IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, October 2023

A Study on Different Attacks in VANET

Sonam Kumari[1], Dr. Harsh Lohiya[2], Dr Rajendra Singh Kushwah[3]
Research Scholar, Department of CSE[1]
Associate Professor, Department of CSE[2], SSSUTMS, Sehore, Madhya Pradesh, India
Professor, Department of CSE[3]
Sri Satya Sai University of Technology and Medical Sciences, Sehore, Madhya Pradesh, India

Abstract: *In the modern generation of technological challenges in information transmission, there's a massive want to become aware of the essential components and tools that are used in moving and receiving information for vehicular gadgets. Vehicular ad-hoc community (VANET) has become one of the most famous areas of studies in past decades. cars are connected in an ad- hoc manner in a wi-fi surroundings known as VANET that is a subpart of MANET. due to common alternate in topological shape, it's miles very hard to make a VANET relaxed. in this research article, it is being located that many safety demanding situations are there wherein studies ought to step-up forward for making VANET extra comfortable. A crucial evaluation is mentioned extensively with recognize to VANET components, security issues and demanding situations, attacks and its solutions.*

Keywords: Sybil, Ad-hoc, VANET, Black Hole, Wormhole

I. INTRODUCTION

With the each day improvement in wi-fi wireless topology and wi-fi of internet in our each day stay exposed the want of environment, the only who ensure the safety of human lives and provides guarantee of relaxed records transmission, this result in the improvement of latest sort of wi-fi community referred to as Vehicular advert-hoc community (VANET), it ensures vehicular communication. The number one goal of VANET is to increase a community between automobiles and look after the communication between them irrespective of the central base station. VANET is a part of cellular ad-hoc community (MANET), VANET acquire a whole lot of interest because of the offerings proved by way of it particularly sharing records associated with site visitors wireless, avenue protection data, and different information (document, audio, video, etc.) the use of accidental internet connectivity. one of the important software of VANET is inside the subject of a scientific emergency where there is a want to pass the data irrespective of infrastructure. According to the data provided by Ministry of Road Transport & Highways, Government of India, the estimated number of death is about 1,50,785 people and hundreds of thousand would have suffered traumatic injury across India only in the year 2016[1].

It is being ascertained that if the driver gets some warning before half a second of the accident, then an accident can be avoidable [2]. VANET comes into light as a solution to avoid these mishaps by proving some prior information about the vehicles near to it.

The primary objective of VANET is to develop a reliable, efficient and secure routing protocol, which perform robustly in a highly dynamic environment even VANET is under some attack.

II. RELATED WORK

VANET security comes into focus in the middle of 2000 and it gets bloomed in 2007. In recent years, numerous research was proposed in the literature for presenting a better solution to detect and analyze different network attacks. We will address some of the research paper over here-

J. P. Hubaux et al. [3] describes how VANET help in reducing road accidents, he also describes the components required in smart vehicle for efficient data transmission. For the authentication of smart vehicles, authors suggest using electronic license plates and for the location verification, they propose two methods, Tamper Proof GPS and second one verifiable multi literation.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, October 2023

J. T. Issac et al. [4] perform analysis on Security attacks and solutions for vehicular ad hoc networks. Author discuss may attack on the network, which were reported before 2010. Authoe proposed solution to prevent security attack and vulnerability.

M. Burmester et al. [5] perform analysis on Strengthening Privacy Protection in VANETs. They proposed a cryptographic mechanism to establish a balance between privacy and accountability in VANET. They predict this approach to be hybrid and proposed symmetric and public key operation for both of the cases authentication and encryption.

J. T. Isaac et al.[20] broadly discussed various security threats and attacks. Author also discussed security challenges with respect various attacks on VANET and analyze security solutions, which has already proposed previously.

H. Lu et al.[18] propose an authentic framework for securing the VANET. Authors propose an ID-based signature scheme, which used to authenticate nodes uniquely in the network. As all nodes have, unique id's so it is easier to track any malicious node on the network.

C. Kerlof et al. [13] have described routing security in an Ad-hoc network and peer-to-peer network. Author perform attacks on network analyze the performance and consequences of those attack, they propose security goals and parameters of routing in a sensor network.

J. Newsome et al.[15] describe how Sybil attack affects the whole network. Sybil attack is one of the most serious attack as the nodes impersonate its self to be at multiple location. Authors also describe types of Sybil attack on the network and propose countermeasure against each type.

S. Park et al.[16] propose a defense mechanism against Sybil attack. Authors suggest timestamp series approach to detect a Sybil attack. Timestamp approach follows simple principle that a vehicle holding single identity may not pass through multiple RSU at same time and if it passes, then that node treated as Sybil attack.

R. Hussain, H. Oh [14] deeply analyze the consequences of Sybil attack and propose tamper resistant model (TRM) in order to avoid Sybil attack and secure the network from attackers.

R. Xiu-li, Y. Wei [22] propose a Sybil attack detection approach for Vehicular ad-hoc network. In the proposed approach, every node checks the range of their neighbor node, if that range does not fit according to the parameter, this shows a particular node is Sybil node. Then topology takes countermeasure according to protocol.

K.F. Ssu et al. [23] discuss security challenges and effect of Sybil attack in WSN. Authors propose a technique for detection of Sybil attack where nodes identity verified by analyzing the neighbors' node table of its own.

Raya, M., and Hubaux [24] authors discuss the security issues in VANET and propose some security solutions. Authors also suggest a set of security protocols that protect privacy and enhance the efficiency of the sensor network.

Muawia Abdelmagid Elsadig and Yahia A. Fadlalla,[25] discuss numerous attacks on VANET in light of performance, achievement and propose security solutions to tackle these attacks.

Vimal Bibhu et al.[26] has described many attacks on the network but primarily focuses on back hole attack. Author did a performance evaluation of black hole attack in a simulation environment.

III. HISTORY

A. VANET

VANET is a vehicular Ad-Hoc network also called Wireless Access in Vehicular Environment (WAVE), which is responsible for communication between vehicles and infrastructure in a certain environment. When implementing a VANET, it is mandatory to implement the communication protocol in an efficient and orderly manner.

a) Components of VANET: The main components of vehicular ad-hoc network are: On Board Unit (OBU), Road Side Units (RSU), Trusted Authority (TA) and Application Units (AU). Each component is crucial for implementing VANET. Listed components of Vehicular Ad-hoc Network are briefly explained below:

b) On-Board Unit (OBU) is equipped on every vehicle supporting ITS. OBU is a network device, which is fixed on vehicles and used for exchanging information with nearby vehicles OBUs or with Road Side Units. Sensors on Electronic control Unit (ECU) collect information about vehicle and surrounding then Application Unit (AU) process that information and generate some messages based on gathered information and share that information with neighbor

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, October 2023

vehicle in order to eradicate any miss-happening. OBU may connect to internet via RSUs through DSRC radio or by Hotspot and in absence of both OBUs can communicate with each other via some cellular network [5].

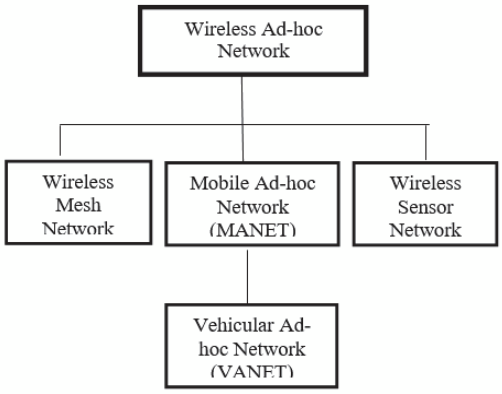


Fig. 1 Hierarchy of Wireless adhoc network

c) Road Side Unit (RSU) standing for the base station or act as the gateway between vehicles and road services provided by VANET. For the reason that RSUs are Static in nature as they have some fixed range, so vehicle in that range only may communicate with that RSU. The frequency and distribution of RSUs are mainly depended on the communication protocol utilized by it. RSU assist Trusted Authority (TA) to revoke communication of authorized node to unauthorized or malicious nodes [6].

d) Trusted Authority (TA) is responsible for issuing digital certificates to RSUs and vehicles, which authenticate vehicle and RSU uniquely in the vehicular ad-hoc network. To isolate untrusted vehicles, Trusted Authority holds a list of malicious vehicle and continuously advertise that list to the network, in order to prevent those vehicles who are not allowed to participate in VANET because of its malicious behavior in past[7].

e) Application Units (AU) is a device equipped in the vehicle. The connection between AU and OBU may be wired or wireless, in some cases, AU and OBU may couple in a single chip. AU handles the services provided by the provider mostly deals in the safety application and personal digital assistance (PDA).

B. In general, there is no fixed communication model or architecture that VANETs must follow. VANETs are very different from MANETs. Nodes in MANET are free to move randomly, while in VANET vehicles or nodes are free to move along a fixed path such as a road or highway.

Communication in VANET is closely categorized into 4 classes.

a) In-vehicle communication is more important in terms of driver concern as it provides information related to vehicle health, performance and driver fatigue and drowsiness which is essential for driver and public safety.

b) Vehicle-to-Vehicle (V2V) communication provides communication between vehicles, where vehicles can communicate directly with other vehicles, including sending and receiving messages.

c) Vehicle-to-infrastructure (V2I) communication refers to communication between vehicles and infrastructure such as traffic lights or road side units (RSU). RSUs are like routers that are fixed at the roadside and have a certain horizontal height when they receive certain information, as any vehicle conveys that information to a specified destination. RSUs are placed at some fixed distance, this limited distance between RSUs depends on the communication limit of RSUs devices. For effective communication, VANET prefers to use the IEEE 802.11 standard.

d) Vehicle to Broadband (V2B) communication defines that the vehicle can communicate through some wireless broadband communication channel such as HSPA(3G) or Long Term Evolution (4G) as these broadband clouds accept additional traffic information and monitoring data. which helps in vehicle tracking. Active Driver Assistance[5].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, October 2023

IV. VANET SECURITY

In this section, we present some security features for VANET. These three characteristics cannot be ignored when it comes to security. Most studies classify attacks based on authenticity, availability, and stealth.

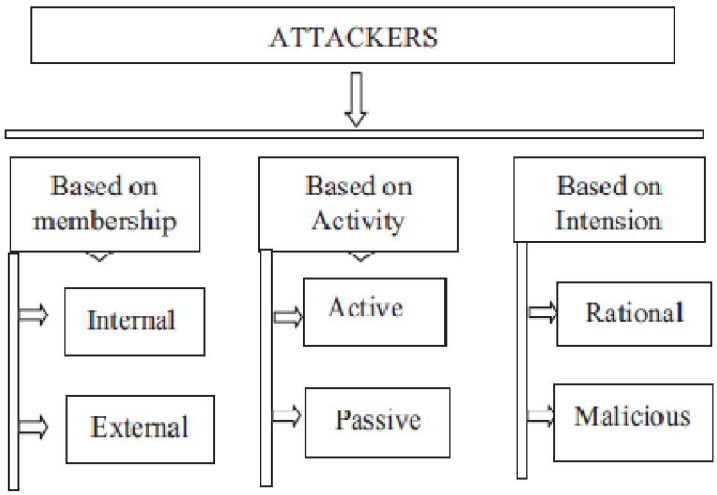
A. Authenticity is important because it confirms that the message was sent in a certified way. It is very important to confirm the authenticity of the messenger.

B. Availability ensures that communication channels and network resources are available, even if the network is subjected to attacks that will not affect the operation of the network.

C. Privacy is achieved by using certain cryptographic techniques in messages. Privacy means confidential communication. After that, when the message is sent, no one but the authenticated recipient can open the message.

V. SECURITY ATTACKS AND APPROACHES

In this section, we present different types of possible attacks on vehicular ad-hoc networks. The impact of an attack on a system depends on the efficiency of the attacker. These attacks are unpredictable and can affect the life-saving applications of VANETs. These attacks can disrupt the entire system or modify the functioning of the system to gain system privileges. Based on the attacks performed by an attacker on VANET, these attackers are classified into following types [9]



A. Classification based on membership: On the basis of membership there are two types of attackers are possible.
The trusted nodes of a network, who used to communicate with the other members of the network, are known as Internal, these authorized members of the network perform this attack in various ways. On the contrary, External does not have direct access to communicate with the member of the network; they have limited capacity to attack.

B. Classification based on Activity: On the basis of activity attacker can be active or passive.
An Active attacker tries to alter the information of the network by generating malicious packets or signals. This type of attackers are much noxious than passive attackers. Whereas Passive attackers only eavesdrop on the wireless channel, they do not alter the network information.

C. On the basis of Intention: This describes the intention behind the attack
A rational attacker seeks personal benefit by imposing attack over the network, these attacks are more predictable whereas malicious attackers not gain any personal benefit, and their intention is to damage the proper functioning of the network, it's difficult to foreseen malicious attack.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, October 2023

VI. ATTACKS

There was countless number of attacks are possible on VANET which may shut down the whole network or can degrade the performance of the network. Some of the attacks are explored below:

A. Denial of Service Attack (DOS): In VANET availability of network is very essential where all Vehicles rely on that. DOS is often one in all the foremost

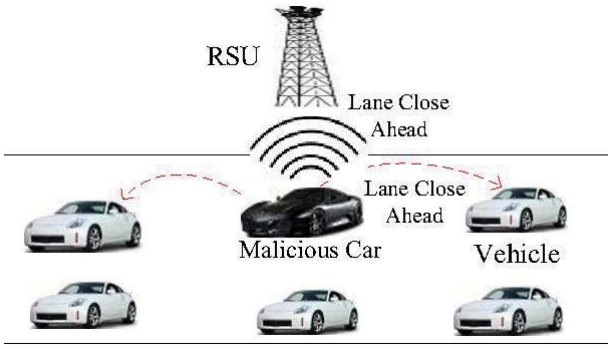


Fig 2. Denial of Service (DOS) Attack

Figure 2 shows that a malicious black car applies a DOS attack to demolish the communication between V2V and V2I by transmitting the dummy messages "Lane close ahead" to the vehicles near to it and also transmit that dummy message to nearest RSU. Because of this, legitimate cars on white receive a false information and take their decision based on false information.

B. Distributed Denial of Service (DDOS) Attack: DDOS attack is much savior attack than DOS in VANET environment as mechanism of this attack is in distributed environment. In 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. That's why it very difficult to prevent or trace this attack.

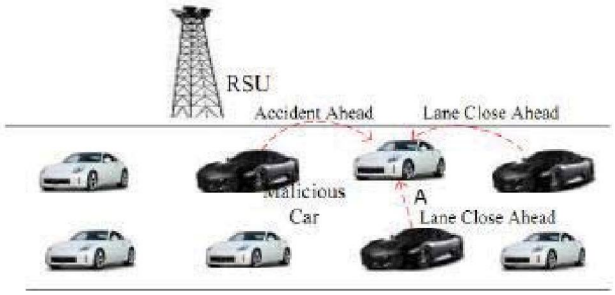


Fig. 3 Distributed Denial of Service (DDOS) Attack

Figure 3 demonstrates DDOS attack where malicious cars in black launch DDOS attack on a legitimate car A form different locations and at a different time because of that car A cannot communicate with other trusted cars [9].

C. Black Hole Attack: In this attack, malicious nodes in a network create an area where the network traffic is redirected or message packets are dropped. The 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 for their benefit [12].

Figure illustrates black hole attack where legitimate cars D and C send packets to malicious cars in black, these cars create a black hole in the network and do not transmit that packet to the other legitimate vehicles i.e E and F.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, October 2023

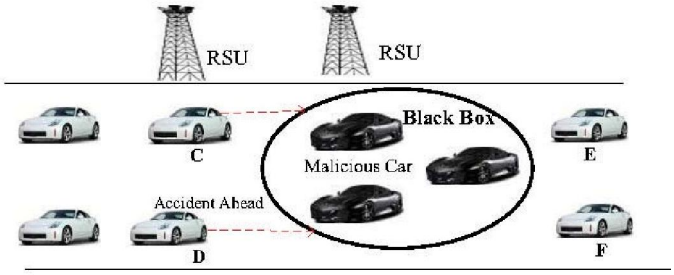


Fig 4. Black Hole Attack

D. Wormhole attack: This attack is a variation of black hole attack, in wormhole attack legitimate cars receive data packet by the malicious cars. In this attack, malicious cars create a wormhole or tunnel between the sender and receiver with minimum hope count and make that entry in the routing table. When sender node needs to transmit data it looks for the destination path with minimum hope count and it identify the route with minimum hope count created by malicious nodes and then start transmitting the data packets by that route. As the communication between the sender and receiver initiated through this malicious tunnel, so malicious nodes have all the freedom either to drop that packet or just listen the data packets or modify the data packet or use data packet for their benefit.

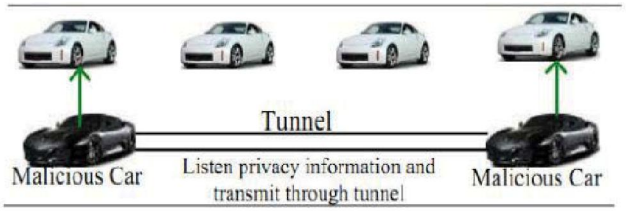


Fig 5. Worm Hole Attack

Figure 5 shows the wormhole attack, where two black malicious cars create a tunnel to transmit the data between legitimate source and destination.

E. Illusion Attack: In this attack, the attacker tries to deliberately manipulate his vehicles reading or incorrect traffic information and transmit that false reading to nearby vehicles and RSU. In VANET driver behavior will depend on the warning messages it receives, as driver receives false warning messages it may change the driver behavior and can cause an accident, traffic jam or can reduce the performance of the network by manipulating network topology.

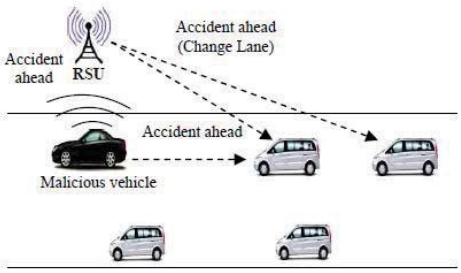


Fig 6. Illusion Attack

Figure illustrates Illusion attack, where black malicious car generates false traffic warning message and broadcast that false message “accident ahead” to the neighbor vehicle and even to RSU.

F. Timing Attack: In VANET vehicles on the road need a real-time data so if the information received at the correct time then it is worth and if not then that information is worthless. So transmission of data at the right time form source vehicle to destination vehicle is important in order to achieve security and integrity. In timing attack, if a malicious vehicle receives an emergency message, they do not forward that message to the destination instantly while it adds a

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, October 2023

time slot to the original message in order to create a delay. Because of that receiver vehicle receives the message after that actually it requires.

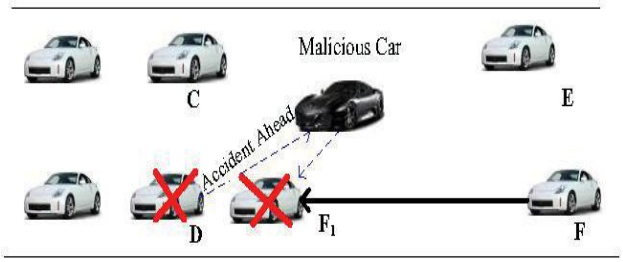


Fig 7. Timing Attack

Figure 7 shows timing attack on VANET network, where a black malicious car receive a message "accident ahead" form car D, it does not transmit that message at correct time, when car F was actually at its right place instead transmit that message by adding some time slot so whenever car F receives that message it is on spot F_1 where accident has actually happened.

G. Man in Middle Attack: In man in middle attack, malicious vehicles include himself into the communication between two vehicles and impersonate both the vehicles in order to gain the access of the information that both vehicles were trying to send each other and inject false information between vehicles, this attack impersonate as it's a normal exchange of information.

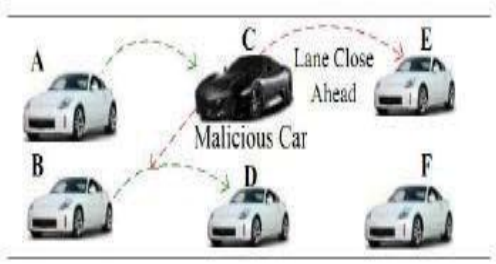


Fig 8. Man in Middle Attack

Figure 8 illustrates man in middle attack where black malicious car C listens to the communication between B and D and transmit false information to E.

H. Global Positioning System (GPS) Spoofing: All the vehicles connected to VANET transmit a signal to GPS satellite, the GPS satellite maintain a location table of all the vehicles by the use of the location of vehicles and vehicle unique identity within the network. In GPS spoofing attack, attackers vehicle push a false reading in the GPS in order to deceive other vehicle to think that they are at the different location. In order to generate false signal vehicle use GPS satellite simulator which generates a false signal that was much stronger than those actual signal.

I. Social Attack: All frail attack comes under this attack. In Social Attack, the intention of the attacker is to indirectly compose a problem for the users of the network. Attacker sends some random messages "You are stupid" to the authentic user of the network with the intention to change the behavior of the user when authenticated user read those messages its behavior get change from positive to negative angry behavior[10].

J. Sybil Attack: Sybil attack is a noxious attack, which was first mentioned in context of a peer-to-peer network. In this, an attacker creates an illusion of the existence of multiple false vehicles in order to dominate over the whole network and infect false information to harm the legitimate user or to demolish the network performance. This attack is one of the most serious attack, as the attacker claimed to be at the different geographical location at the same time [10][11].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, October 2023

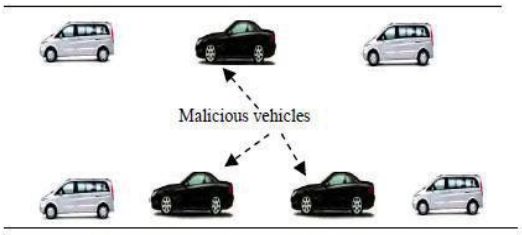


Fig 9. Sybil Attack

Figure 9 shows the Sybil attack where a black malicious car creates an illusion of multiple vehicles on the road because of that, other vehicles on the road realize that there is a heavy traffic on the road. The impact of this attack is serious because after spoofing vehicles identity and location of the vehicle, an attacker can implement any types of attack in the network.

VII. CONCLUSION

As we realize purpose in the back of implementation of VANET is to improve efficiency and protection in transportation. To switch information between nodes VANET use wi-fi medium as the medium is wi-fi there is good hazard for attacker to attack on the network and damage whole community within the contemporary paintings, we have discussed VANET along with its components, types of communications and so forth. Then we discuss outstanding studies difficulty and demanding situations like safety and assaults in VANET. The idea of this paper is to have a look at the research perspective on various assaults primarily based on pastime, Intension, and membership in VANET. inside the destiny work, we will extend our paintings to advise a viable approach to guard the cars from Sybil attack below VANET.

REFERENCES

[1] http://pib.nic.in/newsite/PrintRelease.aspx?relid=170577 assessed on 6 March 2018.
[2] Maxim Raya, Jean-Pierre Hubaux., " The Security of Vehicular Ad Hoc Network", SASN'05. Nov 7, 2005, Alexanderia Virginia, USA, pp 11-21.
[3] J.P. Hubaux, S.Capkun, and J.Luo," The security and privacy of smart vehicles", IEEE Security and Privacy Magazine, Vol. 2, No. 3, pp 49-55,2004.
[4] J.T. Issac, S.Zeaddly, J.S.Camara, "Security attacks and solutions for vehicular ad hoc networks", IET Communications, pp 894-903, 2009.
[5] Wenshuang Liang, Zhuorong Li, Hongyang Zhang, "Vehicular AdHoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends", International Journal of Distributed Sensor Network, Volume: 11 issue: 8, August 2015.
[6] Sabih ur Rehman, M.Arif Khan, Tanveer A., Lihong Zheng, Vehicular Ad-hoc Networks(VANETs) - An Overview and Challenges, Journal of Wireless Networking and Communications, 2013.
[7] Bharti Mishra, Priyadarshini Nayak,Subhashee Behera, Security in Vehicular Adhoc Networks: A Survey, ICCCS '11 Proceedings of the 2011 International Conference on Communication, Computing & Security, ACM Digital Library, Pages 590-595, February 2011.
[8] Rashmi Mishra, Akhilesh Singh, Rakesh Kumar, VANET Security: Issues, Challenges, and Solutions, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 24-Nov-2016. [9] Mohammad Saeed Al-kahtani, Survey on Security Attack in Vehicular Ad-hoc Networks, 6th International Conference on Signal Processing and Communication Systems, Dec. 2012.
[10] Vinh Hoa LA, Ana CA VILLI, Security Attacks and Solution In Vehicular Ad Hoc Networks: A Survey, International Journal on AdHoc Networking Systems(IJANS), Vol 4, No 2, April 2014.
[11] Cheng-ZhongXu, BinXiao, Detecting Sybil attacks in VANETs, Journal of Parallel and Distributed Computing, ELSEVIER, Vol 7, Issue 6, Page 746-756, June 2013.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, October 2023

[12] P Sai Gautham, R Shanmughasundaram, Detection and isolation of Black Hole in VANET, International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), 23 April 2018.
[13] Karlof, C., and Wagner, D. (2003), 'Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures', Ad Hoc Networks, 1, 293-315.
[14] R. Hussain, H. Oh, On secure and privacy-aware Sybil attack detection in vehicular communications, Wireless Pers. Commun., 77(4), 2649- 2673, 2014
[15] J. Newsome, E. Shi, D. Song, A. Perrig, The Sybil attack in sensor networks: analysis & defenses, in Proc. of the Third International Symposium on Information Processing in Sensor Networks, IPSN 2004, pp. 259–268, 2004.
[16] S. Park, B. Aslam, D. Turgut, C.C. Zou, Defense against Sybil attack in vehicular ad hoc network based on roadside unit support, in Proc. of Military Communications Conference, 2009.
[17] J. Grover, D. Kumar, M. Sargurunathan, M.S. Gaur and V. Laxmi, "Performance evaluation and detection of Sybil attacks in vehicular Ad-Hoc networks" Communications in Computer and Information Science Vol. 89 CCIS, pp. 473-482, 2010.
[18] H. Lu and J. Li and M. Guizani, "A novel ID-based authentication framework with adaptive privacy preservation for VANETs," IEEE Computing, Communications, and Applications Conference, February 2012.
[19] Lu, R., Security and Privacy Preservation in Vehicular Social Networks, Doctoral dissertation, University of Waterloo, 2012.
[20] J. T. Isaac, S. Zeadally, J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks" Communications IET, Vol. 4, No. 7, 894-903, 2010.
[21] S. Chang, Y. Qi, H. Zhu, J. Zhao, X. Shen, "Footprint: detecting Sybil attacks in urban vehicular networks," IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 6, 1103-1114, 2012.
[22] R. Xiu-li, Y. Wei, Method of Detecting the Sybil Attack Based on Ranging in Wireless Sensor Network, 5th International Conference on Wireless Communications, Networking and Mobile Computing, WiCom '09, 1–4, 2009.
[23] K.F. Ssu, W.T. Wang, W.C. Chang, Detecting Sybil attacks in Wireless Sensor Networks using neighboring information, Computer Networks 53(18), 3042–3056, 2009.
[24] Raya, M. and Hubaux, J. P. (2007) "Securing vehicular ad hoc networks", Journal of Computer Security, 15, pp.39–68.
[25] Muawia Abdelmagid Elsadig, Yahia A. Fadlalla, "VANETs Security issues and Challenges: A Survey", Indian Journal of Science and Technology, Volume 9, Issue 28, July 2016.
[26] Vimal Bibhu, Kumar Roshan, Kumar Balwant Singh, Dhirendra Kumar Singh, "Performance Analysis of Black Hole Attack in VANET", International Journal of Computer Network and Information Security (IJCNIS), October 2012.