Review of Prevention Schemes for Modification 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) technology is the basis of Intelligent Transportation System (ITS) connectivity that enables the delivery of useful information to and fro between vehicles in vehicle-to-vehicle communication mode; or between vehicle and infrastructure in vehicle-to-infrastructure mode for safety and comfort. However, due to the openness of the wireless medium used by VANET, the technology is vulnerable to security threats in both communication modes. In this study, the essential background of VANET from architectural point of view and communication types are discussed. Then, the overview of modification attack in VANET is presented. In addition, this paper thoroughly reviews the existing prevention schemes for modification attack in VANET. This review paper reveals that there is still a need for a better and more efficient preventive scheme to address the modification attack in VANET.

***Keywords*—** Vehicular Ad hoc Networks (VANETs), Security, Modification Attacks, Authentication and Attacks

I. INTRODUCTION

Nowadays, vehicles have become an indispensable part of our life that is being utilized by many for the transportation of goods and people with the rapid development of manufacturing channels and the proceed of person culture [1]–[3]. The roads, especially in urban areas, are inundated with vehicles such as personal cars, police cars, ambulances, trucks, and buses; and the numbers are increasing every year, without sign of decline. The increase has led to multiple issues, such as increased road accidents, traffic management difficulties and traffic congestion during rush hour. Researchers turned their focus on vehicular networks and intelligent transport systems (ITS) to address these issues [4]–[7].

No vehicular network technologies garnered as much attention as Vehicle Ad hoc Network (VANET). VANET is the technology that forms the backbone of Intelligent Transportation System (ITS) connectivity that enables the delivery of useful information to and fro vehicles for safety and comfort. has been designed to equip every vehicle with an on-board unit (OBU) and to deploy road-side units (RSUs) along the road and at road intersects. VANETs has two modes of communication: vehicles-to-vehicles (V2V) communication and vehicle-to-infrastructure (V2I) communication modes, as shown in Figure 1. Despite of many benefits of VANETs in ITS application, there are also challenges in implementing VANET, such as protection of traffic-related messages, and high computational and communicational costs. As a result, any proposal for new security schemes for VANET should address all these challenges [8]–[10].

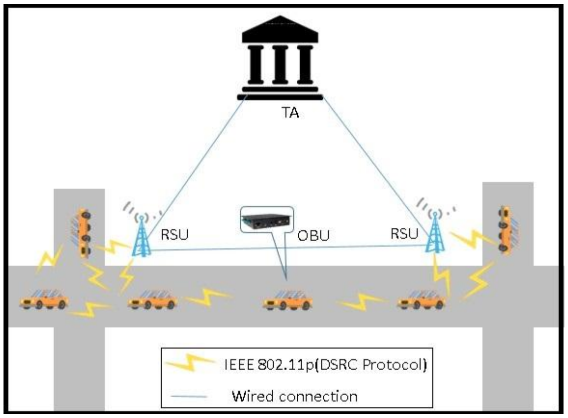

Figure 1: The architecture of VANETs

Security is important first of all because nodes in VANETs can be transmitted via a wireless media. The attacker may control channels of communication for easy capture, deletion, playback, or alteration of messages transmitted by traffic or even other vehicle impersonation. For instance, false traffic messages can be sent by an attacker to mislead vehicles and RSU for incorrect decisions causing traffic jams and accidents. The recipient must thus authenticate the source of the message received and verify their integrity before accepting it [11].

VANET authentication needs to work hand in hand with the privacy of vehicles [12]. Without privacy, an attacker could intercept and analyze the messages to learn the vehicle's true identity or its travel route. Identity-anonymity is, therefore, necessary to ensure that each vehicle is protected and un-linkable. However, the TA should be given the privilege to identify the identity of malicious vehicle that transmits false message in order to revoke its registration.

VANET uses Dedicated short-range communication (DSRC) protocol for wireless communication. The 5.9-GHz DSRC protocol stipulates that each VANET-enabled vehicle must send a message to other vehicles every 100 to 300 ms [13][14]. This could lead to extremely high computation costs for all vehicles to check and verify all these messages [15][16].

These factors (security, privacy and efficiency) form the justification for the need to further improve the computational and communicational efficiency alongside the assurance of safety and privacy of traffic-related messages by proposing an efficient preventive scheme for modification attack in VANET.

The rest of the paper is structured as follows. An architecture of VANETs is presented in Section II, followed by a brief review of the modification attacks in Section III. Several existing works in the literature are reviewed in Section IV. Lastly, Section V concludes this paper.

II. THE ARCHITECTURE OF VANETS

VANET Components

1- Trusted Authority (TA)

TA is a trustworthy entity equipped with high computational and communicational capabilities. The TA is responsible for initializing and providing the other entities in VANET with system parameters. The registration of RSUs and OBUs also falls under the responsibility of the TA for the entire VANET ecosystem.

2- Road-Side Units (RSUs)

The RSUs can be found installed along the roadside as part of the vehicle-to-TA infrastructure. It communicates via wired and wireless technology with the TA and vehicles, respectively. It is also responsible to monitor the traffic for suspicious vehicle behavior and to provide the TA with the vehicle's identity.

3- On-Board Units (OBUs)

Every vehicle that is equipped with an OBU plays an important role in the transmission of information to other vehicles by nearby RSU using DSRC protocol.

B. VANET Communications

VANETs has two modes of communication: vehicles-to-vehicles (V2V) communication and vehicle-to-infrastructure (V2I) communication modes. These wireless communication modes use DSRC protocol.

1- Vehicle-To-Vehicle (V2V) Communication

V2V communication uses multi-hop transmission to propagate messages to other vehicles through several hops. In V2V communication, the vehicle performs message exchanges only with other vehicles. The vehicle uses this information to avoid accident and traffic disruption. For example, when a traffic jam happens, the vehicle broadcasts the situation so that other vehicles approaching the site could make changes to their travel route to avoid the congestion. DSRC protocol stipulates that each VANET-enabled vehicle must send a message to other vehicles every 100 to 300 ms [13]. In a scenario that have 100 vehicles within the range of RSU using such a protocol means that between 333 to 1,000 messages are transmitted every second and must be verified by the receiver [14].

2- Vehicle-To-Infrastructure (V2I) Communication

V2I communication uses single-hop transmission where a broadcast message is transmitted from a fixed structure on the side of the road. In V2I communication, the vehicle performs message exchange with other vehicles or nearby RSU by using DSRC protocol which helps to process, receive and broadcast message during travel. The RSU provides internet access for driver and passenger and forward the message to TA for further use.

III. OVERVIEW OF MODIFICATION ATTACK

The open nature of the wireless communication medium used by VANETs exposes the information exchanged to various types of attacks, such as modification attack. It is common for attackers to alter or modify the intercepted message in V2V and V2I communication. The attackers could deliberately send false information to VANETs to create confusion for vehicles which could lead to severe safety consequences. The presence of modification attack in VANET could result in high computational and communicational costs due to the frequent updates of bogus traffic-related message. The receiver must always check and verify all the messages received from other vehicle to avoid falling victim to modification attack.

IV. LITERTURE SURVEY

A number of studies have been conducted by researchers to address security attacks in VANET. This section presents a critical review on several related works on security schemes to withstand modification attack in VANET.

In 2017, Zhong et al. [17] proposed a security and privacy scheme that uses the list of revocation when it is indicated by the list of registration to minimize the think time available to the adversary. The main aim of the proposed scheme is to reduce the disclosed time of the revocation list. Each vehicle sends message-signature in {T_5, m, σ_m} format to other vehicles and nearby RSUs, where T_5 timestamp, m traffic-related message and σm signature of message. The attacker cannot modify the message-signature {T_5 , m, σ_m} to {T_5, m∗, σ_m∗}.

In the same year, many conditional privacy-preserving authentication schemes utilizing bilinear pairing or ideal tamper-proof devices have been proposed. Wu et al. [18] introduced an efficient location-based conditional privacy-preserving authentication scheme. This scheme is based on location for VANET. Each vehicle sends message-signature in {m_i, $PIDv_i$, T_i, T_{vi}, h_{ki}, R_i, σ_i} format to other vehicles and nearby RSUs, where mi traffic-related message, $PIDv_i$ pseudo-identity, T_i current timestamp, h_{ki} hash message, R_i public key and σ_i signature of message. For the modification attack to be successful, the adversary has to forge a signature σ_i∗ that will be used by the receiver to authenticate itself and validate the message-signature. However, the authors showed that under random oracle model, the adversary cannot generate a legitimate signature with non-negligible probability.

In 2018, Li et al. [19] proposed an efficient, provably secure, and anonymous conditional privacy preserving authentication (EPA-CPPA) approach for V2V and V2I communication. In their scheme, the batch verification supports verification of a large number of messages with improved efficiency. Each vehicle sends message-signature in {M_i, $PID_{i.l}$, $PK_{i,l}$, R_i, T_i, Sig_i} format to other vehicles and nearby RSUs, where M_i traffic-related message, $PID_{i.l}$ the pseudo-identity, $PK_{i,l}$ public key, R_i parameter, T_i current timestamp and Sig_i signature of message. After eavesdropping on VANET connection, the modification attack has the ability to modify the content of M_i. To protect the integrity of the message, a signature of a vehicle on M_i is created. Since only the particular vehicle knows its private key, no modification attack is able to create legitimate message-signature. Besides, the vehicle periodically changes its private key. Therefore, this approach is secure from message modification attack.

In 2019, Alazzawi et al. [20] introduced a robust pseudo-identity-based scheme utilizing a pseudonym instead of an original identity. Each vehicle sends message-signature in the format {T, T_{SK}, PID_V, w, σ_m} to other vehicles and nearby RSUs, where T current timestamp, T_{SK} timestamp of signature, which was obtained from RSU, PID_V the pseudo-identity, w to reduce the computation cost of verifier side and σm signature of message. In their scheme, the message-signature includes the signature σm, which guarantees the safety of the message from modification attack. During the signature verification process, the vehicle does not accept the message. Therefore, this approach is secure against message modification attacks.

In the same year and the same authors, Alazzawi et al. [21] proposed security and privacy schemes based on a pseudonym root. In this scheme, each node stores just one of the main (pseudonym root) to hide its original identity. Thus, the node does not require thousands of pseudonyms within their certificates, therefore removing the large storage requirement for the TA and OBU. This scheme utilizes a cuckoo filter to store the personal information of vehicles within the range of RSU. Each vehicle sends a message-signature in {T, msg, σ_{msg}} format to other vehicles and nearby RSUs, where T current timestamp, msg message traffic-related and σ_{msg} signature of message. The σ_{msg} embedded in each message-signature prevents modification of msg by attackers. This is because of pseudonym Ps of vehicle and private key s of the system that are embedded in each σ_{msg}. Therefore, this scheme is not vulnerable to the modification attack.

V. CONCLUSION

VANETs is gaining significant attention in recent year due to the interest and advancement in smart city and its related technology such as ITS. VANETs provide not only safety application but also support broad range of infotainment applications for drivers and passengers. However, the wireless communication medium used by VANETs is susceptible to security threats due to its open nature. Modification attack is one of the threats facing VANETs where an adversary could change and modify the information contained in the traffic-related message on driving environment which cause disruption of the system. This paper provides an overview of modification attack on VANET. In addition, this paper thoroughly reviews existing prevention schemes for modification attack in VANET. This review paper shows that there is still a need for an efficient preventive scheme to prevent modification 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).

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-3 (June 2020)
https://doi.org/10.31033/ijemr.10.3.22

REFERENCES

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

[2] 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.

[3] M. Alzubaidi, M. Anbar, Y.-W. Chong, & S. Al-Sarawi. (2018). Hybrid monitoring technique for detecting abnormal behaviour in RPL-based network. *J. Commun., 13*(5).

[4] 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.

[5] 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.

[6] M. Al-Shalabi, M. Anbar, & T.-C. Wan. (2018). Proposed mechanism based on genetic algorithm to find the optimal multi-hop path in wireless sensor networks. In: *International Conference of Reliable Information and Communication Technology*, pp. 510–522.

[7] 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.

[8] Z. Lu, G. Qu, & Z. Liu. (2018). A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Trans. Intell. Transp. Syst.*, *20*(2), 760–776.

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

[10] H. Peng, L. Liang, X. Shen, & G. Y. Li. (2018). Vehicular communications: A network layer perspective. *IEEE Trans. Veh. Technol.*, *68*(2), 1064–1078.

[11] M. Wazid, A. K. Das, R. Hussain, G. Succi, & J. J. P. C. Rodrigues. (2019). Authentication in cloud-driven IoT-based big data environment: Survey and outlook. *J. Syst. Archit.*, *97*, 185–196.

[12] F. Qu, Z. Wu, F.-Y. Wang, & W. Cho. (2015) A security and privacy review of VANETs. *IEEE Trans. Intell. Transp. Syst.*, *16*(6), 2985–2996.

[13] V. K. V. Karthikeyan. (2016). *An investigation of the factors leading drivers to overlook privacy issues in the vehicular infotainment system in India*. University of Sheffield.

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

[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, X. Lin, R. Lu, & P.-H. Ho. (2008). RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks. In: *IEEE International Conference on Communications*, pp. 1451–1457.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.