iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** III **Month of publication:** March 2018

DOI: http://doi.org/10.22214/ijraset.2018.3241

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Detection and Mitigation of Denial of Service Attacks in VANETs using Packet Detection Algorithm

Sushil Kumar[1], Kulwinder Singh Mann[2]
[1]*Research Scholar, IKG Punjab Technical University Kapurthala, Punjab*
[2]*Professor, Guru Nanak Dev Engineering College, Ludhiana*

Abstract: ***Network connects systems with each other to share information. The computer systems when tied together to share some information makes a network. VANET are special class of MANET. Firstly various types of network have been discussed in the paper then main focus is pervasive network that contains Wireless Mesh Network (WMN), Mobile ad-Hoc Network (MANET) and Vehicular Ad hoc Network (VANET). The main focus in the paper is on various attacks and mainly to Denial of Service (DoS) attack. The literature survey on VANET is given in detail that gives brief idea about VANETs. In this paper different algorithms are used to perform the required task and MATLAB software is introduced to get the required results. By using MATLAB, results are simulated for both existing and proposed technique. Different graphs and tables are created to shoe the results and comparison of the algorithm. Detection of Malicious Vehicles (DMV) and Attached Packet Detection and proposed technique named as hybrid of Malicious Vehicles (DMV) and Detection of Malicious Nodes (DMN), Attacked Packet Detection Algorithm and Malicious and Irrelevant Packet Detection are discussed. The results have been compared and the main parameters are throughput, end delay, packet drop, packet deliver and false positive rate. It concludes that results can be improved using proposed technique.***

Keywords: VANET, MANET, Matlab, DMN, DMV, DoS.

I. INTRODUCTION

The link of more than one system that gives profit to each other is named as a network. The systems tied with each other to communicate and share information to each other. The computer devices that make communication between each other are combined here within this setup. The environment in which number of system are connected with each other to share data and provide benefits to other resources is called a network. The data communication is provided with the help of networking technology. Within the sharing devices there are software and hardware types of resources available [1].

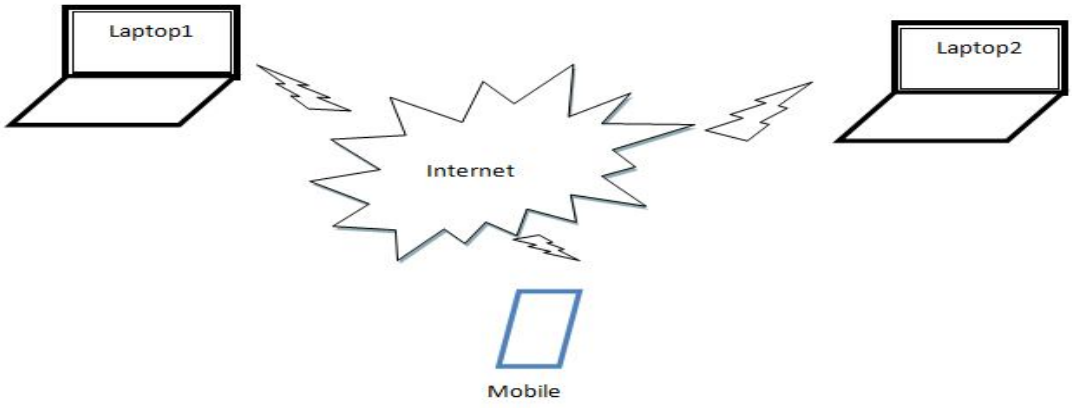


Fig. 1 Representation of computer network

The Fig.1 represents the structure of a computer network. In diagram there are two laptops and one mobile system which all are communicating with each other through the internet. The network can be of two types such as wired networks and wireless types of networks. The wired networks are those0 which utilize wires for providing information amongst each other. The vehicular ad hoc networks (VANETs) are taken as indispensable component. The smart vehicles formed VANETs are special class of mobile ad hoc

networks (MANETs). It is envisioned that in the future vehicles will become smart, in the sense that each vehicle will be equipped with information processing devices (on-board CPU), information collection devices (on-board sensors), on-board display devices as well as wireless communication devices [2].

There are generally two domains in VANETs name as infrastructure domain and ad hoc domain that is based on involved communication nature. The wirelessly communication smart vehicles are formed by ad hoc domain and communication is done with one another (V2V) though dedicated short range communication (DSRC) [3]. The wireless access in vehicular environments (WAVE) technologies each vehicle will periodically broadcast beacons containing like speed, road safety applications support, current location and heading direction like its driving state. In VANETs, a certificate authority (CA) issued security codes are carried by each node that provide security to the network.

II. LITERATURE REVIEW

The literature review of the VANET is discussed below in the form of table. TABLE I shows the survey in which authors have analysed VANET in detail.

TABLE 1
LITERATURE REVIEW

Name of the Authors	Description
Han Yiliang, et. al, (2017) in [10]	The authors have analysed that due to the large scale of networks, easy tracking of mobile devices and freely wireless communication channel in Vehicular Ad hoc Network (VANET) makes it more prone to safety and privacy leakage attack. The attribute based authenticated protocol is motivated by the requirements of security are also presented in the research. In this for verification purpose an attribute scheme was employed and a secret key, messages from RSU to other vehicles has been received securely using signature and signcryption based on attribute. Then on the behalf of group, different attributes with service has been anonymously received by vehicles and even verification is accelerated by applying an attributes scheme. The VANETs secure communication is identified using proposed privacy preserving ABSC technology and different keys are distributed to vehicles according to vehicles different categories that enable different permissions.
Amina Bendouma, et. al, (2017) in [11]	Authors recommended the use of VANET to improve efficiency and safety of transport that has totally changes the vision of road traffic. The human and material losses can be happen due to target for attacks represented by VANET that creates a need of robust security system. In transmission, fluidity and availability has been guaranteed by use of security system that effectively secures a communications between different existing network entities and vehicles. The security scheme has been proposed by authors that uses Elliptic Curve Diffie-Hellman (ECDH) algorithm to ensure RSU identification that shared same secret key to ensure a security between two RSU. In the second section a Elliptic Curve Digital Signature Algorithm (ECDSA) has been used to authenticate the beforehand signing message by vehicle.
Chenyang Yuan, et. al, (2016) in [13]	The authors have studied a Mobility-as-a-Service (MaaS) systems vulnerability to Denial-of-Service (DoS) attacks. The re-despatch process has been model using a queuing theoretical framework that maintains high service availability by operators. The process high potential cyber-attacks as well as service availability has been maintained using it that maintain a model of customer arrival rate. Within a network, a vehicle travelling has been pick up by model at urban area different sections. The MaaS systems DoS cyber attacks has been analyzed by expanding a re-balance model that uses fake reservations or Zombies to control a fraction of the maliciously cars placed in the system. The Zombie work as in a field of computer science where a computer is same like a Zombie that has been accessed for malicious purpose by remote attacker .
Aakash Luckshetty, et.al, (2016)	The authors have represented a Mobile Adhoc Networks (MANETs) subclass i.e., Vehicular Ad hoc Networks (VANET) that helps in providing a remote communication among roadside equipments and vehicles. The car participated may be either hub or remote switch that make a portable system by innovation given by VANET that uses a moving car as a hub. IN commercial as well as industry applications a use of VANET has been found whose main objective is to enhance the passengers' security. In remote communication a lots of importance is given to protection and security as

	VANETs are more prone to disclosure and malicious attacks. The different sorts of security and assaults requirements of VANETS applications have been considered to propose a essential perspective for it. In VANETs protection and security issues has been examined for existing techniques and ended the paper by discussing a different existing challenges and validation schemes in VANETs. The vehicle privacy is considered as a major concern in communication so in order to safeguard for fool proof vehicles driver privacy must be protected.
The Vinh Hoa La, et al, (2014)	The authors have analyzed that VANETs are more prone to attacks that can directly corrupt a networks that leads to losses in terms of money, time and even lives. In order to get knowledge about it they have conducted a review on different attacks in VAMETs along with existing solutions. After this a similar work has been considered carefully and also updated new attacks and categorized them into different classes. As we know that VANETs are the subcategory of Mobile Ad-hoc Network (MANET) that creates an infrastructure for traffic and safety of roads efficiently.
Ujwal Parmar, et al, (2014) [19]	The authors have also presented a comparative study on different VANET attacks. The essential alerts and road safety has been improved by much extent using VANET as emerging technology by enabling inter vehicle communication. In implementing a wireless environment there is need of security as users can be serves as safety and no safety application by Vehicular Ad hoc Network (VANET). There is no as such fixed infrastructure in VANET vehicles due of the reasons that vehicles are nodes with mobility. In VANET, security is becoming a most important concern because both safe and no safe wireless applications are served by it. This has been seen that due to life saving factor a more attention has been gained by automotive industries and researchers.
Irshad Ahmed Sumra, et al,(2010) in [14]	The authors have proposed a different VANET attacks identification and classification solutions. There are large number of attacks that has been generated by attackers in this vehicular network of life saving. They have also proposed five different classes of attacks and every class is expected to provide better perspective for the VANET security. This has been seen that a lot of attention has been gained in the field of VANET in order to improve safety of road and enabled a wide variety of value-added services
Varsha Raghuwanshi, et al, (2015) in [15]	have given a brief review on network availability attacks and its severity levels in VANET environment. In short they have given detail of Denial of Service (DOS) attack, along with that different kind of hybrid Denial of Service attack is also present in it with their existing solutions. Its foundation is based on the co-ordination of vehicles and/or roadside units by which information is disseminated in network in organized way. The lifesaving factor of VANETs makes it more attractive for researchers and automotive industries but the main drawback of it is more prone to time security threats. The main focus behind this research is also providing a security while implementing ad hoc environment and serves users with commercial and safety applications.
K. Deepa Thilak et. al (2016) in [16]	A new approach has been presented that is robust and distributed helps in defending against DoS attacks. The existing consistent IP address information has been used to analyse the malicious vehicles fake identities using proposed scheme. The vehicles announced their presence by periodically exchanging the beacon packets that also make network aware about the next node. The information has been exchanged in their environment where a record of their database has been periodically kept by each node. The similar IP addresses are considered as DoS attacks once they similar IP addresses are observed in the database.

III.FRAMEWORK

In this paper, Matlab software for the implementation of proposed idea is used. Version 2016 has been used to show the results. It is used to calculate the mutual environment and it is prove to be a high level language that used for technical manipulation [23,22]. Tis framework contains a number of inbuilt functions that vary from version to version. These in built functions are used to perform the numerical computation of small and large sizes. It also contains number of toolboxes that also vary from version to version, by updating of new version number of toolboxes increases as well. In this paper author has used this framework for the implementation of a proposed algorithm [20].

IV. THE ALGORITHMS USED FOR THE PERFORMANCE EVALUATION

The Algorithms used for the performance evaluation are discussed below. These algorithms are discussed and their results are explained in the next section:

A. Detection of malicious vehicle (DMV)

The malicious vehicles are detected using this monitoring algorithm and then it is isolated from honest vehicles. The bandwidth is extended for detecting vehicles that helps it in communicating with the Road side units. The vehicles will be considered as malicious one if the vehicle bandwidth exceeded then the network which is the threshold level. This process is detected during packets transmission by the road side units [28].

In DMV algorithm used three concepts has been defined in this:

1) Abnormal behaviour: In network packets are duplicated or drop by vehicles is meant by abnormal behaviour that results in abolish of personal aims based messages or other vehicles are misled.

2) Honest (normal) vehicles: The right messages are generated or correct normal behaviour messages are forwarded using vehicle in case of vehicle having normal behaviour.

3) Malicious vehicles: If the abnormal behaviour of vehicle V is repeated in such a way that Td of V becomes greater than threshold value σ, vehicle V will be called a malicious vehicle. The parameter Td represents the distrust value of behaviour of vehicle V when it forwards messages.

B. Attacked Packet Detection Algorithm

The certain vehicles position is deal using it for transferring a packet to the communication media or road side units. In communication something went wrong when there is rapid change in vehicle speed and frequency of transferring the packet to the road side units. The road side unit's detection the packet locations.

Algorithm:

1) The requirements for position changing are the basis of these requirements. The below given parameters are used to identify attacked packets:

2) The road characteristics determined velocity (v), frequency (f) and alpha.

3) The maximum speed is denoted by VMax, The per second broadcasted number of packets is denoted by frequency (f).

4) The following conditions are used to identify a attacked packets. There is quick change in position due to which V and F are high. If vehicle position will not change quickly then its V and F will be low.

INPUT: Position changing the requirements velocity V, α coefficient, Vmax is the maximum speed and request R.

OUTPUT: V is high and f is high representing attacked packets or invalid request. Otherwise V is low and f is low representing to detect the attacked packets [26].

C. Detection of malicious nodes

In threat detection, this is considered as one of the main procedure in VANET network. The networks decision making scenario is used in this process for the vehicle which shows the standard deviations of the vehicles to communicate the vehicles message passing to the road side units. If there is increase in bandwidth as well as standard deviations then road side units is used to detect such type of malicious vehicles. This causes degradation in operation of VANET.

D. Detection of Malicious Nodes in Vehicular Ad-hoc Networks (DMN) Algorithm

The information generator node in a VANET communication is act as source. The message destination is act by another node and there are relay nodes which are other intermediate nodes between destination and source. The behaviour of nodes is monitored by verifiers or trustier vehicles when a relaying node role is played by vehicular node (VN). The VN received number of packets is checked when VU vehicle works as a VN verifier. Those parameters are represented by:

1) number of packets that VN drops or duplicates as detected by VU (represented by parameter

2) After a particular time has elapsed PL, if vehicle VN does not send forward a received packet or sends its multiple copies, it is considered as abnormal behaviour by verifier VU and hence increases the value of parameter b by 1 unit.

The algorithm for DMN is givn below:

DMN algorithm:

a) Step 1: Vehicle VN joins the vehicular network

b) Step 2: Obtained the cluster keys

c) Step 3: Compute the parameters – Distance, load and distrust value for the nodes in area of VN for verifier selection.
d) Step 4: Decision parameter is given as:

DP. DP= W1* LD + W2 *DV + W3 * DS

Where W1 +W2 +W3 =1. W1, W2, W3 are weight factors for Distance, load and distrust value.

e) Step 5: Find DP <TVS i.e decision parameter value less than selection threshold.
f) Step 6: Distribute nodes that are obtained by step 5 to recently joined vehicle VN
g) Step 7: Verifiers monitors the behavior of recently join vehicle VN.
h) Step 8: If VN shows abnormal behavior then go to step 9 else step 7
i) Step 9: Calculate the new distruct value (DV)of VN
j) Step 10: If DV is less than or equal to detection threshold ,then update white list go to 7 else goto 11
k) Step 11: All nodes receive warning messages.
l) Step 12: In blacklist update the VN Vehicle entry.
m) Step 13: Isolate the detected malicious vehicle from the network.

V. RESULTS AND DISCUSSIONS

The results of the simulations of the approach are discussed below. Different parameters like throughput, end delay, packet drop, packet deliver and false positive rate are shown by using graphs:

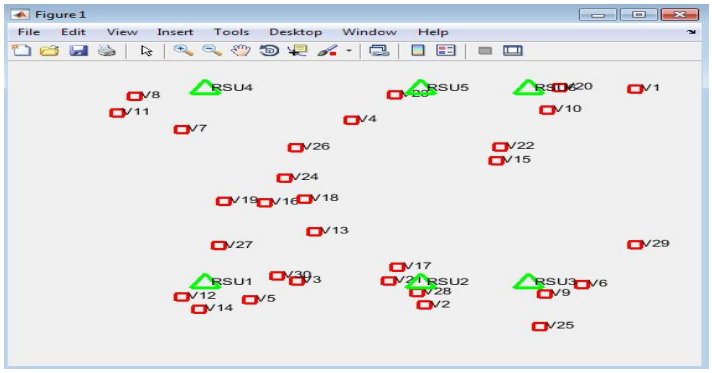


Fig. 1 VANET network

In figure 1, shows the VANET networks are created in which:

1) Vehicular nodes are developed in random fashion and
2) For communication purposes a road side units are deployed among vehicular modes.

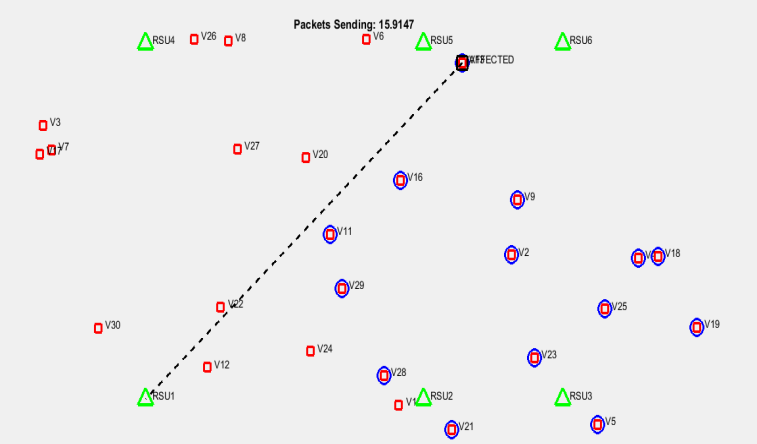


Fig. 2 Packet transmission

The above shown figure 2, gives packet communication between road side unit and vehicle node and transferring affected vehicle to road side units are also shown in it.

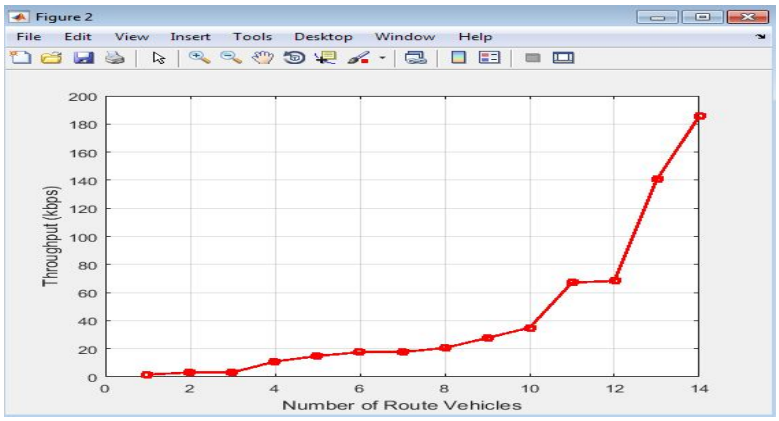


Fig. 3 Throughput of the network

The above figure 3 shows the throughput of the network in kbps which is termed as kilo-bits per second with respect to the route vehicles through which the packets is transmitted through the networks. The throughput of the network increases which shows that the successful packet are delivered.

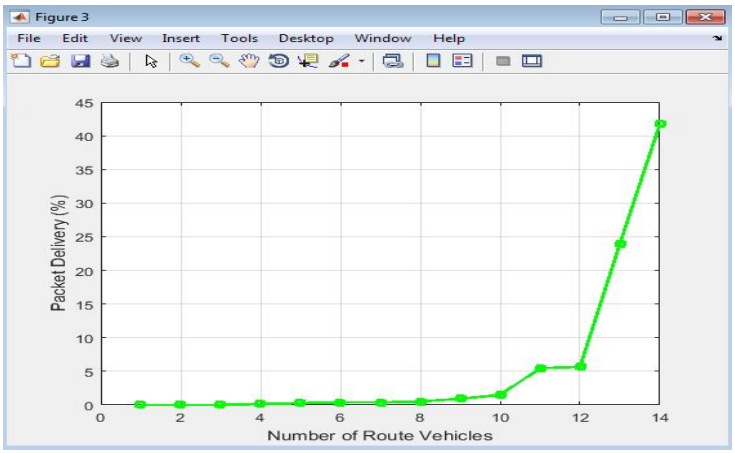


Fig. 4 Packet delivery (%)

In the figure 4 the packet delivery of the network has been shown that gives 43% of the successful delivery of total packets through nodes of vehicle for the successful communication of the network in the VANET systems.

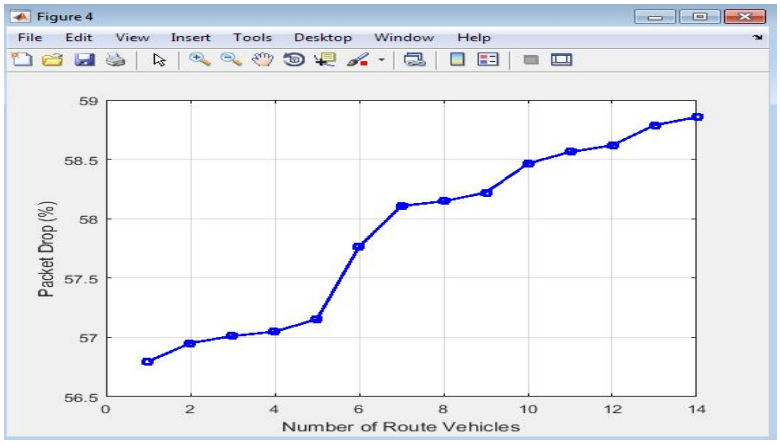


Figure 5: packet drop ratio

In figure 5, the packet drop ratio has been shown that gives packet drop and losses by the vehicles to the road side units. In case of having high delivery of the packets a low packet drop should be here.

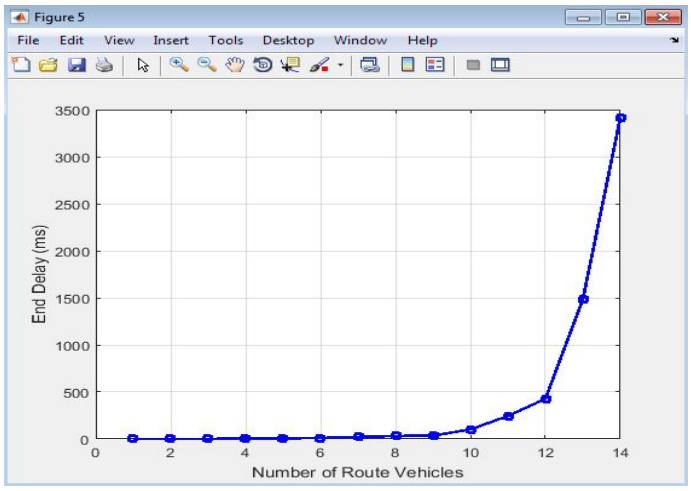


Fig. 6 End delay (ms)

In figure 6, the end to end delay from source to destination has been shown and in case of high rate of communication it should be low. In figure 6, it has been depicted that in the network a 3200 ms is achieved and then a hybrid approach has been used to further reduce it.

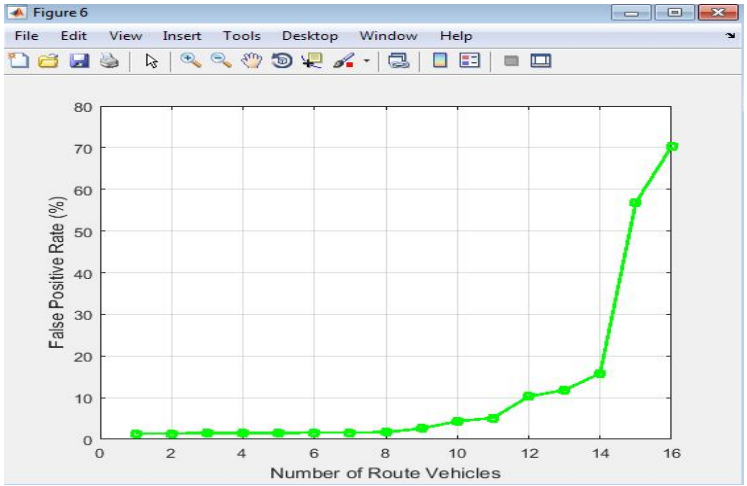


Fig. 7 False Positive Rate (%)

In figure 7, a false positive rate in precent has been shown which are error rates that states by how much amount a VANET system are able to reject right things. In case of high efficient systems it must be low and results show that a 70 percent of false positive rates have been achieved by systems.

Hybrid approach results

The hybrid approach deals with the hybridization of Detection of Malicious Vehicles (DMV) and Detection of Malicious Nodes (DMN) to detect the malicious nodes responsible for DoS attacks and the hybrid approach for Attacked Packet Detection Algorithm and Malicious and Irrelevant Packet Detection Algorithm to mitigate the effect of DoS attacks. The results are discussed below

Fig. 8 Detected malicious vehicles

The above figure shows the detection of the malicious vehicles which shows the ids of the vehicles that are responsible in evaluating the packets transferring from source to the destination

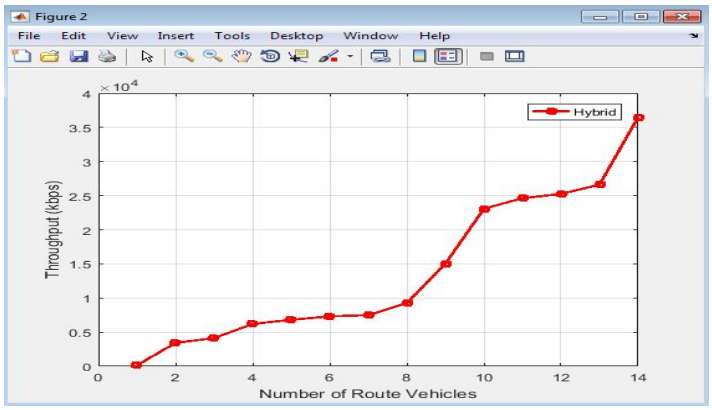


Fig. 9 Throughput of the network (Hybrid)

The figure 9 shows the throughput of the network using hybrid approach which shows that the hybrid is performing better than our first approach which shows the throughput in kilo-bits per second and increasing as the route nodes increases which must be high for the efficient VANET systems

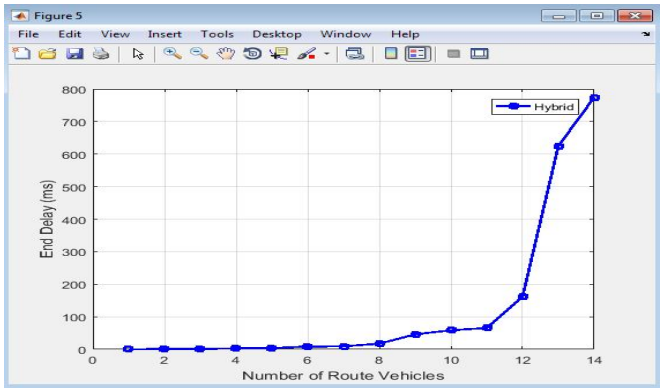


Fig. 10 End Delay (Hybrid)

The figure 10 shows the end to end delay of the VANET network and shows that the delay must be low for the high deliveries of the packets and shows that the packets are taking less delay in our hybrid approach.

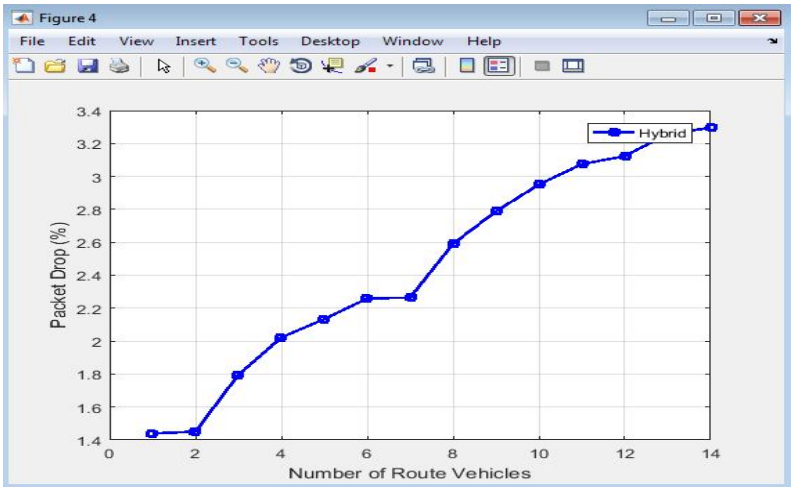


Fig. 11 Packet drop ratio (Hybrid)

The figure 11 shows the packet drop ratio which must be low for the loss of the packets and shows that our proposed approach is able to achieve less packet drop in the VANET system. This must be low which shows that the packet losses are decreasing in an efficient manner

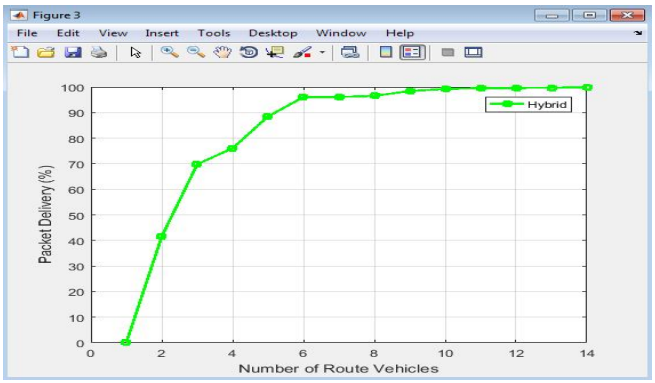


Fig 12 Packet delivery (Hybrid)

The figure 12 shows the packet delivery rate which must be high for the successful delivery of the packets from the source to the destination. This performance parameter must be high for the less loss of the packets and shows the successful delivery of the packet form the route vehicle to the road side unit (RSU).

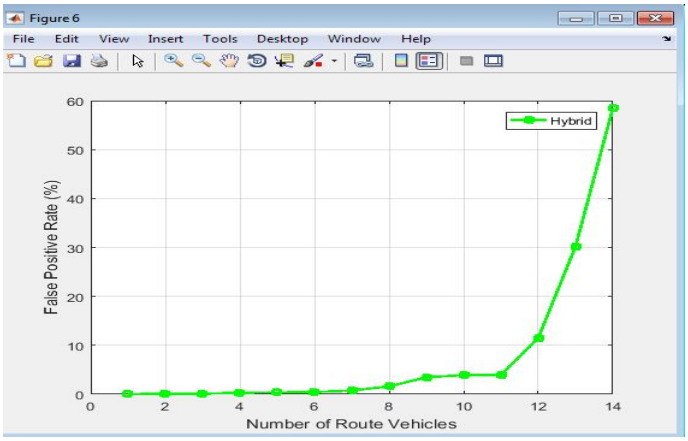


Fig. 13 False positive rates

The figure 13 shows the false positive rate in percent which are the error rates that how much your VANET system are able to reject right things which must be low for the high efficient systems and shows the hybrid approach is having less false positive rates which must be low.

TABLE II
COMPARISION TABLE

Parameters	Detection of Malicious Vehicles (DMV) + Attacked Packet Detection	Malicious Vehicles (DMV) and Detection of Malicious Nodes (DMN) + Attacked Packet Detection Algorithm and Malicious and Irrelevant Packet Detection
Throughput (kbps)	180	4×10^4
End Delay (ms)	3400	800
Packet Drop (%)	58	3.3
Packet Delivery (%)	43	98
False Positive Rate (%)	70	58

This is a comparison table that gives results for existing technique i.e., Selection of Malicious Vehicles (DMV) and Attached Packet Detection and another proposed one name as hybrid of Malicious Vehicles (DMV) and Detection of Malicious Nodes (DMN),

Attacked Packet Detection Algorithm and Malicious and Irrelevant Packet Detection. The results have been compared in terms of throughput, end delay, packet drop, packet deliver and false positive rate.

Result Performance with different number of vehicles in the VANET Network

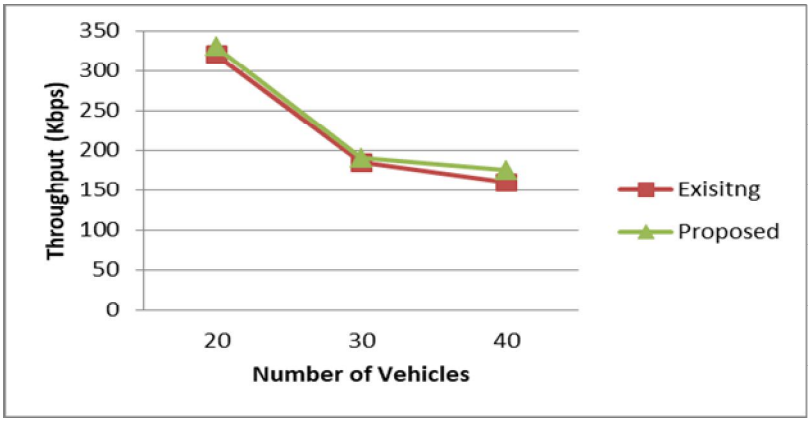


Fig. 14 Throughput Comparisons (Different Vehicles)

TABLE III
THROUGHPUT COMPARISON TABLE

Number of Vehicles	20	30	40
Existing	320	185	160
Proposed	330	190	175

Table II. shows the throughput comparison of existing and proposed algorithms.

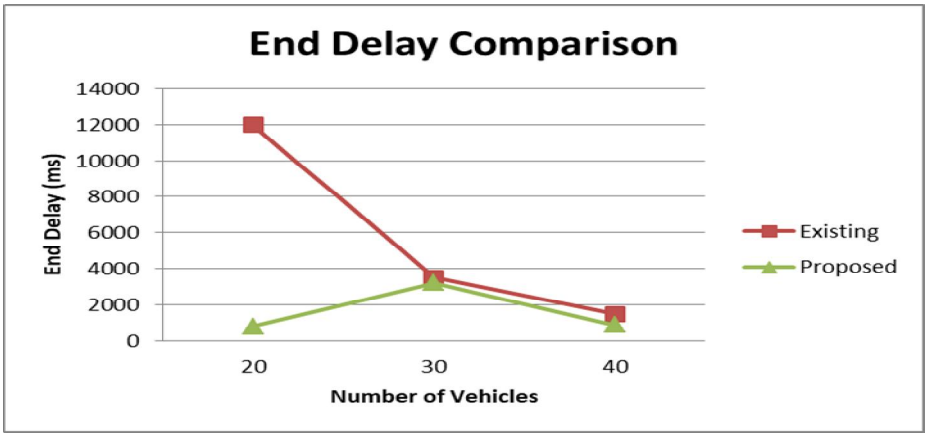


Fig. 15 End Delay Comparison

TABLE IV
END DELAY COMPARISON TABLE

Number of Vehicles	20	30	40
Existing	12000	3500	1500
Proposed	800	3200	900

The TABLE IV gives comparison result for existing and proposed technique in terms of End Delay and it shows that use of the proposed technique reduces the End delay that makes use of hybrid proposed technique desirable.

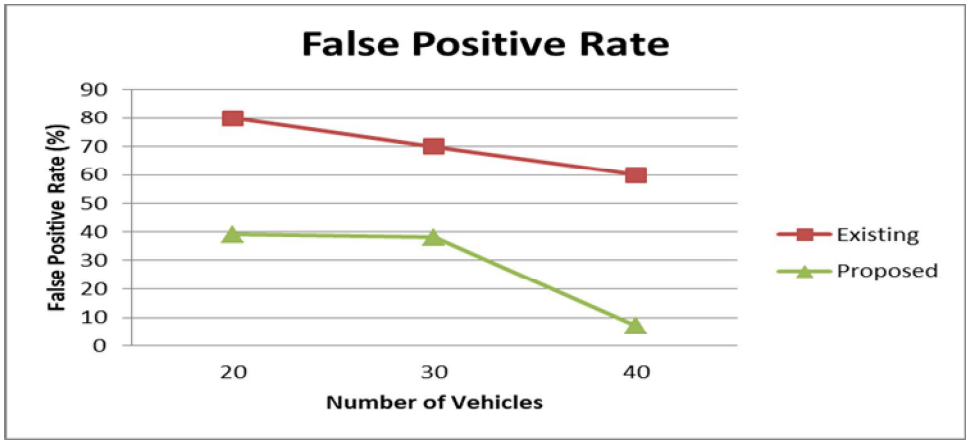


Fig. 16 False Positive Rate Comparison

TABLE V
FALSE POSITIVE RATE COMPARISON TABLE

NUMBER OF VEHICLES	20	30	40
EXISTING	80	70	60
PROPOSED	39	38	7

The TABLE V gives comparison result for existing and proposed technique in terms of False Positive rate and it shows that use of the proposed technique reduces the False positive rate which is desirable.

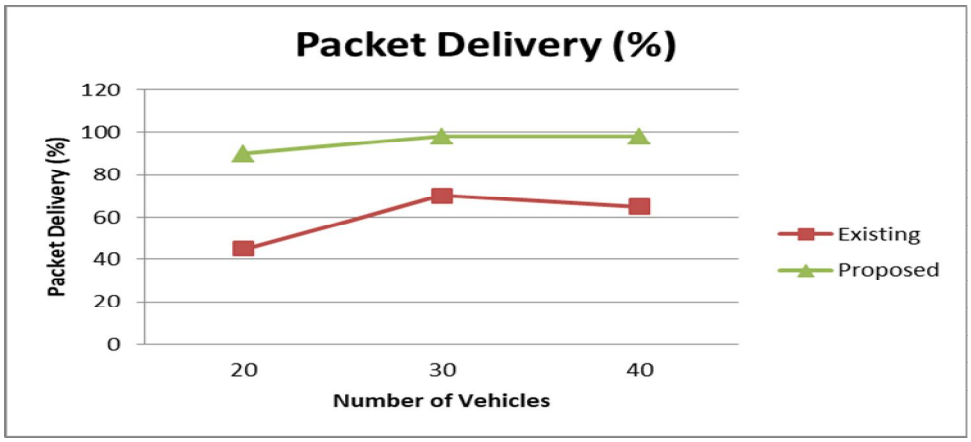


Fig. 17 Packet Delivery Percentage

TABLE VI
PACKET DELIVERY RATE COMPARISON TABLE

Number of Vehicles	20	30	40
Existing	45	70	65
Proposed	90	98	98

The TABLE 6 gives a comparison result for existing and proposed technique in terms of Packet delivery rate and it shows that use of proposed technique increase in number of delivered packets.

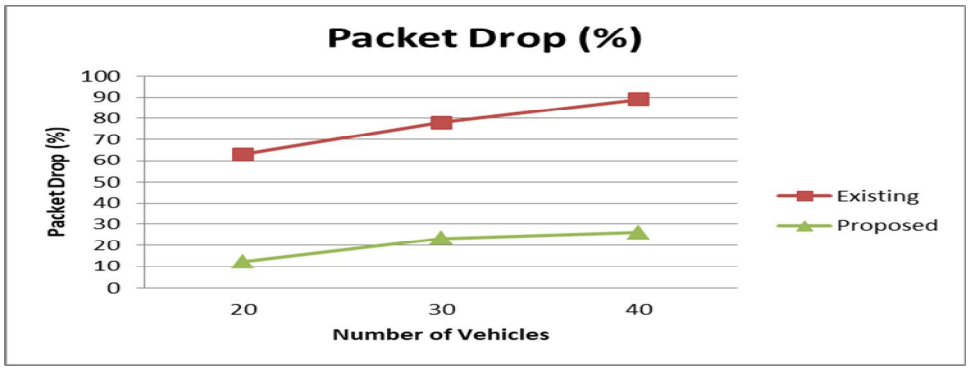


Fig. 18 Packet Drop Comparison

TABLE VII
PACKET DROP COMPARISON TABLE

Number of Vehicles	20	30	40
Existing	63	78	89
Proposed	12.12	23.19	26

The TABLE 7 gives comparison result for existing and proposed technique in terms of Packet drop and it shows that use of proposed technique reduces the drop in packets.
The overall results of existing and proposed techniques gives improved results in terms of throughput, end delay, packet drop, packet deliver and false positive rate.

VI. CONCLUSION

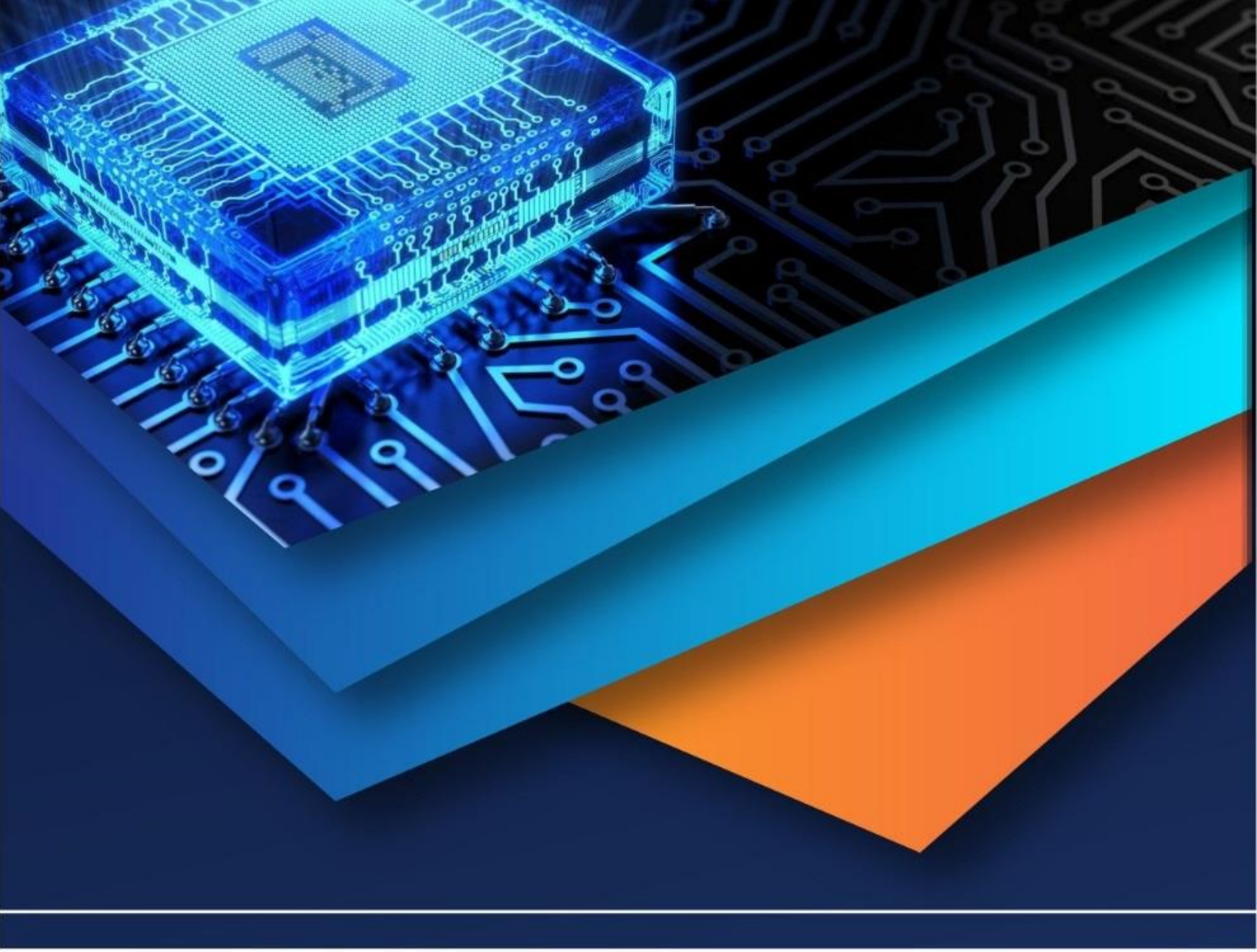
A lot of attention has been gained by VANETs as it helps in improving driving conditions as well as roads safety. The detection of misbehavior in VANETs can be hazardous that makes this task very significant. Since the security in the networking, can be consider as a major concern, protecting the operating system of VANET by detecting a DoS attack was the center of this doctoral thesis. In our work, DoS attack early detections considered as crucial point as by the occurrence of attack whole network can become unreachable. As stated, this doctoral thesis mainly focuses to Denial of Service (DoS) attack in VANET.
Firstly different types of network have been defined then main focus is given to pervasive network that includes Wireless Mesh Network (WMN), Mobile ad-Hoc Network (MANET) and Vehicular Ad hoc Network (VANET). The challenges and issues of VANET is given. The main motivation behind this thesis is given to different attacks and mainly to Denial of Service (DoS) attack. The VANET model, its settings and system architecture or working of VANETs is given in detail that gives brief idea about VANETs. This chapter is ended with Vehicular network challenges and need for security along with brief discussion of DoS attack. After this a literature review of VANET is discussed in details and MATLAB is used for simulating all the work of this paper. A comprehensive literature survey is given about the security threats to VANETs which shows that it needs to be improved. The whole literature survey includes a different paper that defines various types of attacks included in VANETs. The different detection method review is also included in this chapter. The main focus is given to DoS affects and its detection method. It has been found that DoS attacks are more difficult to detect, as VANETs are unreliable in nature and also due to their high mobility.
A dissemination method is started with various research gap of this paper. After this different steps are performed to complete that stated research work. At the end different used algorithm to perform the required task and brief introduction to MATLAB software used to obtain the required results.
Detection of Malicious Vehicles (DMV) and Attached Packet Detection and another proposed one name as hybrid of Malicious Vehicles (DMV) and Detection of Malicious Nodes (DMN), Attacked Packet Detection Algorithm and Malicious and Irrelevant Packet Detection are analyzed. The results have been compared in terms of throughput, end delay, packet drop, packet deliver and false positive rate. It shows that improved results can be improved using proposed technique.

VII. 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] J. Hoebeke, I.Moerman, B. Dhoedt and P. Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges," IJSER, vol. 23, pp. 231-238, 2005.
[2] L. ZHOU,Z. HAAS, "Securing Ad Hoc Networks. IEEE Network," vol. 13, pp. 24-30, 1999.
[3] N. Raza, M.Umar , M. Qasim , O. Ashraf, M. Irfan, "Mobile Ad-Hoc Networks Applications and Its Challenges," Communications and Network, vol. 12, pp. 131-136, 2016.
[4] G. Ding and B. Bhargava, , "Peer-to-peer File-sharing over Mobile Ad hoc Networks", Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW'04), vol. 6, pp.1-5, 2005.
[5] C.Penkins et al., "DSDV Routing over a Multihop Wireless Network of Mobile Computers," vol. 12 , pp. 53–74,2001.
[6] C. Siva Ram Murthy, B.S. Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols," Prentice Hall PTR, New Jersey, USA,pp-222-245, 2004.
[7] D. Chayal, V. Singh Rathore, "Assessment of security in mobile ad-hoc networks (MANET)," vol 2, pp.137-139, 2009 .
[8] I. Kaur, N.. Kaur, "Challenges and Issues in Adhoc Network," International Journal of Computer Science And Technology (IJCST), vol. 7, pp.63-65, 2016.
[9] Y. hu, A. Perrig, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Wireless Networks Springer Science + Business Media, vol. 11, pp.21-38.2005.
[10] S. Sharma, R. Kumar Bansal, S. Bansal, "Issues and Challenges in Wireless Sensor Networks," IEEE International Conference on Machine Intelligence Research and Advancement, vol. 4, pp.58-62, 2013.
[11] S.M. Chen, P, Lin, D¬W Huang, S¬R Yang, "A study on distributed/centralized scheduling for wireless mesh network," in Proceedings of the 2006 International Conference on Wireless Communications and Mobile Computing, vol. 5, pp 599-604, 2006,.
[12] A. Pirzada, M. Portmann, "Wireless Mesh Networks for Public Safety and Crisis Management Applications", IEEE Internet Computing, vol. 12, pp. 18-25, 2008.
[13] I. Chlamtac, M. Conti, and J. Liu, "Mobile Ad Hoc Networking: Imperatives and Challenges," Ad Hoc Networks, vol.1, pp. 13–64, 2003.
[14] S. Eichler, "Security Challenges in MANET-based Telematics Environments," In Proceedings of the 10th Open European Summer School and IFIP WG 6.3 Workshop, vol. 3, pp. 210-218, 2004.
[15] J. Hoebeke, I. Moerman, B. Dhoedt, and P. Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges," The Communications Network,vol. 3, pp. 45-53, 2003.
[16] "FCC Report and Order, "Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz Band," vol. 2, pp. 12-20,2003.
[17] V. Rai, F. Bai, J. Kenney and K. Laberteaux, "Cross- Channel Interference Test Results: A report from the VSCA project," IEEE 802.11 Task Group p report, vol. 4, pp. 234-240, 2007.
[18] H. Moustafa , Y.Zhang, "Vehicular networks: Techniques, Standards, and Applications," CRC Press, vol. 12, pp. 42-50, 2009.
[19] M .Raya, P. Papadimitratos, JP. Hubaux, "Securing Vehicular Communications," IEEE Wireless Communications, vol. 13, pp. 123-131, 2006.
[20] B. Parno and A. Perrig, (2005), "Challenges in Securing VehicularNetworks," Proc. of HotNets-IV, vol. 21, pp. 320-328, 2005.
[21] P. Tyagi, D. Dembla, "Investigating the Security Threats in Vehicular ad hoc Networks (VANETs): Towards Security Engineering for Safer on-road Transportation," 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 523-529, 2014.
[22] J. Hubaux, S. Hapkun and J. Luo, "The Security and Privacy of Smart Vehicles," Magazine of IEEE Security and Privacy, vol. 7, pp. 1023-1031.
[23] S. Al-Sultan, "A comprehensive survey on vehicular Ad hoc network," Journal of Network and Computer Applications, vol. 3, pp. 232-239, 2004.
[24] H.Hasbullah, "Denial of Service (DOS) and its possible solutions," World Academy of Science, vol. 4, pp. 15-25, 2010.
[25] R. Gilles Engoulou, "VANET security survey," Computer Communications, vol. 44, pp. 1-13, 2014.
[26] Q. Liu, "A hierarchical security architecture of VANET. University of Armed Police Force," vol. 5, pp. 21-29, 2013.
[27] S. Zeadally, R. Hunt, Y. Chen, A. Irwin, A. Hassan, "Vehicular Ad Hoc Networks (VANETs): Status, Results, and Challenges," in Telecommunication Systems, vol. 50, pp 217-241, 2012.
[28] I.Ahmed S. Iftikhar Ahmad, H. Hasbullah, "Classes of attacks in VANET," in Tenth International Conference on Wireless and Optical Communications Networks (WOCN), vol. 5, pp 1 – 5, 2013.
[29] A. kahtani, A. Kharj, "Survey on security attacks in Vehicular Ad hoc Networks (VANETs)," in 6th International Conference on Signal Processing and Communication Systems (ICSPCS), vol. 4, pp 1 – 9, 2912.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY