Open Access License Notice

Techniques to Overcome Network Attacks (Sybil Attack, Jamming Attack, Timing Attack) in VANET

Sinan Ameen Noman
Department of Computer Science
University of Alabama
Tuscaloosa, USA
sanoman@crimson.ua.edu
0000-0002-9169-4452

Travis Atkison
Department of Computer Science
University of Alabama
Tuscaloosa, USA
atkison@cs.ua.edu
0000-0001-7258-7355

***Abstract*—VANET is a type of Ad hoc network that enables the communication between vehicles and roadside units. It provides a broad range of applications, such as blind crossing, accident avoidance, protection, interactive route planning, traffic situation monitoring in real-time, etc. These applications are required to be very secure to achieve a reliable service and provide safety for drivers. This paper sheds light on three different types of attacks (Sybil Attack, Jamming Attack, Timing Attack) that can critically affect the vehicular ad hoc network environment. Furthermore, we present techniques that can overcome these attacks.**

Keywords—VANET, Sybil attack, jamming attack, timing attack introduction

I. INTRODUCTION

Mobile communication technologies have reshaped the automotive industry over the last decade by providing communication between different devices everywhere at any time. This ease of communication enables the valuable information between devices to be exchanged just on the go. The fast and efficient exchange of real-time information has proven to be a new paradigm in the industrial sector. As a result, the improvements in communication and information technology have effectively endorsed the idea of communication between mobile devices. Among these improvements, the Vehicular Ad hoc Networks (VANETs) concept came to light, which brought new opportunities for the use of safety applications.

Vehicular ad hoc networks (VANETs) are created by applying the principles of mobile ad hoc networks (MANETs). In VANET, different vehicles and other connected devices in the network exchange valuable information with each other via a wireless medium.

At the same time, a small network is being set up with other devices and vehicles acting as nodes in the network. The nodes will exchange all information to all other nodes. Likewise, all nodes after transmitting their data set receive data transmitted by other nodes. After collecting all these data, the nodes will generate valuable information from the dataset and then transmit it again to other devices. The communication between devices extends in such a manner that nodes have the capability to freely join and leave the network. VANET technology allows other vehicles to communicate with each other and supply helpful information to the driver and help the driver make informed decisions safely. On the other hand, Autonomous Vehicles (AVs) have autonomous capabilities, such as self-parking, self-driving, and auto-collision avoidance.

The new vehicles, nowadays, comes with an integrated on-board unit that makes it easier for the vehicle to join the network and take advantage of VANET. The following factors can characterize the VANET:

- Sporadic Connectivity: The connectivity between vehicles changes frequently, as the connection between two vehicles that exchange information can be disconnected at any time. Frequent disconnections are caused by the high dynamic topology.
- Dynamic Topology: The vehicle speed and direction are constantly changing, resulting in high dynamic topology.
- Unlimited storage and power: There is no limit to the power or storage that a node in a VANET can have. As a result, there are no limits on how much data the nodes can send or receive in terms of storage or power usage.
- On-Board Unit (OBU): Each vehicle must have on-board devices to transmit and receive data to other nodes inside the VANET.
- Mobility Patterns: A large number of vehicles tends to follow a specific pattern of movement that are dependent primarily on speed limits, on traffic signals, highways, roads, road conditions, etc. These patterns enhance the development of routing protocols for VANET.

Additionally, VANET plays a crucial role in Intelligent Transportation Systems (ITS), as insights are generated from messages exchanged by nodes and other devices. The remainder of the paper is structured as follows: Section II

explains the architecture of VANET. Section III exhibits three types of attacks in VANET. Section IV presents the techniques that will overcome Sybil attack, Jamming attack and Timing attack in VANET.

II. VANET ARCHITECTURE

In this section, we present the VANETs system architecture from domain perspective. Then, we present the layered architecture and communication architecture for VANETs.

A. VANET system architecture from domain perspective

The system architecture of VANETs can be categorized into three domains: infrastructure, ad hoc, and in-vehicle domain.

- Infrastructure domain: There are two different types of access in Infrastructure domain, Roadside Units (RSUs) and Hotspots (HSs) [8]. The On-Board Unit (OBU) may communicate with the internet using HSs or RSU. The on-board units can additionally communicate with each other through cellular networks, such as 4G, 5G,UMTS, or GPRS. The UMTS stands for Universal Mobile Telecommunication Systems. It is a 3G broadband, capable of transferring text, voice and multimedia at data rates up to 2 (Mbps). On the other hand, the GPRS stands for General Packet Radio Service. It is an old technology, known also as 2G, can theoretically transfer data up to 120kb per second.
- Ad hoc domain: This domain consists of vehicles equipped with OBUs to communicate with RSUs. The RSU is a static node, and the OBU is considered as an Ad hoc node.
- In-vehicle domain: This domain consists of several Application Units (AUs) and OBUs. The connections between these components are usually wired, but they can also be wireless.

B. Communication types in VANET

In VANETs, communication types can be classified into four main types. As previously stated, these types are strongly related to VANET domains.

- Vehicle-to-Vehicle (V2V) Communication: The V2V communication enables the nodes to exchange messages with each other as well as warning messages. These messages have the potential to increase driver assistance.
- Vehicle-to-Infrastructure (V2I) Communication: This type of communication helps the driver to receive weather/traffic updates in real-time and provide them with environmental monitoring.
- In-Vehicle Communication: This type of communication is crucial as it can identify the vehicle's performance and the driver's fatigue, both of which are critical for public safety.
- Vehicle-to-Broadband Cloud: This type of communication enables the vehicle to communicate with the infrastructure via cloud using cellular services such as 4G, 5G [8]. Due to the possibility that the broadband cloud contains more traffic and environmental data, vehicle tracking and active drivers can benefit from this communication.

C. Layered architecture in VANET

In general, the architecture of VANET may vary from one region to another. Therefore, the interfaces and protocols differ as well. Fig. 1 shows the Dedicated Short Range Communication (DSRC) protocol stack in the United States. DSRC is explicitly designed for vehicle-to infrastructure and vehicle-to vehicle communications, and uses a similar set of standards and protocols. It plays a vital role in saving peoples' lives by alerting drivers when there is an imminent dangerous condition to take preventive or evasive actions. DSRC use the Orthogonal Frequency Division Multiplexing (OFDM) scheme, a cutting-edge technology that uses a multi-carrier transmission scheme that has proven robust against fading and interference. In comparison to standard Wi-Fi usage, the OFDM operates with "half clock", which doubles the temporal parameters, and reduces the channel frequency that commonly used from 20 MHz to 10 MHz [9].

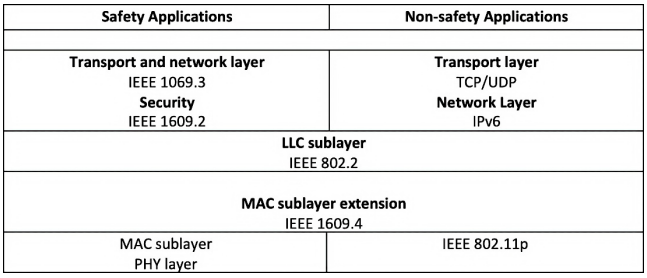

Fig. 1. The layered architecture of DSRC communication.

In the United States, the Federal Communications Commission (FCC) allocated 75MHz of spectrum for DSRC transmission, ranging from 5.850 GHz to 5.925 GHz. [1]. Different protocols are designed to be utilized at different layers.

The IEEE 802.11p is a modification to the IEEE 802.11 standard that allows for wireless communication in vehicle environments. This is known as WAVE, or vehicular communication system. [2]. It is mainly focused on the MAC sublayer and the physical layer of the stack. IEEE 1609 represents a family of standards that support safety applications in VANETs and based on the IEEE 802.11p, while other protocols support non-safety applications. In particular, A non-safety application uses three protocols for network and transport layer services: TCP, UDP, and IPv6. [4].

III. SECURITY ASPECTS

Security in VANET can be achieved under several important conditions, which are discussed as follows.

- Data Integrity: It ensures that messages between vehicles and RSUs are not altered by adversaries. Otherwise, the driver's safety is definitely at risk. For instance, if a vehicle (X) sends a message to vehicle (Y) and (Y) alter this message before sending it to vehicle (Z), (Z) will be affected by this message and might be at risk.
- Authentication: Vehicles should only accept transmitted messages by authorized members of the VANET network. Therefore, authenticating the operator of the message is essential.
- Availability: The goal of availability is to make sure that network services continue to work properly even in the face of malicious or faulty conditions. In the context of VANET, availability is particularly important because it is closely related to safety applications. In many ways, availability can be seen as the most critical aspect of security in VANET.
- Privacy: The data privacy such as location and user identity are sensitive and essential in the VANET communication process. The system should guarantee the authentic identity and prevent data leakage.

IV. ATTACKS IN VANET

VANETs are susceptible to many attacks because of their characteristics, like high mobility, which frequently causes network disconnection.

A disruption in the communication link between vehicles can occur, as the vehicle's speeds are much faster than (20 m/s) [3]. This disruption makes VANETs more vulnerable to various types of attacks and makes it harder to identify suspicious vehicles. As the safety messages transmit in an open-access environment, the entire communication in VANETs can be disrupted if an attacker alters, intercepts, or injects fake messages into the vehicular network environment. This increases the susceptibility of VANETs to attacks and the difficulty of detecting potential threats.

The attackers in VANETs are divided into four types (1) Inside vs. Outside attacker: The inside attacker is a verified user with extensive knowledge of the network, while the outside attacker is an unverified user with less ability to attack the network than the inside attacker; (2) Active vs. Passive attacker: Active attackers either inject false information or fail to forward received messages, while passive attackers only listen to messages without altering them; (3) Rational vs. Malicious attackers: The primary goal of rational attackers is to gain personal benefits from VANETs, while the aim of malicious attackers is to disrupt and harm the network without seeking personal gain, and (4) Local vs. Extended attacker: Local attackers exploit limited resources on specific nodes, while Extended attackers use all available resources to control multiple networks. To provide secure communication in VANETs, it is necessary to have a thorough understanding of attacks and threats in order to address all security challenges. In this section, we discuss the threats of (Sybil attack, Jamming attack, and Timing attack) in VANET. These three attacks are considered the most dangerous in VANETs as it directly threatens the efficiency of the VANETs system and human lives [10] [11] [12]. Also, it prevents the vehicles from disseminating information between them or falsifying information inside the network, which leads to traffic congestion, disruption, and reduced efficiency of the service provided.

A. Sybil attack

Sybil attack is a severe threat that reduces the functionality of VANETs. It enables the attacker to send multiple messages to other vehicles in the network with multiple identities [5]. This enables the attacker to simulate multiple vehicles in the network. The fake vehicles are called Sybil nodes, and the vehicle that creates fake identities is called a malicious node. Sybil attackers can also inject bogus information when sending messages in the network through simulated nodes. For instance, if there is an accident on a highway, the first vehicle to observe the accident will send a message to other vehicles to change their route or warn them to slow down. Other vehicles may pass on this message to warn others. However, a Sybil attacker could interrupt this process by not transmitting the warning message to other vehicles, putting the lives of drivers at risk. Sybil attacks can be divided into three categories, as shown in Fig. 2.

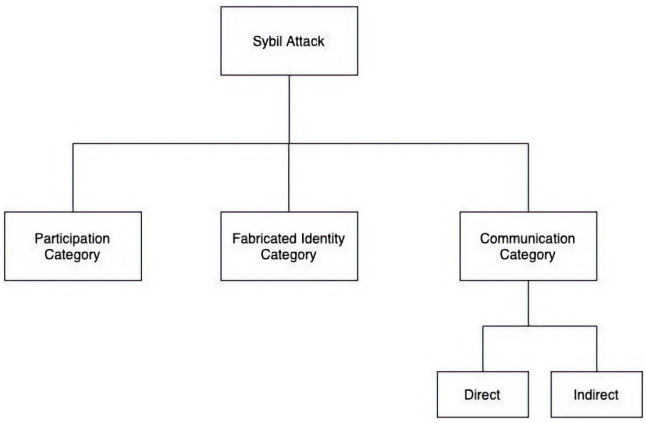

Fig. 2. Categories of Sybil attack.

1. Participation Category: A malicious attacker can create multiple Sybil identities that can participate in an attack simultaneously. The attacker can also use these identities one at a time. A single identity may join or leave the network multiple times. The number of identities that the attacker can use is less than or equal to the number of real identities.
2. Fabricated Identity Category: The attacker creates a new Sybil identity, which can be a 32-bit integer (Fake ID), or the attacker can use one of their neighbor's legitimate identities.
3. Communication Category: Communication between Sybil nodes and legitimate nodes can be either direct or indirect. In the direct method, Sybil nodes create a malicious node to communicate with

legitimate nodes. In the indirect method, legitimate nodes communicate with Sybil nodes via a malicious node.

B. *Jamming attack*

The jamming attack is a major threat to VANETs because it can disrupt communication between legitimate nodes deliberately [6]. Within this attack, the legitimate node will not send/receive messages from the jammed regions as the continuously received signals indicate that the channel is busy at all times. The packet delivery ratio (PDR) is reduced in a jamming attack as the sender will be able to send the packets successfully. However, the other nodes will not be able to receive the packet when the jamming attack starts. There are various types of information that the jamming attack can interrupt, such as accidents, and weather conditions. As we can see, this attack can put the passenger's life at risk if the packets did not send or receive at the right time. It is very difficult to prevent the adversary from joining the network due to the fact that they have unlimited mobility and they do not need to comply with other protocols. The jamming effect on the network depends on radio transmitting power. Primarily, the jammer can be divided into two main categories: proactive, and reactive.

1. Proactive Jammers: The proactive jammer sends jamming signal(s) whether the data communication exists in a network or not. It transmits packets or random bits to the operation channel, putting all other nodes in that channel in non-operational mode. The proactive jammer sends the jamming signal(s) on one channel exclusively until its energy is consumed.
2. Reactive Jammers: The reactive jammer only starts jamming when a network activity takes place on a specific channel. The reactive jammer can interrupt both large and small-sized packets. Reactive jammer is less energy efficient than proactive jammer and needs to monitor the network continuously. The reactive jammer is much more challenging in detection because the PDR cannot be accurately determined in practice.

C. *Timing attack*

A timing attack is a type of attack in which the attacker's main goal is to delay the network by inserting a time slot without changing the content of the message [7]. The legitimate node will be able to receive the message when the delay time expired. This type of attack allows the users to obtain multiple copies of the same message in different time slots, which can cause data redundancy problems. Data redundancy is often the result of timing attacks. Timing attacks can be divided into two types.

1. Basic Level Attack: This type of attack is a unicast attack, also called (peer-to-peer) attack. The threat-level of timing-attack on the communication level is low because only one legitimate node is affected. Fig. 3 illustrates a timing attack scenario where the adversary adds a delay to the original message and causes the blue vehicle to change its direction, where the accident occurs. Fig. 4 shows that the blue vehicle has been deceived by the red vehicle (adversary) and chose the wrong direction.
2. Extended Level Attack: This type of attack is a multicast attack, also called (one-to-many) attack. The attacker can target a specific group of legitimate nodes in the network, which will obviously cause a traffic jam. Fig. 5 illustrates an example of extended level attack, where the adversary deceives a group of vehicles.

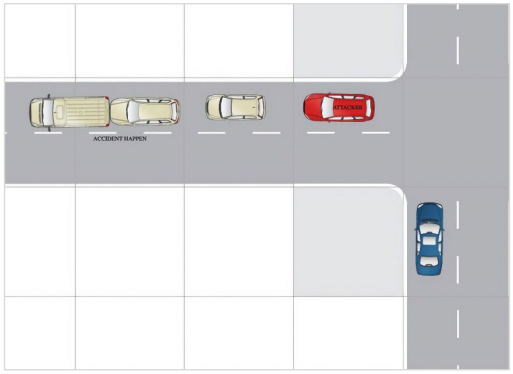

Fig. 3. Before P2P timing attack.

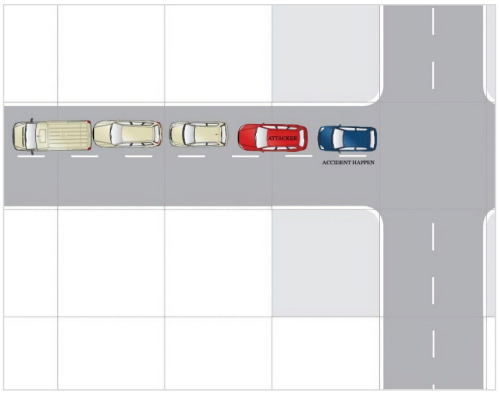

Fig. 4. After P2P timing attack.

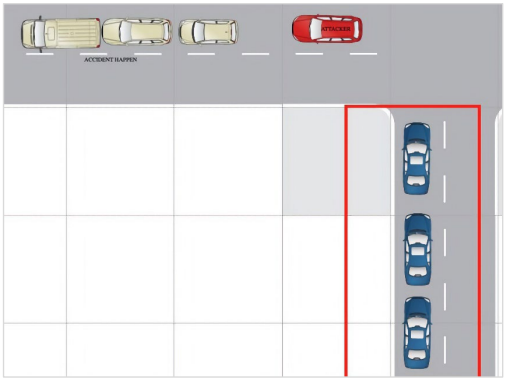

Fig. 5. After P2P timing attack.

V. DETECTION AND MITIGATION TECHNIQUES

In vehicular ad hoc networks, human lives are at stake, so it is important to ensure that only accurate and authentic information is disseminated through the network. Overcoming these attacks is essential and requires an effort to reach a secure environment. This section presents the techniques that can be used to detect and mitigate the three types of attacks that we discussed in VANET.

A. Sybil attack detection and mitigation techniques

There are several techniques that can be used to detect and prevent Sybil attacks in VANETs. These include:

1. Radar: The radar can be used to detect the adjacent vehicles' physical parameters as it can be considered a priority data source. The oncoming traffic radar can be used to detect the physical parameters of non-adjacent vehicles and can be considered a secondary source of data [13] [14]. The radar can detect the physical parameters of non-neighboring vehicles as a second priority.

   The third priority data source is the neighbors' reports. To mitigate this attack, a history of the vehicles' data movement needs to be built based on these priorities, as it will help screen faked data from the real data. To isolate trusted vehicles from suspicious vehicles, a table can be created to classify the level of trust in each vehicle (trusted, untrusted, suspicious).

2. Timestamp: This technique relies on the prevention of Sybil attacks and provides privacy for drivers as well. It operates effectively for the first development phase of VANETs with the availability of the RSU infrastructure [15] [16]. The general idea behind this technique is the fact that two vehicles infrequently pass through several RSUs as each RSU is far apart from each other at the same time. The RSU creates digital timestamps for every vehicle that passes through it. The vehicle sent out a traffic message that contains many identical timestamps to the previously passed RSUs. Hence, the vehicle might be suspected as an attacker if multiple messages come from one source. This technique is economical as it does not use Internet-accessible RSUs or Public Key Infrastructure (PKI), which is expensive.

3. Active Position Detection: Position detection can be used to collect the relative angle, position, and velocity of each vehicle in VANET [17] [18] [19]. Two events can initiate radar detection. The first event is called the timeout threshold. This event can be triggered when a vehicle does not receive any data from other vehicles. The timeout threshold will be increased by one after a certain amount of time, and the vehicle will send a signal to the radar to verify the position of the observed vehicle. The radar detection can also be initiated at a random time, and the main idea behind it is to ensure that the trusted vehicle remains trustworthy inside the VANET environment.

4. Trusted Certificate Authority: This technique is by far the most effective technique that can be used to mitigate Sybil Attacks. It requires the presence of a Certificate Authority (CA) that verifies the one-to-one communication between the vehicle identity and the network [20] [21]. This CA eliminates the problem of creating a trust relationship between two nodes. Furthermore, the certificate authority can revoke a certificate of any suspicious node in the network. This technique may acquire an appreciable performance cost in real-world applications, primarily if it's performed on large scale systems manually.

5. Random Key Distribution with Validation Key Test: This technique enables the nodes in VANET to communicate with each other securely. The main idea behind this technique are the key validation and the association of the node identity with the key [22]. The forged identity of the Sybil attack will not pass the validation test as the keys associated with a random identity do not have a significant intersection most of the time with the compromised key.

B. Timing attack detection and mitigation techniques

The following are the techniques that can be used to detect and mitigate timing attacks in VANET.

1. Monitoring Vehicle Behavior: When a vehicle communicates with other vehicle in the network, a trust is established based on the correctness of information communicated. The behavior of the vehicle in traffic lights, junctions, amount of CO2 emissions of the vehicle, and speed of vehicle are used to compute the node reputation value. This technique may help in building a trust database to isolate the trusted vehicle from the untrusted one in the network [23] [24] [25] [26] [27] [28] [29].

2. Signature Based Intrusion Detection SYSTEM: As discussed, with timing attack, the users receive multiple copies of the same message, which pose data redundancy in the network. The RSU can be equipped with a signature-based intrusion detection system that may help in detect any suspicious activity or violation by malicious node. This technique provides a sufficient protection until attackers become more advanced [30].

C. Jamming attack detection and mitigation techniques

The Following are techniques to counter the effect of jamming attack and maintain availability and reliability in VANET.

1. Channel Switching technique: The DSRC spectrum is divided into seven 10 MHz channels. Fig. 6 illustrates the types of channels in DSRC. The adversary jamming one single channel, and the

OBU can evade from this attack by switching to another channel using Frequency Hopping Spread Spectrum (FHSS) when the channel is jammed. The FHSS changes the frequency range of communication channel using pseudorandom number generator sequences.

2. Multiple Radio Transceivers: The OBU can have multiple transceivers for sending and receiving messages, which can be achieved using multiple input multiple output design principles. This will allow the system to switch from one transceiver to another in the event of jamming attacks.

3. Channel Signal Strength: A reactive jammer's goal is to prevent the legitimate node from transmitting packets to other nodes in the network by making the channel always appear busy. To detect this type of jamming, a technique is needed to track the total time spent waiting for the channel to become inactive, as well as to monitor the location of the node and packet signal strength. These metrics can be used to compare them to regular traffic times to determine if jamming is occurring in the channel. The idea behind using channel signal strength is to check if the value of the data transmission is consistent with the threshold value. If the threshold value is higher than the maximum packet of a particular node, then that node is identified as a jammer. However, if the threshold value is lower than a particular node's packet, then it may or may not be identified as a jammer, as it could be due to weak signals during transmission [31] [32].

4. Technology Switching: There are various communication technologies that can function with VANET, such as Wi-Fi, 3G, 4G, 5G, and Wi-MAX—switching between them for accessing the network paves less chance for the adversary from launching a successful jamming attack [33].

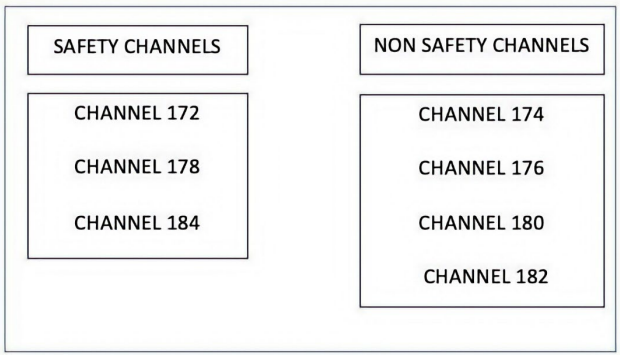

Fig. 6. DSRC spectrum.

VI. CONCLUSION

Human life is involved directly in the Vehicular Ad hoc Network. Hence, only accurate and authentic information should be disseminated through the network. Overcoming VANET attacks requires an effort to reach a secure environment. This paper presents the VANETs system architecture from a domain perspective. Next, we demonstrate the layered architecture and communication architecture of VANETs. Finally, we give an overview of three types of attacks in VANET (Sybil attack, jamming attack, and timing attack) and presents all techniques that can be used to detect and mitigate these types of attacks in VANETs.

REFERENCES

[1] Kuciemba, S., Timcho, T., McLaughlin, K., Perry, F., & Bezzina, D. (2021). Evaluation and Synthesis of Connected Vehicle Communication Technologies (No. NCHRP Project 23-10).

[2] Tahir, M. N., Katz, M., & Rashid, U. (2021, January). Analysis of VANET wireless networking technologies in realistic environments. In 2021 IEEE Radio and Wireless Symposium (RWS) (pp. 123-125). IEEE. Chicago

[3] Irshad, A., Shafiq, M., Chaudhry, S. A., & Usman, M. (2022). Security Hardened and Privacy Preserved Vehicle-to-Everything (V2X) Communication. Security and Communication Networks, 2022.

[4] Mohamed, T. M., Ahmed, I. Z., & Sadek, R. A. (2021). Efficient VANET safety message delivery and authenticity with privacy preservation. PeerJ Computer Science, 7, e519.

[5] Hamdi, M. M., Dhafer, M., Mustafa, A. S., Rashid, S. A., Ahmed, A. J., & Shantaf, A. M. (2022, June). Effect Sybil attack on security Authentication Service in VANET. In 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-6). IEEE.

[6] Shetty, S. R., & Manjaiah, D. H. (2022). A comprehensive study of security attack on VANET. In Data Management, Analytics and Innovation (pp. 407-428). Springer, Singapore.

[7] Zheng, B., Sayin, M. O., Lin, C. W., Shiraishi, S., & Zhu, Q. (2017, November). Timing and security analysis of VANET-based intelligent transportation systems. In 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD) (pp. 984-991). IEEE.

[8] Al-shareeda, M. A., Alazzawi, M. A., Anbar, M., Manickam, S., & Al-Ani, A. K. (2021, July). A Comprehensive Survey on Vehicular Ad Hoc Networks (VANETs). In 2021 International Conference on Advanced Computer Applications (ACA) (pp. 156-160). IEEE.

[9] Costandoiu, A & Leba, Monica. (2019). Convergence of V2X communication systems and next generation networks. IOP Conference Series: Materials Science and Engineering. 477. 012052. 10.1088/1757-899X/477/1/012052.

[10] T. Zaidi and Syed.Faisal, "An Overview: Various Attacks in VANET," 2018 4th International Conference on Computing Communication and Automation (ICCCA), 2018, pp. 1-6, doi: 10.1109/CCAA.2018.8777538.

[11] C. H. O. O. Quevedo, A. M. B. C. Quevedo, G. A. Campos, R. L. Gomes, J. Celestino and A. Serhrouchni, "An Intelligent Mechanism for Sybil Attacks Detection in VANETs," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), 2020, pp. 1-6, doi: 10.1109/ICC40277.2020.9149371.

[12] Mokdad, L., Ben-Othman, J., & Nguyen, A. T. (2015). DJAVAN: Detecting jamming attacks in Vehicle Ad hoc Networks. Performance Evaluation, 87, 47-59.

[13] B. Liu, B. Khorashadi, H. Du, D. Ghosal, C-N. Chuah and M. Zhang, "VGSim: An Integrated Networking and Microscopic Vehicular Mobility Simulation Platform", IEEE Communication Magazine Automotive Networking Series, vol. 47, no. 5, pp. 134-141, May 2009.

[14] Hamdan, S., Hudaib, A., & Awajan, A. (2018, October). Hybrid algorithm to detect the Sybil attacks in VANET. In 2018 Fifth international symposium on innovation in information and communication technology (ISIICT) (pp. 1-6). IEEE.

[15] Faisal, S. M., & Zaidi, T. (2020). Timestamp Based Detection of Sybil Attack in VANET. Int. J. Netw. Secur., 22(3), 397-408.

[16] Sharma, S., & Sharma, S. (2016, December). A defensive timestamp approach to detect and mitigate the Sybil attack in vanet. In 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I) (pp. 386-389). IEEE.

[17] Yan, Gongjun & Choudhary, Gyanesh & Weigle, Michele & Olariu, Stephan. (2007). Providing VANET security through active position detection. Computer Communications. 31. 73-74. 10.1145/1287748.1287762.

[18] Penna, K., Yalavarthi, V., Fu, H., & Zhu, Y. (2014, July). Evaluation of active position detection in vehicular ad hoc networks. In 2014 International Joint Conference on Neural Networks (IJCNN) (pp. 2234 - 2239). IEEE.

[19] M. Baza et al., "Detecting Sybil Attacks Using Proofs of Work and Location in VANETs," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 39-53, 1 Jan.-Feb. 2022, doi: 10.1109/TDSC.2020.2993769.

[20] Reddy, D. S., Bapuji, V., Govardhan, A., & Sarma, S. S. V. N. (2017, February). Sybil attack detection technique using session key certificate in vehicular ad hoc networks. In 2017 international conference on algorithms, methodology, models and applications in emerging technologies (ICAMMAET) (pp. 1-5). IEEE.

[21] Soni, M., & Jain, A. (2018, February). Secure communication and implementation technique for Sybil attack in vehicular ad-hoc networks. In 2018 Second International Conference on Computing Methodologies and Communication (ICCMC) (pp. 539-543). IEEE.

[22] Ehdaie, M., Alexiou, N., & Papadimitratos, P. (2016). Random Key Pre-Distribution Techniques against Sybil Attacks. Journal of Communication Engineering, 5(1), 1-13.

[23] A. Tigga and P. Arun Raj Kumar, "Towards a Vehicle's behavior monitoring and Trust Computation for VANETs," 2019 IEEE Conference on Information and Communication Technology, 2019, pp. 1-6, doi: 10.1109/CICT48419.2019.9066210.

[24] Kadam, M., & Limkar, S. (2014). Detection and Mitigation of Misbehaving Vehicles from VANET. In ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol I (pp. 267-276). Springer, Cham.

[25] So, S., Sharma, P., & Petit, J. (2018, December). Integrating plausibility checks and machine learning for misbehavior detection in VANET. In 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA) (pp. 564-571). IEEE.

[26] Hasrouny, H., Samhat, A. E., Bassil, C., & Laouiti, A. (2019). Misbehavior detection and efficient revocation within VANET. Journal of information security and applications, 46, 193-209.

[27] Zacharias, J., & Fröschle, S. (2018, December). Misbehavior detection system in VANETs using local traffic density. In 2018 IEEE Vehicular Networking Conference (VNC) (pp. 1-4). IEEE.

[28] Schmidt, R.K., Leinmüller, T., Schoch, E., Held, A., & Schäfer, G. (2008). Vehicle Behavior Analysis to Enhance Security in VANETs.

[29] Santos J., L.M., Moreira, E. An evaluation of reputation with regard to the opportunistic forwarding of messages in VANETs. J Wireless Com Network 2019, 204 (2019). https://doi.org/10.1186/s13638-019-1518-x

[30] Haydari, A., & Yilmaz, Y. (2022). RSU-Based Online Intrusion Detection and Mitigation for VANET. Sensors, 22(19), 7612.

[31] Jesus Manuel Gonzalez De Jesus, "Exploring Jamming Attacks Using Opnet 12.0", M. Science In Telecommunications thesis, University Of Pittsburgh, Pittsburgh, PA, USA November 2008.

[32] Nadeem Sufyan, Nazar Abbass Saqib and Muhammad Zia, EURASIP Journal on Wireless Communications and Networking 2013, 2013:208 doi:10.1186/1687-1499-2013-208.

[33] M. N. Tahir, M. Katz and U. Rashid, "Analysis of VANET Wireless Networking Technologies in Realistic Environments," 2021 IEEE Radio and Wireless Symposium (RWS), 2021, pp. 123-125, doi: 10.1109/RWS50353.2021.9360381.