e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-5 (October 2020)
https://doi.org/10.31033/ijemr.10.5.10

Review of Security and Privacy Scheme for Vehicular Ad Hoc Networks (VANETs)

Israa M. Al-dulaimi[1] and Ayman Khalil[2]
[1]Student, Faculty of Engineering, Islamic University of Lebanon, Beirut, LEBANON
[2]Lecturer, Faculty of Engineering, Islamic University of Lebanon, Beirut, LEBANON

[2]Corresponding Author: ayman.khalil23@gmail.com

ABSTRACT

Vehicles in a vehicular ad-hoc network (VANET) broadcast information about the driving environment in the road. Due to the open-access environment, this means that the VANET is susceptible to security and privacy issues. However, none of the related works satisfies all security and privacy requirements. Besides, their proposed has huge overhead in terms of computation and communication. The present paper is a provide a thorough background on VANETs and their entities; different security attacks; and all requirements of the privacy and security for VANETs. This paper may serve as a guide and reference for VANETs in the design and implementation of any new techniques for protection and privacy.

Keywords**—** Vehicular Ad Hoc Network, Elliptic Curve Cryptography, Security, VANET Efficient, Privacy

I. INTRODUCTION

In recent year, vehicle ad hoc networks (VANET) has become particularly involved in the utilize of traffic and protection services [1]–[3]. Vehicles in these technology are fitted to a wireless transmission instrument and could receive and send information related with traffic situation in important faster movements in comparison mobile ad-hoc networks (MANETs). The traffic information is exchange among vehicles as they move on the system [4]–[7].

For study, shopping, work or for some different reasons, humans have always been commuting. The mobility of people have improved a lot since the advent of vehicles[8][9]. Also the density area has increased traffic as an outcome. With high traffic increased, a large number of deaths and road accidents are occurred in road environment[10]–[12]. For these reasons, researchers are motivated to enhance an Intelligent Traffic System (ITS) which will decrease a number of injured and death humans. VANETs become a promising part of ITS, it must be secure enough to resist the possible vulnerabilities and attacks.

The VANET includes both many vehicles and some roadside unit (RSU). Vehicles are fitted to on-board units (OBUs) which refers to devices of wireless communication, thus enables vehicles to share message related to traffic with nearby vehicles and neighbor RSUs. VANET communication could classified into two communications, vehicle-to-infrastructure (V2I) communication and vehicle-to-vehicle (V2V) communication, as shown in Figure 1.

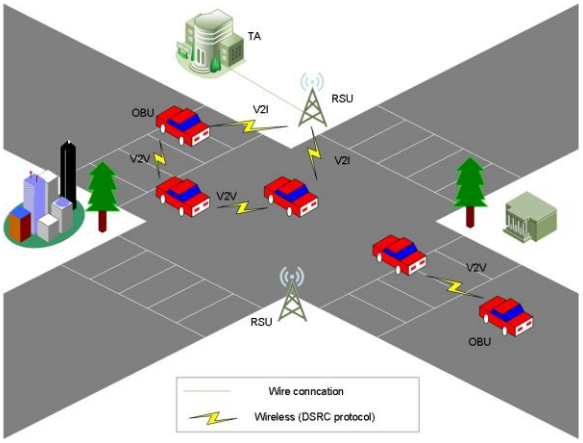

Figure 1: System model

VANETs have many applications that could benefit tremendously from the road condition as already introduced [13]. Still, the blade is double-edged. Privacy and security problems should be carefully considered in VANETs. Malicious vehicles can disturb the traffic road and get desired advantages. For instance, malicious vehicle that generates messages to create an emergency situation to misinform other vehicles to slow down, pull over and yield; a compromised vehicle that acts as an RSU can misinform other vehicles to a specific position and trigger a traffic issues [14]. If an adversary continues jamming a huge number of fake messages into a VANET, normal receiver and authentication of messages would be delayed; sensitive information such as the travail path of valid drivers may be leaked if the adversary passively scans traffic related messages in a specific region[15][16].

Clearly, such attacks may cause serious issues and can cause to traffic accidents. Thus, it is imperative to improve protection and privacy measures to avert these malicious attacks before applications of VANET are located and put into commercial utilize.

The rest of this paper is organized as follows. We bring some background information of VANET in Section II. In Sect. III, we present the security and privacy in VANET. Section IV describes the cryptographic algorithm. Section V reviews the existing work. A conclusion is finally stated in Section VI.

II. BACKGROUND

A. Vehicular Ad Hoc Networks (VANETs)

Almost more 1 million humans are injured and deaths by accidents of road per year. Traffic of road injuries are the ninth leading cause of death globally and incur the loss of around 3\% or USD 1 trillion of world Gross Domestic Product (GDP). Accident of road is evaluated to be the fifth causing death by 2030. Also, jams of traffic waste fuel and time [17].

The Intelligent Transportation System (ITS) plays a critical role in the movement related of new life in present. It is being introduced in order to structure vehicles of intelligent via the fast wireless communication technology growth[18]. New manufacturers of vehicle have accepted the fact that device of wireless will be an integral fraction of each vehicle, enabling it to communicate with road infrastructures and other vehicles.

B. Components of VANET

As illustrated in Figure 1, the proposed scheme consists of three entities[19] [20]: TA, RSU, and OBU. The three items are discussed below.

- **TA:** Is a completely trusted party in a VANET and is responsible for initializing and supplying RSUs and vehicles with device parameters including public and private key pairs.
- **RSU:** They are situated along the road as vehicle routers, and are considered part of the network infrastructure. An RSU manages the connectivity of all OBUs within its region and publishes messages relating to traffic.
- **OBU:** An OBU is a radio system mounted in a vehicle operating on the DSRC protocol for transmitting and receiving beacons from other rest of VANET components.

C. Communications of VANET

To enhance safety, traffic flaw, and avoid congestion of road, ITS technology focuses on the communication between components on the road by utilizing VANETs. As shown in Figure 1, there are main two kind of modes of communication: Vehicle-To-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications.

Vehicle-To-Vehicle (V2V)

In VANETs, vehicles broadcasts messages about traffic situation with others every 100 to 300 ms utilizing 5.9-GHz DSRC technology [21].

Vehicle-To-Infrastructure (V2I)

The TA supports beneficial applications and other traffic-related information to the passengers and drivers visualized via Graphic User Interface (GUI) of the system of infotainment. Besides, RSUs also broadcasts messages to ensure better traffic management and safety within their coverage area.

D. Applications

Communication of VANET supports passengers as well as drivers with numerous significant applications and provides a large number of non-safety and safety services regarding information [22][23]. As shown in Figure 2, applications of VANET could be classified into the following two categories:

1) Applications of Safety

The major aim of the applications of safety is to enhance the preserve the life and health of all nodes within environment of VANETs, including pedestrians. Some advantages of applications of safety [5] are as follows:

- Enhance road and traffic safety.
- Avert accidents and collisions.
- Support streaming of emergency video.
- Send lane altering warning.

2) Applications of Non-safety

The applications of non-safety of VANETs are also known as services of comfort with the aim to enhance luxury passenger and driving experience. Some of the utilities of applications of non-safety \cite{sheikh2019survey} are as follows:

- Update of Weather condition.
- Location restaurants and stations.
- Communication among users.
- Internet access.

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-5 (October 2020)
https://doi.org/10.31033/ijemr.10.5.10

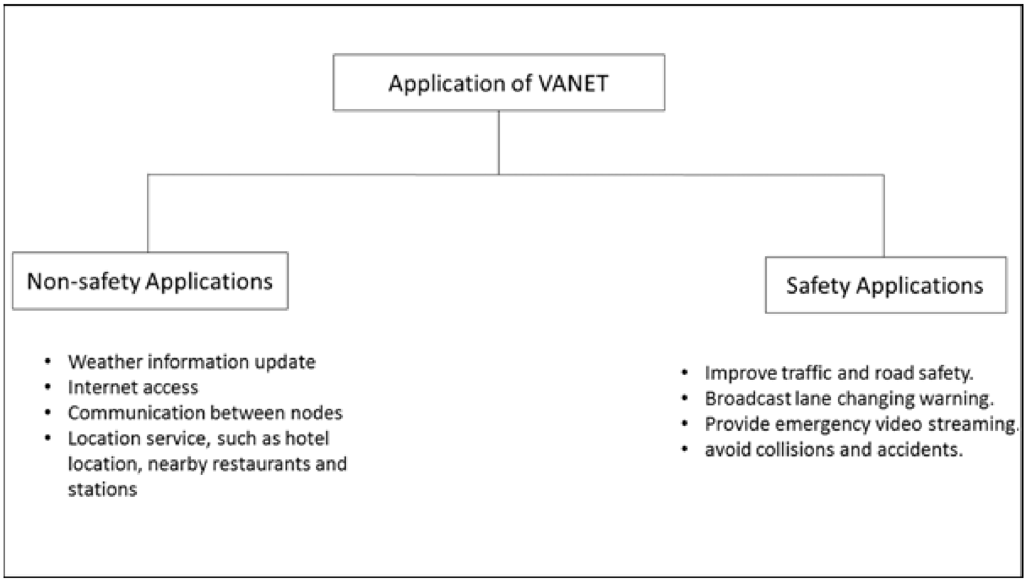
Application of VANET
Non-safety Applications
Weather information update
Internet access
Communication between nodes
Location service, such as hotel location, nearby restaurants and stations
Safety Applications
Improve traffic and road safety.
Broadcast lane changing warning.
Provide emergency video streaming.
avoid collisions and accidents.

Figure 2: Applications of VANET

III. SECURITY AND PRIVACY IN VANETs

Communication of VANET supports the passengers as well as drivers with the numerous applications and provides a large number of services. However, characteristic always come with challenges. Clearly, the privacy and security challenges on communication VANET should be carefully considered. Because of the open-access communication in VANET, the node suffers from challenges of security and privacy.

Security is an important requirement in VANET. Because of the open-access communication in VANET, it is vulnerable to various attacks. Thus, the adversary could launch numerous operations on message sent. Instance of these operations are: replays, modify and intercepts acquired broadcasted message to the recipient.

Privacy issues have become equally critical. During the communication, the adversary can obtain the real identity of vehicle or even set its traveling paths by analyzing the captured messages. Furthermore, the attackers have ability to link two or more broadcasted messages that by same source. So, an anonymous communication is needed to provide the vehicle privacy-preserving.

A. Security and Privacy Requirements

The proposed scheme should be satisfying security and piracy requirements as follows,

1. Security Requirements

- **Entity Authentication:** In the VANET, a recipient node has ability to verify the messages it has received and to guarantee the signer legitimacy.
- **Integrity:** The vehicle has ability to verify every message received from nodes, and the recipient have ability to detect any alteration to the messages.
- **Non-Repudiation:** The sender does not have ability to deny or dispute the its messages that were sent.
- **Traceability and Revocation:** These are essential criteria in a VANET, as they provide anonymity on condition. This means a TA should be able to track a malicious vehicle, disclose its original identity and revoke it from continuing to participate in VANET.

2. Privacy Requirements

- **Privacy-Preserving:** The scheme must satisfy the privacy protection requirement in a VANET, ensuring that private information about vehicles such as their location and identification should be protected and should not be exposed by the broadcast messages.
- **Unlinkability:** Malicious vehicle does not have ability to link two or more message which sent by same sender.

B. Types of Attacks

VANETs are easily vulnerable to specific security attacks since open-access V2V and V2I communications. In this subsection, we will present some vulnerabilities in the VANETs as follows.

- **Replay Attack:** A replay attack is a network attack kind where captured message is re-sent belatedly fraudulently to generate the illusion that incident is happening.

- **Modification Attack:** An attacker could send changed messages into the VANET system to achieve their given goal[24].
- **Impersonation Attack:** This attack aims other registered vehicles by broadcasting false messages to other nodes in which the attacker attempts to impersonate as a registered vehicle.
- **Man-in-the-Middle Attack:** The adversaries intercept messages and allows manipulation and sniffing of information[25] [26].

IV. CRYPTOGRAPHIC ALGORITHMS

To secure V2V and V2I communications in VANETs, many researchers use cryptographic algorithms such as Elliptic Curve Cryptography (ECC) and bilinear pair for signing and verifying messages.

A. Elliptic Curve Cryptography

1. ECC

Consider F_p indicates an order p finite field on E, where E is non-singular elliptic curve and p is a large prime value. Suppose an infinity point O set on E over F_p uses an equation $y^2 = x^3 + ax + b \mod p$, where the discriminant $\Theta = 4a^3 + 27b^2 \neq 0$ and $a, b \in F_p$. The elliptic curve E outputs a group G of additive cyclic under the point addition operation $P + Q = R$. Operation of scalar multiplication over F_p is expressed as $nP = P + P + ... + P$ for n times, where $n \in Z_q^*$ and $n> 0$.

2. Problems of Computational Hard

Problems of computational hard based on group G are presented as follows:

- **Elliptic Curve Discrete Logarithm (ECDL) problem:** Set two P and Q random points group G on E. The primary function of this problem is to discover an integer $s\in Z_q^*$ that fulfills $Q= sP$, where the unknown number s is difficult to calculate. Therefore, it is supposed that the ECDL problem becomes computational infeasible for any Probabilistic Polynomial Time (PPT) algorithms to resolve with probability of non-negligible.
- **Elliptic Curve Computational Differ-Hellman (ECCDH) problem:** Set two K and Q random points of group G on E, where $K=bP$, $Q=sP$ and $b,s \in Z_q^*$, the point $bsP \in G$ is difficult to compute. Therefore, it is supposed that the ECCDH problem becomes computational infeasible for any PPT algorithms to resolve with probability of non-negligible.

B. Bilinear Pair

Consider G_1 indicates a group of cyclic additive with generator P and G_2 indicates a group of cyclic multiplicative the same prime order p.

A bilinear pairing is a map $e : G_1 * G_1 \to G_2$ which fulfills features as follows [27],

- **Bilinearity:** For all $X, Y \in G_1$ and $a, b \in Z_p^*$, $e(aX, bY), (X, Y)^{ab}$.
- **Non-Degeneracy:** $e (P, P); \neq 1$.
- **Computability:** For all $X, Y \in G_1$, there is an efficient algorithm to calculate $e(X, Y)$.

V. EXISTING WORK

Recently, many research proposed security and piracy scheme for V2V and V2I communications in VANET. In this section, we present the existing schemes related to our proposed scheme as follow,

In 1984, Shamir published the first work using ID-based schemes [28]. The identification information is used as the public key of the node, while private keys are generated via a TA and then distributed to nodes using the same identity information. The recipients validate the message via the public key of the sender and sign the message using the private key of the sender.

Zhang et al. [29][30] used the vehicle user's identity in an ID-based scheme in which a vehicle does not need to save a large number of public and private keys and their certificates. This scheme therefore mitigates the amount of storage needed as well as the communication and computation costs. Additionally, it avoids the need for certificate management and a CRL.

The schemes proposed by Zhang et al. [29][30] support batch verification based on bilinear pairing for the messages received by a vehicle and an RSU, and thus achieve low verification costs, allowing several messages to be verified concurrently.

In 2009, Jiang et al. [31] used an ID-based scheme to propose the binary authentication tree (BAT) for V2I communication. BAT achieves high efficiency and meets the security and privacy requirements in VANETs.

In 2011, Huang et al. [32] proposed a new authentication scheme termed PACP, which depends on using pseudonyms rather than real identities, providing conditional privacy and efficiency in performance.

Chim et al. [33] pointed out, in 2011 that the schemes proposed in [29][30] have flaws that mean that an OBU can use a fake identity to eliminate the traceability requirement.

In the same context, Bayat et al. [34] introduced a new protection and privacy-preserving scheme based on RSU. In this system the RSUs are stored in the RSU's tamper-proof computer master keys.

Ming and Cheng [35] have introduced an elliptic curve-based, certificateless conditional privacy security scheme.

VI. CONCLUSION

VANETs are one of the most significant technologies in ITS since its role in supporting continuation among all the entities. This enables ITS to provide of a large number of services including increase traffic safety and efficiency for drivers and road users internet connectivity and entertainment facilities. Nevertheless, the VANET still address some issues due to its often-changing network topology since fast movement of nodes, and a large number of security attacks such as replay, modification, impersonation and MITM attacks. This paper presents the survey of existing schemes to prevent security attacks in VANET. The review paper provides that a number of new prevention schemes are required to cope with the growing security issues in V2V and V2I communications.

REFERENCES

[1] M. A. Al-shareeda, M. Anbar, I. H. Hasbullah, & S. Manickam. (2020). Survey of authentication and privacy schemes in vehicular ad hoc networks. *IEEE Sens. J.*, 1.

[2] M. A. Al-Shareeda, M. Anbar, S. Manickam, & A. A. Yassin. (2020). VPPCS: VANET-based privacy-preserving communication scheme. *IEEE Access*, *8*, 150914–150928.

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

[4] M. M. Hamdi, L. Audah, S. A. Rashid, A. H. Mohammed, S. Alani, & A. S. Mustafa. (2020). A review of applications, characteristics and challenges in vehicular ad hoc networks (VANETs). In: *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pp. 1–7.

[5] M. S. Sheikh, J. Liang, & W. Wang. (2019). A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets). *Sensors*, *19*(16), 3589.

[6] I. Ali, A. Hassan, & F. Li.m. (2019). Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey. *Veh. Commun.*, *16*, 45–61.

[7] M. Al Shareeda, A. Khalil, & W. Fahs. (2018). Towards the optimization of road side unit placement using genetic algorithm. In: *2018 International Arab Conference on Information Technology (ACIT)*, pp. 1–5.

[8] M. S. Talib, A. Hassan, B. Hussin, Z. A. Abas, Z. S. Talib, & Z. S. Rasoul. (2018). A novel stable clustering approach based on Gaussian distribution and relative velocity in VANETs. *Int. J. Adv. Comput. Sci. Appl.*, *9*(4), 216–220.

[9] M. S. Talib, A. Hassan, Z. A. Abas, A. Abdul-hussian, M. F. A. Hassan, & Z. J. AL-Araji. (2019). Clustering based affinity propagation in VANETs: Taxonomy and opportunity of research. *Int. J. Recent Technol. Eng.*, *7*, 672–679.

[10] A. H. Mohammed, M. M. Hamdi, S. A. Rashid, & A. M. Shantaf. (2020). An optimum design of square microstrip patch antenna based on fuzzy logic rules. In: *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pp. 1–7.

[11] M. Al Shareeda, A. Khalil, & W. Fahs. (2019). Realistic heterogeneous genetic-based RSU placement solution for V2I networks. *Int. Arab J. Inf. Technol*., 16(3A), 540–547.

[12] M. M. Hamdi, S. A. Rashid, M. Ismail, M. A. Altahrawi, M. F. Mansor, & M. K. AbuFoul. (2018). Performance evaluation of active queue management algorithms in large network. In: *2018 IEEE 4th International Symposium on Telecommunication Technologies (ISTT)*, pp. 1–6.

[13] A. K. Malhi, S. Batra, & H. S. Pannu. (2020). Security of vehicular ad-hoc networks: A comprehensive survey. *Comput. Secur.*, *89*, 101664.

[14] Y. Ming & X. Shen. (2018). PCPA: A practical certificateless conditional privacy preserving authentication scheme for vehicular ad hoc networks. *Sensors*, *18*(5), 1573.

[15] A. S. Mustafa, M. M. Al-Heeti, M. M. Hamdi, & A. M. Shantaf. (2020). Performance analyzing the effect of network size on routing protocols in MANETs. In: *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pp. 1–5.

[16] M. M. Hamdi, L. Audah, S. A. Rashid, A. S. Mustafa, & M. S. Abood. (2020). A survey on data dissemination and routing protocol in VANET: Types challenges opportunistic and future role. *Int. J. Adv. Sci. Technol*, *29*(5), 6473–6482.

[17] M. A. Alazzawi, H. Lu, A. A. Yassin, & K. Chen. (2019). Efficient conditional anonymity with message integrity and authentication in a vehicular ad-hoc network. *IEEE Access*, *7*, 71424–71435.

[18] I. Ali, M. Faisal, & S. Abbas. (2017). A survey on lightweight authentication schemes in vertical handoff. *Int. J. Coop. Inf. Syst.*, 26(01), 1630001.

[19] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, & N. Kumar. (2020). A lightweight privacy-preserving authentication protocol for VANETs. *IEEE Syst. J.*

[20] I. Ali & F. Li. (2020). An efficient conditional privacy-preserving authentication scheme for vehicle-to-infrastructure communication in VANETs. *Veh. Commun.*, *22*, 100228.

[21] Z. Lu, G. Qu, & Z. Liu. (2018). A survey on recent

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-5 (October 2020)
https://doi.org/10.31033/ijemr.10.5.10

advances in vehicular network security, trust, and privacy. *IEEE Trans. Intell. Transp. Syst.*, *20*(2), 760–776.

[22] M. A. Al-Shareeda, M. Anbar, M. A. Alazzawi, S. Manickam, & A. S. Al-Hiti. (2020). LSWBVM: A lightweight security without using batch verification method scheme for a vehicle ad hoc network. *IEEE Access*, *8*, 170507–170518.

[23] X. Yang *et al.* (2019). A lightweight authentication scheme for vehicular ad hoc networks based on MSR. *Veh. Commun.*, *15*, 16–27.

[24] M. A. Al-shareeda, M. Anbar, S. Manickam, & I. H. Hasbullah. (2020). Review of prevention schemes for modification attack in vehicular ad hoc networks. *International Journal of Engineering and Management Research*, *10*(3), 153-158.

[25] F. Ahmad, A. Adnane, V. N. L. Franqueira, F. Kurugollu, & L. Liu. (2018). Man-in-the-middle attacks in vehicular ad-hoc networks: evaluating the impact of attackers' strategies. *Sensors*, *18*(11), 4040.

[26] M. A. Al-shareeda, M. Anbar, S. Manickam, & I. H. Hasbullah. (2020). Review of prevention schemes for man-in-the-middle (MITM) attack in vehicular ad hoc networks. *International Journal of Engineering and Management Research*, *10*(3).

[27] E. Vahedi, M. Bayat, M. R. Pakravan, & M. R. Aref. (2017). A secure ECC-based privacy preserving data aggregation scheme for smart grids. *Comput. Networks*, *129*, 28–36.

[28] A. Shamir. (1984). Identity-based cryptosystems and signature schemes. In: *Workshop on the theory and application of cryptographic techniques*, pp. 47–53.

[29] C. Zhang, R. Lu, X. Lin, P.-H. Ho, & X. Shen. (2008). An efficient identity-based batch verification scheme for vehicular sensor networks. In: *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, pp. 246–250.

[30] C. Zhang, P.-H. Ho, & J. Tapolcai. (2011). On batch verification with group testing for vehicular communications. *Wirel. Network*s, 17(8), 1851.

[31] Y. Jiang, M. Shi, X. Shen, & C. Lin. (2008). BAT: A robust signature scheme for vehicular networks using binary authentication tree. *IEEE Trans. Wirel. Commun.*, *8*(4), 1974–1983.

[32] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, & A. Lioy. (2007). Efficient and robust pseudonymous authentication in VANET. In: *Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks*, pp. 19–28.

[33] T. W. Chim, S.-M. Yiu, L. C. K. Hui, & V. O. K. Li. (2011). SPECS: Secure and privacy enhancing communications schemes for VANETs. *Ad Hoc Networks*, *9*(2), 189–203.

[34]M. Bayat, M. Pournaghi, M. Rahimi, & M. Barmshoory. (2019). NERA: A new and efficient RSU based authentication scheme for VANETs. *Wirel. Networks*, pp. 1–16.

[35] Y. Ming & H. Cheng. (2019). Efficient certificateless conditional privacy-preserving authentication scheme in VANETs. *Mob. Inf. Syst.*, 2019.