ISSN : 2455-9679
SJIF Impact Factor : 6.008

IJRTSM

INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

# "CHALLENGES SECURITY ISSUES OF VEHICULAR ADHOC NETWORKS (VANET): A REVIEW"

***Shilpa Dashare [1], Amit Shrivastava [2]***

*[1] M Tech Scholar, Department of Electronics and Communication Engineering, VNS Faculty of Engineering, Bhopal*

*[2] Associate Professor, Department of Electronics and Communication Engineering, VNS Faculty of Engineering, Bhopal*

## ABSTRACT

***In the past few years, Vehicular Adhoc Networks (VANETs), known as Vehicle-to-Vehicle and Vehicle-to-Roadside wireless communications, have received a huge amount of well-deserved attention in the literature. Indeed, because of their unmistakable societal impact that promises to revolutionize the way we drive, various car manufacturers, government agencies and standardization bodies have spawned national and international consortia devoted exclusively to VANET. Examples include the Car-2-Car Communication Consortium, the Vehicle Safety Communications Consortium, and Honda's Advanced Safety Vehicle Program among others. 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.***

***Key Words:*** *VANET architecture, Attacks, Challenges, DSRC, On- Board Unit, Inter vehicular Communication.*

## I. INTRODUCTION

The field of VANETs started gaining attention after 1980s and has, now-a-days, been an active field of research and development. Various types of challenges in vehicular communications have been identified and addressed. A large number of routing protocols have been proposed for VANET. [1]A routing protocol governs the way that two communication entities exchange information; it includes the procedure in establishing a route, decision in forwarding, and action in maintaining the route or recovering from routing failure. VANET routing protocols can be classified as topology- based and geographic (position-based). Topology-based routing protocols can further be divided into proactive (table- driven) and reactive (on-demand) routing. Enough research has already been carried out which includes the comparison of various routing protocols and their performance evaluation based on different mobility models. It will be interesting to evaluate the performance of one of the routing protocol by varying the number of mobile nodes. For this purpose, Ad Hoc on Demand Distance Vector (AODV) routing protocol is simulated because it has been observed that AODV is a better approach as compared to both Destination- Sequenced Distance Vector (DSDV) and Dynamic Source Routing (DSR).

The networks that interconnect vehicles on road are called Vehicular Ad hoc Networks (VANETs). A mobile ad hoc network (MANET) consists of mobile nodes that connect themselves in as decentralized, self-organizing manner and may also establish multi-hop routes. If mobile nodes are cars, this is called vehicular ad hoc network. A Vehicular

ISSN : 2455-9679
SJIF Impact Factor : 6.008

Ad Hoc Network or VANET is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters from each other to connect and, in turn, create a network with a wide range. [2] As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile network is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. VANETs come under the category of wireless ad-hoc network. In vehicular ad-hoc network, the node may be a vehicle or the road side units. They can communicate with each other by allowing the wireless connection up to a particular range. Inter- Vehicular Communications (IVC) also known as vehicular ad hoc networks (VANETs) have become very popular in recent years. A main goal of VANETs is to increase road safety by the use of wireless communications. To achieve these goals, vehicles act as sensors and inform each other about abnormal and potentially hazardous conditions like accident, traffic jams and glazes. Vehicular networks closely resemble ad hoc networks because of their rapidly changing topology. Therefore, VANETs require secure routing protocols. The constraints and optimizations are remarkably different. From the network perspective, security and scalability are two significant challenges. A formidable set of abuses and attacks become possible. Hence, the security of vehicular networks is indispensable. The growing importance of inter vehicular communications (IVC) has been recognized by the government, corporations, and the academic community.[3].

## II. VANET MODEL OVERVIEW

There are many entities involved in a VANET settlement and deployment. Although the vast majority of VANET nodes are vehicles, there are other entities that perform basic operations in these networks. Moreover, they can communicate with each other in many different ways. [4] Fig. 1 shows the typical VANET scheme.

VANET is a new technology that incorporates the potential of new wireless networks in automobiles. VANET is designed to provide mobile users with (i) continuous mobile connectivity, enabling them to connect with other users through home and office networks, and (ii) effective telephone communication between them. Between vehicles without having to access the built-in Internet infrastructure.

Therefore, VANET is also known as the vehicle interface (IVC). VANET devices (for example, in-car devices) interact with the car and act as a born bird and transmit messages through wireless networks. These tools provide drivers and passengers with the most up-to-date information on accidents, floods, showers, accidents, and all interruptions. By accessing such information at the right time, drivers can make the right decisions and avoid accidents. In the logic of self-organization, self-management, low bandwidth and communal radio show situations continue unchanged, VANET's function is usually like to operating knowledge of movable self-organizing network (MANET). However, major operational obstacle to VANET originates from tall haste or momentary mobility of mobile nodes (vehicles) sideways path (unlike MANET). This fact demonstrates that efficient design of routing protocols must improve the MANET building to effectively adapt to the rapid mobility of VANET nodes. This issue brings many study challenges to designing appropriate routing protocols. This article focuses on a major network problem: the VANET routing protocol. The primary purpose of delivering protocols is to reduce communication time when using a small network of resources. Many on-premises protocols are for MANET, and few protocols can be used directly with VANET. However, the simulation results show that the results of the VANET are affected by the following elements: fast moving vehicles, the transmission of powerful information, and one-way traffic at different speeds that differ from each other. 'The MANET. Therefore, identifying and managing VANETs is a difficult task. This fact presents a variety of research challenges in designing potential archives.

Warning carters around roads, traffic situations or connected conditions are critical to care and or vehicle flow directive. For this, appropriate and precise info is important. As shown in Figure 1, VANET can usually solve this problem [5]

ISSN : 2455-9679
SJIF Impact Factor : 6.008

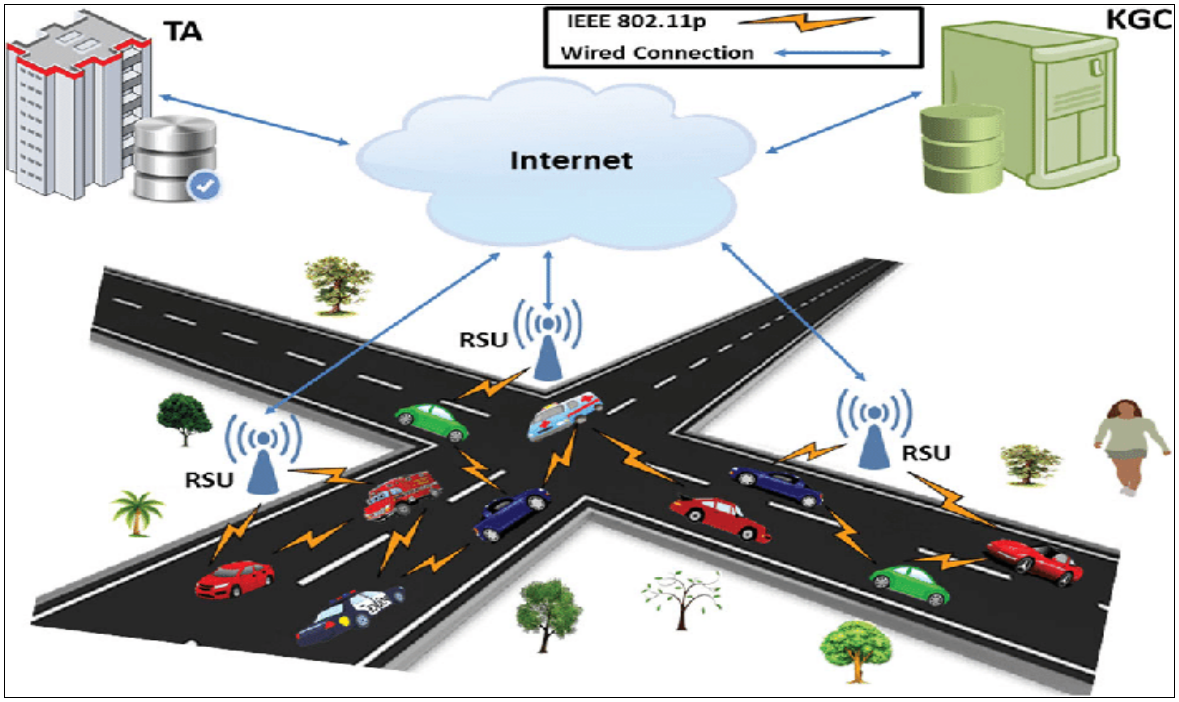


**Figure 1: VANET Model**

Three categories of network architecture of VANET are Pure cellular/ WLAN, Pure Ad hoc and hybrid as shown in Fig. 2. Entities in infrastructure environment can be permanently interconnected. It is mainly composed by those entities that manage the traffic or offer an external service. [6] From the VANET point of view, they are equipped with three different devices. Firstly, they are equipped with a communication unit (OBU, On- Board Unit) that enables Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I, I2V) communications. On the other hand, they have a set of sensors to measure their own status (e.g. fuel consumption) and its environment (e.g. slippery road, safety distance).

**System Architecture and Working of VANETs**

Vehicular Networks System consists of large number of nodes, approximately number of vehicles exceeding 750 million in the world today, these vehicles will require an authority to govern it, each vehicle can communicate with other vehicles using short radio signals DSRC (5.9 GHz), [7] for range can reach 1 KM, this communication is an Ad Hoc communication that means each connected node can move freely, no wires required, the routers used called Road Side Unit (RSU), the RSU works as a router between the vehicles on the road and connected to other network devices. [8]

Each vehicle has OBU (on board unit), this unit connects the vehicle with RSU via DSRC radios, and another device is TPD (Tamper Proof Device), this device holding the vehicle secrets, all the information about the vehicle like keys, driver‘s identity, trip details, speed, route etc. [9] The architecture of VANET implies that the communicating nodes in a VANET are either vehicles or base stations. Vehicles can be private or public. Base stations can belong to the government or to private service providers. the vehicles can communicate with each other and communicate with Road Side Units (RSU) interchangeably. [10]

ISSN : 2455-9679
SJIF Impact Factor : 6.008

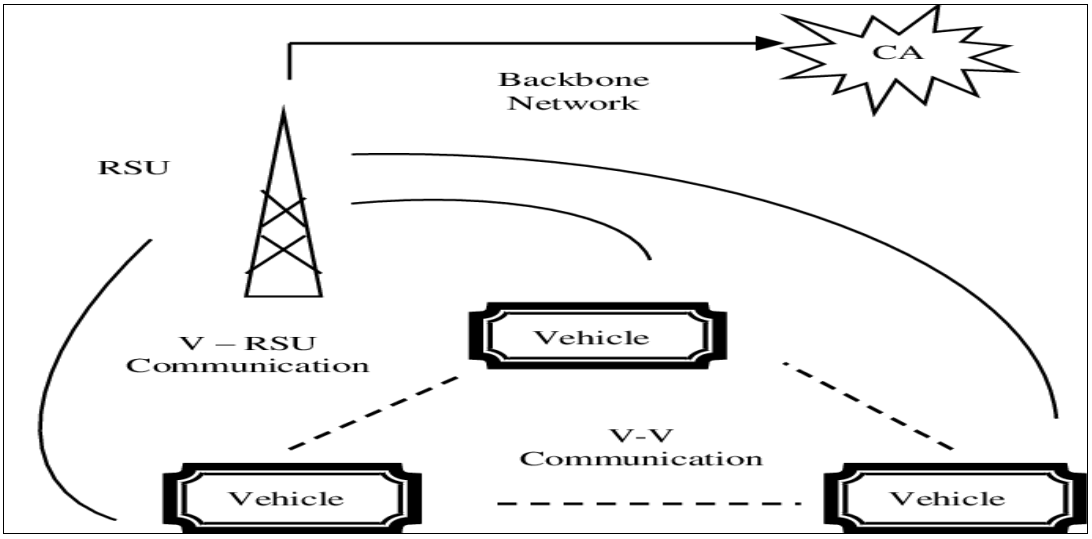


**Figure 3: Architecture of VANET**

**Challenges and Issues**

The security challenges which are faced in Pervasive Network are because of the weak connecting link between different nodes. As the nodes are distributed in the wireless medium, they can communicate by making proper utilization of signal propagation through air medium. So, it is easy to faucet. The resources are very much limited for the nodes present in the pervasive environment. Therefore, proficient schemes with less overhead are required and preferred. Due to its dynamic nature, there is a requirement of the self-organizing, self- healing algorithm for tolerance of the security attacks. [11] The attacks generally observed and often occurs in Pervasive Network may be broadly categorized into two categories: Passive and Active attacks. Eaves dropping fall into the category of passive attack. In this, the intruder captures the data while it is transmitted. On the other hand, in the active attack, the malicious node misleads other nodes to affect the communication. All types of ad-Hoc networks come under Pervasive Networks. In this research work, the Vehicular Ad hoc Network is taken to provide the security from location based attack. [12]

.

## III. 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 [13]. Furthermore, this kind of technologies can be used to create safe autonomous transport system in the smart city development process [14].

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 [15].

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 [16]. Also In the VANET, there are several issues, including QoS provisioning, high connection and bandwidth, and vehicle and individual privacy protection. 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,

ISSN : 2455-9679
SJIF Impact Factor : 6.008

extremely low latency, top security, and high mobility.

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 [17]. 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[18].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 [19]. 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 .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.

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].

## IV. ATTACKS ON THE PHYSICAL

**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 vehiclenode. Detecting such an attacker is tough since they do not respond in the existing network [23].

**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, aDoS will occur [26]. Finally, users do not have access to networks. DOS is not permitted on VANETs, whereimportant 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.

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

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].

**Distributed Denial of Service (DDOS) attack**

Multiple malicious vehicles launch attack on a legitimate vehicle from different locations and they may use different

ISSN : 2455-9679
SJIF Impact Factor : 6.008

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 largenumber 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].

**Illusion attack**

In this attack, the attacker tries to intentionally tamper with his vehicle's readings or traffic information, and 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, thiscan lead to an accident, a traffic jam, or a reduction in network performance via modifying network topology [24].

**Message tampering attack**

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

**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 sendsout repeated radio signals in the targeted region to disrupt connection between the station's nodes [27][25].

**Other Attacks**

**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 signalsin order to deceive the cars and lead them astray [26]. Position Faking is another name for this assault. In thissort 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].

**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 signalsin order to deceive the cars and lead them astray [26]. Position Faking is another name for this assault. In thissort 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].

**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].

**Black Hole attack**

Malicious nodes transmit a false routing information and pretend to have an optimum route for the destination in order

ISSN : 2455-9679
SJIF Impact Factor : 6.008

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 inwhich 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].

**Grey Hole attack**

The Gray Hole [31] assault is a version of the black hole attack that is based on the notion of selectiveforwarding. 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 attackthat'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 Wormhole attack

In a wormhole attack, legitimate automobiles receive data packets from hostile cars, which is a versionof 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 attacksare tunnels built between two malicious nodes [23].

**Sink Whole 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].

**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].

**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 datahave been used in previous publications. The writers in the first category utilize clustering methods to create residences for mobile users [27].

**Bogus information attack**

The VANETs make use of the data generated or sent by other vehicles or RSUs. However, there is achance 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].

**Spamming attack**

Spamming is a sort of attack that allows an attacker to transmit a large number of spam messages through a network in

ISSN : 2455-9679
SJIF Impact Factor : 6.008

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 difficultto control [28][25][29].

**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 trafficattacks or reptile attacks [27].

**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].

**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].

**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].

**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].

**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].

**density Disclosure attack**

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

**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

ISSN : 2455-9679
SJIF Impact Factor : 6.008

identities, the network poses a significant security risk becauseone 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 afalse 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 tolegitimate users, such as there is more traffic on a certain journey road, so choose a different route. The attackerwill construct an illusion and send a similar message to the same vehicle [23][25][29].

## V. 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 VIIssue 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.