TIERS Information Technology Journal
Vol.3, No.1, June 2022, pp. 17~27
ISSN: 2723-4533 / E-ISSN: 2723-4541
DOI: 10.38043/tiers.v3i1.3520

Security Issues of Vehicular Ad Hoc Networks (VANET): A Systematic Review

Sahabdeen Aysha Asra
ashrasahabdeen005@seu.ac.lk
Department of Information Technology, South Eastern University of Sri Lanka

ABSTRACT

A vehicular ad hoc network (VANET) is a wireless network that connects groups of stationary or moving automobiles. VANETs are a subset of mobile ad hoc networks (MANETs) that refer to a group of connected cars. The various networking layers in common Internet protocol stack topologies are linked to security vulnerabilities in VANETs. A security breach in a VANET is typically serious and harmful. Also Current VANET security standards handle the bulk of the security issues that vehicle networks confront. This paper presents VANET's different types of security attacks in a systematic review approach. The information was gathered by a systematic examination of existing research articles. However, as technology is growing and VANETs are getting more popular, security vulnerabilities are increasing rapidly, which ultimately restricts the widespread usage of the VANETs. In this article, the security vulnerabilities of VANETs are surveyed. The article also provides layer-specific attack classification in the VANETS protocol stack.

Keywords: VANET; MANET; Security issues; ad hoc network;

Article Info

Accepted	: 03-05-2022
Revised	: 29-04-2022
Published Online	: 25-06-2022

Correspondence Author:

Sahabdeen Aysha Asra
Department of Information Technology,
South Eastern University of Sri Lanka,
316/A, Bulugohatenna, Akurana, Kandy, Sri Lanka. postal code: 20850
Email: ashrasahabdeen005@seu.ac.lk

1. INTRODUCTION

Smart Trasportation system can be developed through various emerging technologies such as IoT, Big Data, and many more [1], [2]. The VANETs are a subset of MANETs that refer to a group of smart automobiles on the road. These cars use wireless Local Area Network (LAN) technology to communicate with one another or with Road Side Infrastructure (RSU) [3][4].

In a VANET, security must ensure that intruders do not insert or modify shared messages. In addition, drivers' responsibility is vital for accurately informing the traffic situation within a time restriction. Because of the unique properties of VANET, unique security concerns arise. Mishandling these security concerns will result in a slew of restrictions [5]. Insecure information transfer via VANET connection might lead to disaster. As a result, this data must be precise, efficient, and dependable. Every project in the VANET domain has as its goal the effective provision of road safety through frequent information exchange across network nodes. Any successful attack can result in major fatalities, financial losses, or accidents [6].

Various software and hardware components are used in the construction of automobile ad hoc networks. Vehicles on a VANET network are equipped with an OBU (On Board Unit) that is mounted in the vehicle. The security assurances for end-users and customers are crucial for the commercial adaption of VANET to establish a secure Intelligent Transportation System (ITS). The majority of the security difficulties faced by vehicle networks are addressed by current VANET security standards [7]. The rapid expansion of vehicle networks has resulted in a rise in security needs. Users of the vehicular network, like users of other networks, need security in terms of data confidentiality, availability, and integrity among other things. Everyone who drives a car need privacy [8].

This is how the rest of the paper is organized. The basic principles and state of the art in VANET are presented in Introduction. The related articles are stated in literature review and methodology includes in next section respectively. The VANET security problems are discussed in Results. Finally, conclusion brings this article to a close.

2. LITERATURE REVIEW

A VANET security compromise is frequently significant and dangerous. Indeed, because to the essential nature of some VANETs applications, any misconceptions, modifications, or other errors might result in catastrophic repercussions such as life and/or financial losses. Furthermore, the VANET's great mobility and its usage of wireless media, as well as dynamic character, render it vulnerable to assaults that take advantage of wireless communication's open and broadcast nature [9]. Furthermore, this kind of technologies can be used to create safe autonomous transport system in the smart city development process [10], [11].

VANET security concerns are essential since vulnerabilities occur during information transfer, exposing VANET to attackers. The VANET security system must meet the standards in order to maintain secure vehicular communication and networks. Some of the criteria are mandatory for all networks, while others are exclusive to the VANET [12].

VANETs, on the other hand, are confronting a slew of security issues, including Denial of Service Attack (DOS), Sybil, impersonation, replay, and other related threats, as autonomous vehicle technology advances [13]. Also In the VANET, there are several issues, including QoS provisioning, high connection and bandwidth, and vehicle and individual privacy protection [14]. The fast proliferation of cars has resulted in the vehicular network becoming diverse, dynamic, and large-scale, making it difficult to match the fifth-generation network's stringent standards, such as massive connections, extremely low latency, top security, and high mobility [15].

When VANET security standards are put on their constructions, many threats may be discovered and compromised. Intruders do not alter information transferred between VANET nodes; rather, the dependability or trustworthiness of the message delivered is examined [16]. Security is a critical responsibility in VANETs that must be maintained to avoid assaults in vehicle-to-vehicle (V2V) communication. Strong authentication mechanisms are essential to prevent attackers from joining the vehicle group and engaging in harmful behaviors that cause collisions [17]. In order to protect VANET networks against attack, VANET designs must fundamentally provide on security for services in terms of information, availability, integrity, authentication, non-repudiation and confidentiality. The protection of personal information is also a significant challenge [18]. The attacker vehicle/s sends out a high number of unwanted messages in order to drain network resources or loses data packets or traffic status packets [19]. Any malicious action on a system that is extremely destructive is referred to be an attack. The main goals of the assault are to steal information or corrupt the system, among other things. They destroy the system's integrity and secrecy. Vehicle networks, like other systems, are subject to a variety of threats [8].

VANETs' wireless access medium puts them in direct conflict with attackers attempting to hack the networks [20]. The most serious damage has been caused by assaults that have caused the network to go down [21]. A VANET is a self-organizing, infrastructure-free system of mobile phones that may communicate with each other remotely. These can communicate with one another via OBU or RSU dependent on Wireless Local Area Network (WLAN) advancements. Vehicles are viewed as communication nodes in this system, and they can be connected to a self-sorting system without prior knowledge of the other's essence [22].

3. RESEARCH METHOD

The systematic review approach was used to write this study, which involved an analysis of previously published research and review articles. The research was carried out using a qualitative approach to examine security issues of VANET technology. The majority of the essential mandatory data was acquired from reliable sources. This analysis identifies and highlights the major issues. Those are Denial of Service Attack (DOS), Distributed Denial of Service (DDOS) Attack, GPS and Tunneling attack, Global Positioning System (GPS) Spoofing, Replay Attack, Black Hole Attack, Grey Hole Attack, Wormhole attack, Sink Hole Attack, False position information, Inferring work and home locations, Bogus information attack, Spamming Attack, Illusion Attack, Passive eavesdropping attack, Passive eavesdropping attack, Timing Attack, Man in Middle Attack, Social Attack, Malware Attack, Masquerading Attack, dentity Disclosure Attack, Sybil Attack, Impersonation attack, Massage tempering, Free-Riding Attack, Jamming attack, Hidden vehicle attack, Bogus information Attack, Node Impersonation attack, Illusion attack, Snooping attack, Masquerading attack, ID Disclosure attack, Message tampering attack, Brute force attack, Social attack, Timing attack, Eavesdropping Attack, Masquerading Attack, Prank Attack as well as Application Attack on safety and Non Safety messages.

3.1. Article selection criteria

The following crucial parameters were considered to shortlist the downloaded papers from respectable publishers such as IEEE, Sage, Sciencedirect, Springer and Emerald. A flowchart of the systematic literature review categorization approach is also shown in Figure 1. This research focuses on publications which are written in English, varies types of attacks, high-indexed open-access articles, and full-length papers.

The following are shows how to create research questions (RQ) for the article in order to specify the data required for this study's analysis.

- What is VANET ad hoc technology?
- What are the issues identified in VANET technology?

According to RQ the objective of this study is to identify the definition of VANET technology and the security issues of VANET adhoc technology.

Almost 29 article were reviewed out of the 155 articles for this study. The reasons for the deduction of the articles are given below figure 1:

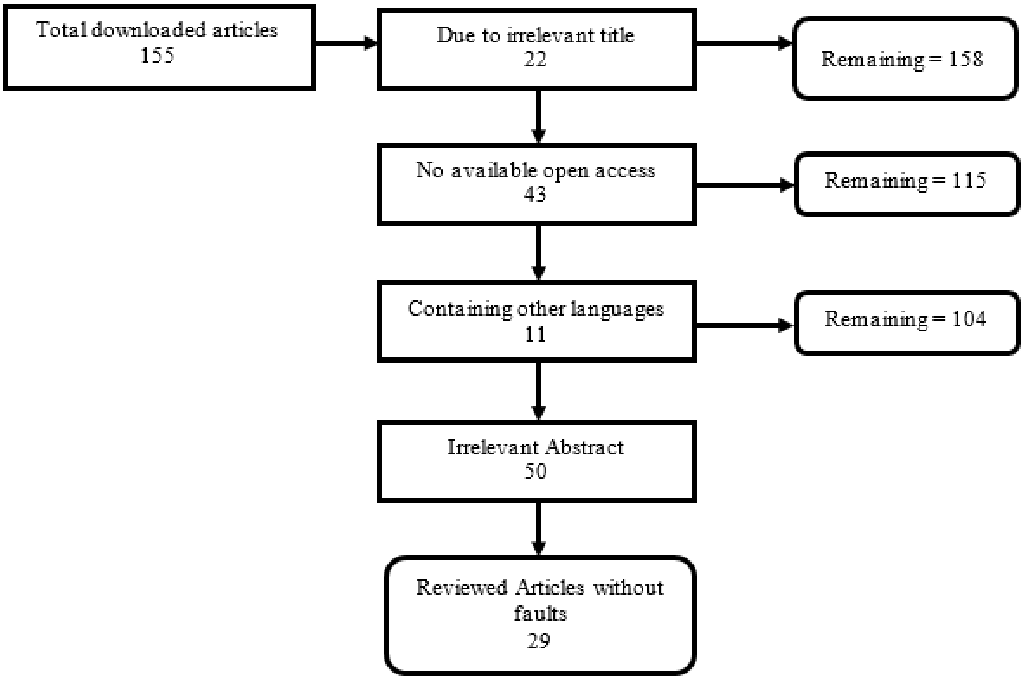

Figure 1. Study Selection

4. RESULTS AND DISCUSSION

Because of the nature of the open wireless channel utilized in VANET, the VANET is vulnerable to a variety of assaults. As a result, the possibilities of an assault are quite high. The attackers' goal is to cause problems for genuine users, and as a result, services are unavailable. The following are some of the assaults.

4.1. Attacks on the Physical Layer

4.1.1.Eavesdropping attack

This is a passive assault that targets the networks confidentially. The attackers collect the network's private data. Attackers stealthily monitor network traffic or the present location and actions of a specific vehicle node. Detecting such an attacker is tough since they do not respond in the existing network [23].

4.1.2 Denial of Service attack (DOS)

Attacker transmit several dummy messages to jam the network in order to conceive attention or to take privilege of the network or to disrupt the efficiency of the network [24][25]. When an attacker enters the network and gains control of the car resources or jams communication between nodes and the roadside unit, a DoS will occur [26]. Finally, users do not have access to networks. DOS is not permitted on VANETs, where important data is delivered safely and on time to its intended destination. In a nutshell, attackers can access DOS attacks in three ways: blocking the communications channel, loading the networks, and shutting the packets. The DOS assaults are presented in three tiers below [27]. Malicious, disruptive, and remote DoS attacks have three major characteristics.

a. Malicious - The activity is carried out with the intention of achieving a certain outcome.
b. Disruptive - This assault has the potential to compromise network capabilities or resources.
c. Network-based - The assault is carried out through the internet [28].

In a DOS attack, the attacker targets the service provider's services. Even when free recourses are accessible, legitimate users will not be able to use the network's services. The major communication channel is jammed by the attacker. This form of attack is restricted within the service provider's range [23].

4.1.3.Distributed Denial of Service (DDOS) attack

Multiple malicious vehicles launch attack on a legitimate vehicle from different locations and they may use different time slots for sending those messages [24]. DDOS attacks are created when a distributed DOS assault is managed. In a DDOS attack, numerous attackers target a single or several service providers from different locations in order to cause disruption in the usage of the service provider's services [25]. A large number of malicious OBU nodes are implicated in this attack, which prevent other legitimate users from accessing services from one or more RSUs. By delivering spam messages into the network, attackers create needless network transmission delay [23][29].

4.1.4.Illusion attack

In this attack, the attacker tries to intentionally tamper with his vehicle's readings or traffic information, then send that bogus information to adjacent automobiles and RSU. In a VANET, a driver's behavior is influenced by the warning signals he or she gets; if the driver receives false warning messages, this can lead to an accident, a traffic jam, or a reduction in network performance via modifying network topology [24].

4.1.5.Message tampering attack

This attack seeks to corrupt or change data in order to disrupt communication between V2V or Vehicle to Roadside (V2R) units. This attack might result in the loss of life in safety-critical applications [28].

4.1.6.Jamming attack

A radio transmission can become trapped or interfered in this manner, causing alerts to be distorted or lost. In fatalities and a failure to obtain important data such as road conditions and accidents. Jammer sends out repeated radio signals in the targeted region to disrupt connection between the station's nodes [27][25].

4.2 Other Attacks

4.2.1. GPS and Tunneling attack [30]

In VANET, a database is kept containing information about the vehicle's position, geographic locations, and identification as determined by the Global Positioning System (GPS) satellite. To launch the assault, the malicious user uses a GPS emulator that generates stronger signals than the genuine satellite signals in order to deceive the cars and lead them astray [26]. Position Faking is another name for this assault. In this sort of assault, the attacker attempts to alter the user's current geographic location identification and get false information from the GPS system. By employing this strategy, the user hides his current location from the network and displays the incorrect location to others [23].

4.2.2.Global Positioning System (GPS) Spoofing [30]

In VANET, a database is kept containing information about the vehicle's position, geographic locations, and identification as determined by the Global Positioning System (GPS) satellite. To launch the assault, the malicious user uses a GPS emulator that generates stronger signals than the genuine satellite signals in order to deceive the cars and lead them astray [26]. Position Faking is another name for this assault. In this sort of assault, the attacker attempts to alter the user's current geographic location identification and get false information from the GPS system. By employing this strategy, the user hides his current location from the network and displays the incorrect location to others [23].

4.2.3.Replay attack

Users in VANET are recognized by their Internet Protocol (IP) and Media Access Control (MAC) addresses. However, these are insufficient estimates to keep intruders at bay, since they may fake the IP and MAC to get the identity of a legitimate user and use it to gain access to the system and hide [26]. The replay assault has the unique feature of being able to be carried out by unauthorized nodes. A replay attack is when the attacker broadcasts [29] messages that have previously been forwarded to the nodes, with the goal of misleading the other nodes in the network by lowering priority messages from the queue. The system's efficiency would be harmed by repeated replaying, and the cost of bandwidth would rise as a result [28].

4.2.4.Black Hole attack

Malicious nodes transmit a false routing information and pretend to have an optimum route for the destination in order to attract sender node. As the sender node transmits that packet, malicious vehicles drop that packet or missus that packet [24][25]. A black hole is a region in a network where there are no nodes. The attacker can launch a black hole attack [31] by offering himself as a path to link with other nodes in the VANET, thereby circumventing the routing mechanism. The attacker nodes may keep the packets, drop them, or pass them to any node they wanted because of the forged established route [26][27]. It is a form of routing attack in which the attacker uses the shortest path to the desired transmitter node to entice other network nodes to transmit packets through it. It drops the packets after receiving them [23].

4.2.5.Grey Hole attack

The Gray Hole [31] assault is a version of the black hole attack that is based on the notion of selective forwarding. Instead of discarding all data packets, malicious nodes will pick and choose which ones to drop, while the others are transmitted, lowering the network's packet delivery ratio [28]. It's a form of routing attack that's also known as a Black hole extension since instead of discarding all packets, it just loses a subset of them. Because such an assault is not continuous, it is extremely difficult to detect. It is only made for a set period of time and for a specific sort of packet [23].

4.2.6.Wormhole attack

In a wormhole attack, legitimate automobiles receive data packets from hostile cars, which is a version of the black hole assault. Malicious automobiles establish a wormhole or tunnel between the sender and recipient with a low hope count and record it in the routing database in this attack [24]. Because the attacker nodes establish a tunnel between the end nodes and the malicious nodes, worm hole attacks are difficult to detect and prevent. Inside the tunnel, packets are broadcast to the network [25]. When attacker nodes may exploit their position to inflict harm, such as obtain illegal access, disrupt routing, or launch a DoS assault, this is a dangerous condition [26][27]. The operations of routing protocols such as AODV and DSR in transferring messages on VANETs are hampered by the Worm Hole attack. Malicious nodes or worm holes might get illegal access and use it to launch a denial of service attack, jeopardizing the security of transmitted data packets [28]. It's also a form of routing attack in which an attacker's malicious node receives data packets from a legal user at any point on the network, tunnels them, and forwards them to another network point. Wormhole attacks are tunnels built between two malicious nodes [23].

4.2.7.Sink Hole Attack

Sink Hole Attacks attempt to route communication between nearby nodes through rogue nodes in order to change the data sent before re-transmitting it. Other assaults, such as the Gray Hole and Black Hole attacks, are performed using it [28][29].

4.2.9.False position information

One of the major issues in VANETs is distorted information, because total security is dependent on reliable location information. Furthermore, the study found that on VANETs, misrepresenting the location resulted in a 90 percent reduction in total packet delivery. To summarize, disseminating false information has a negative impact on dependability, security, and performance [27].

4.2.10.Inferring work and home locations

The preceding techniques solve the challenge of extracting significant location information from an alias. Numerous methods for recognizing notable sites based on spatial and temporal evidence of location data have been used in previous publications. The writers in the first category utilize clustering methods to create residences for mobile users [27].

4.2.11.Bogus information attack

The VANETs make use of the data generated or sent by other vehicles or RSUs. However, there is a chance that the data will be tampered with. There is a possibility that a vehicle will create inaccurate information and send it. The attacker's purpose is very harmful from the standpoint of vehicle manipulation [27].

4.2.12.Spamming attack

Spamming is a sort of attack that allows an attacker to transmit a large number of spam messages through a network in order to use more bandwidth. Furthermore, due of the presence of spam messages in VANET, transmission delay will rise [26]. Spamming is a type of attack in which an attacker frustrates users by delivering spam messages such as ads, with the express purpose of using bandwidth and causing voluntary collisions. The main goal is to cause network congestion and delay, hence degrading the network's performance. Due to centralized governance and the lack of fundamental infrastructure, this attack is difficult to control [28][25][29].

4.2.13.Passive eavesdropping attack

Unintentional passive assaults are another sort of attack that includes network monitoring to follow vehicle traffic or eavesdropping on one's conversation by using wireless media characteristics. Malicious vehicles have the ability to infiltrate network communications. Passive assaults are sometimes known as traffic attacks or reptile attacks [27].

4.2.14.Timing attack

When a malicious vehicle gets an emergency message, it does not immediately transfer it to the intended destination, instead adding a time slot to the original message to create a delay. As a result, the message is received by the receiving vehicle, which then necessitates [24][27].

4.2.15.Man in Middle attack

In order to gain access to the information that both vehicles were trying to send each other and inject false information between vehicles, malicious vehicles insert themselves into the communication between two vehicles and impersonate both vehicles. This attack impersonates as a normal exchange of information [24]. The attacker will very probably get through the user authentication procedure, but will be linked with the possession approval step, a basic example of the man in the middle attack [27]. The data integrity and privacy goals of security standards are both violated by this assault. In this sort of attack, the attacker puts oneself between two genuine nodes/vehicles, eavesdrops on their communication, and injects phony information or alters messages between them, all while the two nodes believe they are interacting directly with each other. The legitimacy of sent information is negatively damaged as a result of this assault, and network security is jeopardized [28].

4.2.16.Social attack

This assault targets all weak attacks. In a Social Attack, the attacker's goal is to create a problem for the network's users indirectly [24]. This phony node deceives VANET neighbors by sending bogus alarms or information about traffic jams and accidents. It can even generate data in the form of an increased number of cars on the road [26].

4.2.17.Malware attack

Malware attacks are carried out by injecting malware such as viruses and worms into the VANET, which can wreak havoc on its functioning. When the OBU and RSU are doing patches or software upgrades, malware can be deployed by an insider rather than an outsider [26][25][29].

4.2.18.Masquerading attack

Masquerading is similar to launching a physical attack on a network. Nodes may simply enter and exit the network, much like in VANET. Each node has its own MAC address as well as an IP address. These addresses can be used by attackers to discover the identities of other nodes [26].

4.2.19.1dentity Disclosure attack

Insiders with a passive and malignant appearance carry out identity disclosure attacks. It may keep an eye on the targeted nodes and use this assault to discover their identities [26].

4.2.20.Sybil attack

The poisonous Sybil assault [31] was initially mentioned in the context of a peer-to-peer network. An attacker creates the illusion of several bogus vehicles in order to gain control of the whole network and infect false information in order to damage genuine users or degrade network performance [24]. It's thought to be one of the most dangerous assaults in VANETs. Because the malicious node in the Sybil attack [26] has several identities, it's impossible to tell if the information received is from a legitimate and innocent node or from a malicious node. Because each node has multiple identities, the network poses a significant security risk because one can deceive other vehicles on the road by creating a deception of multiple vehicles on the road or by sending fake messages such as traffic jam messages, incorrect route directions, or false positions, causing the entire network to be disrupted and putting passengers' lives at risk [28]. Through Sybil attack attacker generates many identities of nodes which propagate the erroneous information in the network. Data is transmitted with a false identity in this sort of attack. This form of assault done by the attacker OBU on the other valid OBU for receiving the varied rewards. In this assault, the attacker vehicle creates various identities and sends signals to legitimate users, such as there is more traffic on a certain journey road, so choose a different route. The attacker will construct an illusion and send a similar message to the same vehicle [23][25][29].

4.2.21.Impersonation attack

To deliver bogus messages to other cars and distant nodes, the malicious vehicle ensures that it is a real vehicle. Every car in the VANETs has a unique identification, and each vehicle is identified in the VANETs environment using these identities. When an occurrence occurs, it becomes increasingly significant. An attacker's node can modify its character and pass itself off as a real message sender in an identity assault. The attacker obtains the message from the message's disseminator and modifies the message's content to his or her benefit [27].

4.2.22.Massage tempering

To illustrate the constant quality of communications, researchers used the similarity algorithm, information connection, and challenge character confirmation technique [27].

4.2.23.Free-Riding attack

This is a relatively typical attack that is started by a hostile user who makes fake login attempts while using cooperative messaging authentication. In this type of attack, the malicious user takes use of other users' authentication contributions without providing its own, which is referred to as a freeriding attack. This exploit might put the cooperative message authentication system in jeopardy [30].

4.2.24.Hidden vehicle attack

The concealed vehicle attack involves the attacker cheating with positioning information by transmitting bogus position information to nearby nodes. The attacker deceives nearby nodes into believing that its position is the best spot to relay the warning message to other cars; the attacker then sends bogus accident messages to other nodes or remains silent after receiving the safety messages [27].

4.2.25.Bogus information attack

In Bogus Information attack, the objective is to transmit bogus or false information in the network to divert the existing behavior of drivers. For example, malicious node may disseminate false in-formation regarding the accident to route the traffic to other routes or emergency vehicle warning just to slow down the traffic. In this way, the performance of the network is affected by such fake messages [28].

4.2.26.Node Impersonation attack

This attack is a breach of network authentication. Each vehicle in a VANET has a unique identity that it uses to identify itself in the network, and this identity is important in the event of any hazardous conditions. The hostile node alters its id for his or her own profit in a Node Impersonation attack [26]. It alters the data it gets from the source node and forwards it to other cars after modifying its id. Other cars mistakenly believe that a message has been received from a genuine node, exposing private information [28]. In a Node Impersonation Attack, the attacker updates the message and pretends it came from a trusted source. The attacker sends bogus information over the network on purpose. This form of message is sent to cause misunderstanding in communication or to encourage selfish conduct on the part of a node in order to obtain a benefit. A Message Tempering attack is another name for it. In the VANET, such changes in life-critical messages will become prohibitively expensive [23].

4.2.27.Illusion attack

This hack jeopardizes data security and trust. The attackers are adequately authenticated in this attack, and sensors are placed in the network to create useless or fraudulent information. Because of the inaccurate information, the system will send out incorrect traffic alerts to neighbors, disrupting network connectivity and perhaps causing accidents. Because the attacker enters the network in a legitimate and permitted manner, an illusion attack is difficult to detect [28].

4.2.28.Snooping attack

This attack belongs to the passive group of assaults, in which the attacker first watches the data to determine the pattern of communication between the communicating nodes, and then obstructs and accesses the data for its own gain depending on the requirement [28].

4.2.29.Masquerading attack

It is an active attack in which the attacker disguises himself as a valid node in order to send fraudulent messages via the network or change the received message [28].

4.2.30.ID Disclosure attack

The authentication and privacy requirements are both violated by this attack. The attacker transmits malicious code to nodes in the area of the target node with the goal of remotely observing the target vehicle's pattern, which in turn takes the target vehicle's position and id, causing them to lose their privacy. Rental car owners commonly use this attack to keep track of their own vehicles and safeguard them from mishaps [28].

4.2.31.Brute force attack

Cryptographic algorithms rely heavily on keys to keep information secure. The attacker utilizes a hit-or-miss approach to obtain sensitive information such as passwords and personal information in this attack. The attacker makes several tries since decoding encrypted data with a brute force technique takes time [28]. If the target node is out of range, the sender vehicle must enlist the assistance of another vehicle to deliver the data to the destination vehicle. Sender cars may encrypt their data and transfer it to the destination via any mediator vehicles to ensure confidentiality. This is a sort of cryptography attack in which a mediator vehicle takes on the role of an attacker and attempts to decipher the encrypted data by repeatedly attempting various alternative methods [23].

4.2.32.Social attack

It's an emotional assault in which the attacker transmits unscrupulous messages via the network in order to enrage legitimate users. As a result, the vehicle's driving behavior is changed, causing an issue in the network [28].

4.2.33.Timing attack

In VANETs, time is a critical component for both safety and non-safety applications, because messages received after a delay are useless and may pose major risks. Instead of altering the contents, the attacker merely adds additional time slots to the original message with the purpose of delaying delivery and so rendering the communication worthless [28].

4.2.34.Masquerading attack

In this form of attack, the attacker uses the identity of another vehicle to impersonate it. Users will lose faith in VANET if they are subjected to such an assault [23].

4.2.35.Prank attack

The perpetrator pulls pranks on other automobiles in this form of attack. Users have lost faith in the system as a result of such attacks [23].

4.2.36.Application attack on safety and Non Safety messages

One of the key uses of VANET is safety messaging. Users will get alerts such as Bump Ahead, Traffic Congestion Details, Blind Turn Ahead, Accident, and Slow down Speed for Safety through the VANET. The attacker will change the message's content and send incorrect information to the real user. Attackers can also change non-safety application notifications such as the closest accessible, Hotels, Petrol Pump or Service Station among other things [23].

Moreover cyber-attack classify in to two parts. Those are active and passive cyber-attacks. Active cyber-attacks are inherently aggressive. Attempts are made to change messages sent over the wireless network and to destroy the system or any files containing useful information by such attackers. Worms, modification, DoS attacks, Viruses, masquerade, modification, and replay and so on are examples. Passive cyber-attacks frequently monitor network traffic and attempt to use the information for illicit purposes or unauthorized access. Traffic analysis, interception, and other examples [32].

5. CONCLUSION

Traditional wireless networks have a number of network security issues. However, because of the network scale, high mobility, frequent topological changes, and the many classes of applications and services with varying requirements given to such networks, security challenges in VANETs are inherent and distinct [27]. VANETs are infrastructure-free networks made up of mobile communicative elements with sporadic connection. The security issues in VANETs are connected to the numerous networking layers in typical Internet protocol stack topologies [33]. This study focused on the security issues in VANET technology. Furthermore this paper gives a systematic review in the area of VANET ad hoc technology which has identified in earlier reviews. It gives overall review about the VANET security issues. Furthermore, the study's shortcomings were the dataset's size and the absence of quality characteristics.

REFERENCES

[1] R. K. A. R. Kariapper, P. Pirapuraj, M. S. Suhail Razeeth, A. C. M. Nafrees, and K. L. M. Rameez, “Smart Garbage Collection Using GPS Shortest Path Algorithm,” in *2019 IEEE Pune Section International Conference, PuneCon 2019*, 2019.

[2] A. C. M. Nafrees, A. M. A. Sujah, and C. Mansoor, “Smart Cities: Emerging technologies and Potential solutions to the Cyber security threads,” in *2021 5th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT)*, 2021, pp. 220–228.

[3] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, “VANET security surveys,” *Comput. Commun.*, vol. 44, pp. 1–13, 2014.

[4] M. N. Mejri, J. Ben-Othman, and M. Hamdi, “Survey on VANET security challenges and possible cryptographic solutions,” *Veh. Commun.*, vol. 1, no. 2, pp. 53–66, 2014.

[5] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, “VANet security challenges and solutions: A survey,” *Veh. Commun.*, vol. 7, no. January, pp. 7–20, 2017.

[6] R. Mishra, A. Singh, and R. Kumar, “VANET security: Issues, challenges and solutions,” *Int. Conf. Electr. Electron. Optim. Tech. ICEEOT 2016*, pp. 1050–1055, 2016.

[7] R. Hussain, F. Hussain, and S. Zeadally, “Integration of VANET and 5G Security: A review of design and implementation issues,” *Futur. Gener. Comput. Syst.*, vol. 101, pp. 843–864, 2019.

[8] R. Kaur, T. P. Singh, and V. Khajuria, “Security Issues in Vehicular Ad-Hoc Network(VANET),” *Proc. 2nd Int. Conf. Trends Electron. Informatics, ICOEI 2018*, no. Icoei, pp. 884–889, 2018.

[9] R. Abassi, “VANET security and forensics: Challenges and opportunities,” *WIREs Forensic Sci.*, vol. 1, no. 2, pp. 1–13, 2019.

[10] A. R. M. Nizzad *et al.*, “Internet of Things Based Automatic System for the Traffic Violation,” in *2021 5th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT)*, 2021, pp. 371–376.

[11] A. C. M. Nafrees, S. M. S. Raseez, C. G. Ubeshanan, K. Achutharaj, and A. L. Hanees, “Intelligent Transportation System using Smartphone,” in *2021 5th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT)*, 2021, pp. 229–234.

[12] M. A. Hezam Al Junaid, A. A. Syed, M. N. Mohd Warip, K. N. Fazira Ku Azir, and N. H. Romli, “Classification of Security Attacks in VANET: A Review of Requirements and Perspectives,” *MATEC Web Conf.*, vol. 150, pp. 1–7, 2018.

[13] J. Mahmood *et al.*, “Security in Vehicular Ad Hoc Networks : Challenges and Countermeasures,” vol. 2021, no. 1, 2021.

[14] S. Rehman, M. A. Khan, T. A. Zia, and L. Zheng, “Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges,” vol. 3, no. 3, pp. 29–38, 2013.

[15] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, “A Comprehensive Survey: Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET,” *IEEE Access*, vol. 8, pp. 91028–91047, 2020.

[16] S. Sumithra and R. Vadivel, “An Overview of Various Trust Models for VANET Security Establishment,” *2018 9th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2018*, pp. 1–7, 2018.

[17] B. T. Rao, R. S. M. L. Patibandla, and V. L. Narayana, “Comparative Study on Security and Privacy Issues in VANETs,” *Cloud IoT-Based Veh. Ad Hoc Networks*, pp. 145–162, 2021.

[18] Z. A. Abdulkader, A. Abdullah, M. T. Abdullah, and Z. A. Zukarnain, “Vehicular Ad Hoc Networks and Security Issues : Survey,” vol. 11, no. 5, pp. 30–41, 2017.

[19] R. Mishra and M. T. Scholar, “International Journal of Innovative Research in Technology & Science Volume VI

Issue IV , July 2018 Attacks , Routing Protocols and Security challenges in VANET International Journal of Innovative Research in Technology & Science Volume VI Issue IV , July," vol. VI, no. Iv, 2018.

[20] Y. Al-raba and M. Al-refai, "Toward Secure Vehicular Ad Hoc Networks an Overview and Comparative Study," pp. 12–27, 2016.

[21] H. Hasbullah, I. A. Soomro, and J. L. Ab Manan, "Denial of service (DOS) attack and its possible solutions in VANET," *World Acad. Sci. Eng. Technol.*, vol. 65, no. 5, pp. 411–415, 2010.

[22] R. Kumar and M. Shanmugam, "A Detailed Case Study on VANET Security Requirements, Attacks and Challenges," *Adv. Model. Anal. B*, vol. 62, no. 2–4, pp. 48–52, 2019.

[23] A. N. Upadhyaya and J. Shah, "Attacks on VANET Security," *Int. J. Comput. Eng. Technol. (IJCET*, vol. 9, no. 1, pp. 8–19, 2018.

[24] T. Zaidi and S. Faisal, "An overview: Various attacks in VANET," *2018 4th Int. Conf. Comput. Commun. Autom. ICCCA 2018*, pp. 1–6, 2018.

[25] Z. Afzal and M. Kumar, "Security of Vehicular Ad-Hoc Networks (VANET): A survey," *J. Phys. Conf. Ser.*, vol. 1427, no. 1, pp. 0–9, 2020.

[26] M. R. Ghori, K. Z. Zamli, N. Quosthoni, M. Hisyam, and M. Montaser, "Vehicular Ad-hoc Network (VANET): Review," *2018 IEEE Int. Conf. Innov. Res. Dev.*, pp. 1–6, 2018.

[27] M. Arif, G. Wang, M. Zakirul Alam Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges," *Veh. Commun.*, vol. 19, p. 100179, 2019.

[28] S. Sharma and B. Kaushik, "A survey on internet of vehicles: Applications, security issues & solutions," *Veh. Commun.*, vol. 20, p. 100182, 2019.

[29] A. Quyoom, A. A. Mir, and D. A. Sarwar, "Security Attacks and Challenges of VANETs : A Literature Survey," *J. Multimed. Inf. Syst.*, vol. 7, no. 1, pp. 45–54, 2020.

[30] M. S. Sheikh and J. Liang, "A comprehensive survey on VANET security services in traffic management system," *Wirel. Commun. Mob. Comput.*, vol. 2019, 2019.

[31] M. Jain and R. Saxena, *VANET: Security attacks, solution and simulation*, vol. 712. Springer Singapore, 2018.

[32] P. Kohli, S. Painuly, P. Matta, and S. Sharma, "Future trends of security and privacy in next generation VANET," *Proc. 3rd Int. Conf. Intell. Sustain. Syst. ICISS 2020*, pp. 1372–1375, 2020.

[33] B. Mokhtar and M. Azab, "Survey on Security Issues in Vehicular Ad Hoc Networks," *Alexandria Eng. J.*, vol. 54, no. 4, pp. 1115–1126, 2015.