Vulnerabilities in Vehicular Ad Hoc Networks and Possible Countermeasures

Ghassan Samara

January 7, 2023

Vulnerabilities in Vehicular Ad Hoc Networks and Possible Countermeasures

Ghassan Samara
Computer Science Department
Zarqa University
Zarqa- Jordan
gsamarah@zu.edu.jo

***Abstract*— Recently, the Vehicular Ad Hoc Network, or VANET, has emerged as the most essential topic for researchers and the automobile industry to discuss in order to enhance the level of safety enjoyed by road users. Users of VANET need to be able to access both safety-related and non-safety-related apps. In this paper, we offer sixteen different kinds of attacks, as well as potential defenses against them.**

I. INTRODUCTION

In recent years, wireless technologies have seen widespread adoption, leading to an increase in the number of wireless goods being used on automobiles that are driven on public roads. The Vehicular Ad hoc Network, also known as VANET, has attracted the attention of the research community due to the safety of vehicles [1, 2, 3, 4, 5, 6, 7, 8, 9]. The primary aim is to ensure the safety of users and to save their lives on the road by reducing the likelihood of being involved in an accident [10, 11, 12]. Both safety and non-safety are uses of VANET that can be used to increase driver and passenger protection on the road. In many applications, security is the primary concern because sending the erroneous message could result in an accident. Recently, several different kinds of attacks against VANETs have emerged, which has frightened the already unpleasant position regarding the security of VANET networks [13, 14, 15]. In every node of the VANET, we have a road side unit (RSU) mounted on the vehicle so that it can remain within network range.

The Dedicated Short Range Communication (DSRC) protocol, which uses the 5.9GHz frequency spectrum to function, is the communication medium that is employed [16, 17, 18]. Seven channels, each with a bandwidth of 10 MHz, are made available for use in safety and non-safety applications respectively [19]. The normal data rate provided by DSRC is between 6 and 27 Mbps, and it has a communication range of 1000 meters [20, 21, 22, 23, 24, 25]. On this connection, both safety and non-safety messages can be passed between vehicles using the Vehicle to Vehicle (V2V) protocol and vehicles using the Vehicle to Infrastructure (V2I) protocol. An attacker causes issues in the network by initiating some attacks utilizing DSRC, which causes the troubles [26, 27, 28, 29].

II. LITERATURE REVIEW

In [30], the authors detailed some of the security vulnerabilities that had been discovered on VANET. Additionally, they provided a way to prevent these attacks from happening in the future. The types of attacks that they concentrated on are known as Replay attack, DOS attack, DDOS attack, Sybil attack, Timing Attack, (GPS) attack, Hidden spamming attack, virus attack, Illusion Attack, and ID.

The authors of [31] described some of the security threats that had been discovered on VANET, as well as the recommended solutions for these attacks. [4] Network Attacks, Application Attacks, Timing Attacks, Social Attacks, and Monitoring Attacks were the primary security areas that were the focus of their attention.

The authors of [32] described some of the security threats that had been discovered on VANET, and then they provided a way to prevent these attacks from happening in the future. The primary areas that they concentrated on were the Sybil attack, Bogus Information and Bush telegraph, Timing Attack, Global Positioning System (GPS) Spoofing, Hidden vehicle and Tunnel Attack, Illusion Attack, ID Disclosure Denial of Service (DoS) and Distributed Denial of Service (DDoS), Malware and Spam, and Man in the Middle Attack (MiMA).

The Sybil attack is an important problem that is also known as a harmful attack. It was initially described.

The authors of [33] addressed some of the important security attacks that have been reported on VANETs in the past, including those that took place in 2010. They also discussed the related security remedies that have been offered to prevent those security flaws and attacks. Anonymity key management, privacy, reputation, and location were some of the primary focuses of their attention when it came to matters of security. When it comes to the physical identity of mobile nodes, anonymity is a crucial problem in VANETs. The identity of mobile nodes should be kept a secret from the perspective of unauthorized components.

III. POSSIBLE ATTACKS

A. *Denail of Service(DOS)*

The goal of a DOS attacker is to stop legitimate users from accessing network services [34]. The attacker will make the network unavailable to users in order to accomplish this goal.

The Denial of Service attack is depicted in Figure 1, where the attacker A attempts to stop communication between users by launching a DOS attack (A, B and C).

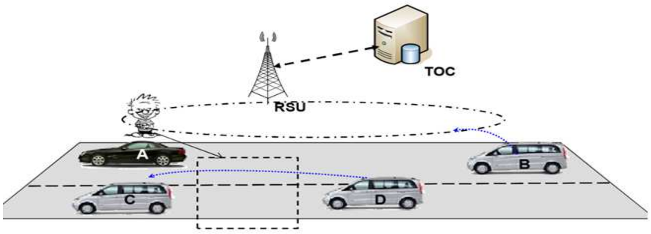

Figure 1: DOS attack between V2V and V2I

B. *Distributed Denial of service (DDOS) Attack*

In this scenario, assailants will start their attacks from a variety of different positions. It's possible that they'll employ a variety of time windows for sending the communications. There is a possibility that the nature of the messages and the time period will change from one vehicle of the attackers to another. The purpose of each attack is the same, which is to bring the network to a halt. Both V2V and V2I are vulnerable to attack from the attacker [35].

- In V2V

The scenario of a vehicle-to-vehicle (V2V) DDOS attack is depicted in Figure 2, in which the attackers (B, C, and D) conduct DDOS against vehicle A.

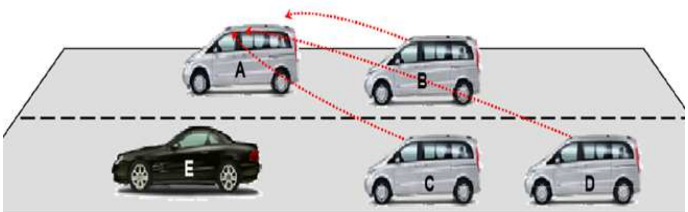

Figure 2: DDOS in V2V communication

- In V2I

Figure 3 provides an explanation of a DDOS attack on infrastructure, in which many attackers (B, C, and D) execute attacks against the infrastructure from separate places. The infrastructure is said to be overloaded when other cars (A, E) in the network try to use the network.

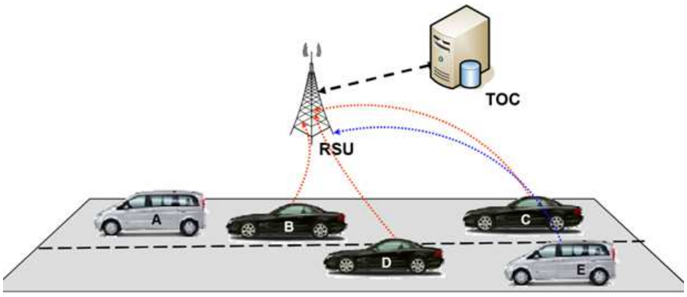

Figure 3: DDOS in V2I communication

C. *Sybil Attack*

The adversary communicates with other cars by sending them messages, and each message has a false source identity. It gives the impression of reality to other vehicles by sending them incorrect messages, such as the message for a traffic congestion [36]. Figure 4 describes the Sybil attack, which occurs when many attackers share the same identity. The purpose is to convince the drivers of the other vehicles on the road to pull off the road so that the attacker may continue driving.

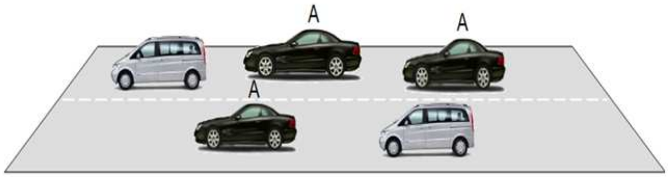

Figure 4: Sybil attack

D. *Node Impersonation Attack*

In VANET, every vehicle has its own distinctive identification, which is utilized for the purpose of verifying the message in the event that an accident occurs as a result of sending incorrect messages to other cars [33]. This hypothetical situation, in which vehicle A is involved in an accident at point Z, is explained in Figure 5. When the police identify the driver because it is related with the driver's identity, the attacker simply refuses to accept their identification and changes his identity.

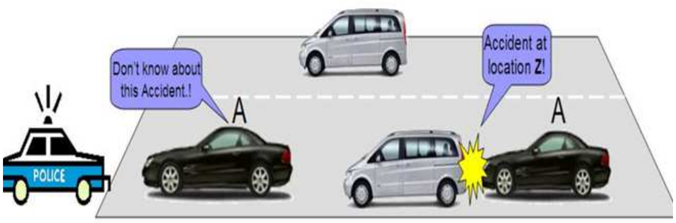

Figure 5: Node impersonation attack

E. *Spamming Attack*

During this particular attack, the attacker sent spam messages to a specific user community [37]. These notifications, similar to advertisement messages, are of little importance to the user and should be ignored.

F. Malware Attack

VANET is typically affected by these attacks whenever there is a software upgrade in either the VANET devices themselves or the RSU [32]. Embedded anti-malware frameworks are still a contentious subject in the VANETs research community. In this scenario, the attackers are typically hostile insiders rather than malicious outsiders.

G. Message suppression

During this type of attack, the adversary is able to thwart the delivery of messages to users, even if those messages contain vital information for the recipient [38]. For instance, an adversary could delete the congestion alerts that it receives in order to force users to sit in traffic by making it impossible for them to choose an alternate route to their destination. This attack takes place when the massage transmission is delayed, when a previously transmitted message is replayed, or when a specific part of the message is altered. For instance, an attacker could obtain the data, manipulate it, and then indicate dishonestly that a heavily congested highway is nearby.

H. Replay

This type of attack is typically carried out by an authorized user in order to impersonate a genuine user or RSU. This type of attack takes place when the attacker replays the transmission of created frames in fresh connections. The attacker takes a screenshot of the created frame and uses it in other areas of the network [38].

I. GPS spoofing

The perpetrator of the attack will provide bogus GPS readings, giving the impression to other users that he is at a different place [30, 39].

J. Timing Attack

As part of this attack, the attacker adds some time slot to the message in order to produce a delay in its delivery; as a result, the user will only get the message after the allotted amount of time [37]. Figure 6 accompanied with an explanation.

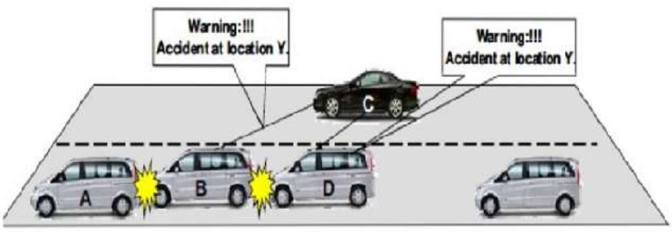

Figure 6: Timing attack

K. Social attack

The attacker sends the user a message that made him furious, which in turn caused him to alter his driving habit by driving more quickly, which resulted in an accident [37].

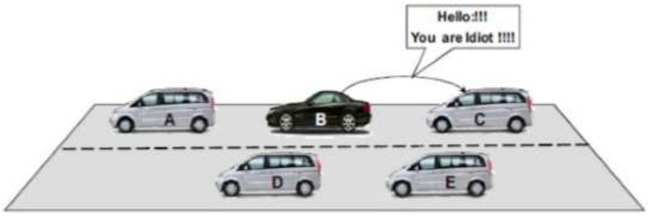

Figure 7: Social attack

L. Home attack

During this type of attack, the attacker connects the user car to the internet in order to take control of it. There are three distinct methods that an assailant might employ to carry out an attack on a house [37].

• The attacker gains control of the user vehicle's software (either the AU or the OBU).

• The adversary seizes control of the sensor that is installed on the user's car. in order for him to alter the functions of the sensor.

• The adversary seizes command of the user's vehicle's electronic control unit (ECU). After that, he will have the ability to raise or lower the vehicle's speed.

M. Traffic analysis

Analyses are performed by the attacker on the communication packets that are exchanged between the V2V or V2I in this attack [33, 38]. The attacker makes advantage of the packet, which contains the position of Vehicle ID as well as the traveling path of the vehicle, in order to extract the necessary information for its own purposes.

N. Bogus information

The malicious attacker spread inaccurate information throughout the vehicle network. That effect on other cars brought about by the dissemination of that incorrect information across The network [40, 41].

O. Man in the Middle Attack (MiMA)

An attacker will listen to the communications that are taking place between two cars, then pretend to be either one of the vehicles so that they may react to the other and inject fake information between the vehicles [32]. In the Man in the Middle attack depicted in Figure 8, the adversary C acts as an eavesdropper on the conversation taking place between vehicles B and D, while also providing vehicle E with inaccurate information that was obtained from adversary A.

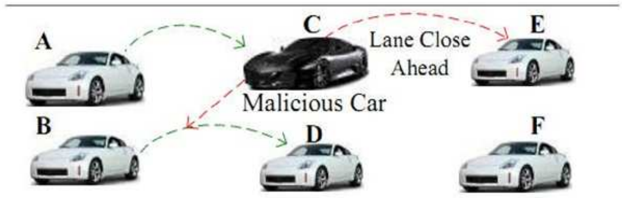

Figure 8: Man in the middle attack (MiMA)

P. Black Hole Attack

In this type of attack, a car will refuse to participate in the network, or an existing vehicle will drop out of the network, creating a black hole. The effect of this is that all of the network's traffic is sent toward a particular vehicle that really does not exist, which causes data to be lost [32].

IV. Solutions For Different Attacks

The following is a list of potential countermeasures to some of the threats that we discussed:

DOS solutions are built on an OBU, which is a "on board unit," and are installed on each vehicle node. In order to counteract this attack, the Processing Unit will recommend to the OBU that it swap its technology, channel, or utilize a frequency hopping approach [41].

In order to prevent timing attacks, we have to get rid of extra time slots by employing data integrity verification. TPM (Trusted Platform Module) [42] is one of the most important security measures since it maintains the message's integrity by making use of powerful cryptographic functional modules. In conjunction with two protocols, namely Direct Anonymous Attestation and Privacy Certification Authority (PCA) (DAA).

Using packet sequence numbers in a packet header is the answer to the black hole attack [43]. This ensures that if any packet is lost, the destination may easily identify it from the missing packet sequence number.

To prevent replay attack [44] we must use global synchronized time for all nodes and nonce (timestamp), other proposed solution to reduce this attack is to verify the received data in correlation with the data received from other sources.

V. CONCLOSION AND FUTURE WORK

In this paper, we detailed a wide variety of attacks that can compromise a VANET, as well as some of the ways that they can be prevented, and we discussed how our new approach to message encryption can be tested in simulation. Overall, we believe that this paper provides a comprehensive overview of the topic.

References

[1] Samara, G., Alsalihy, W.A.A. and Ramadass, S., 2011. Increasing Network Visibility Using Coded Repetition Beacon Piggybacking. *World Applied Sciences Journal*, *13*(1), pp.100-108.

[2] Samara, G., Alsalihy, W.A.H.A. and Ramadass, S., 2011. Increase emergency message reception in vanet. *Journal of applied sciences*, *11*(14), pp.2606-2612.

[3] Samara, G. and Alsalihy, W.A.A., 2012, June. A new security mechanism for vehicular communication networks. In *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)* (pp. 18-22). IEEE.

[4] Samara, G., 2018. An intelligent routing protocol in VANET. *International Journal of Ad Hoc and Ubiquitous Computing*, *29*(1-2), pp.77-84.

[5] Samara, G. and Alsalihy, W.A.A., 2012. Message broadcasting protocols in VANET. *Information Technology Journal*, *11*(9), p.1235.

[6] Samara, G., 2020. Intelligent reputation system for safety messages in VANET. *IAES International Journal of Artificial Intelligence*, *9*(3), p.439.

[7] Samara, G., 2020, November. Wireless Sensor Network MAC Energy-efficiency Protocols: A Survey. In *2020 21st International Arab Conference on Information Technology (ACIT)* (pp. 1-5). IEEE.

[8] Samara, G., Ramadas, S., Al-Salihy, W.A.H. 2010. Safety message power transmission control for vehicular Ad hoc Networks. *Journal of Computer Science,, 6(10), pp. 1056–1061.*

[9] Samara, G., Al-Salihy, W.A. and Sures, R., 2010, May. Efficient certificate management in VANET. In *2010 2nd International Conference on Future Computer and Communication* (Vol. 3, pp. V3-750). IEEE.

[10] Samara, G., Abu Salem, A.O. and Alhmiedat, T., 2013. Dynamic Safety Message Power Control in VANET Using PSO. *World of Computer Science & Information Technology Journal*, *3*(10).

[11] Hussain, I., Samara, G., Ullah, I. and Khan, N., 2021, December. Encryption for End-User Privacy: A Cyber-Secure Smart Energy Management System. In *2021 22nd International Arab Conference on Information Technology (ACIT)* (pp. 1-6). IEEE.

[12] Alhmiedat, T. and Samara, G., 2017. A Low Cost ZigBee Sensor Network Architecture for Indoor Air Quality Monitoring. *International Journal of Computer Science and Information Security (IJCSIS)*, *15*(1).

[13] Aljaidi, M., Aslam, N., Chen, X., Kaiwartya, O., Al-Gumaei, Y.A. and Khalid, M., 2022. A Reinforcement Learning-based Assignment Scheme for EVs to Charging Stations, 2022 IEEE 95th Vehicular Technology Conference

[14] Almatarneh, S., Gamallo, P., ALshargabi, B., Al-Khassawneh, Y. and Alzubi, R., 2021, December. Comparing Traditional Machine Learning Methods for COVID-19 Fake News. In *2021 22nd International Arab Conference on Information Technology (ACIT)* (pp. 1-4). IEEE.

[15] Almatarneh, S. and Gamallo, P., 2017, November. Searching for the most negative opinions. In *International Conference on Knowledge Engineering and the Semantic Web* (pp. 14-22). Springer, Cham.

[16] Jiang, D., Taliwal, V., Meier, A., Holfelder, W. and Herrtwich, R., 2006. Design of 5.9 GHz DSRC-based vehicular safety communication. *IEEE wireless communications*, *13*(5), pp.36-43..

[17] Aljaidi, M., Aslam, N. and Kaiwartya, O., 2019, April. Optimal placement and capacity of electric vehicle charging stations in urban areas: Survey and open challenges. In *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)* (pp. 238-243). IEEE.

[18] Aljaidi, M., Aslam, N., Chen, X., Kaiwartya, O. and Al-Gumaei, Y.A., 2020, October. Energy-efficient EV charging station placement for E-mobility. In *IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society* (pp. 3672-3678). IEEE.

[19] Samara, G. and Aljaidi, M., 2018. Aware-routing protocol using best first search algorithm in wireless sensor. *Int. Arab J. Inf. Technol.*, *15*(3A), pp.592-598.

[20] Rahman, S.U. and Falaki, H., 2009. Security & Privacy for DSRC-based Automotive Collision Reporting. *www. cs. ucla. edu/falaki/courses/security project. pdf.*

[21] Samara, G. and Aljaidi, M., 2019. Efficient energy, cost reduction, and QoS based routing protocol for wireless sensor networks. *International Journal of Electrical & Computer Engineering (2088-8708)*, *9*(1).

[22] Samara, G. and Blaou, K.M., 2017, May. Wireless sensor networks hierarchical protocols. In *2017 8th International Conference on Information Technology (ICIT)* (pp. 998-1001). IEEE.

[23] Samara, G., Al-Okour, M. 2020. Optimal number of cluster heads in wireless sensors networks based on LEACH, *International Journal of Advanced Trends in Computer Science and Engineering, , 9(1), pp. 891–895*

[24] Samara, G., Albesani, G., Alauthman, M., Al Khaldy, M., Energy-efficiency routing algorithms in wireless sensor networks: A survey, *International Journal of Scientific and Technology Research, 2020, 9(1), pp. 4415–4418.*

[25] M Khatari, G Samara, 2015, Congestion control approach based on effective random early detection and fuzzy logic, *MAGNT Research Report, Vol.3 (8). PP: 180-193.*

[26] Salem, A.O.A., Samara, G. and Alhmiedat, T., 2014. Performance Analysis of Dynamic Source Routing Protocol. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(2).

[27] Salem, A.O.A., Alhmiedat, T. and Samara, G., 2013. Cache Discovery Policies of MANET. *World of Computer Science & Information Technology Journal*, *3*(8).

[28] Alhmiedat, T.A., Abutaleb, A. and Samara, G., 2013. A prototype navigation system for guiding blind people indoors using NXT Mindstorms. *International Journal of Online and Biomedical Engineering (iJOE)*, *9*(5), pp.52-58.

[29] Aljaidi, M., Aslam, N., Chen, X., Kaiwartya, O. and Khalid, M., 2020, April. An energy efficient strategy for assignment of electric vehicles to charging stations in urban environments. In *2020 11th International Conference on Information and Communication Systems (ICICS)* (pp. 161-166). IEEE.

[30] Rawat, A., Sharma, S. and Sushil, R., 2012. VANET: Security attacks and its possible solutions. *Journal of Information and Operations Management*, *3*(1), pp.301-304.

[31] Malla, A.M. and Sahu, R.K., 2013. Security attacks with an effective solution for dos attacks in VANET. *International Journal of Computer Applications*, *66*(22).

[32] La, V.H. and Cavalli, A.R., 2014. Security attacks and solutions in vehicular ad hoc networks: a survey. *International journal on AdHoc networking systems (IJANS)*, *4*(2), pp.1-20.

[33] Isaac, J.T., Zeadally, S. and Camara, J.S., 2010. Security attacks and solutions for vehicular ad hoc networks. *IET communications*, *4*(7), pp.894-903.

[34] Parno, B. and Perrig, A., 2005, November. Challenges in securing vehicular networks. In *Workshop on hot topics in networks (HotNets-IV)* (pp. 1-6).

[35] Rawat, A., Sharma, S. and Sushil, R., 2012. VANET: Security attacks and its possible solutions. *Journal of Information and Operations Management*, *3*(1), pp.301-304.

[36] Raya, M. and Hubaux, J.P., 2007. Securing vehicular ad hoc networks. *Journal of computer security*, *15*(1), pp.39-68.

[37] Sumra, I.A., Ahmad, I. and Hasbullah, H., 2011, October. Behavior of attacker and some new possible attacks in vehicular ad hoc network (VANET). In *2011 3rd international congress on ultra modern telecommunications and control systems and workshops (ICUMT)* (pp. 1-8). IEEE.

[38] Ghassan, S., Al-Salihy, W.A. and Sures, R., 2010. Security analysis of vehicular ad hoc networks (VANET). In *2010 second international conference on network applications, protocols and services, national advanced IPv6 center. Universiti Sains Malaysia Penang, Malaysia*.

[39] Samara, G., 2021. Lane prediction optimization in VANET. *Egyptian Informatics Journal*, *22*(4), pp.411-416.

[40] Samara, G., Hussein, M. and Khaled, A.Q., 2021, December. Alarm System at street junctions (ASSJ) to avoid accidents Using VANET system. In *2021 Global Congress on Electrical Engineering (GC-ElecEng)* (pp. 37-41). IEEE.

[41] Verma, K., Hasbullah, H. and Kumar, A., 2013. Prevention of DoS attacks in VANET. *Wireless personal communications*, *73*(1), pp.95-126.

[42] Guette, G. and Bryce, C., 2008, May. Using tpms to secure vehicular ad-hoc networks (vanets). In *IFIP International Workshop on Information Security Theory and Practices* (pp. 106-116). Springer, Berlin, Heidelberg.

[43] Mahmood, R.R. and Khan, A.I., 2007, November. A survey on detecting black hole attack in AODV-based mobile ad hoc networks. In *2007 International Symposium on High Capacity Optical Networks and Enabling Technologies* (pp. 1-6). IEEE.

[44] Doetzer, F., Kohlmayer, F., Kosch, T. and Strassberger, M., 2005, March. Secure communication for intersection assistance. In *Proceedings of the 2nd International Workshop on Intelligent Transportation, Hamburg, Germany*.