International Journal of Engineering and Management Research e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-4 (August 2020)
www.ijemr.net https://doi.org/10.31033/ijemr.10.4.23

Proposal: An Efficient Security and Privacy Scheme based on Elliptic Curve Cryptography (ECC) for Vehicular Ad hoc Network (VANET)

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. To address the above issues, we will propose the security and privacy scheme based on Elliptic Curve Cryptography (ECC) and one secure hash function. Hence the reliability of each message being signed and checked has been improved. The main aim of this work is to satisfy all aspect requirements of security and privacy and reduce the computational complexity of the system.

Keywords— Elliptic Curve Cryptography, Vehicular Ad hoc Network, Security, Privacy

I. INTRODUCTION

Recently, vehicle ad hoc networks (VANETs) have become particularly involved in the use of protection and traffic services[1][2][3]. Vehicles in these technologies are equipped with a wireless transmission instrument and can send and receive messages with significantly higher movements compared to mobile ad-hoc networks (MANET)[4]. The traffic information is shared between vehicles as they move on the network. This helps drivers to control their ways of avoiding crowds, get warnings about road conditions and be alerted in advance of potential traffic coincidence[5][6][7].

A VANET consists of both vehicles and roadside units (RSUs). Vehicles are equipped with on-board units (OBUs) which indicate to wireless communication devices, therefore allows vehicles to exchange information related to traffic with each other and nearby RSUs[8][9]. The communication of VANET can divide into two modes, vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication[10], [11][12].

VANETs have several exciting applications that could benefit tremendously from our driving experience as already described. Still, the blade is double-edged. Security and privacy issues should be carefully considered in VANET[13]. Malicious vehicles can disturb the traffic road and obtain the desired benefits. For example, the malicious vehicle that produces 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 particular location and trigger a traffic problem. If an attacker continues jamming a large number of bogus messages into a VANET, normal receipt and authentication of messages would be delayed; private information such as the driving route of legitimate drivers may be leaked if the attacker passively scans traffic-related messages in a given area.

Obviously, such attacks may cause serious problems and can lead to traffic accidents. Therefore, it is imperative to develop protection and privacy measures to avoid these malicious attacks before VANET applications are deployed and put into commercial use.

Therefore, we propose an efficient security and privacy scheme against attacks and reduce the overhead of the system in terms of computation and communication cost. The rest of this paper is organized as follows. We bring some related work in Sect. II. In Sect. III, we present the background of the proposed scheme. Section IV describes the phases of the proposed scheme. A conclusion is finally stated in Sect. V.

II. RELATED 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 [14]. 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. [15][16] used the vehicle user's identity in an ID-based scheme in which a vehicle does not need to save a large

This work is licensed under Creative Commons Attribution 4.0 International License.

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-4 (August 2020)
https://doi.org/10.31033/ijemr.10.4.23

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. [15][16] 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. [17] 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. [18] 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. [19] and Lee and Lai [20] pointed out, in 2011 and 2013 respectively, that the schemes proposed in [15][16] have flaws that mean that an OBU can use a fake identity to eliminate the traceability requirement. In the same context, Bayat et al. [21] introduced 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 [22] have introduced an elliptic curve-based, certificateless conditional privacy security scheme.

III. BACKGROUND

A. Problem Sstatement

Detailed documentation is available in IEEE Trial Use Standard [23] for VANET security, including a choice of cryptograms. The rests of VANET components must sign messages with their private keys to authenticate a message sender and ensure the integrity of the message before transmitting traffic-related messages.

Figure 1 presents the format of a [23] signed traffic-related message. We can see for every 69-byte VANET message that a 125-byte certificate and a 56-byte ECDSA signature must be attached. Of course, the overhead cryptography (the certificate and the signature) constitutes a large part of the total packet size.

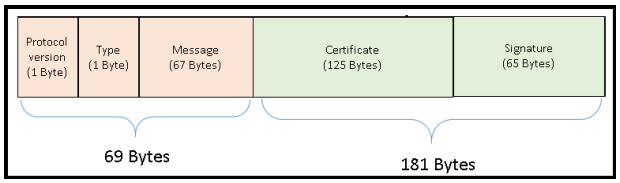

Figure 1: Signed Message Format

B. System Model

1-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.

2-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[24].

3-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. Security and Piracy Requirements

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

1-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.

2-Authentication and integrity: A receiver (vehicle or RSU) should have the capacity in a VANET to check the receiving beacon and make sure the sender is legitimate. In addition, the beacon's material should be checked to ensure it was delivered without abuse.

3-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.

4-Unlinkability: Malicious vehicle does not have the ability to link two or more message which sent by the same sender.

5-Security attacks resistance: An successful scheme in a VANET can withstand general attacks such as MITM attacks[25], replay, modification [26] and impersonation.

D. Research Methodology

As Figure 2, to attain the objectives, several methodological stages are followed:

1-review of the literature,
2-development of a new framework,
3-design and implementation,
4-testing and evaluation

In the first stage, the research problem is defined comprehensively analyzed through a critical review of existing schemes. In the second stage, the solution to the research problem is presented. The solution consists of several phases that select preliminaries, select phases and design scheme.

This work is licensed under Creative Commons Attribution 4.0 International License.

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-4 (August 2020)
https://doi.org/10.31033/ijemr.10.4.23

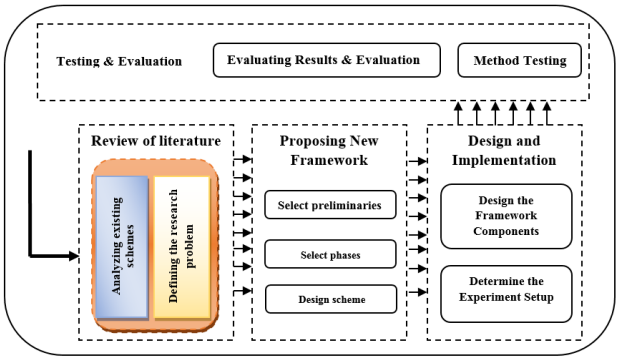

Figure 2: Main Stages of the Research Process

IV. PROPOSAL SCHEME

VANETs' protection and privacy concerns surrounding V2I and V2V contact should be handled carefully as soon as possible. Several researchers have recently suggested schemes for the widespread deployment of VANETs to cope with the above-mentioned problems. The proposed scheme typically has the following four phases: initialization of the system, signing message, verification message and trace of the original identity. The TA is responsible for defining and transmitting public parameters of the scheme to the rest of the entities in VANETs. The vehicle should be authenticated to that TA during the joining process, in order to exchange a traffic-related message based on the parameters via secure communication. The vehicle then computes its signature message and the verifier checks those signatures. If a complaint is received about a malicious vehicle, the TA should be able to locate and revoke the malicious vehicle by disclosure of the vehicle's original identity.

A. Initialization Phase

The TA is responsible for measuring the system-based ECC 's public parameter {p, q, a, b, P} and transmitting it to the remaining entities in VANETs.

B. Signing Message Phase

After the vehicle entering the RSU, it signs the message M_i \in{0, 1}^* with its pseudonym PID_i, chooses random r \in Z_q^*, picks the timestamp and calculates the signature \sigma_i.

C. Verification Message Phase

The timestamp validity is checking firstly after the checking receiver receives the message M_i. If new, By one of the following, it begins to verify the message M_i:

1-Single verification message (SVM)

In this method, checking receiver checks the signature\sigma_i on message M_i for pseudonym identity PID_i from a vehicle V_i. If the signature \sigma_m is not ligimtate, the receiver does not accept the message M_i. Otherwise, it accepts the message M_i.

2-Batch verification message (BVM)

If the checking recipient receives a large number of messages \{M_1, PID_1, \sigma_1\}, \{M_2, PID_2, \sigma_2\},.....,\{M_n, PID_n, \sigma_n\}, the signatures can be at the same time checked. In this method, vehicle gets a signatures batch \sigma_i = \{\sigma_1, \sigma_2, ..., \sigma_n\} on n messages M_i =\{M_1, M_2,.....,M_n\} for n pseudonym PID_i= \{PID_1, PID_2, ..., PID_n\} from n vehicle V_i = \{V_1, V_2, ..., V_n\}, where i= \{1, 2, ...,n\}. If the signature \sigma_i is not legitimate, the vehicle does not accept the messages M_i. Otherwise, it accepts message M_i.

D. Original Identity Trace Phase

In this method, when RSU broadcasts the report to TA about an unauthentic vehicle, which should be able to track and prevent the malicious vehicle by disclosing the vehicle's original identity.

V. CONCLUSION

Owing to the nature of an open-access environment, VANETs can cause serious challenges and problems. An efficient, conditional privacy-preserving authentication scheme for secure V2V and V2I communication is proposed in this paper. The purpose of the proposed will be to resist attacks on model safety and to meet security and privacy requirements in VANETs. Future work will be to implement the security and privacy scheme, in addition to evaluating and comparing the performance parameter related to the computation and communication model between the proposed and other existing schemes.

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.*, pp. 1.

[2] M. S. Talib, A. Hassan, B. Hussin, & A. A. Hassan. (2018). Vehicular ad-hoc networks: Current challenges and future direction of research. *Jour Adv Res. Dyn. Control Syst*, *10*(2), 2065–2074.

[3] 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.

[4] 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: *International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pp. 1–5.

[5] J. Zhang, J. Cui, H. Zhong, Z. Chen, & L. Liu. (2019).

This work is licensed under Creative Commons Attribution 4.0 International License.

PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. *IEEE Trans. Dependable Secur. Comput.*

[6] H. Zhong, B. Huang, J. Cui, Y. Xu, & L. Liu. (2017). Conditional privacy-preserving authentication using registration list in vehicular ad hoc networks. *IEEE Access*, *6*, 2241–2250.

[7] 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: *IEEE 4th International Symposium on Telecommunication Technologies (ISTT)*, pp. 1–6.

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

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

[11] 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*.

[12] 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: *International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pp. 1–7.

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

[14] A. Shamir. (1984). Identity-based cryptosystems and signature schemes. In: *Workshop on the Theory and Application of Cryptographic Techniques*, pp. 47–53.

[15] 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.

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

[17] 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.

[18] 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.

[19] 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.

[20] C.-C. Lee & Y.-M. Lai. (2013). Toward a secure batch verification with group testing for VANET. *Wirel. Networks*, *19*(6), 1441–1449.

[21] 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.

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

[23] M. Raya & J.-P. Hubaux. (2005). 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.

[24] 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.

[25] 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*. Available at: https://ijemr.net/ojs/index.php/ojs/article/view/519.

[26] 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), 149-152.

This work is licensed under Creative Commons Attribution 4.0 International License.