no. 3, pp. 184-189, 2006, doi: 10.1016/j.cose.2005.09.002.

[47] M. Raya and J.-P. Hubaux, "Security aspects of inter-vehicle communications," in *5th Swiss Transport Research Conference (STRC),* 2005, no. CONF.

[48] G. Samara, W. A. Al-Salihy, and R. Sures, "Security issues and challenges of vehicular ad hoc networks (VANET)," *4th International Conference on New Trends in Information Science and Service Science*, 2010, pp. 393-398.

[49] M. Azees, P. Vijayakumar, and L. J. Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks," *IET Intelligent Transport Systems*, vol. 10, no. 6, pp. 379-388, 2016.

BIOGRAPHIES OF AUTHORS

Mustafa Maad Hamdi was born in Al-Anbar, Iraq. He received the B.Eng. degree in Computer Engineering Technology from Al-Maarif University College, Iraq. and the M.Sc. degree in Communication and Computer Engineering from University Kebangsaan Malaysia (UKM), Malaysia. He is currently pursuing the Ph.D. degree in the department of communication engineering, University Tun Hussein Onn Malaysia (UTHM), Malaysia. His research interests include Wireless and Mobile Communications, VANET, MANET and Satellite Communication, and Cryptographic.

Lukman Audah was born in Kuala Lumpur, Malaysia. He received the B.Eng. degree in telecommunications from Universiti Teknologi Malaysia, in 2005, and the M.Sc. degree in communication networks and software and the Ph.D. degree in electronic engineering from the university of Surrey, U.K. He is currently a lecturer with the communication engineering Department, University Tun Hussein Onn Malaysia. His research interests include wireless and mobile communications, Internet traffic engineering, network system management, data security, and satellite communication.

Mohammed Salah Abood was born in Baghdad, Iraq, in 1981. He received the B.Eng. Degree in computer engineering from University of Technology, Baghdad-Iraq, in 2004, and the master's degree in communication and computer engineering, University Kebangsaan Malaysia (UKM), Malaysia, in 2016. He is currently studying toward the PhD degree in the field of information and communication engineering in Beijing Institute of Technology (BIT), Beijing, China, starting on 2019. His current research interests include network function virtualization. 5G.

Sami Abduljabbar Rashid was born in Al-Anbar, Iraq. He received the B.Eng. degree in computer engineering technology from Al-Maarif University College, Iraq. and the M.Sc. degree in communication and computer engineering from Universiti Kebangsaan Malaysia (UKM), Malaysia. He is currently pursuing the Ph.D. degree in the department of communication engineering, University Tun Hussein Onn Malaysia (UTHM), Malaysia. His research interests include wireless and mobile communications and VANET.

Ahmed Shamil Mustafa received his Master of Communication and Computer Engineering from Universiti Kebangsaan Malaysia (UKM), Malaysia in 2015. Currently serving as a lecturer in the Department of Computer Engineering Techniques at Al Maarif University College. He is highly interested in Communication, Computer Engineering, Image Signal Processing, and Digital Signal Processing (DSP).

Hussain Mahdi is a lecturer at Computer and Software, College of Engineering, University of Diyala, Iraq. He received the PhD from university of Kebangsaan Malaysia and Master of Science from University of Technology, Bagdad, Iraq. He is IEEE Region 10 Humanitarian activities committee (2017-2020), IEEE PES Young Professional Committee academic lead (2017-2020), IEEE IAS Chapters Area Chair, R10 Southeast Asia, Australia and Pacific (2018-2019), and IEEE Region 10 PES students Chapters Chair (2019-2020), IEEE PES Day 2019 Global Chair, and IEEE HAC Event committee member 2019-2020.

Ahmed Shakir Al-Hiti received his B.Eng in Electrical Engineering from the University of Baghdad, Iraq in 2008, computer Engineering from Al-Maarif University College, Iraq in 2012, and received his M.Sc. in communications and networks Engineering from University Putra Malaysia, Malaysia in 2017. He is currently working as a researcher in fiber lasers at the University of Malaya. His research interests include networks, control systems, wireless communications, photonics, and laser-plasma accelerators.