DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.5069

ISSN No. 0976-5697

Volume 8, No. 9, November-December 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

COMPREHENSIVE SURVEY OF DENIAL OF SERVICE ATTACKS IN VANETS

Sushil Kumar
Research Scholar
IKGPPTU,
Kapurthala, India

Dr. Kulwinder Singh Mann
Professor,
Guru Nanak Dev Engineering College
Ludhiana, India

Abstract: Vehicular Adhoc Networks (VANETs) is the form of network which contains vehicles with high mobility as nodes. Since the nodes are moving, the vehicles entering and leaving the network is at very high pace making the VANETs self-organizing. Due to this, the dissemination of information to correct nodes and making the network secure from active as well as passive attackers is one of the vulnerable task in VANETs. There are number of attacks by which the network can be attacked but in this paper we have discussed Denial of Service (DoS) attack which attacks on the availability of the network. All the possible reasons of DoS attacks are reviewed and also all the possible solutions are defined in this paper.

Keywords: VANETs, Security, Availability, DoS, Simulation Model

1. INTRODUCTION

Pervasive Networks (PN) are the networks which have mobile nodes as the components; all the nodes are arranged independently with high mobility. PN includes the names of MANETs (Mobile Adhoc Networks), WMN (Wireless Mesh Networks) and VANETs[4] (Vehicular Adhoc Networks) in the list of its best examples. VANETs are the specialized form of MANETs in which the vehicles acts as the mobile nodes in creation of a network. All the information is passed between the vehicles or nodes through this wireless network and also they communicate with the Road Side Units (RSUs). The appropriate range of nodes participation is upto 300 meters.

The unique characteristics of VANETs includes high mobility, rapidly changing network topology, large network size, frequently exchange of information, deals with time critical information etc[2]. The various applications of VANETs includes monitoring of the traffic, route optimization between source and destination, forecasting of weather conditions, online services provision, prevention of collision etc.[4]

All the adhoc networks communicate with each other through single hop connection which can create problems in the network. Same is in the case of VANETs, so, multi-hop connection is used[6] in this with the help of Bluetooth and other technologies to lessen the effect of problems in adhoc networks.

The reason behind the creation of VANETs by ITS (Intelligent Transportation System) is the figure of people being injured in the road accidents which is given by National Highway Traffic Safety. With the help of VANETs, 60% of the accidents can be avoided by sending warning messages to the driver before time. Road safety, drivers' assistance and safety is increased with the evolution of VANETs[24]. They are required when we need to disseminate some information related to traffic jam ahead, and prior alert if the vehicle in front is applying breaks, any accident ahead, vacancy in nearby parking area etc.[2] VANETS helps in disseminating this type of information to the vehicles nearby and also to the RSUs using the wireless connection upto some particular range. Nowadays, all the car manufacturers and telecommunication industries are collaborating with each other in developing the vehicles which should be capable of cope up with the existing wireless technologies.

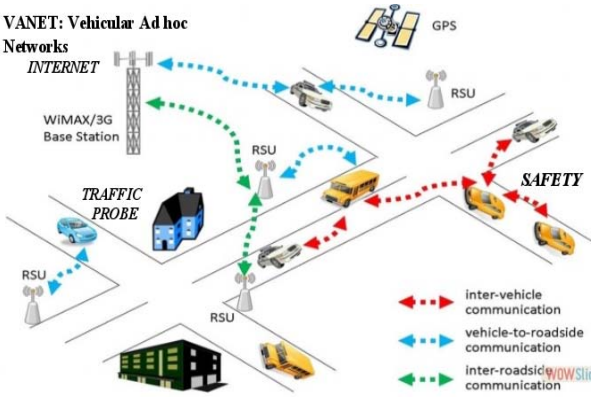

Figure 1: Architecture of VANETs [5]

Figure 1[10] shows the architecture of VANETs and information is disseminated between the vehicles and the RSUs in VANETs. Two types of communication is done in this type of adhoc networks that is V2V (Vehicle-to-Vehicle) and V2I (Vehicle-to-Infrastructure). Under V2V, the information or the messages exchanged between the vehicles depends upon the nature and purpose of messages to be disseminated[4]. The various communication patterns used in V2V are Warning propagation, Group communication, Beaconing, I2V/V2I Warning. Warning propagation is used when there is a need to send information to nearby vehicles regarding some accident nearby, Group communication is dependent upon features of vehicles in a group whether static or dynamic, Beaconing is used to send information to nearby vehicles periodically about the speed, brakes etc, I2V/V2I warning messages are sent either by the infrastructure to vehicle or from vehicle to infrastructure regarding any danger nearby[24].

Characteristics of VANETs includes independent vehicles with varying speeds, varying topology, minimized power consumption, high mobility etc.

2. SECURITY REQUIREMENT OF VANET

As the nodes in VANETs are self dependent which make the network self-organized and more vulnerable to attacks. So, there is a strong requirement to check the security of the network. The various security requirements are[9][24]:-

- ***Data Authentication and Integrity****:*-This requirement of security in VANETs needs every node to verify the messages before passing it for its authentication and identification. It also checks that the messages should be sent to the correct destination of vehicles.
- ***Data Confidentiality:-*** The data between the various nodes and network is transferred by using various encryption schemes.
- ***Vehicle Privacy and Anonymity:-*** The messages need to be used by only the authorized vehicles and also the authorized nodes can identify the legitimate users not the nodes with malicious behavior.
- ***Access Control:-*** The local as well as remote nodes can access the resources of the network.
- ***Data Non-Repudiation:-*** If the sender does not disclose their identity, then this results in lack of cooperation between the nodes and can also sometimes leads to misleading of vehicles.
- ***Vehicle ID Traceability:-***The real identification of the vehicles needs to be traceable by other vehicles
- ***Scalability:-*** The VANETs can be scaled to any range with the addition of any number of vehicles in the network. Although this decreases the performance of the network and also complexity is increased since the messages need to be disseminated to the large number of vehicles.
- ***Forgery:-***Sometimes, the messages sent by the malicious nodes misleads the networks and causes troubles.
- ***Availability:-*** The network should be available all the time for the nodes in the network. If there is number of attacks in the network, then also all the resources should be available.
- ***Anti-Jamming:-*** The network is jammed by the malicious nodes by sending large number of messages to the legitimate nodes[24].

3. RELATED WORK

VANETs are prone to number of attacks and all types of attacks need to be detected, avoided, prevented and most importantly their possible solutions need to be found. Attacks effects the security of wireless networks very adversely and because of this insecure environment, human lives can be affected if wrong message is passed to the vehicles.

A. Types of Attackers

Saeed et al. differentiated the attackers according to the capability of the problems they can create in the network.

Insider v/s Outsider Attacker:- Insider attacker is the one authentic node in the network which chooses to send wrong information to the nodes in the network. Since the insider nodes have more details about the network configuration, so they can create more severe problems in the network[2]. Outsider attacker is some intruder which uses the protocols and other information of the network for launching attacks. The range of insider attacker is high as compared to outsider attacker.

Malicious v/s Rational:- A malicious attacker has the intention of damaging the network and its nodes without gaining anything from the network. But, the rational attacker has its own benefit in damaging the network and hence, they are easily detectable[2].

Active v/s Passive:- An active attacker damage the wireless network by generating new messages in the form of packets while the passive attacker just eavesdrop in the wireless channel but cannot generate any new message or packet[2].

Local v/s Extended:- This class of attacker is different from each other in relation to its scope. If the scope is limited then the attacker is local, but if it is scattered amongst some other wireless channel then it is under the category of extended attacker[22].

B. Categories of Attacks

Sumra et al. categorized attacks into different classes according to the behavior of attackers[9].

- ***Network Class Attacks:-*** The attacks in this class affects the communication medium between the vehicles and infrastructure. The wireless networks with network class attacks are not able to give resources to legitimate users. They can create problems for the whole network and hence the legitimate users are not able to communicate with each other due to their unavailability. The various attacks under this category are Denial of Service Attacks (DOS), Distributed Denial of Service (DDOS), Sybil Attack, Node Impersonation Attack[4].
- ***Application Class Attacks:-*** The attacks under this class alters the information that is being disseminated between the different vehicles in the network. Due to this alteration in the messages, wrong information is sent to legitimate users and the accident can be caused by this. This class of attacks can affect both safety and non safety applications. Bogus information attack can affect safety applications and non safety applications include availability of parking, location finding services in mall or for any restaurant[4].
- ***Timing class attacks:-*** This class of attacks unable the users in the network to get the messages on time by adding delay in the messages being disseminated. Since the requirement of the VANETs is to get the messages on time as the messages contain the safety related information. So, the network is adversely affected if for e.g. the information of some accident is in the message and that got delayed due to timing attacks[4].
- ***Social class attacks:-*** This class of the attacks affects the legitimate users by sending the social messages which just irritates the user and that indirectly affects the way user behaves while driving. Same message is sent again and again causing unnecessary traffic in the network and avoiding the dissemination of useful messages within the nodes and the infrastructure[4].
- ***Monitoring class attacks:-*** This class of attacks just monitors the network and the communication between the vehicles and infrastructure. Whenever there is any

message containing any information related to the attacker is disseminated within the network, it is also sent to the attacker in priority and thus affects the network. This is usually used by the criminals for leaking the information of the police planning against them[4].

C. Possible attacks in VANET

- ***Sybil Attack:-*** In this type of attack, false information is broadcasted by the fake nodes in the network. Each disseminated message has different identity causing the passage of wrong messages to legitimate users. Sybil attack can be encountered by using session keys given by Certificate Authority (CA) [9]and by some statistical and probability algorithms[22].
- ***Node Impersonation:-*** In this attack, false message is disseminated in the network claiming that it is from a correct node. The algorithms used for isolating the fake node is Detection of Malicious Vehicle (DMV)[23] and Detection algorithm[24].
- ***Sending False Information:-*** Chaos can be created in the network by different nodes by sending false information in a periodic manner. The actual work of the network is disrupted due to passage of this false information by the attackers for their own reasons. This type of attack can be encountered by using password technique for each message by which each receiving node will check for the authentication of the message[13].
- *ID Disclosure:-* By monitoring the target nodes, the attacker track the location of the nodes in the network. The nodes disclose their ID and their location with the attacker nodes. This type of attack can be encountered by using Public Key Infrastructure technique[13].
- ***Black Hole Attack:-***This attack is caused by the malicious nodes in which they inform to every node in the network that they have optimum route to the destined node. If the node replies to this , then the forged route is maintained which will ultimately lead to the passage of messages to black hole rather than to the actual node[14].
- ***DoS and DDoS Attack:-*** Denial of Service (DoS) and Distributed Denial of Service attack (DDoS) attacks the communication medium of the network making it and its resources unavailable for some reasons[13].
- ***Gray Hole Attack:-*** In this type of attack, the behaviour of malicious node is unpredictable as it can behave as a honest node and sometimes it can behave as an attacker node. Due to its this nature, it is very difficult to detect. Other reasons for its non-detection are congestion, overload etc. which can ultimately lead to low performance of the network[21].

4. DENIAL OF SERVICE ATTACK

Denial of Service (DoS) attacks affects the availability of the wireless networks for legitimate users. The attacker jams the communication medium by sending fake messages, or can overwhelm the node resources. So, the attackers stop the legitimate users from doing the useful work either by jamming the wireless channel or by flooding the network. The mobile nodes are busy in tackling the irrelevant messages instead of doing the useful messages. In VANETs, this type of strategy is used by the attackers to distract the drivers in a network to take a wrong decision while travelling based on fake messages which results in insecure network. In other case, by doing this, if the attackers take control of the critical components in the network, then any incident can happen with the mobile nodes with the passage of wrong and irrelevant messages[12]. In all the above cases, the services provided by the network to the mobile nodes are disrupted and hence, it is known as DoS (Denial of Service) attack. DoS attacks disturb the network channel in the following manner:-

- ***Impersonation:-*** In this type of attack, the original message by the originator is replaced by its modified version which in turn is used for attacking the network by claiming that it comes from real originator[2].
- ***Jamming:-*** An attacker attacks the channel by sending higher frequency messages. By this, the nodes are unable to send or receive messages as their communication medium is jammed by attacker. The number of messages sent by the attacker is very high, so Road Side Unit becomes busy in validating the IP address and hence is unavailable for the legitimate users. This is known as unavailability of the network due to IP-CHOCK. This attack can occur both in V2V as well as in V2I communication[8].
- ***Overwhelming of Node Resources:-*** This type of DoS attack can occur both in V2V as well as in V2I communication. In both the cases, the attacker keeps busy all the nodes by overwhelming their resources. So, the nodes cannot perform the useful tasks in the communication. Hence, it is difficult to disseminate the life critical information to other nodes in the network.
- ***Distributed Denial of Service Attack (DDoS):-*** The attack in this DoS attack is distributed geographically in nature. That is, the attacker attacks from different locations onto the communication channel as well as onto the mobile nodes. The number of messages by different malicious nodes is sent to the legitimate users in different time slots and due to which the communication between the mobile nodes themselves and with the infrastructure is obscured. Hence, the network is unavailable for useful work. Since, the number of messages is sent from different locations, the network is busy in validating them, so, it denies the work of legitimate users and therefore, Distributed Denial of Service attack occurs in the communication.

D. Possible Solutions of DoS

According to different authors, following are the different ways for tackling with DoS attacks in VANET**s:-**

a) Using On Board Units (OBU) in Vehicles:-The OBU is in the vehicles and connected to the wireless network all the time. When there is DoS attack in the network, the OBU in the vehicles decides to take any action. The various actions that can be taken are Frequency Hopping, Switching of the Channel, switching of technology. Dedicated Short-Range Communication (DSRC) divides the provided seven channels into safety and non-safety applications. Whenever, there is any attack in the given channel, the channel can be switched onto other channel to communicate with the

authentic nodes. The various technologies used for communication in VANETs can be Wi-fi, Wi-Max etc. Once there is DoS attack in any one technology, the OBU can switch to any other technology for safer communication[9]. So that no information should be delayed while reaching to the authentic nodes as they have life critical information. The bandwidth of the network can be increased by adding different frequency channels. This also helps in prevention of the network from the DoS attacks. If the attacker attacks one frequency channel, then other channel can be used for providing the service to the legitimate users. This technique is known as frequency hopping spread spectrum technique (FHSS)[9]. Total network collapse can be avoided by adding multiple radio transceivers in the network. If any transceiver is attacked by the DoS attack, then other can be used for effective communication between the mobile nodes.

b) To overcome **impersonation**, an unique IP address is given to each mobile node in the network and that is checked for identification of real and correct originator[15].

c) Rate decreasing algorithm:- Transmission rate of emergency warning messages is reduced to half once its value reaches the threshold value. And a complete check is done on source node, if the transmission rate is not reduced by the source node, then that node is blocked using voting scheme [4].

d) State Transition:- Broadcast storm which causes DoS and DDoS attacks can be effectively dealt by using state transition method. The various states are initial abnormal state, flagger state and non-flagger state depending upon the value of transmission rate [4].

e) ***Packet Detection Algorithm:-*** There are number of variations of packet detection algorithms.

- **Attacked Packet Detection Algorithm (APDA)** helps in reducing the probability of any network to be attacked by DoS attack by its flooding form. In this algorithm, a transductor is used which saves the information of every vehicle in the network like its location, timestamp etc., and then it verifies every message sent by the vehicle based on its timestamp and discards or passes the message according to the value of the timestamp[10].
- **Request and Response Detection Algorithm (RRDA):-** After APDA algorithm, the further probability of DoS attack can be reduced by RRDA Algorithm. RRDA algorithm works for the new nodes that want to enter the network. APDA validates the nodes before the verification process but the RRDA algorithm validates the nodes when they send new requests to be in network, thus this validation will allow only the legitimate users to enter in the network[6].
- **Enhanced Packet Detection Algorithm (EPDA)** helps in detection of malicious nodes during the verification process by checking the transmission rate of sending the packets by the source node. If the transmission rate is double the actual rate, then that node is not legitimate node and can further helps in DoS attack[7].
- **Malicious and Irrelevant Packet Detection Algorithm (MIPDA)** [3]helps in confining the DoS attacks to the source nodes by validating the packets sent by them. If the packets are malicious, then that vehicles nodes are tracked for their further work. Otherwise, if the node is legitimate, then the messages are transferred without any disruption in the network. By this method, security is enhanced in the VANETs by reducing the overhead delay.

f) Cryptographic Solutions:-VANET network affected from DoS can be dealt using the following cryptographic algorithms:-

- **ECDSA (Elliptic Curve Digital Signature Algorithm):-** In this algorithm, digital signatures are used to authenticate the legitimate users. Elliptic curve scheme is used to generate digital signatures. But this method increases the overhead by computation of digital signature every time there is any communication between the nodes[1][20].
- **TESLA (Timed Efficient Stream Loss-Tolerant Authentication) and TESLA++:-** The various cryptographic methods used in TESLA are symmetric key authentication and hashing technique. Due to usage of these techniques, the overhead is decreased. Only there is a requirement of single key which is used for authentication. The only problem with TESLA is that it requires more memory to store the messages, hash function details and key information. The disadvantage of TESLA is removed in TESLA++ by storing less information and by applying re-hashing for compressing the information further. But still TESLA++ has its own disadvantages in the form of scalability[24].
- **VAST (VANET Authentication using Signature and TESLA++):-** In this technique, both digital signatures and TESLA ++ are used for authentication of legitimate users. The disadvantages of both the methods are removed in this solution and can be effectively used as a solution for the DoS attack[24].
- **FastAuth and SelAuth:-** Fast authentication is used to authenticate single-hop messages and Selective Authentication is used to authenticate multi-hop messages. It helps in distinguishing between the malicious nodes and legitimate users[24].

5. SIMULATORS FOR VANET

VANETs are different from MANETs as they use well defined and established paths for their movement and also there speed is very speed in comparison. Since the deployment of VANETs is very expensive and also if deployed effectively, then it need to be tested which can be very costly if any case it fails. So, prior simulation is a very good alternative. Any VANET simulation software includes VANET Simulators, Network Simulators and Mobility Generators[23].

Mobility Generators:- They are used in VANETs to increase the realism in the simulation. The location of each and every vehicle in the network is given as output by the mobility generator after taking the details of the road and vehicles as input in the network. While simulating the VANETs in any open source simulator, mobility generators need to model the traffic well in advance so that the radio transmission model can be prepared.

The traffic models are categorised into three categories named as macroscopic, mesoscopic and microscopic models. In macroscopic models, traffic is modelled in large groups of nodes or vehicles, in mesoscopic, details of traffic are modelled in few numbers of vehicles in comparison with

macroscopic models. Lastly, in microscopic models, the detail level is up to individual vehicle or node. Since the microscopic models give the highest detail, so they are appropriate for VANETs simulation.

Further, vehicular movements are defined in macro as well as micro mobility level while simulating the VANETs environment. Macro mobility deals with the aspects having coarse grain behaviour in simulation like topology of the road, various rules of safety, traffic signs, movements of car etc. while the micro mobility deals with aspects with fine details like driver's behaviour in network and disseminating the information to different nodes in the network, his criteria of driving, overtaking etc. The mobility generators take into consideration both the micro as well as macro mobility behaviour of the nodes.

Various examples of mobility generators are SUMO[16], MOVE[17], CityMob[18], FreeSim[19] STRAW [20]. The comparison of these all is shown in Table 1.1. These all are compared using the parameters given by software, maps, traces, mobility and traffic models. From this type of quantitative comparison, it is cleared that no mobility generator is best for all types of parameters. SUMO is very hard to use but all parameters are easy to use and understand. Setting up of SUMO and STRAW is easy as compared to CityMob, MOVE and FreeSim. Similarly, all other differences are shown clearly.

But all the mobility generators have some unique property due to which they can be used effectively for simulation of VANETs. The shortest notification time is given by CITYMOB, VANETMobiSim and SUMO in descending order. SUMO results the best in terms of dissemination of messages to other vehicles in the network from the victim vehicle. CityMob, VanetMobiSim and SUMO have the highest packet acceptance ration in comparison with other vehicles.

According to comparison quantatively shown in Table I on the basis of performance parameters, VANETMobiSim and SUMO outperforms all other mobility generators and hence widely used for the simulation of network.

Network Simulators:- They help the researchers to simulate the VANET network in fast, cheap and effective manner. Since the deployment and testing of the VANET network is very expensive if done on real vehicles, hardware and network. So, simulation is done prior to the deployment. It is also necessary since the VANET network carries life critical information of human beings. All the simulation can be done in an controlled and effective manner, and when tested fully can be deployed on the real network as when required. Various network simulators available are NS-2, GloMoSim, SWANS, QUALNET, Staged Network Simulator (SNS). All the network simulators are compared in Table II All the simulators are near about same to each other but NS-2 is not suitable for large networks and is only suitable for small networks[11].

The network simulator does not simulate VANETs effectively as they are not capable to do so. Only NS-2.33 is capable to simulate the vehicular network. All others does not consider vehicular traffic flow model and hence, not useful for VANETs.

VANET Simulators:- This software helps the vehicles or nodes in the network in taking their decisions if there is any problem in the network. The vehicles can choose either to stop or change his way depending upon the severity of the warning message.

Various existing VANETs simulators are TraNS (Traffic and Network Simulation Environment), GrooveNet, NCTUns (National Chiao Tung University Network Simulator), MobiREAL.The comparison table is shown in Table 1.3. They are compared on the basis of their capability with the Mobilty generators, network simulators, topology of road, traffic lights, trip model, ease of setup and use etc.

All the simulators provide support for traffic simulation in microscopic way using random speed models. The implementation of IEEE 802.11p is only provided by TraNS and NCTUns while inbuilt provision for VANET is provided by GrooveNet and TransNS. The results given by these simulators is very different from each other since they focus on different things while simulating VANET. Accoding to the researchers, GrooveNet and NCTUns is used frequently in simulation all the four simulators are Open Source[23].

Table I. Comparison of Mobility Generators

Parameter /Mobility Generator	*SUMO*	*MOVE*	*CityMob*	*FreeSim*	*STRAW*
Software:					
Portability	Yes	Yes	Yes	Yes	Yes
Freeware	Yes	Yes	Yes	Yes	Yes
Opensource	Yes	Yes	Yes	Yes	Yes
GUI	Yes	Yes	Yes	Yes	Yes
Setup Ease	Moderate	Easy	Easy	Easy	Moderate
Ease of Use	Hard	Moderate	Easy	Easy	Moderate
Maps					
Real	Yes	Yes	No	Yes	Yes
User – defined	Yes	Yes	No	No	--
Random	Yes	Yes	Yes	No	No
Manhattan	No	No	Yes	No	No
Voronoi	No	No	No	No	No

Mobility RWP	Yes	Yes	Yes	No	No
Traffic Models					
Macroscopic	No	Yes	No	Yes	No
Microscopic	Yes	Yes	Yes	Yes	Yes
Multilane roads	Yes	Yes	Yes	--	Yes
Lane Changing	Yes	Yes	Yes	--	Yes
Speed	Yes	Yes	Yes	Yes	Yes
Constraints	Yes	Yes	Yes	--	Yes
Traffic Signs	---	---	No	--	--
Overtaking	Yes	Yes	Yes	--	--
Collision free Route Calculation	Yes	Yes	No	Yes	Yes
Support					
NS-2	No	Yes	Yes	No	No
GloMoSim	No	Yes	No	No	No
Qualnet	No	Yes	No	No	No
SWANS	No	No	No	No	Yes
XML – based	No	No	No	No	No

Table II. Comparison of Network Simulators

Parameter /Mobility Generator	***NS-2***	***GloMoSim***	***SWANS***	***SNS***
Software				
Portability	Yes	Yes	Yes	Yes
Freeware	Yes	Yes	Yes	Yes
Opensource	Yes	Yes	Yes	Yes
Available	Yes	Yes	Yes	Yes
Examples	Yes	No	Yes	No
Continuous	No	Yes	Yes	Yes
development	Yes	Yes	Yes	Yes
Large Networks	Yes	Yes	Yes	Yes
Console	Poor	High	High	High
GUI	Easy	Moderate	Hard	Easy
Scalability	Hard	Hard	Hard	Hard
Ease of Setup				
Ease of use				
VANET				
802.11p	Only for NS-2.33	No	No	No
Obstacles	No	No	No	No
Vehicular traffic flow model	No	No	No	No

Table III. Comparison of VANET Simulators

VANET Simulators/ Parameters	***TraNS***	***GrooveNet***	***NCTUns***	***MobiReal***
Mobility Generator	SUMO	GrooveNet	NCTUns	MobiReal
Network Simulator	NS-2	---	---	---
Mobility Models	Random routes	RWP	Random roues	Probabilistic rule-

				based
Speed Models	Street Speed	Uniform speed	Random	Street speed
Traffic flow model	Car following	Car following	Car following	Car following
Traffic Lights	Manually defined	Manually defined	Automatically generated	Manually defined
Trip Model	Random, manually defined	Djikstra	Manually defined	Manually defined
Ease to setup	Moderate	Moderate	Hard	Easy
Ease to use	Moderate	Hard	Hard	Hard
VANET facilities	Road danger warning, dynamic reroute	Vehicle warning, adaptive rebroadcast	Controls driving behavior on road	Designed for MANETs, but can work for VANETs also.

6. CONCLUSION

Due to high mobility of the nodes in the network, the VANET network is vulnerable to number of attacks. The attack which hinders the availability of the network is the DoS attack. The malicious users can attack the network in number of ways making the resources of network unavailable to the legitimate users. Also, the network can be saved from being attacked by number of ways. All the reasons and the methods to overcome the network is reviewed and categorized in this paper. It is concluded after reviewing that the there is requirement of other solutions for saving the network from DoS attack.

7. ACKNOWLEDGEMENT

Acknowledgement:- Authors are highly thankful to the RIC department of IKG Punjab Technical University, Kapurthala, Punjab, India for providing the opportunity to conduct this research work.

REFERENCES

[1] P Rai., N, Mouzna J., "Mitigation of Insider and outside DOS attack against Signature based Authentication in VANETs'', Proc. IEEE Asia-Pacific Conference on Computer Aided System Engineering, pp.152-157, February 2014, doi 10.1109/APCASE.2014.6924490.

[2] R Raw, M Kumar, N Singh "Security challenges, Issues and Their Solution For VANET," in IJNSA, Volume 5, No 5, September 2013, pp 95-105.

[3] A. Quyoom, Ali, N. Gouttam , H Sharma ,"A Novel Mechanism of Detection of Denial of Service Attack in VANET using Malicious and Irrelevant Packet Detection Algorithm,'' Proc. IEEE in ICCCA ,pp.414-419, IEEE 2015, doi 10.1109/CCAA.2015.7148411.

[4] A. Malla , R Sahu ., "Security Attacks with an effective solution for DoS attacks in VANETs" IJCA(0975-8887), Vol 66, No 22, March 2013, pp 45-49.

[5] R. Fotohi , Y. Ebazadeh , M. Seyyar , "A New Approach for improvement security against DoS attacks in Vehicular Adhoc Network" IJACSA, Vol 7, No.7, 2016, pp 10-16.

[6] U. Gandhi, V. Keerthana, "Request Response Detection Algorithm for Detection of DoS attack in VANET", Proc. IEEE, ICROIT, February 2014,MRIU, India, doi 10.1109/ICROIT.2014.6798334.

[7] A. Singh, and P. Sharma, "A novel mechanism for detecting DOS Attack in VANET using Enhanced Attacked Packet Detection Algorithm" Proc. IEEE International Conference RACES,21-22 December, 2015, doi 10.1109/RACES.2015.7453358.

[8] M. Raya, P. Papadimitratos, J. Hubaux, "Securing Vehicular Communications" IEEE Wireless Communications, Vol 13,Issue 5, October 2006, pp 8-15.

[9] I. Sumra, " Denial of Service Attacks and its Possible Solutions in VANET" Research Gate, World Academy of Science, Engineering and Technology, 65, 2010, pp 411-450.

10] V. La, A. Cavalli," Security Attacks and Solutions in Vehicular Adhoc Networks: A Survey", International Journal on Adhoc Networking System(IJANS), Vol. 4, No. 2, April 2014, doi: 10.512/ijans.2014.4201, pp1-20.

[11] S. Rakhi, K. Shobha, H. Sampada, "A Comprehensive Survey on Security Issues in VANETs for Safe Communication", International Journal of Emerging Technology in Computer Science & Electronics, Vol 14, Issue 2, April 2015, pp 447-454.

[12] F. Martinez, C. Toh, J. Cano, C. Calafate, P. Manzoni, "A Survey and comparative study of simulators for vehicular adhoc networks", Wireless Communication Mobile Computing, 2009, doi 10.1002/wcm.

[13] B. Mokhtar, M. Azab," Survey on Security Issues in Vehicular Adhoc Networks", Alexandria Engineering Journal, Aug 2015, pp1116-1125.

[14] S. RoselinMary , M Maheshwari ., M. Thamaraiselvan , "Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA)" Proc. IEEE, ICICES, February 2013, doi 10.1109/ICICES.2013.6508250.

[15] A. Sultan , Saif, "A comprehensive survey on vehicular Ad Hoc network." Journal of Networks and Computer Applications,Vol. 37, Jan 2014, pp 380-392.

[16] K. Verma, . H. Hasbullah , A. Kumar , "Prevention of DoS attacks in VANETs" Springer Science, Wireless Personal Communication, Business Media New York, Vol 73, Issue 1, pp 95-126, Nov 2013.

[17] A. Dak, S. Yahya, M. Kassim, "A Literature Survey on Security Challenges in VANETs", International Journal of Computer Theory and Engineering" Vol.4, No. 6, Dec 2012, pp 1008-1010.

[18] P. Sharma, A. Singh, "A Review On Detection and Prevention Techniques Of Denial of Service Attack In Vanet" International Journal of Advanced Research in Computer Science(IJARCS), Volume 6, No. 5, May - June 2015,pp 47-49.

[19] A. Khan, "Minimization of Denial of services attacks in Vehicular Ad hoc networking by applying different constraints" International Journal of Academic Research in Business and Social Sciences July 2013, Vol. 3, No. 7 ISSN: 2222-6990.

[20] C. Rossel, D.Krazewicz ,"Simulation of Urban Mobility (SUMO). German Aerospace Centre, 2007.

[21] MOVE(MObility model generator for VEhicular Networks): Rapid Generation of Realistic Simulation for VANET, 2007

[22] F. Martinez, J. Cano , T. Calafate, P. Manzoni , Citymob: a mobility model pattern generator for VANETs. In IEEE Vehicular Networks and Applications Workshop (Vehi-Mobi, held with ICC), Beijing, China, May 2008.

[23] STRAW - Street Random Waypoint - vehicular mobility model for network simulations (e.g. car networks), 2008.

[24] S. Manvi, M. Kakkasageri, and D. Adiga, "Message authentication in vehicular ad-hoc networks: ECDSA based approach" Proc. Future computer and communications, pp 16-20, April 2009.