e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-3 (June 2020)
https://doi.org/10.31033/ijemr.10.3.23

Review of Prevention Schemes for Man-In-The-Middle (MITM) Attack in Vehicular Ad hoc Networks

Mahmood A. Al-shareeda[1], Mohammed Anbar[2], Selvakumar Manickam[3] and Iznan H. Hasbullah[4]
[1]Student, National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM), 11800, Penang, MALAYSIA
[2]Senior Lecturer, National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM), 11800, Penang, MALAYSIA
[3]Associate Professor, National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM), 11800, Penang, MALAYSIA
[4]Research Officer, National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM), 11800, Penang, MALAYSIA

[2]Corresponding Author: anbar@nav6.usm.my

ABSTRACT

Vehicular Ad-Hoc Network (VANET) is an indispensable part of the Intelligent Transportation System (ITS) due to its abilities to enhance traffic management and safety. Many researchers have been focused on specific areas involving management and storage data, protocols standardization, network fragmentation, monitoring, and quality of service. The benchmarks of security of VANET are studied and figured out in this paper. VANET provides the driver and passenger with the safety application as well as entertainment service. However, the communication between nodes in VANET is susceptible to security threats in both communication modes, which indicates the main hazard. In this paper, we identified different Man-In-The-Middle (MITM) attacks with various behaviors such as message tampering, message delaying, and message dropping, according to the literature. In this study, the essential background of VANET from architectural point of view and communication types are discussed. Then, the overview of MITM attack in VANET is presented. In addition, this paper thoroughly reviews the existing prevention schemes for MITM attack in VANET. This review paper reveals that there is still a need for a better and more efficient preventive scheme to address the MITM attack in VANET. This review paper could serve as evidence and reference in the development of any new security schemes for VANETs.

Keywords— Vehicular Ad hoc Networks (VANETs), Security, Man-In-The-Middle (MITM), Authentication and Attacks

I. INTRODUCTION

With the huge amount of road crashes, traffic density, consumption of fuel, and pollution of the environment, these issues have put human life in danger. To reduce and manage these issues, the Intelligent Transportation System (ITS) introduced the modern technology Vehicular Ad-Hoc Network (VANET) which does not only provide safety application for driver and passenger but also offer the entertainment service during travailing in driving environment[1]–[3]. This network is a class of mobile ad-hoc network (MANET) [4]–[9].

Typically, the structure of VANET contains the three main components, and one Trusted Authority (TA), multiple fixed Road-Side Units (RSU), and a large number of mobility On-Board Units (OBUs) which equipped for each vehicle. The nodes of VANETs can exchange information about its status in the driving road with others by Vehicle-To-Vehicle (V2V) communication and Vehicle-To-Infrastructure (V2I) communication via Dedicated Short-Range Communication (DSRC) technology.

Due to the nature of V2V and V2I communications, VANET is susceptible to different types of attacks, which can change, replay, and impersonate the authentic message during the broadcasting process. Therefore, security issues should be carefully considered in VANET. Many researchers have been focused on specific areas involving management and storage data, protocols standardization, network fragmentation, monitoring, and quality of service, but the benchmarks of security of VANET are studied in this work.

However, the communication between nodes in VANET is susceptible to various attackers, such as Man-In-The-Middle (MITM) attacks, which indicates the main hazard. In this paper, we identified different MITM attacks with various their behavior, such as message tampering, message delaying, and message dropping. This study could serve as evidence and reference in the development of any new security schemes for VANETs.

The rest of the paper is structured as follows. An architecture of VANETs is described in Section II. Section III briefly reviews the MITM attacks. A few current works are listed in Section IV. Section V provides the conclusion of this work.

II. THE ARCHITECTURE OF VANETs

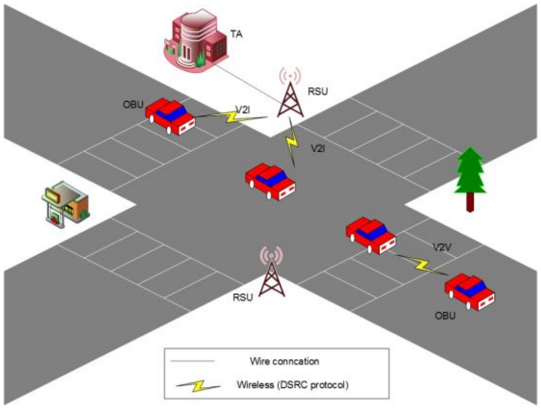

Figure 1: The architecture of VANETs

A. VANET Components

As shown in Figure 1, there are three of main components in VANETs [10][11].

1- Trusted Authority (TA)

Is fully trusted by all components in VANET with strong resource in terms of computation, communication and storage. The main responsibility of TA is to register the other rest components and issue the public parameter of system [12][13]. The communications between TA and RSU, RSU, and OBU are wired technology and wireless technology, respectively. The connection between TA and RSU is ensured by a secure channel. Besides. The TA has the ability to disclose the original identity of misbehavior vehicles. Therefore, it traces the behavior of vehicles during travailing in VANET[14][15].

2- Road-Side Units (RSUs)

Is installed to the roadside and works as interface application between TA and vehicles [16][17]. The main responsibility of RSU is to provide network access to all the nodes within its range of communication. Moreover, the RSU also sends the entertainment content to nearby vehicles.

3- On-Board Units (OBUs)

To enhance traffic management and driving experience, each vehicle is fitted with OBU, which allows the vehicle to exchange information with other vehicles or nearby RSUs within its range of communication. Each OBU has TPD, which is possible by the attacker to reveal the sensitive information stored [18]–[20].

B. VANET Communications

As shown in Figure 1, there are two of main mode communication [21][22].

1- Vehicle-To-Vehicle (V2V) Communications

In communications of V2V [23][24], the vehicle periodically exchanges the information about its driving environments such as speed, location, and brake status among the vehicles within range of communication [25]. Due to vehicle can only get the message from another vehicle, this communication becomes deficient in guaranteeing the owner of vehicle safety during travailing in VANET.

2- Vehicle-To-Infrastructure (V2I) Communications

In communications of V2I [26][27], the vehicle can exchange the information to nearby infrastructures such as RSU among the road. The vehicle can request entertainment service and access the internet [28]. This type of communication is supplement with V2V communications. The main aim of V2I communication is to enhance traffic management and driving environment.

III. Overview of Man-In-The-Middle (MITM) Attack

"Man-In-the-Middle" is the term used by basketball players who attempt to intercept the ball in the middle while two other players are attempting to pass it [29][30]. In this context, the MITM attacker hazards communication and alter information sent between authentic vehicles in VANETs. This type of attack is a leading creation disaster on the communication in VANETs especially if information sent content includes critical information about the statues road during the driving environment. To lunch the MITM attack by an adversary, he/she should be meet the following two situations, (i) the information including important data should be received by the misbehaving vehicle, and (ii) the adversary has the ability to interpret the information content [30]. Figure 2 shows the two types of MITM in VANETs.

- Passive Attacker: Passively, MITM can eavesdrop on the network among authentic vehicles.
- Active Attacker: Actively, MITM can delays, drops, or tampers the received message content in the communication channel.

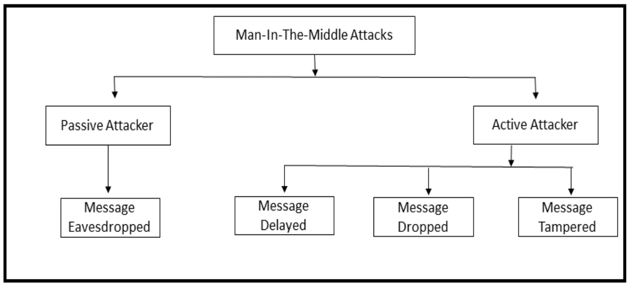

Figure 2: Man-In-The-Middle Attacks in VANET

Figure 4 shows the explanation of passive and active MITM attacks in VANET. It can be shown that passively, MITM can eavesdrop on the network among authentic vehicles, and actively, MITM can delays, drops, or tampers the received message content in the

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-3 (June 2020)
https://doi.org/10.31033/ijemr.10.3.23

communication channel. we identified different MITM attacks with various their behavior such as message tampering, message delaying, and message dropping, according to [30].

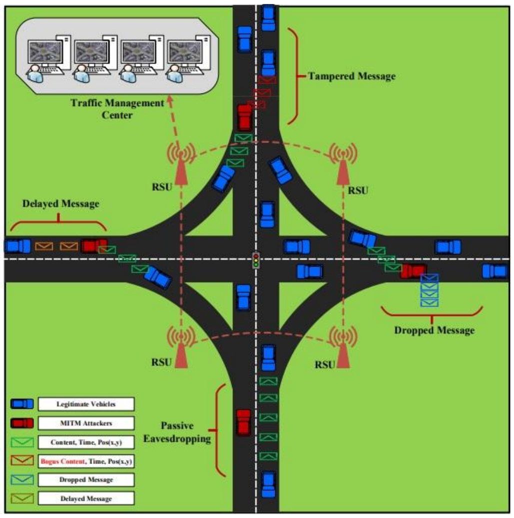

Figure 3: Explanation of Passive and Active MITM Attacks in VANET [30]

1- MITM as Message Delayed

In MITM as message delayed, the attacker intentionally delays the messages, i.e., the messages are sent to the next vehicle with a 'delay' factor. This delay causes severe consequences in the communication channel. Therefore, this case can put the life of a person in hazard [30].

2- MITM as Message Dropped

MITM as message dropped also indicates to "black hole" attacks, where adversary deliberately drops the received authentic information from the vehicle in VANETs, therefore suppressing the extra propagation of information[31]. Dropping such safety-related messages can put the life of a person in hazard as they are prohibited from receiving the personal message by the adversary [30].

3- MITM as Message Tampered

In MITM as message tampered, the adversary essentially goals the received information content. Whenever the attacker can receive a message, he/she alters the information content. This tampered lead to a severe impact on communication as the content may include a personal message [30].

IV. LITERATURE SURVEY

He et al. [32] introduced security scheme based privacy-preserving for both V2V and V2I communication in VANETs. This scheme firstly utilizes Elliptic Curve Cryptography (ECC) rather than bilinear pair operation during the broadcasting procedure. This scheme supports the batch verification process to authenticate a large number of messages related to driving the environment in VANET. According to a random oracle model related to authentication of the message, they provide authentication between the signer and the receiver. Therefore, the MITM is resisting in their scheme.

Ali and Li [33] introduced an identity security scheme based privacy-preserving for V2I communication in VANETs. This scheme utilizes the operation of the bilinear map to increase the process of message authentication at RSU. Thus, they support the batch verification process, which allows the RSU to verify multiple messages during the broadcasting process. It utilizes general one-way hash functions instead of map-to-point hash functions during the verification in density area with high traffic. The authentication process involves between the signer and the receiver from a vehicle of traffic-related messages transmitted. Therefore, the MITM attack is resisting in V2I communication in their scheme.

Wu et al. [34] proposed a security scheme based conditional privacy-preserving for V2V and V2I communication in VANETs. This scheme depends on location-based to use the position information to assign partial master key of vehicles. To hide the original identity of the vehicle, its sign information with unassociated pseudonyms. This scheme does not utilize the TPDs and bilinear pairing operations during the deployment of VANETs. The adversary can set this MITM more easily. Despite directly communicating with each other, the MITM cannot relay and alter the communication between singer and receiver in their scheme. Therefore, they should be able to withstand the MITM attack.

Ming and Cheng [35] proposed security scheme based privacy-preserving for V2I communication. This scheme is based on certificateless cryptography and (ECC). In their scheme, they do not use operations of bilinear pairing and map-to-point hash function, which them time-consumed. By using the verifying equation from the verifier side, the MITM attack cannot modify any message sent.

Cui et al. [36] introduced the data downloading scenario in VANETs; therefore, they proposed a privacy-preserving data downloading scheme to deal with multiple huge numbers of data on Social media and real traffic. This is because it's not fully efficient to plainly download the form RSU. This scheme is based on the concept of edge computing for V2V and V2I communication. By utilizing the Advanced Encryption Standard (AES) algorithm, the vehicle encrypted the downloading request sent to the content service provider. Because of the hardness of AES security, the MITM attack cannot decrypt the vehicle of encrypted the downloading request sent without obtaining the key messages of each session. Therefore, MITM may need to obtain the key messages of each session from the key agreement phase. Nevertheless, the MITM attack cannot obtain the key messages of each session due to the hardness of solving Elliptic Curve Computational Diffie Hellman Problem (ECCDHP).

Alazzawi et al. [37] proposed a pseudo-ID-based scheme for V2V and V2I communication. This scheme based on utilizing a pseudonym rather than the original identity and supports conditional anonymity, authentication, and integrity of the message. In their scheme, the time-consumed bilinear pairing operation is not used during the signing and verifying the message. The creation of the mutual authentication process is executed between the signer and the receiver. If an attacker tries a MITM attack, he/she requires to forge message-signature to communicate with the signer and the receiver. Nevertheless, according to the random oracle model, it is impossible for an attack to release an MITM attack.

Li et al. [38] presented a provably-secure scheme based conditional privacy-preserving to cope with the problem of master key of the system, high overhead in terms of computation cost during the broadcasting process. This scheme supports security and privacy needed in the services of VANET. This scheme also supports the mutual authentication process to authenticity between the singer and receiver. Therefore, their scheme is able to resist MITM attacks in VANETs.

Ali et al. [39] introduced an identity security scheme based privacy-preserving to secure communication for V2V communication in VANETs. This scheme based on ECC and supports the batch verification method. To migrate the computation complexity, they utilize the general one-way hash functions rather than Map-To-Point hash functions. Due to the limit of V2V communication that guarantees the absence of attackers. Therefore, this scheme is protected against MITM attacks

V. CONCLUSION

VANET is one of the most important technologies in ITS due to its role in providing connectivity between all the components. This allows ITS to offer of a wide range of services including entertainment facilities, internet connectivity, and increase traffic safety and efficiency for drivers and road users. However, the VANET still confronts many challenges due to its often-changing network topology due to high mobility of vehicles on the road, and numerous security attacks such as MITM attacks. This paper presents the survey of existing schemes to prevent MITM attacks in VANET. This review paper shows that there is still a need to address the growing problems of security in VANET communication for a robustness preventive scheme to prevent MITM attack on VANET.

ACKNOWLEDGEMENT

This work is partially supported by National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia and External Grant by UMobile Sdn Bhd (Grant no: 304/PNAV/650958/U154).

REFERENCES

[1] 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.

[2] Z. Afzal & M. Kumar. (2020). Security of vehicular Ad-hoc networks (VANET): A survey. In *Journal of Physics: Conference Series*, *1427*(1), 12015.

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

[4] B. H. Khudayer, M. Anbar, S. M. Hanshi, & T.-C. Wan. (2020). Efficient route discovery and link failure detection mechanisms for source routing protocol in mobile ad-hoc networks. *IEEE Access*, *8*, 24019–24032.

[5] 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.

[6] M. Al-Shalabi, M. Anbar, T.-C. Wan, & A. Khasawneh. (2018). Variants of the low-energy adaptive clustering hierarchy protocol: Survey, issues and challenges. *Electronics*, *7*(8), 136.

[7] M. Al-Shalabi, M. Anbar, T.-C. Wan, & Z. Alqattan. (2019). Energy efficient multi-hop path in wireless sensor networks using an enhanced genetic algorithm. *Inf. Sci. (Ny).*, *500*, 259–273.

[8] M. A. Al-Shalabi, M. Anbar, & A. Obeidat. (2019). Alternating sensing process to prolong the lifetime of wireless sensor networks. *J. Theor. Appl. Inf. Technol.(JATIT)*, *97*(7), 2132–2141.

[9] A. K. Al-Ani, M. Anbar, A. Al-Ani, & D. R. Ibrahim. (2020). Match-prevention technique against denial-of-service attack on address resolution and duplicate address detection processes in IPv6 link-local network. *IEEE Access*, *8*, 27122–27138.

[10] J. Cui, W. Xu, Y. Han, J. Zhang, & H. Zhong. (2020). Secure mutual authentication with privacy preservation in vehicular ad hoc networks. *Veh. Commun.*, *21*, 100200.

[11] S. Wang, K. Mao, F. Zhan, & D. Liu. (2020). Hybrid conditional privacy-preserving authentication scheme for VANETs. *Peer-to-Peer Netw. Appl.*, 1–16.

[12] M. A. Alazzawi, K. Chen, A. A. Yassin, H. Lu, & F. Abedi. (2019). Authentication and revocation scheme for VANETs based on Chinese Remainder Theorem. In: *IEEE 21st International Conference on High Performance*

Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pp. 1541–1547.

[13] S. A. Alfadhli, S. Alresheedi, S. Lu, A. Fatani, & M. Ince. (2019). ELCPH: An efficient lightweight conditional privacy-preserving authentication scheme based on hash function and local group secrete key for VANET. In: *Proceedings of the 2019 The World Symposium on Software Engineering*, pp. 32–36.

[14] J. Cui, D. Wu, J. Zhang, Y. Xu, & H. Zhong. (2019). An efficient authentication scheme based on semi-trusted authority in VANETs. *IEEE Trans. Veh. Technol.*, *68*(3), 2972–2986.

[15] X. Zhang, L. Mu, J. Zhao, & C. Xu. (2019). An efficient anonymous authentication scheme with secure communication in intelligent vehicular ad-hoc networks. *TIIS*, *13*(6), 3280–3298.

[16] 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.

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

[18] 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.

[19] S. M. Pournaghi, B. Zahednejad, M. Bayat, & Y. Farjami. (2018). NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET. *Comput. Networks*, *134*, 78–92.

[20] S. E. Shladover. (2018). Connected and automated vehicle systems: Introduction and overview. *J. Intell. Transp. Syst.*, *22*(3), 190–200.

[21] J. Zhang, J. Cui, H. Zhong, Z. Chen, & L. Liu. (2019). *PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks*. Available at: https://leicester.figshare.com/articles/PA-CRT_Chinese_Remainder_Theorem_Based_Conditional_Privacy-preserving_Authentication_Scheme_in_Vehicular_Ad-hoc_Networks/10237562/1.

[22] J. Cui, L. Wei, J. Zhang, Y. Xu, & H. Zhong. (2018). An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.*, *20*(5), 1621–1632.

[23] M. S. Sheikh, J. Liang, & W. Wang. (2020). *Security and privacy in vehicular ad hoc network and vehicle cloud computing: A survey*. Available at: https://www.hindawi.com/journals/wcmc/2020/5129620/..

[24] D. Manivannan, S. S. Moni, & S. Zeadally. (2020). Secure authentication and privacy-preserving techniques in vehicular ad-hoc NETworks (VANETs). *Veh. Commun.*, pp. 100247.

[25] J. B. Kenney. (2011). Dedicated short-range communications (DSRC) standards in the United States. *Proc. IEEE*, *99*(7), 1162–1182.

[26] M. A. Alazzawi, H. Lu, A. A. Yassin, & K. Chen. (2019). Robust conditional privacy-preserving authentication based on pseudonym root with cuckoo filter in vehicular ad hoc networks. *KSII Trans. Internet Inf. Syst.*, *13*(12), 6121–6144.

[27] 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.

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

[29] G. N. Nayak & S. G. Samaddar. (2010). Different flavours of man-in-the-middle attack, consequences and feasible solutions. In: *3rd International Conference on Computer Science and Information Technology*, *5*, 491–495.

[30] 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.

[31] J. Tobin, C. Thorpe, & L. Murphy. (2017). An approach to mitigate black hole attacks on vehicular wireless networks. In: *IEEE 85th Vehicular Technology Conference (VTC Spring)*, pp. 1–7.

[32] D. He, S. Zeadally, B. Xu, & X. Huang. (2015). An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Trans. Inf. Forensics Secur.*, *10*(12), 2681–2691.

[33] I. Ali & F. Li. (2020). An efficient conditional privacy-preserving authentication scheme for Vehicle-To-Infrastructure communication in VANETs. *Veh. Commun.*, *22*, 100228.

[34] L. Wu, J. Fan, Y. Xie, J. Wang, & Q. Liu. (2017). Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks. *Int. J. Distrib. Sens. Networks*, *13*(3), 1550147717700899.

[35] Y. Ming & H. Cheng. (2019). *Efficient certificateless conditional privacy-preserving authentication scheme in VANETs*. Available at: https://www.hindawi.com/journals/misy/2019/7593138/.

[36] J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu, & L. Liu. (2020). Edge computing in VANETs- an efficient and privacy-preserving cooperative downloading scheme. *IEEE J. Sel. Areas Commun.*, *38*(6), 1191–1204.

[37] 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.

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-3 (June 2020)
https://doi.org/10.31033/ijemr.10.3.23

[38] J. Li *et al.* (2018). EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *Veh. Commun.*, *13*, 104–113.

[39] I. Ali, T. Lawrence, & F. Li. (2020). An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs. *J. Syst. Archit.*, *103*, 101692.