A Survey on Security Schemes based on Conditional Privacy-Preserving in Vehicular Ad Hoc Networks

Zeyad Ghaleb Al-Mekhlafi[1†] and Badiea Abdulkarem Mohammed [2††],
Ziadgh2003@hotmail.com *b.alshabani@uoh.edu.sa*
University of Ha'il, Computer Science and Engineering, Ha'il 81481, Saudi Arabia

Abstract
Contact between Vehicle-to-vehicle and vehicle-to-infrastructural is becoming increasingly popular in recent years due to their crucial role in the field of intelligent transportation. Vehicular Ad-hoc networks (VANETs) security and privacy are of the highest value since a transparent wireless communication tool allows an intruder to intercept, tamper, reply and erase messages in plain text. The security of a VANET based intelligent transport system may therefore be compromised. There is a strong likelihood. Securing and maintaining message exchange in VANETs is currently the focal point of several security testing teams, as it is reflected in the number of authentication schemes. However, these systems have not fulfilled all aspects of security and privacy criteria. This study is an attempt to provide a detailed history of VANETs and their components; different kinds of attacks and all protection and privacy criteria for VANETs. This paper contributed to the existing literature by systematically analyzes and compares existing authentication and confidentiality systems based on all security needs, the cost of information and communication as well as the level of resistance to different types of attacks. This paper may be used as a guide and reference for any new VANET protection and privacy technologies in the design and development.

Key words:
Vehicular Ad-hoc networks (VANETs), classification, authentication, conditional privacy-preserving, adversary.

1. Introduction

Over 1 million people are affected every year by a road incident. The damage to the driving circumstances is uniformly the 9th cause of death-rate and contributes to a absence of over 2% or 1 trillion dollars of the world's GDP [1], [2]. In addition, major fuel congestion waste and time.

Smart transport systems (ITSs) recently play an extremely important role in the digital world of the movement of the new citizen. ITSs include creative, in-depth software to track these unpleasant incidents, to increase vehicle traffic in future [3], [4]. It is designed for the construction of smart vehicles through the rapid development of wireless communication technologies [5]. The fact that wireless instruments become an essential component of each vehicle, enabling them to communicate with other cars or road structures, have been introduced by New Car telcos and manufacturers.

This vehicle is an ad hoc network that is known as the network node of the vehicle. These are called the Vehicle Ad-hoc Networks (VANET) a type of mobile ad-hoc networks (MANETs) which use wireless technology for the proximity and communication infrastructure vehicles[6],[7].

VANET communications are either classified as a car for infrastructure (V2I) or as a car for vehicles. communications (V2V). Each vehicle transmits a periodic security message with its location, traffic events, speed and heading with these communications. Even if a vehicle is legitimately or illegally protected, these security messages will be exchanged since VANET's propagation in an open communication.

Nevertheless, this would also enable opponents to change, replay, and transmit these safety messages into the system. Through the broadcasting of these updated and falsified safety alerts, situations such as road crashes, traffic disturbance, etc., may lead to the call for amendments to messaging safety. The safety problems in VANETs have to be dealt with carefully before they become realistic [8].

The rest of this paper is organized as follows: Section II presents the background regarding VANETs. Section III introduced security and privacy requirements. Section IV shows security schemes classification in VANETs. Conclusions of the this work are shown in Section V.

2. Background

2.1 VANET Components

As shown in Figure 1. The VANET System Model consists of three components, OBU, RSU and TA.

Manuscript received November 5, 2021
Manuscript revised November 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.11.14

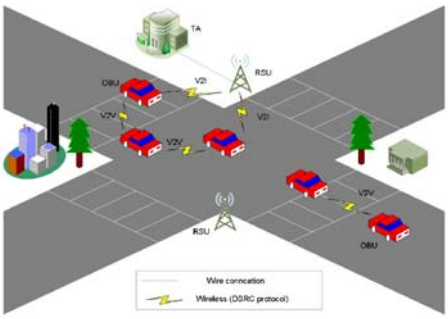

Fig. 1: The structure of system model in VANETs

- TA:

High computing and networking tools are accessible to trusted authorities. TA's liability for each vehicle creates public and pseudo-ID parameters for the device.

- RSU:

The Roadside Unit (RSU) is an infrastructure node, a wireless system situated at the lane. The RSU connects to TA via the cable channel and connects to wireless vehicles.

- OBU:

VANET vehicles have the onboard unit (OBU) to provide vehicles with the possibility for safety messages to be stored, received and broadcasted. OBUs are equipped with a TPD that is tamperproof and uses vital data for saving.

2.2 VANET Characteristics

The characteristics of the VANETs are:

- Driver safety:

VANET's primary benefits are providing both driver and passenger with convenient applications and improving traffic flow. It can communicate with multiple applications between RSUs and OBUs.

- Frequent network disconnection:

Due to speed movement between vehicles and other weather issues, VANETs are frequently disconnected. In addition, multiple vehicles on the road may cause the repeated disconnection.

- Dynamic network topology:

The VANET system varies rapidly, thanks to the easy and high mobility of vehicles. Owing to rapid alterations in topology of VANETs, vehicles are further vulnerable to offensives and are often more exposed to users or malicious vehicles.

- Frequent disconnection of the network:

Because of high-level-speed transport between other limitations and vehicles, for instance the weather, VANET connections are often sporadic. Furthermore, too few vehicles on the road may result in the repeated disconnection.

- Driver safety:

VANET's primary benefits are providing both driver and passenger with convenient applications and improving traffic flow. It can communicate with multiple applications between RSUs and OBUs.

- High mobility:

The key attribute of VANETs is high versatility in comparison to the MANETs and this plays a very critical role in VANETs. Every VANET node normally moves very quickly and that node movement minimizes the contact window for VANET vehicles.

- Dynamic network topology:

With regard to the fast and superior flexibility of the vehicle, the VANET system differs easily. Owing to the rapid changes in VANETs, vehicle attacks are more frequent and malicious vehicles cannot easily be detected.

2.3 Equations

The main function of VANETs is to promote and communicate through extra vehicles. VANET functions can be listed in this manner:

- Vehicle Application:

The application offers information for the driver on the road to increase vehicle safety.

- Driver Application:

The request alerts the driver to conditions such as road crashes, congestion and crashes. It supports the guide parking driver and the nearby base station.

- Comfort Application:

Different entertainment facilities are available for both drivers and passengers.

- Safety Application:

The application improves passenger protection by preventing any negative occurrences by warning blind spots of a safe transmission or by overtaking and leaving assistance.

3. VANETS SECURITY AND PRIVACY

3.1 Security and Privacy Requirements

The scheme proposed should meet the safety criteria of V2I and V2V communications inside the device in this manner:

- Integrity and authentication:

Wireless elements in VANETs need to be capable of determining any change in the protection messages received and need to be capable to verify safety messages receive and authenticate nodes for communications safety.

- Identity privacy preservation:

An opponent needs to be able to reveal the identity of the vehicle by collecting a variety of safety messages. Therefore, the character of the vehicle keeps other legal and illegal vehicles secret in order to protect drivers' privacy.

- Traceability and revocation:

In order to prevent malicious vehicles from refusing trust in their disturbance by sending bogie safe messages to other authenticated vehicles, the TA must be able to reveal the identity of the vehicle from its safety messages.

3.2 Security Attacks

Some security attacks are simple for opponents to lunch, because VANETs' contact is open to nature. In this segment, the abilities of an adversary in VANETs are briefly confronted with some vulnerabilities.

- Replay attacks:

The goal of mistreating cars is to replay the recipient with the old legal signature to make the idea that incidents occur.

- Modification attacks:

The aim is to adjust the authentic safety messages of vehicles and relay them to other nodes. A malicious vehicle, for instance, may feed messages to close vehicles. Therefore it is difficult to conduct the checking receiver with modified messages.

- Impersonation attacks:

The purpose of misbehaving vehicles is to send a proper security message to other vehicles where the assailant attempts to disguise himself as a registered vehicle.

- Man-In-The-Middle attacks.

The goal of misbehaving vehicles is to sniff and interrupt information on two contact sides.

3.3 Performance Evaluation Metrics

This paper concludes the Raya and Hubaux [11] efficiency parameter values, which include findings and the comparison of different schemes. We assigned corresponding language values for each of these parameters: strong, moderate or low. Table 1 displays a spectrum of device, medium and communications total high, medium or low values. The summation of these overheads gives the overall computational overhead after measurement of the calculation overhead for signature and verification of the message. In the meantime, the overhead communication is proportional to the size of the message for each device, varying from that of your payload in the message. The overhead is directly linked to the size of the post. Table 1 enables us to decide objectively which schema has low overall computational and communicative overheads, medium or high.

Table 1 Parameter Value of Performance

Parameter of performance	*Low*	Medium	High
Communicational Cost (bytes)	1 to 50	51 to 100	101 to 140
Computational Cost (ms)	1 to 3	3.1 to 6	6.1 to 10

4. Classifications of Security Schemes Based on Conditional Privacy-Preserving

Authentication and privacy are two key security aspects, which are essential for a VANET trust to be developed among vehicles. The use of proper authentication and privacy mechanisms makes it easier to recognise unlawful nodes and false messages for the protection of a VANET. Many investigators have put forward authentication mechanisms to tackle common VANET attacks for safe communications. Most schemes that use signatures of messages and signatures depend on different techniques. These schemes are divided into three sections in this paper: public key infrastructure-based security schemes based on conditional privacy-preserving (PKI-SCPP) schemes, group signatures-based security schemes based on conditional privacy-preserving (GS-SCPP) schemes, and identity-based security schemes based on restricted privacy-preserving (IDSCPP) schemes. In order to meet safety criteria, attack resistance and performance, existing systems were examined (communicational overheads and computational).

4.1 Public Key Infrastructure-Based Security Schemes Based on Conditional Privacy-Preserving (Pki-Scpp) Schemes

A wide, anonymous pool of around 43,800 certificates and their respective private keys will be preloaded at their necessary levels with authentication schemes using Public Key infrastructure (PKIs). The certificates, all of them signed by the TA, do not contain any identifying information concerning the vehicle identity, which makes them completely anonymous. To ensure long-term safety and privacy, for example for one year, each car will have enough preloaded certificates.

Wasef et al.[9] introduced the Expedite Message Authentication Protocol (EMAP) which adopts PKI for authentication of vehicles and a hash authentication code to optimize the integrity monitoring process.

Three overall reductions and robustness optimization have been identified for Calandriello et al.[10]. The first optimization involves a sender signing each pseudonym only once as the entire pseudonym remains the signature unchanged. Only when the pseudonym has been received can the verifier confirm its signature. The checker then saves the signature to be used later. The second optimisation is to only apply the pseudonym certificate until any message has the same validity duration.

Raya et al.[11] distributed thousands of pseudonyms in the first research into vehicles with the required privacy keys. The message sender chooses one pseudonym and is used for signing the messages with the corresponding

private key. The recipient shall be able to validate the pseudonym with the correct certificate.

4.2 Group Signatures-Based Security Schemes Based on Conditional Privacy-Preserving (Gs-Scpp) Schemes

This scheme allows group members to register behalf of the whole unit anonymously. But in the event of a disagreement, the musical group director may disclose the identity of the signature. Anonymity may also be maintained in group signature schemes in protected authenticated communications. Such schemes can also ensure safe contact with conditional confidentiality. These programs may be used to make signs missives to conceal the identity of the signatory.

Lim et al. [12] introduced to check the community signatures for a well-organize load distribution system from the TA to the RSU.

Shao et al. [13] suggested that bilinear pairings be used in distributed groupings with anonymous authentication protocol. It is based on a new community signing scheme which provides anonymous protocol with threshold authentication features.

Table. 3. Summary of Performance Evaluation Metrics

Schemes	Class	Computation Overhead	Communication Overhead
Wasef et al. [9]	PKI-SCPP	Low	High
Calandriello et al. [10]	PKI-SCPP	Medium	High
Raya et al. [11]	PKI-SCPP	High	High
Lim et al. [12]	GS-SCPP	High	-
Shao et al. [13]	GS-SCPP	High	-
Hasrouny et al. [14]	GS-SCPP	High	High
Zhang et al. [15]	ID-SCPP	Medium	Medium
Cui et al. [16]	ID-SCPP	Low	High
Ali et al. [17]	ID-SCPP	High	Medium

Hasrouny et al. [14] IEEE Security Standard 1609.2 offers ways to secure WAVE devices for message formats, application messages and messaging systems. It proposed to combine a stable VANET identity authentication system with community signatures and [18] ID-based signing systems.

4.3 Identity-Based Security Schemes Based on Conditional Privacy-Preserving (Id-Scpp) Schemes

Many researchers have suggested identity-based systems to overcome the weakness of PKI-based and group-based schemes. The essence of identification schemes is that information on identity is extracted by the government key, while private key is determined by TA.

The Chinese remaining theorem (CRT) was designed by Zhang et al. [15], to secure VANET communication. You suggested an authentication system that guaranteed privacy and required genuine TPDs to guarantee the highest level of protection for the entire VANET. The master key of the device must not be preloaded into the vehicle's OBU in their system.

A privacy conservation method for uploading data is suggested for the Cui et al. [16] by adapting the principle of VANET edge computing. Their schema enables the RSU, without compromising the privacy of download requests, to discover popular data by collecting encrypted requests transportation from nearby nodes.

In a bilinear plan for communication between the vehicles and infrastructure, Ali et al. [17] proposed an effective authentication system. This method uses one-way general hash functions instead of map-to-point hash functions. Table 2 and 3 summaries security schemes and their overhead.

Table. 2. Security and Privacy Requirements Fulfilled by Gp-Sps

Papers	***Class***	***Entity and Messaae auth.***	***Traceability***	***Privacy***	***Unlinkability***	***Replay attacks***	***Modification attacks***	***Impersonation attacks***	***MITM attacks***
Wasef et al. [9]	PKI-SCPP	✓	×				×	✓	
Calandriello et al. [10]	PKI-SCPP	✓	×				✓	✓	
Raya et al. [11]	PKI-SCPP	✓	×				×	✓	
Lim et al. [12]	GS-SCPP	✓	✓				✓	✓	
Shao et al. [13]	GS-SCPP	✓	✓				✓	✓	
Hasrouny et al. [14]	GS-SCPP	✓	×				✓	✓	
Zhang et al. [15]	ID-SCPP	✓	✓				✓	✓	
Cui et al. [16]	ID-SCPP	✓	×				×	✓	
Ali et al. [17]	ID-SCPP	✓	✓				✓	×	

5. Conclusion

VANET is a critical technology in ITS, which permits the transmission and exchange of messages between vehicles in order to support the security and road management services. In addition, ITS provides drivers and passengers with a variety of convenience and entertainment applications through VANET. However, VANET is susceptible to different types of attacks due to the use of free wireless networking media. Therefore, a security framework that satisfies all security and privacy criteria is required to resolve threats to the security and privacy of VANET. public key infrastructure-based security schemes based on conditional privacy-preserving (PKI-SCPP) schemes, group signatures-based security schemes based on conditional privacy-preserving (GS-SCPP) schemes, and identity-based security schemes based on conditional privacy-preserving (IDSCPP) schemes. In all three categories, we research and compare the strengths and weaknesses thereof, compliance with the protection and privacy criteria, the level of attack resistance and the results thereof (computational and communicational overheads). The safety and effectiveness of current VANET authentication schemes was analyzed and presented to enable researchers and developers to recognize and identify key features of VANET privacy and safety.

References

[1]. 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, pp. 1–1, 2020.

[2]. 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.

[3]. I. T. S. Committee et al., "IEEE trial-use standard for wireless access in vehicular environments-security services for applications and management messages," IEEE Vehicular Technology Society Standard, vol. 1609, p. 2006, 2006.

[4]. M. A. Al-Shareeda, M. Anbar, M. A. Alazzawi, S. Manickam, and A. S. Al-Hiti, "Lswbvm: A lightweight security without using batch verification method scheme for a vehicle ad hoc network," IEEE Access, pp. 1–1, 2020.

[5]. I. Ali, M. Faisal, and S. Abbas, "A survey on lightweight authentication schemes in vertical handoff," International Journal of Cooperative Information Systems, vol. 26, no. 01, p. 1630001, 2017.

[6]. M. A. Al-Shareeda, M. Anbar, S. Manickam, and A. A. Yassin, "Vppcs: Vanet-based privacy-preserving communication scheme," IEEE Access, vol. 8, pp. 150 914–150 928, 2020.

[7]. M. A. Al-shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "An efficient identity-based conditional privacy-preserving authentication scheme for secure communication in a vehicular ad hoc network," Symmetry, vol. 12, no. 10, p. 1687, 2020.

[8]. 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, vol. 8, pp. 144 957–144 968, 2020.

[9]. A. Wasef and X. Shen, "EMAP: Expedite message authentication protocol for vehicular ad hoc networks," IEEE transactions on Mobile Computing, vol. 12, no. 1, pp. 78–89, 2011.

[10]. G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks, 2007, pp. 19–28.

[11]. 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, 2005, pp. 11–21.

[12]. K. Lim, K. M. Tuladhar, X. Wang, and W. Liu, "A scalable and secure key distribution scheme for group signature based authentication in VANET," in 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON). IEEE, 2017, pp. 478–483.

[13]. J. Shao, X. Lin, R. Lu, and C. Zuo, "A Threshold Anonymous Authentication Protocol for VANETs," IEEE Transactions on Vehicular Technology, vol. 65, no. 3, pp. 1711–1720, 2015.

[14]. H. Hasrouny, C. Bassil, A. E. Samhat, and A. Laouiti, "Group-based authentication in v2v communications," in 2015 Fifth International Conference on Digital Information and Communication Technology and its Applications (DICTAP). IEEE, 2015, pp. 173–177.

[15]. J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "Pa-crt: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," IEEE Transactions on Dependable and Secure Computing, 2019.

[16]. J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu, and L. Liu, "Edge computing in vanets-an efficient and privacy-preserving cooperative downloading scheme," IEEE Journal on Selected Areas in Communications, vol. 38, no. 6, pp. 1191–1204, 2020.

[17]. I. Ali and F. Li, "An efficient conditional privacy-preserving authentication scheme for Vehicle-To-Infrastructure communication in VANETs," Vehicular Communications, vol. 22, p. 100228, 2020.

[18]. D. Tiwari, M. Bhushan, A. Yadav, and S. Jain, "A novel secure authentication scheme for vanets," in 2016 Second International Conference on Computational Intelligence & Communication Technology (CICT). IEEE, 2016, pp. 287–297.

Zeyad Ghaleb Al-Mekhlafi received the B.Sc. degree in computer science from the University of Science and Technology, Yemen, in 2002, the M.Sc. degree in computer science from the Department of Communication Technology and Network, Universiti National Malaysia (UKM), in 2011, and the Ph.D. degree from the Department of Communication Technology and Network, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, in 2018. He is currently a Lecturer with the University of Ha'il, where he is also an Assistance Professor with the Faculty of Computer Science and Engineering. His current research interests include wireless sensor networks, energy management and control for wireless networks, time synchronization, bio-inspired mechanisms, and emerging wireless technologies standard.

Badiea Abdulkarem Mohammed received his BSc in Computer Science from Babylon University, Iraq in 2002, M.Tech in Computer Science from University of Hyderabad, India in 2007 and PhD from Universiti Sains Malaysia, Malaysia in 2018. He is currently an Assistant Professor in the College of Computer Science and Engineering at University of Hail, KSA. He is permanently Assistant Professor at Hodeidah University, Yemen. His research focuses on Wireless Networks, Mobile Networks, Vehicle networks, WSN, Cybersecurity, and Image Processing. He is an IEEE member, Member, IAENG member, and ASR member. In his research area, he has published many papers in reputed journals and conferences.