JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 8, ISSUE 01, 2021

A Deep Survey on Types of Cyber Attacks in VANET

[1]Gayathri M, [2]C.Gomathy

[1,2]Electronics and Communication Engineering College of Engineernig and Technology SRM Institute of Science and Technology,Vadapalani No:01,Jawaharlal Nehru Road,Vadapalani Tamilnadu,India

gm0717@srmist.edu.in vp.academics.vdp@srmist.edu.in

ABSTRACT

Vehicular Ad hoc Network (VANET) are used to provide inter vehicular communication. VANET uses wireless mode for communication between vehicles so there is a lot of possibilities to get interrupted or attacked by hackers since each message which are transmitted are broadcasted messages in VANET communication. Therefore, a secure and confidential transmission of messages plays a major challenge in VANET. This paper focuses on VANET Architecture, Security mechanism and various types of attacks and challenges faced in communication. By using the proposed survey, a detailed explanation of various attacks and security challenges are discussed in this paper.

Keywords— VANET, WAVE, Security system, On board sensors, DSRC

1.INTRODUCTION

VANETs are subset of Mobile Ad hoc network. VANETs communication are deployed on roads. VANETs are used in very wide area of application. VANETs provide internet facilities to each other vehicles in order to obtain Real time traffic condition, accidents ahead, Emergency electronic brake light, pre-crash warning and many safety applications. VANETs provide a path to Intelligent Transportation system (ITS). VANETs uses wireless mode of communication, hence it is easy to connect a greater number of devices based on its availability. The major disadvantage of wireless mode of communication is that they get easily hacked or attacked. Each and every message which are sent are broadcasted messages and hence they are prone to get attacked easily. Therefore, a secure communication mechanism is needed to transmit all information without any loss in packet delivery of data. A secure communication and routing play a significance role in VANET communication. The paper is divided into various section; In section 2 The architecture of VANET is discussed in brief. Section 3 focuses on the different characteristics of VANET. Section 4 concentrates on Security requirements of VANET. In Section 5 we discuss about the various attacks in VANET communication. Section 6 classifies the different survey paper based on its objective and limitation in security attacks. In Section 7 we conclude our paper.

2.THE COMMUNICATION TOPOLOGY OF VANET

The architecture of VANET can be classified into three communication types as inter vehicle communication(V2V), vehicle which communicates with Infrastructure(V2I) and hybrid architectures [1]. These architectures are divided based on its communication platform.

2.1 Communication Between vehicles(V2V):

V2V communication allows the communication directly between vehicles without depending on any fixed infrastructure. Fig1 shows the basic architecture of V2V communication. This communication can be used for emergency purpose and safety application.

ISSN- 2394-5125 VOL 8, ISSUE 01, 2021

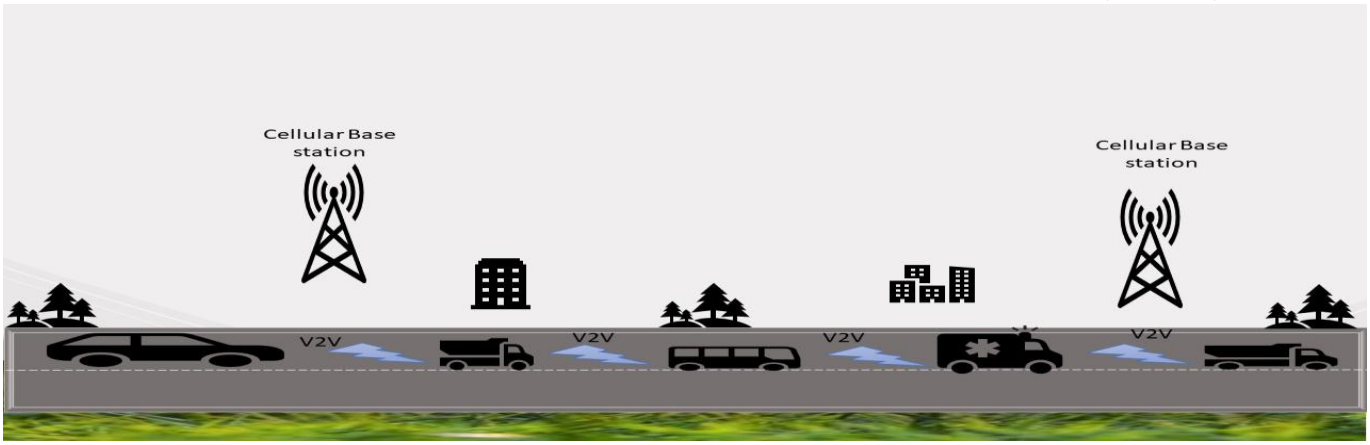


Fig.1. vehicular communication

2.2 Communication between Vehicle and Infrastructure

V2I is used for the communication between Roadside unit and other infrastructure available in path of the vehicles. Fig 2 shows the basic architecture of V2I.This type of communication is normally used to gather data and information needed for the users.

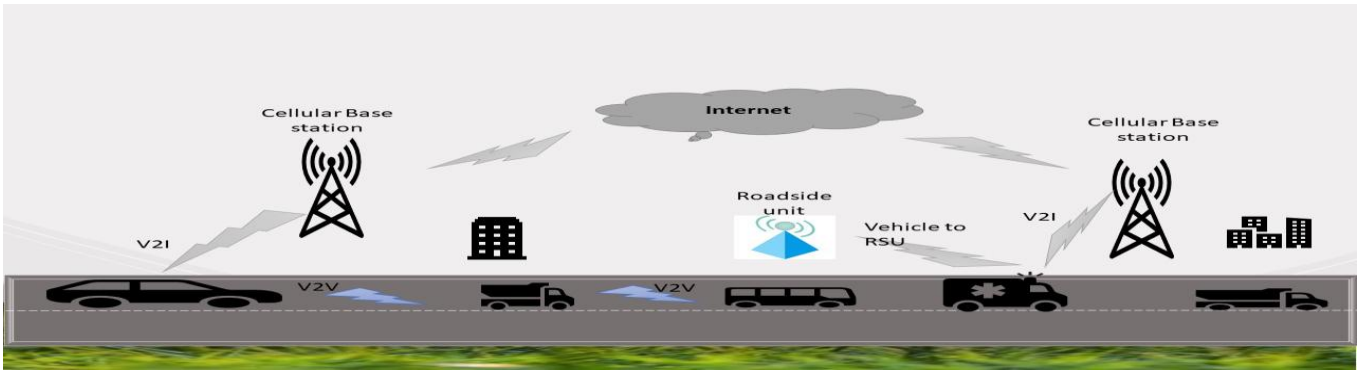


Fig.2. Communication between Vehicle and Infrastructure

2.3 Hybrid Architecture

As the name implies hybrid architecture uses both V2V and V2I communication. In this communication all vehicles, road side unit, Infrastructure units will be involved in communication. Fig 3 explains the hybrid architecture. This mode of communication uses long and multihop mode for communication.

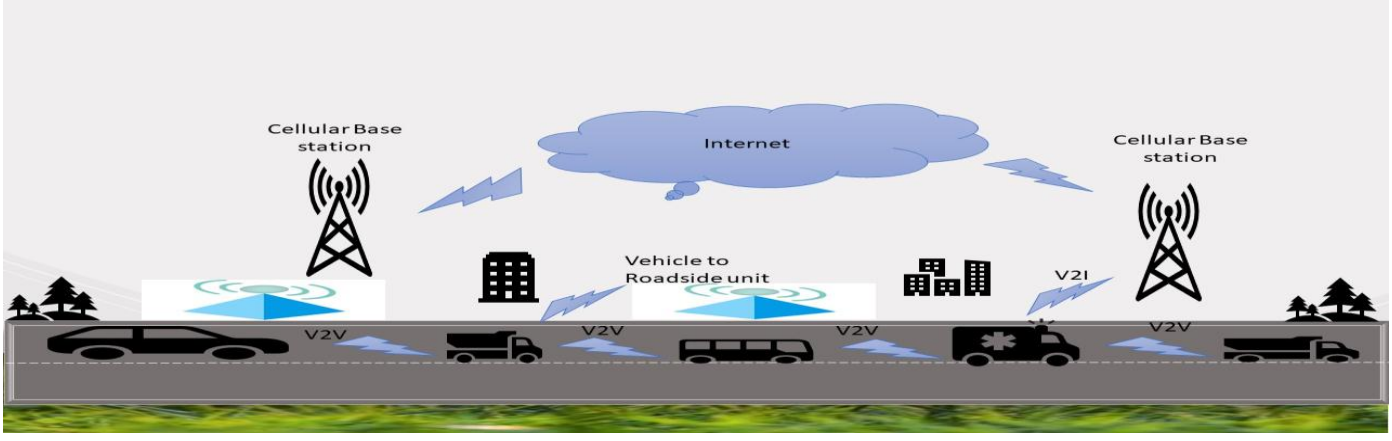


Fig.3. Hybrid Architecture

ISSN- 2394-5125 VOL 8, ISSUE 01, 2021

2.4 The Overall Architecture of VANET

VANET uses Road Side unit (RSU), On Board units (OBU) and Trusted Authorities (TA) as a tool for communication. Road side units are deployed across the road path, in order to provide internet connectivity to the VANET users [2]. On board units are placed inside the vehicles which form mobile ad hoc network to provide communication between the vehicles in a distributed manner. Since vehicle have a high mobility and dynamic topology the distributed network is used for communication. In VANET Wireless Access in Vehicular Environment (WAVE) protocol is used which is based on the IEEE 802.11p standard. This protocol uses DSRC communication among vehicles, Dedicated Short Range Communication [3]. Trusted Authorities (TA) are used for managing the whole VANET system [4]. These trusted authorities play a vital role to prevent the malicious node entering into the communication. Trusted authorities are used for authenticating the messages which are being transmitted in between vehicles. This authentication uses registered vehicle identity and user identity to maintain trust between vehicles. Fig 4 shows the overall architecture of VANET.

3.MAJOR CHARACTERISTICS OF VANET

VANETs are ad hoc in nature, uses dynamic topology of a network, high mobility because of vehicles movement.
VANETs have very different characteristics when compared to MANET.

- ❖ High Mobility: The vehicles are called as node which usually move at a very high speed. Hence VANETs have a nature of high mobility.

- ❖ Network Topology: Since each and every node have high mobility based on their movement network topology changes which results in distributed network for communication.

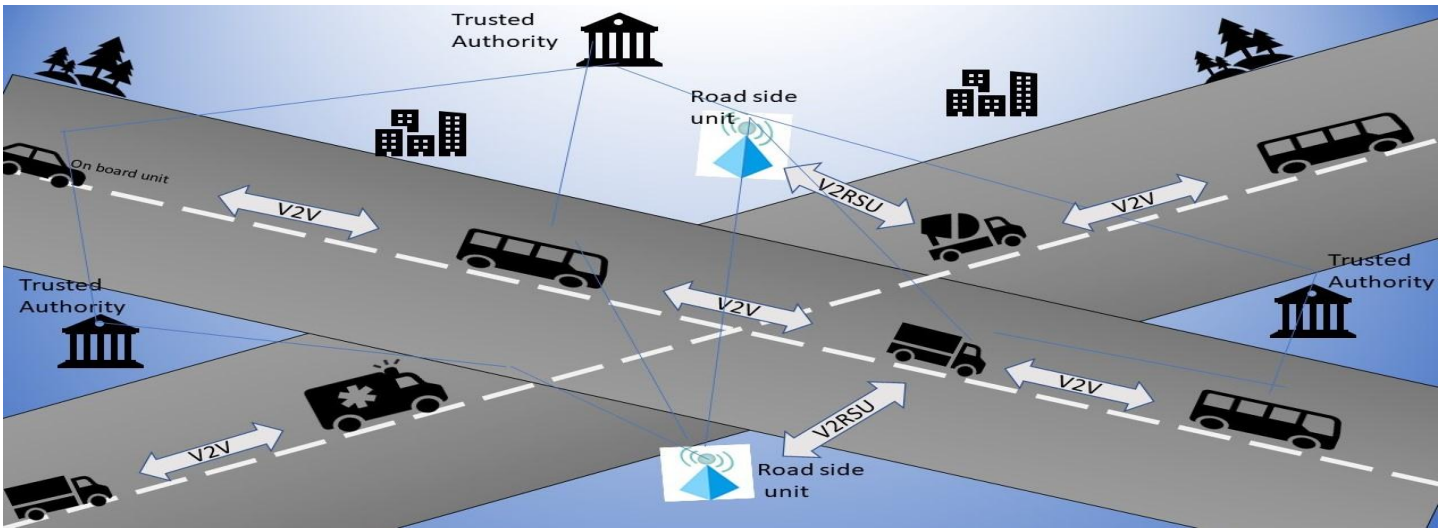


Fig.4. The overall Architecture of VANET

- ❖ Exchange of Information: There are lot of information change in VANET based on their need in ad hoc manner.

- ❖ Geographically unbounded network size**:** VANET communication can be implemented in all geographical range such as cities and countries.

ISSN- 2394-5125 VOL 8, ISSUE 01, 2021

- Access of Infrastructure**:** Due to mobility of vehicles the it is somewhat difficult to maintain the connectivity. Therefore, communication infrastructure such as roadside unit, access point and hotspot play a vital role in reduce the delay of connectivity.

4.REQUIREMENT OF SECURITY SERVICES IN VANET

The security and privacy mechanism are classified into following types

Availability**:** Most of the attackers try to attack the nodes based on the availability of resources on real time basis. High care should be taken to secure the availability resources.[5]
Authentication: Data which are transferred in VANET communication should be authenticated to ensure that each and every and every node receives a secure message.
Confidentiality: It is used to prevent the secret listening of attackers to track the confidential data without the knowledge of users [6].
Data Integrity**:** It should be ensured that the data which are transferred from a node reaches to the correct node.
Non-Repudiation**:** The messages which are transmitted in vehicular communication should be very secure. The attacker may also act as a genuine node and send wrong information to the user. Hence Non repudiation is used to identify the sender with a proof as a digital signature

5.CLASSIFICATION OF VARIOUS VANET ATTACKS.

There are various kind of attacks which are involved in VANET Communication. These attackers try to jam the communication, change the format of communication, modify the message which are sent, delay the services and mislead the whole VANET communication. They are classified based on security mechanism [4]. Fig 5 shows the block diagram for security mechanism in VANET.

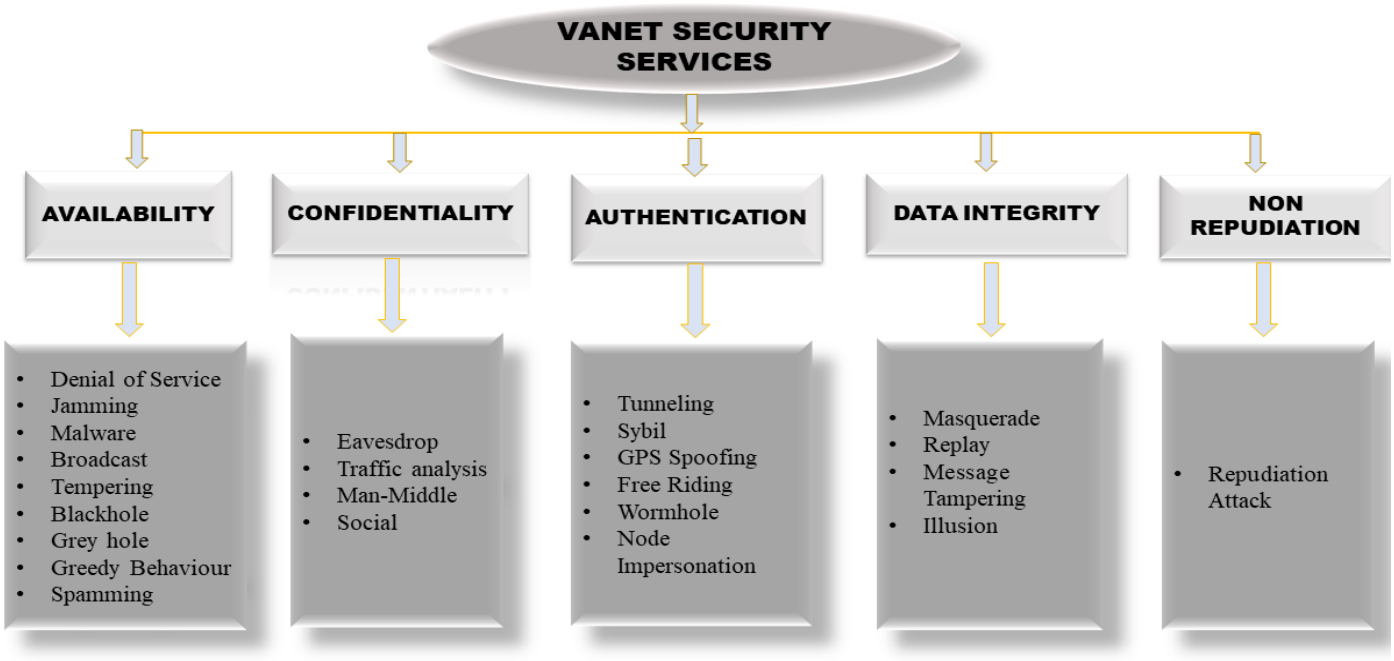


Fig.5. Block diagram of security mechanism

5.1 Attacks on Availability

a) Denial of Service Attack:

The hacker denies the communication between vehicles in Denial-of-Service attack. It tries to prevent the node to access the network [7]. Attacker tries to deny all the services which are provided to the node users causing a delay or packet drop in a communication.Fig.6. shows Denial of Service attack.

ISSN- 2394-5125 VOL 8, ISSUE 01, 2021

b) Malware Attack:

The attacker injects virus or malware in the communication channel of VANET [8]. These viruses destroy the components of on-board unit and Road side unit which causes disturbance in Communication between nodes.Fig.7. shows malware attack in VANET.

c) Jamming Attack:

The radio signals are intentionally transmitted to disturb the communication by decreasing signal to noise ratio [8].

The jamming signals are classified into four types based on its behavior.

Constant Jamming*:* They transmit the data at a constant rate without checking weather channel is idle or not.

Deceptive Jamming: The packets are transmitted randomly to without giving time gap between each transmission which will cause a jamming of communication due to overhead.

Random jamming: They conserve energy by operating both in jam and sleep intervals. In sleep interval it remains silent when traffic on network. In jam interval it acts as a persistent jammer [10].

Reactive Jamming: This starts to function when it senses a transmission in a channel otherwise it remains dormant when channel is idle. It tries to drop a packet which is kept for transmission [10]

d)Broadcast Tampering

Each and every message transmitted in VANET is Broadcasted message. The attacker tries to modify the message being carried out in a communication channel, discard some packets and drop some packet.

e) Black hole attack

The attack is carried out by malicious node in VANET's Routing protocol. They advertise themselves as genuine node and pass the information that they have least hop path to reach to required node and divert a trusted user [12].

f) Grey hole attack

It is difficult to identify genuine node and malicious node in grey hole attack. In this attack only partial data is sent and partial data are dropped without the knowledge of VANET user.

h) Spamming

In this type of attack spam or unwanted messages which are not necessary is sent by attackers. This spam messages will be in the form of ad messages which occupies more bandwidth causing delay in communication.

i)Greedy behavior attack

Greedy behavior attack detection is difficult in VANET because of high dynamic mobility of nodes [13]. This behavior attack is common "DoS" attack. It normally attacks the MAC layer operation. Attacker keeps on denying all the services to VANET user and try to use all the services for own use

ISSN- 2394-5125 VOL 8, ISSUE 01, 2021

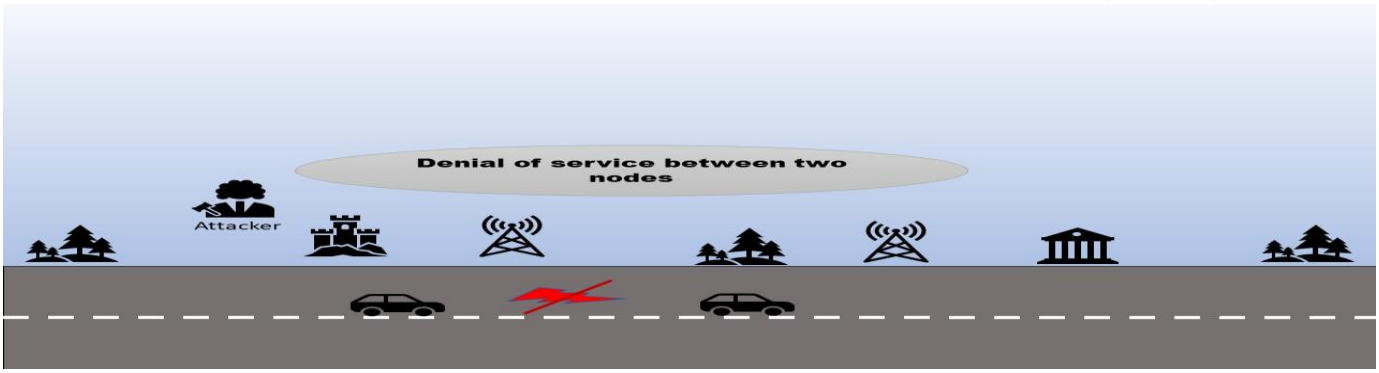


Fig.6. Denial of Service attack

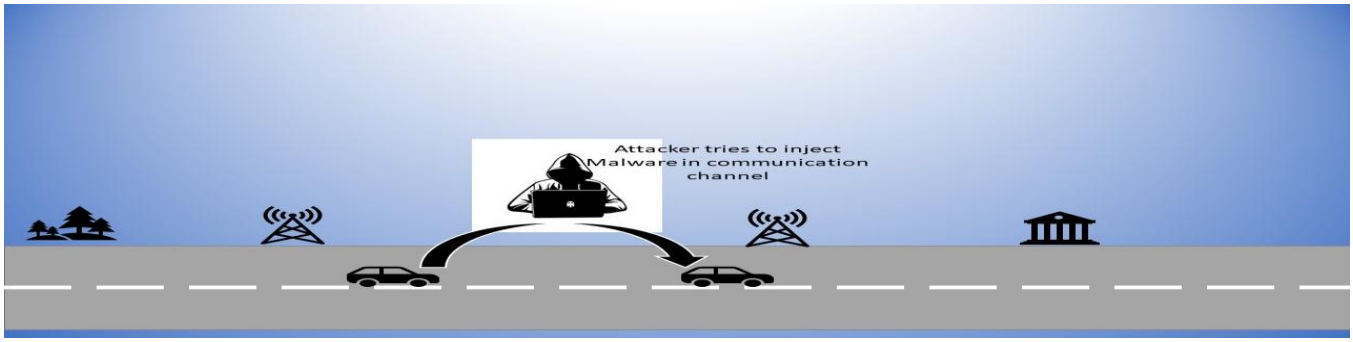


Fig.7. Malware attack

5.2 Attacks on Authentication

a) Tunneling attack

The attacker tries to do the attack the node at any moment of time [14]. The attacker connects two distant nodes using an extra communication link Tunnel. Two distant nodes assume that they are neighbor and send data. Tunnel attacker will secretly operate on data which are transmitted in communication link.Fig.7 shows tunnel attack.

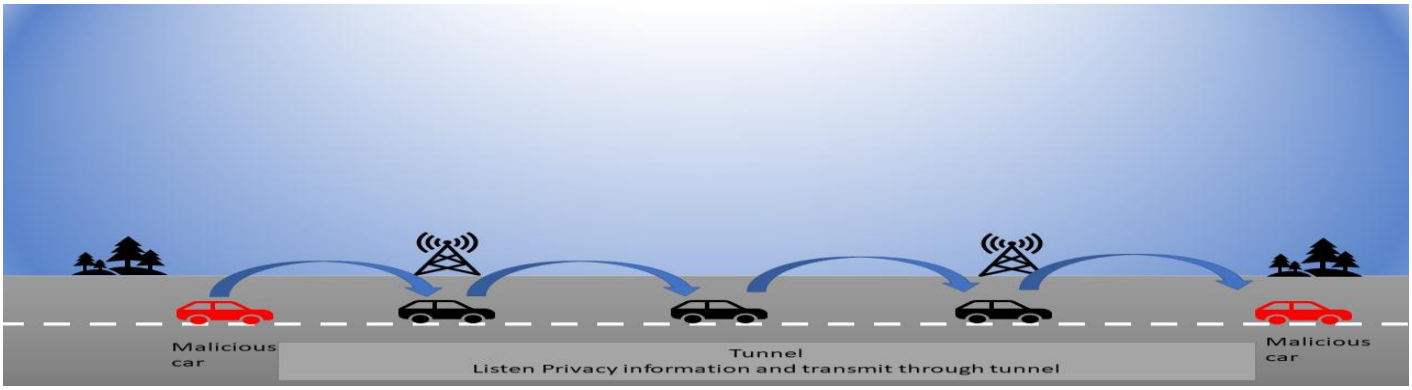


Fig.8. Tunnel attack

b) Sybil Attack

In this VANET Attack, the hacker or attackers acquires multiple fake identities [15]. These multiple identities keep on sending false messages to the node which creates confusion among the vehicles in the communication track.

c)Free Riding Attack

A node tries to utilize the service of the other nodes in the network but node does not return to network. It tries to tunnel the TCP header, that causes a false transmission of communication.

d)GPS Spoofing

ISSN- 2394-5125 VOL 8, ISSUE 01, 2021

GPS signals are vulnerable to in band interferences because of weak broadcasted signals in VANET [16]. Hence it becomes very easy to jam or spoof GPS in a certain kilometer range. The attacker tries to mislead the VANET user's location and divert him to his way or stop him from his work by spoofing GPS.

e) Node Impersonation

Impersonation means the act of pretending to be another person to involve in fraudulent activities [17]. Attacker easily masquerades its identity and act as a genuine node. This type of attack mainly happens in accident zone.

f) Replay Attack

Replay attack can be even termed as playback attack. A valid or true message is purposely transmitted or delay is produced to cause hazardous effect in VANET.

g) Message Tampering

In VANET all the messages are transmitted through wireless medium, hence it is very easy for attackers to hack the communication. In message Tampering the attacker changes the messages or alter the messages which are being transmitted in VANET communication.

5.3Attacks on Confidentiality

a) Traffic Analysis Attack

The hacker aims to get all imperative information by keenly observing traffic in a network communication [18]. The attacker analyses the frequency of communication signal transmission and tries to extract all the useful information needed and then indulges in malicious attack.

b) Eavesdropping

Eavesdropping is to secretly listen to conversation between to nodes [19].The attacker secretly uses these fading effects and secretly listen the conversation and give the information to another non registered users. Fig 9 discusses about Eavesdropping attack.

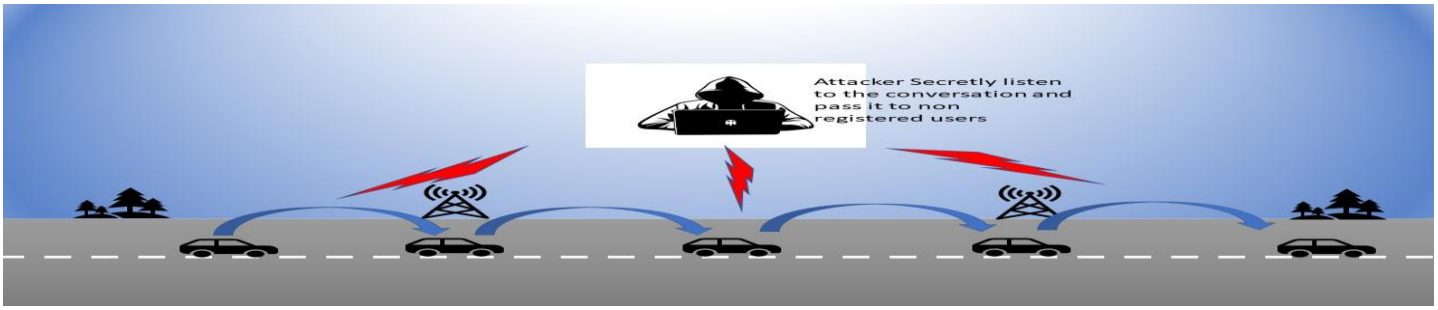


Fig.9. Eavesdropping

c)Man in the Middle attack

This attack is considered as a major attack in security mechanism. In this attacker try to hack the data flow in end-to-end communication. Man in the middle attack is based on several parameter sech as location of attacker, mode of communication and node impersonation [20]. Fig.10 shows Man in the middle attack.

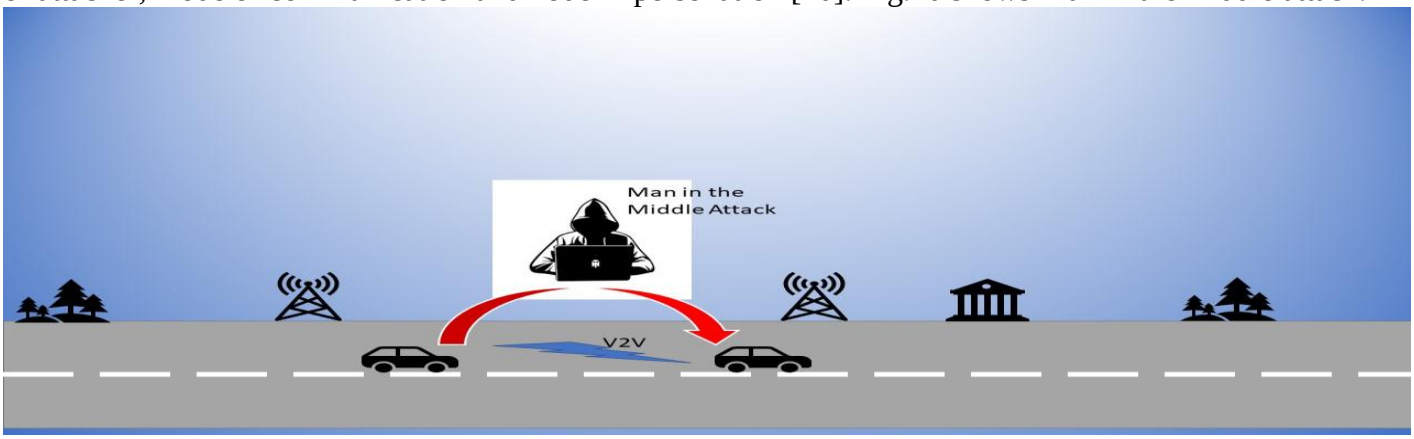


Fig.10 Man in the Middle attack

d)Social Attack

The attacker intentionally steals the information from users by sending immoral or spam messages. These attacks can be prevented by spoofed e-mail detection by spam filtering, Fake social networking detection, detection of hacking by keeping password secrets without sharing to unknown users and by avoiding downloading unwanted messages in the form of viruses [21].

5.4 Attacks on Data Integrity

a) Masquerading Attack

In this attack one entity pretends to be another entity. It involves in active attacks. IN this attacker creates a false identity to perform a malicious access in personal computing device through acceptable access. The output which are gained from various analysis such as window data, File access data, command line data and authentication data are analyzed in multiple layers to detect masquerading attack [22].

b) Illusion Attack

The attacker creates an illusion of happenings in road to the user. This attack can cause car accident, heavy traffic, they can even divert the user from his route by providing illusion to neighbor node. plausibility validation network (PVN) model, introduced to resolve this problem [23]. Fig.11 shows the illusion attack caused by attacker in VANET.

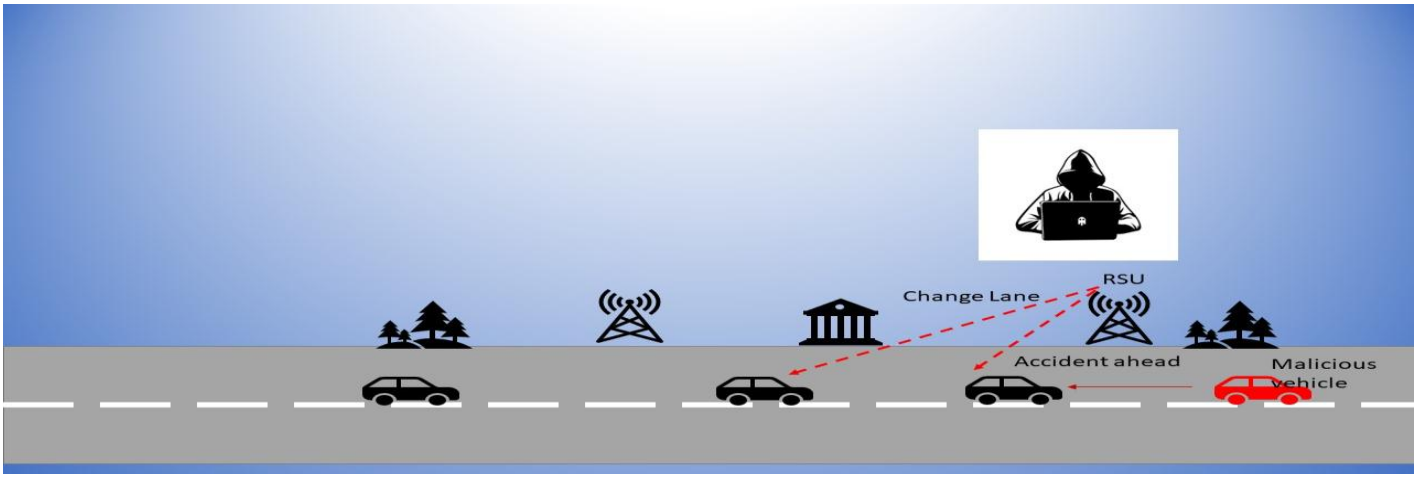


Fig.11 Illusion Attack

)Message Tampering Attack

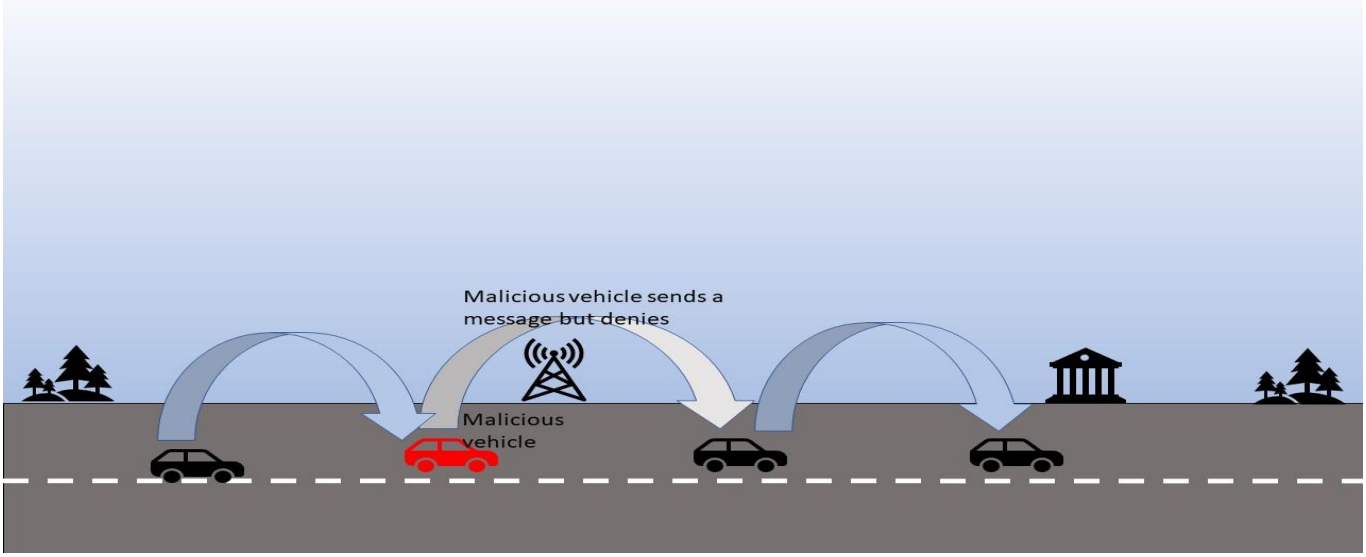
The messages which are transferred from one node to other, one node to infrastructure is exchanged, altered or dropped to provide false information to the user.

5.5 Attacks on Non repudiation

a) Attack on repudiation:

Authentication is very important in wireless mode of communication to ensure that only registered users are sending and receiving messages rather than an attacker. Each and every message should be digitally signed to ensure secure communication. This attack arises when he/she denies the activity of communicating between devices. A novel Authentication framework with Conditional Privacy-preservation and Non-repudiation (ACPN) for VANETs is produced to reduce repudiation attack [24]. public-key cryptography, existing ID-based signature (IBS) scheme for

the authentication can be used to reduce attacks on repudiation. Fig. 12 shows attacks on repudiation.



6.SURVEY OF EXISTING DETECTION SCHEME FOR VARIOUS ATTACKS

Year	Author and paper	Objective	Algorithm	Limitation
2019	Sherazi HHR, Iqbal R, Ahmad F, Khan ZA, Chaudary MH. Ddos attack detection: A key enabler for sustainable communication in internet of vehicles. Sustain Comput: Inform Syst 2019	The buffer usage was decreased and this paper detects DDOS attack	Artificial Intelligence, Machine learning and fuzzy logic	Lot of computation is needed
2019	R. Kumar, X. Zhang, W. Wang, R. U. Khan, J. Kumar, and A. Sharif, ‘‘A multimodal malware detection technique for Android IoT devices using various features,’’ IEEE Access, vol. 7, pp. 64411–64430, 2019.	Objective of this paper is to detect Various malware attacks.	Machine learning, Block chain technology	Dynamic malware detection is not proposed.
2019	Hymlin Rose, S. G., & Jayasree, T. (2019). Detection of jamming attack using timestamp for wsn. Ad Hoc Networks, 101874.	To detect Jamming attack in wireless sensor network	Clustering approach and time stamp method	The total jamming zone is bypassed.
2020	Cherkaoui B, Beni-hssane A, Erritali M. Variable control chart for detecting black hole attack in vehicular ad-hoc networks. J Ambient Intell Humaniz Comput 2020;1–10.	Easy Implementation	Variable control chart	More testing is required.

Fig 12 Attacks on repudiation

2007	Chen L, Almoubayed KA, Leneutre J. Detection and prevention of greedy behavior in ad hoc networks. In: International conference on risks and security of internet and systems (CRISIS 2007). 2007	The selfishness resistant MAC protocol for ad hoc networks problem is proposed	Distributed Coordination function	Hostile Environment should also be concentrated.
2020	Lim K, Islam T, Kim H, Joung J. A sybil attack detection scheme based on ADAS sensors for vehicular networks. In: 2020 IEEE 17th annual consumer communications & networking conference (CCNC). IEEE; 2020	ADAS (Advanced Driving Assistant System) which are installed on a vehicle to detect sybil attack.	Deep Learning	Evaluation is not enough
2019	Liang C. et al. (2019) Detection of GPS Spoofing Attack on Unmanned Aerial Vehicle System. In: Chen X., Huang X., Zhang J. (eds) Machine Learning for Cyber Security. ML4CS 2019. Lecture Notes in Computer Science, vol 11806. Springer, Cham.	prior configuration method is minimal and uses real time traffic to detect GPS Spoofing	Information fusion based on the GPS receiver and inertial measurement unit (IMU) is used	It is somewhat difficult to track and identify threats in real time

7.CONCLUSION

This paper discusses in brief bout Vehicular Ad hoc network (VANET). Since VANET operates in the mode of wireless communication there are lot of possibilities that communication which are done in wireless medium gets affected easily by threats. Various Attackers try to attack the communication and try to get information to interrupt the communication or to discard the packets. By doing so attackers try to reduce the performance of VANET, steal information to follow a genuine user, divert a VANET user from his path to get traffic less path, intentionally cause car accident by providing wrong information. This paper focuses on different types a security attacks which are caused by various unknown attackers in VANETs and provides a survey of different attack detection system

REFERENCES

[1] Felipe Domingos da Cunha, Leandro Villas, Azzedine Boukerche, Guilherme Maia, Aline Carneiro Viana, et al. " Data Communication in VANETs: Survey, Applications and Challenges". Ad Hoc Networks, Elsevier, 2016

[2] H. Hasrouny, A. E. Samhat, C. Ba Cherkaoui B, Beni-hssane A, Erritali M. Variable control chart for detecting black hole attack in vehicular ad-hoc networks. J Ambient Intell Humaniz Comput 2020;1–10.ssil, and A. Laouiti, "VANet security challenges and solutions: a survey," Vehicular Communications, vol. 7, pp. 7–20, 2017.

[3] Shrestha, R., Bajracharya, R., & Nam, S. Y. "Challenges of Future VANET and Cloud-Based Approaches". Wireless Communications and Mobile Computing, 2018.

[4] Muhammed Sameer Sheik,Jun Liang, "A Comprehensive Survey on VANET Security services in Traffic management Systems."Wireless communication and mobile computing,vol.2019

[5] Tanwar, S., Vora, J., Tyagi, S., Kumar, N., & Obaidat, M. S. " A systematic review on security issues in vehicular ad hoc network. Security and Privacy"2018.

[6] Malhi, A. K., Batra, S., & Pannu, H. S., "Security of Vehicular Ad-hoc Networks: *A* Comprehensive Survey". Computers & Security,2019

[7] Adil Mudasir Malla and Ravi Kant Sahu, Article: "Security Attacks with an Effective Solution for DOS Attacks in VANET". International Journal of Computer Applications 66(22):45-49, March 2013.

[8] Ghori, M. R., Zamli, K. Z., Quosthoni, N., Hisyam, M., & Montaser, M. "Vehicular ad-hoc network (VANET): Review". 2018 IEEE International Conference on Innovative Research and Development (ICIRD).

[9] S. Malebary and W. Xu, "A survey on jamming in vanet," International Journal of Scientific Research and Innovative technology, vol. 2, no. 1, 2015

[10] Sufyan, N., Sagib, N.A., & Zia, M. Detection of jamming attacks in 802.11b wireless networks. *J* Wireless Com Network 2013, 208 (2013).

ISSN– 2394–5125 VOL 8, ISSUE 01, 2021

[11] Azees, M ; Vijayakumar, P ; Deborah, L J, "Comprehensive survey on security services in vehicular ad-hoc networks." IET Intell. Transp. Syst. 2016, *10*, 379–388.

[12] Vimal Bibhu Kumar Roshan Kumar Balwant Singh Dhirendra Kumar Singh,"Performance Analysis of Black Hole Attack in Vanet", IJCNIS, vol.4, no.11, pp.47-54, 2012.

[13] Meiri, M. N., & Ben-Othman, J. (2017). GDVAN: A New Greedy Behavior Attack Detection Algorithm for VANETs. IEEE Transactions on Mobile Computing, 16(3), 759–771. doi:10.1109/tmc.2016.2577035

[14] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges." Telecommunication Systems, vol. 50, no. 4, pp. 217–241, 2012.

[15] Kumar Karn, G., & Prakash Gupta, G. (2016). "A Survey on VANETs Security Attacks and Sybil Attack Detection." International Journal of Sensors Wireless Communications and Control.

[16] A. Boudhir, M. Benahmed, A. Ghadi and M. Bouhorma, "Vehicular navigation spoofing detection based on V2I calibration," 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt), Tangier, Morocco, 2016, pp. 847-849, doi: 10.1109/CIST.2016.7805006.

[17] R. S. Raghav , R. Danu, "Detection of Node Impersonation for Emergency Vehicles in VANET" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 12, December - 2013 IJERT ISSN: 2278-0181

[18] Fu, Xinwen (2005). "On traffic analysis attacks and countermeasures". Doctoral dissertation , Texas A&M University. Texas A&M University.

[19] Xuran Li, Hao Wang, Hong-Ning Dai, "An Analytical Study on Eavesdropping Attacks in Wireless Nets of Things" Hindawi Publishing Corporation Mobile Information Systems Volume 2016.

[20] M. Conti, N. Dragoni and V. Lesyk, "A Survey of Man In The Middle Attacks," *in* IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2027-2051, third quarter 2016.

[21] S. Gupta, A. Singhal and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2016, pp. 537-540, doi: 10.1109/CCAA.2016.7813778.

[22] Salioogbineiad, H., Bhukya, W.N. (2012). "Layered Security Architecture for Masquerade Attack Detection." Lecture Notes in Computer Science, vol 7371. Springer, Berlin, Heidelberg.

[23] N. Lo and H. Tsai, "Illusion Attack on VANET Applications - A Message Plausibility Problem," 2007 IEEE Globecom Workshops, Washington, DC, USA, 2007, pp. 1-8, doi: 10.1109/GLOCOMW.2007.4437823.

[24] J. Li, H. Lu and M. Guizani, "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs," in IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 4, pp. 938-948, April 2015, doi: 10.1109/TPDS.2014.2308215.

[25] Sherazi HHR, Iqbal R, Ahmad F, Khan ZA, Chaudary MH. Ddos attack detection: A key enabler for sustainable communication in internet of vehicles. Sustain Comput: Inform Syst 2019

[26] R. Kumar, X. Zhang, W. Wang, R. U. Khan, J. Kumar, and A. Sharif, ''A multimodal malware detection technique for Android IoT devices using various features,'' IEEE Access, vol. 7, pp. 64411–64430, 2019.

[27] Hymlin Rose, S. G., & Jayasree, T. (2019). Detection of jamming attack using timestamp for wsn. Ad Hoc Networks, 101874.

[28] Cherkaoui B, Beni-hssane A, Erritali M. Variable control chart for detecting black hole attack in vehicular ad-hoc networks. J Ambient Intell Humaniz Comput 2020;1–10.

[29] Chen L, Almoubayed KA, Leneutre J. Detection and prevention of greedy behavior in ad hoc networks. In: International conference on risks and security of internet and systems (CRISIS 2007). 2007

[30] Lim K, Islam T, Kim H, Joung J. A sybil attack detection scheme based on ADAS sensors for vehicular networks. In: 2020 IEEE 17th annual consumer communications & networking conference (CCNC). IEEE; 2020. p. 1–5.

[31] Liang G, et al. (2019) Detection of GPS Spoofing Attack on Unmanned Aerial Vehicle System. In: Chen X., Huang X., Zhang J. (eds) Machine Learning for Cyber Security. ML4CS 2019. Lecture Notes in Computer Science, vol 11806. Springer, Cham. https://doi.org/10.1007/978-3-030-30619-9_10