Efficient Technique For of Enhancing The Safety And Efficiency of Ground Transportation Networks

Mr. Raj Kumar[1], Mr Rahul Gaba[2]
[1, 2] Dept of Computer Application
[1, 2] Chandigarh Group of Colleges Landran

Abstract- *Intelligent Transport Systems (ITS) are designed in order to ensure the security of users within the vehicle-specific applications. The users communicate with each other in order to exchange important information which can avoid any kind of losses. There are various applications of the ITS which are also related to the Vehicle Transportation. For the purpose of enhancing the safety and efficiency of ground transportation networks, real-time information is required for which the Vehicular Ad hoc Networks (VANETs) were introduced.*

Keywords- Intelligent Transport Systems, Vehicular Ad hoc Networks, security

I. INTRODUCTION

A type of self-configuring network that supplies vehicle to vehicle and vehicle to road communications is known as an ad hoc vehicle network. The information is distributed on the network through the nodes that are represented as servers or clients. The computerized system comprises various components, such as computers, communications, and management technologies, as well as sensors and control innovations. The operation of a transport system can be improved by integrating these functions. Warnings regarding environmental hazards, traffic and road conditions and the transmission of local information among vehicles are provided using VANETs. If there is such a condition where there are traffic jams, road closures or accident accidents, the information may be spread across the network. This could help drivers avoid specific routes as well as save time. Vehicles spread warnings on other vehicles by appropriate communication [1].

II. PROPOSED WORK

In this research paper, propose the technique that can detect and isolate the harmful nodes in the network that are responsible for triggering the DDOS attack. DDOS attack is denial of the type of service attack in which the malicious node can select some of the nodes that can flood the victim's node with raw packets. In this paper, the mutual authentication technique is proposed for detecting harmful nodes in the network. Nodes that are unable to prove their identity will be detected as harmful nodes in the network.

III. OBJECTIVES

Following are the various research objectives:-

1. To study various security vulnerabilities of vehicular Adhoc network and existing schemes to handle it.
2. To propose a novel techniques for detection of DDOS attack in VANETs.
3. To implement the proposed scheme using simulation.
4. To compare the proposed scheme with the some of existing scheme in terms of throughput, packet delivery ratio and routing overhead.

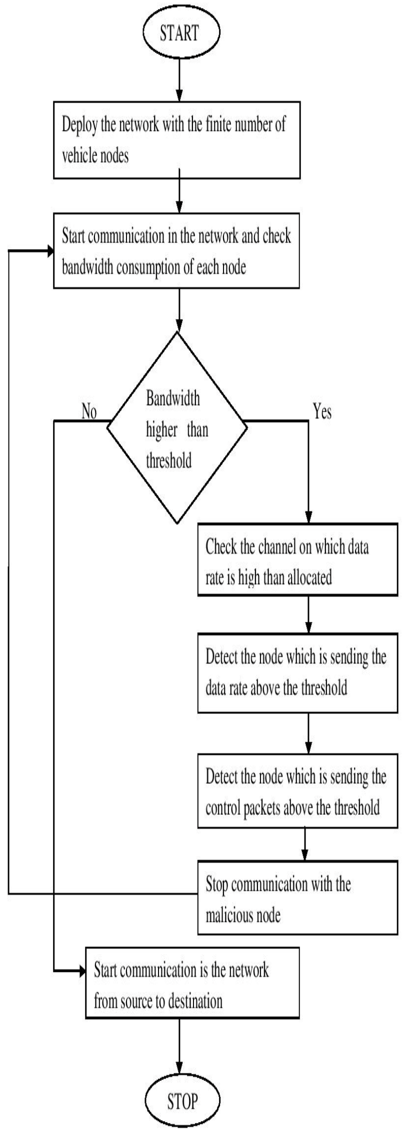
IV. IMPLEMENTATION STRATEGY

In this paper, we propose the technique that will detect the harmful nodes in the network and will detect the harmful nodes by following the steps to be followed: -

1. In the first step, the network will be implemented with the finite number of nodes of the vehicle. . The fixed bandwidth will be allocated to each node of the vehicle in the network.
2. The roadside units will begin to analyze the bandwidth consumption of each node of the vehicle, and the node that will use the bandwidth above the allocated value will be the harmful node.
3. In the third stage, the roadside units will check the type of packets that the node using bandwidth sends over the allocated value. When the node sends the data packets to the victim's node, it may be the malicious node.
4. In the last step, the nodes that will send the harmful data packets, if that node will receive control packets from any node, then that node will be detected as the malicious node that will be responsible for triggering the DDOS attack.

V. PROPOSED ALGORITHM

The technique is proposed in this research paper for the detection and isolation of harmful nodes in the network. Harmful nodes are responsible for triggering the DDOS attack on the network. The proposed technique is based on two types of messages which are data packets and control packets. Vehicles and road side units are responsible for detecting harmful nodes in the network. DDOS attack is the special type of attack in which the harmful nodes select the nodes that flood the victim's node. Nodes that do not represent a small maximum number of packets in the network and nodes that flood the maximum number of packets are selected as IDS nodes. IDS nodes detect harmful nodes. When the network flow has been reduced to the threshold value, then the technique of monitoring mode is applied in which each node follows its adjacent node. The node that sends data packets above the threshold value is marked as harmful nodes. At the same time, if the nodes marked as malicious receive control packets, the nodes that send control packets are marked as harmful nodes. The proposed technique does not require additional hardware or software to detect harmful nodes in the network.


START
Deploy the network with the finite number of vehicle nodes
Start communication in the network and check bandwidth consumption of each node
Bandwidth higher than threshold
No
Yes
Check the channel on which data rate is high than allocated
Detect the node which is sending the data rate above the threshold
Detect the node which is sending the control packets above the threshold
Stop communication with the malicious node
Start communication is the network from source to destination
STOP

5.1 ISOLATION ALGORITHM

```
Input: Sensor node, malicious node
Output: Secure path establishment
1. The network is deployed with the finite number of sensor nodes
2. The source flood route request messages in the network
3. Check the round trip time by sending and receiving route request, reply messages in the network
4. if source receive route reply from malicious nodes
        Discard the route reply
        If the route trip time is high
        Discard the route reply
Else
Process the request
5. Select the path from source to destination on the basis of hop count and sequence number
        If malicious node exists in the path
        Discard path
        Else
Process the path for data transmission
```

VI. RESULT AND DISCUSSION

An open-source simulator that provides substantial support for routing using multicast and IP protocols is known as Network Simulator

This simulator runs on similar Unix operating systems. There are several benefits to using this simulator. More protocol numbers are supported by it, and network traffic is graphically detailed here. In addition, to perform queuing and queuing, different algorithms are supported by this tool. The routing algorithm accepts the directing and broadcasting of the local network. Other algorithms, such as the right tail, the round faucet, and the first one are also executed by the standby algorithm.

In the late 1990s, NS2 was introduced as a variant of the REAL network simulator. The dynamic behavior of the flow and congestion control mechanisms within the packet switched data networks was evaluated using the REAL network simulator.

A simulated program known as VINT (Virtual Internetwork Test-pat) is responsible for introducing NS2. Several MAC layer protocols, routing, and multicasting protocols are supported by Transmission Control (TCP) and User Datagram Protocol (UDP) simulations. The simulation is stored in the track files based on the user's requirement. Based on the different components, the tracking files are fed as input. The following are the two major components of this tool:

1. To generate a simulated scenario, use the NAM (.nam) file.
2. To generate graphical results using a component known as graph X, a trace file (.tr) is used.

VII. IMPLEMENTATION

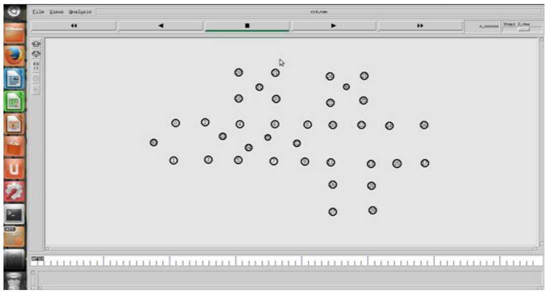


Fig 7.1: Deployment of network

As shown in figure 4.1, the vehicular adhoc network is deployed with the finite number of vehicle nodes. In the network road side units are deployed which will pass the sensed information to the vehicle nodes

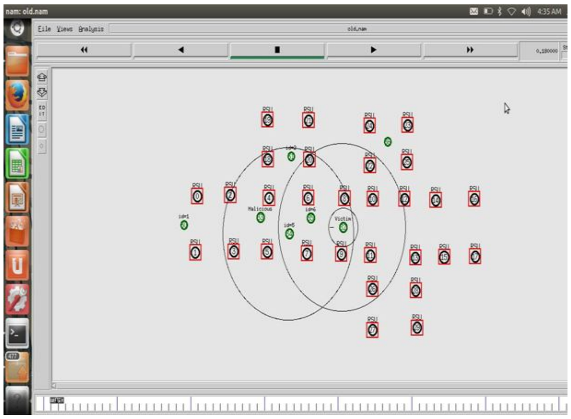


Fig 7.2: Communication in the network

As shown in the figure 7.2, the network is deployed in which vehicle nodes can communicate with each other. The malicious nodes select its victim nodes which trigger attack on the legitimate node

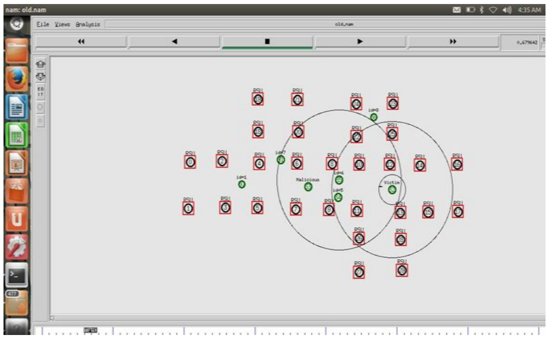


Fig 7.3: Trigger of attack

As shown in figure 4.3, the malicious node selects its victim node which triggers attack on the victim node. This leads to reduction in network throughput, increase delay and packet loss

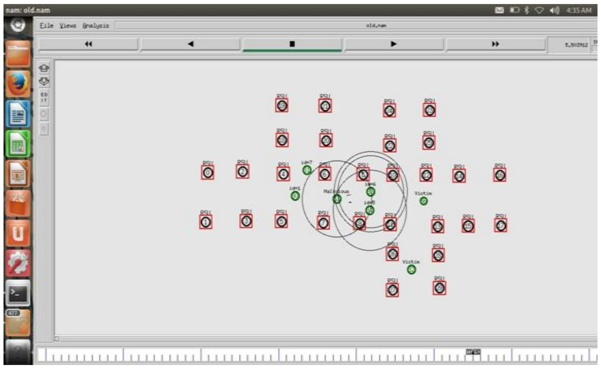


Fig 7.4: Attack Scenario

As shown in figure 7.4, the malicious node selects its victim node which triggers attack on the victim node. This leads to reduction in network throughput, increase delay and packet loss

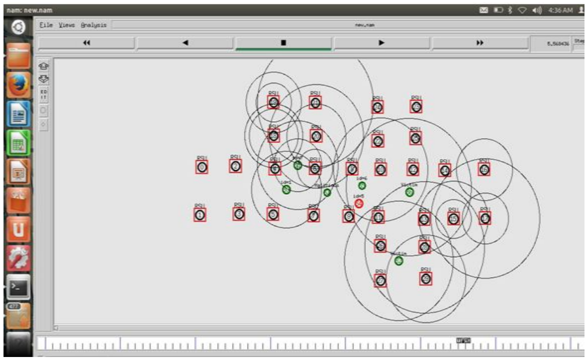


Fig 7.5: Marking of nodes which are sending data packets

As shown in figure 7.5, the malicious node selects its victims which will flood the network with the rouge data packets. The bandwidth is allocated to each node and node which is using above allocated bandwidth will may be the malicious node.

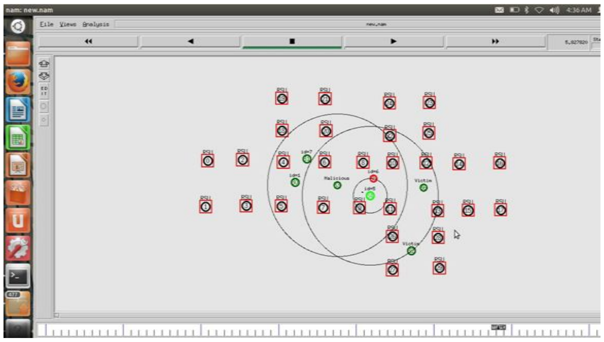


Fig 7.6: Marking of nodes which are sending control packets

As shown in figure 4.6, the node which is sending the data packets above the threshold values will be the malicious node. In this figure the node is detected which send data packets.

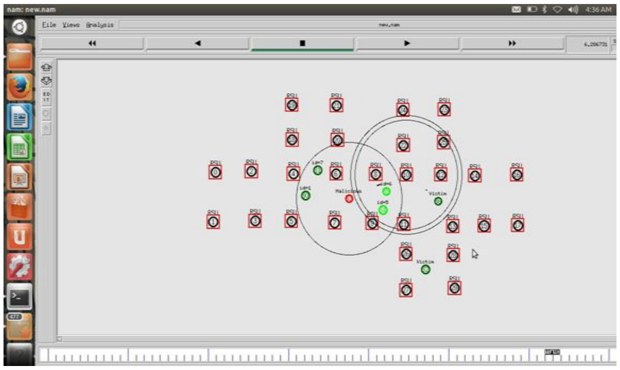


Fig 4.7: Isolation of malicious nodes

As shown in figure 4.7 the node which is sending the data above the threshold value will be detected as the malicious node.

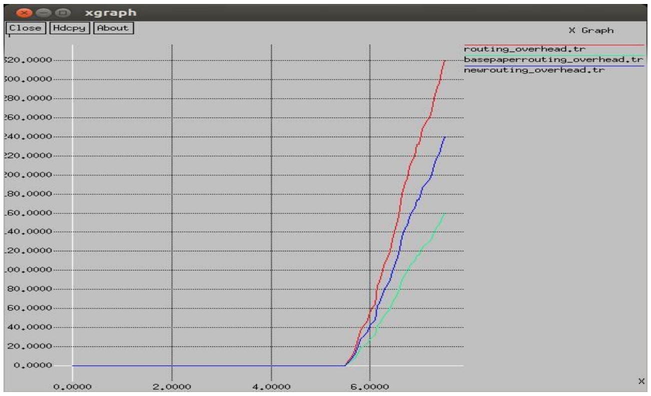
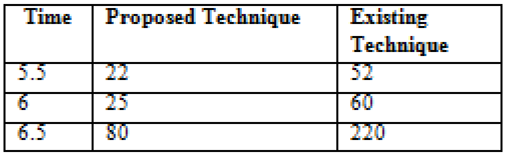


Fig 7.8: Routing overhead

As shown in figure 7.8, the routing overhead is compared between the existing technique, proposed technique and when the attack is triggered in the network.

Table 7.1: Routing Overhead



Time	Proposed Technique	Existing Technique
5.5	22	52
6	25	60
6.5	80	220

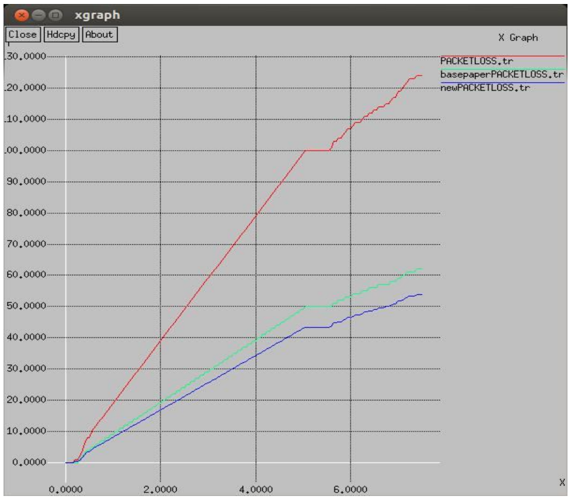


Fig 7.9: Packet loss

As shown in figure 7.9, the packet loss of the proposed, existing and attack scenario is compared and it is been analyzed that packet loss of the proposed technique is minimum as compared to other scenarios.

Table 7.2: Packet loss Comparison

Time	Proposed Technique	Existing Technique
5.5	40	90
6	45	120
6.5	55	220

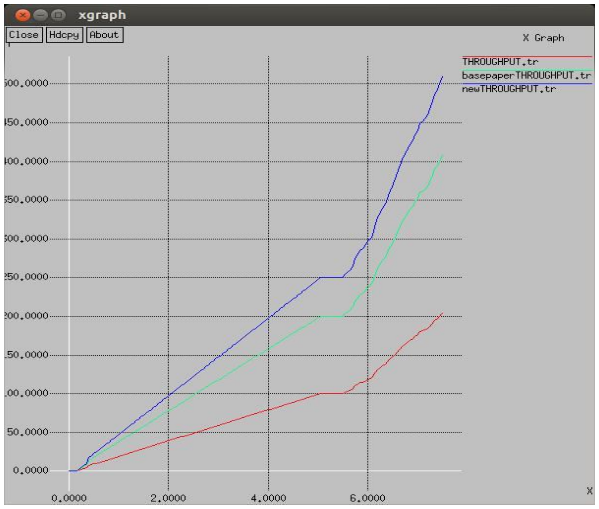


Fig 7.10: Throughput

As shown in figure 7.10, the throughput of the proposed, existing and base paper technique and it is been analyzed that network throughput of proposed technique is maximum due to isolation of DDOS attack.

Table 7.3: Throughput Comparison

Time	Proposed Technique	Existing Technique
5.5	220	100
6	300	120
6.5	500	220

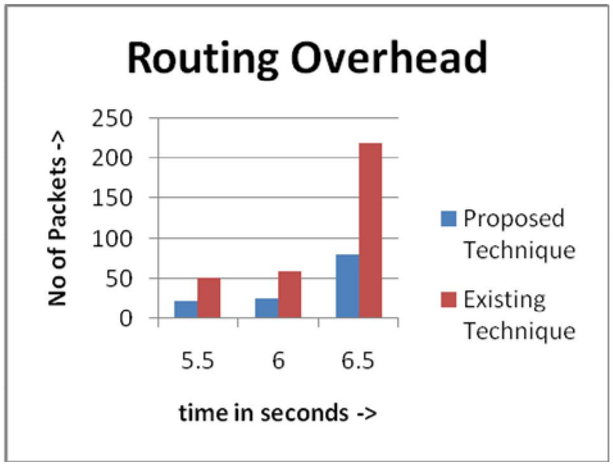


Fig 7.11: Comparison of Routing Overhead proposed vs existing technique

As shown in figure 7.11, the routing overhead of the proposed and existing technique is compared for the performance analysis. It is analyzed that due to occurrence of DDOS attack in the network, the routing overhead is quite high. When the malicious node detect from the network, the routing overhead is reduced in the network

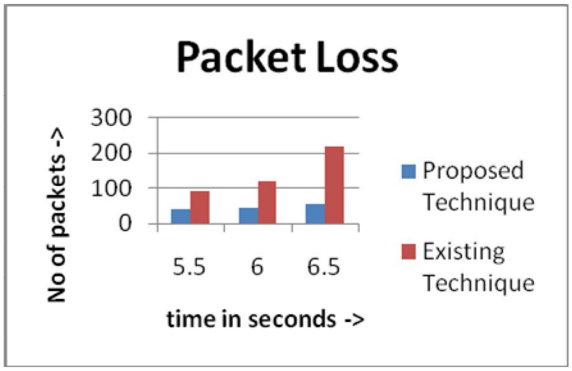


Fig 7.12: Comparison of Packet loss proposed vs existing technique

As shown in figure 7.12, the packet loss of the proposed and existing algorithms is compared for the performance analysis. Due to occurrence of DDOS attack in the network, the packet loss is high and when the malicious nodes are detect from the network, the packet loss is reduced and efficiency of the network is increased

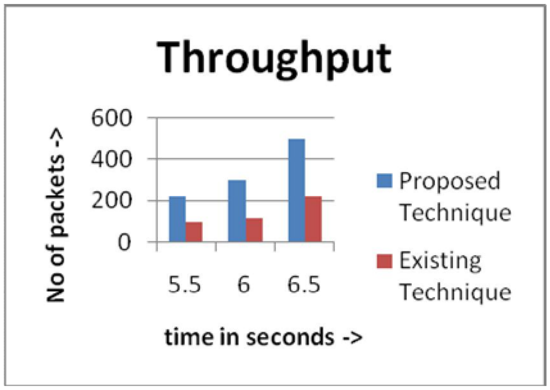
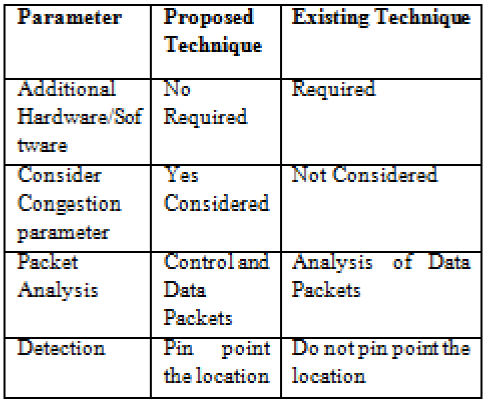


Fig 7.13: Comparison of Throughput proposed vs existing technique

As shown in figure 7.13, the throughput of the proposed and existing techniques is compared for the performance analysis. It is analyzed that throughput of the proposed technique is high due to isolation of malicious nodes from the network when compared to scenario which has malicious nodes.

QUALITATIVE COMPARISON

Table 7.4 Qualitative Comparison



Parameter	Proposed Technique	Existing Technique
Additional Hardware/Sof tware	No Required	Required
Consider Congestion parameter	Yes Considered	Not Considered
Packet Analysis	Control and Data Packets	Analysis of Data Packets
Detection	Pin point the location	Do not pin point the location

As shown in table 7.4, the existing and proposed algorithms are compared in terms of various parameters. It is analyzed that proposed algorithm works well in terms of qualitative parameters

VIII. CONCLUSION AND FUTURE WORK

VANETs are gaining popularity in the field of research due to their increase in demand within the real-time applications. There is no infrastructure required within these networks and all the vehicles as well as roadside units are linked with each other to exchange the information. Along with the exchange of information, certain warning messages are also forwarded as per the traffic conditions so that disasters can be prevented. A very commonly used technology to deploy VANETs today is Wi-Fi IEEE 802.11. Either the 802.11b or 802.11 g are the two various standards used to access the media within all the connected vehicles of wireless network interface. They are basically the general purpose standards in which the requirements of high dynamic network are not fit exactly. Within the scenarios that have short or medium range communication service within VANETs, the DSRC (Dedicated short-range communication) is proposed in this work as a communication standard. The latency is reduced and exchange data rate is increased with the implementation of proposed algorithm. During the mobility of vehicles, only limited range of communication is possible as per the IEEE 802.11 standard. Therefore for increasing the effective data packet exchange and minimizing the transmission time and network utilization, very optimal configuration protocols are to be introduced. The DDOS is the active type of attack which is triggered by the malicious nodes in the network. The DDOS attack reduces network efficiency in terms of various parameters like throughput, packet delivery ratio and end to end delay. In this research work, the technique will be designed which will be based on the threshold technique. In the threshold technique when the malicious node is transmitting data above the threshold value will be detected as the malicious nodes from the network. The proposed improvement leads to increase network performance and detection of malicious nodes from the network. The proposed algorithm is implemented in NS2 and simulation results shows improvement in terms of throughput, packet loss and delay

<u>8.1 FUTURE WORK</u>

Following are the future prospective of this research work:-

1. The proposed algorithm can be further improved which ensure the data integrity in the network
2. The proposed algorithm can be further compared with the other algorithms which ensure data security.

REFERENCES

[1] Archana S. Pimpalkar, Prof. A. R. Bhagat Patil " DDOS Attack Defense against Source IP Address Spoofing Attacks" International Journal of Science and Research (IJSR) , Vol. 4 , Issue 3, March 2015.

[2] A.Nandan, S. Das, G. Pau, M. Gerla, and M. Y. Sanadidi, "Co-operative downloading in vehicular ad-hoc wireless networks," IEEE Wireless On-demand Network Systems and Services, St. Moritz, Switzerland, volume no. 8, issue 3, pp. 32–41, 2005.

[3] B.Ayyappan and Dr. P.Mohan kumar,"Vehicular Ad Hoc Networks (VANET): Architectures, Methodologies And Design Issues," IEEE International Conference on

Science Technology Engineering and Management (ICONSTEM), volume 95, issue 12, pp. 2299-2313, 2016.

[4] Bassem Mokhtar, Mohamed Azab, "Survey on Security Issues in Vehicular Ad Hoc Networks, ELSEVIER, volume 5, issue 2, pp- 932-940, 2015.

[5] Christina Fragouli, Jörg Widmer, and Jean-Yves Le Boudec," Efficient Broadcasting Using Network Coding", IEEE/ACM Transactions On Networking, Volume 16, issue 2,pp-161-175,2008.

[6] Deeksha, Manu Bansal,Ajay Kumar, "A review on VANET security attacks and their countermeasure, IEEE International Conference on Signal Processing, Computing and Control (ISPCC),volume 3,issue 15,pp-334-354,2017.

[7] Deepak Raghuvanshi, Deepak Jain, Pankaj jain," Performance Analysis of Non Local Means Algorithm for Denoising of Digital Images", International Journal of Advanced Research in Computer Science and Software Engineering , volume 3, Issue 11, pp- 551-558, 2013.

[8] Dong Nguyen, Tuan Tran, Thinh Nguyen, and Bella Bose," Wireless Broadcast Using Network Coding", 2009, IEEE Transactions On Vehicular Technology, Volume 58, issue 2, pp-147-197,2005.

[9] Elias C. Eze, Sijing Zhang and Enjie Liu, "Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward", IEEE International Conference on Automation and Computing,volume 29, issue 2.pp-110-118,2014.

[10] Hoang D. T. Nguyen, Le-Nam Tran, and Een-Kee Hong,"On Transmission Efficiency for Wireless Broadcast Using Network Coding and Fountain Codes", IEEE communications letters, Volume 15, issue 5,pp-130-145,2011.

[11] Kanza Bayad, "Comparative Study of Topology-based Routing Protocols in Vehicular ad hoc Network using IEEE802.11p," IEEE International Conference on Electrical and Information Technologies , volume 5, issue 2, pp. 1015–1020, 2016.

[12] Kirti A. Yadav and P. Vijayakumar, "VANET and its Security Aspects: A Review", Indian Journal of Science and Technology , volume 9, Issue 18, pp- 104-118, 2016.

[13] Kiattikun Kawila, Tanapoom Danmanee, Kultida Rojviboonchai," Cobra-Q: A Cooperative-Bloom Filter-Assisted Query Protocol for Data Access in VANET", IEEE International Conference on Communication Technology, volume 44,issue18,pp-128-139,2013.

[14] Leandro Aparecido ,"Data dissemination in vehicular networks: Challenges, solutions, and future perspectives", IEEE International Conference on New Technologies, Mobility and Security (NTMS),volume 7,issue 11,pp-220-243,2015.

[15] Muhammad Anwar Shahid ,Arunita Jaekel ,Christie Ezeife , Qasim Al-Ajmi ,Ikjot Saini , "Review of potential security attacks in VANET ",IEEE Majan International Conference (MIC),volume 4,issue15,pp-1241-1239,2018.

[16] Mohamed Nidhal Mejri and Jalel Ben-Othman, "GDVAN: A New Greedy Behavior Attack Detection Algorithm For VANETs", Journal Of IEEE Transaction On Mobile Computing, volume 4, issue 7, pp- 53-62, 2016.

[17] Munazza Shabbir, Muazzam A. Khan, Umair Shafiq Khan, Nazar A. Saqib, " Detection and Prevention of Distributed Denial of Service Attacks in VANETs", IEEE Computational Science and Computational Intelligence , volume 8, issue 14, pp- 123-129, 2016.

[18] M. Li, Z. Yang and W. Lou, "CodeOn: Cooperative Popular Content Distribution for Vehicular Networks using Symbol Level Network Coding," IEEE Journal on Selected Areas in Communication., volume 29,issue 8 , pp. 223-235, 2011.

[19] Mahdi Zamani, Mahnush Movahedi, Mohammad Ebadzadeh, Hossein Pedram, "A DDOS-Aware IDS Model Based on Danger Theory and Mobile Agents", International Conference on Computational Intelligence and Security, volume 4, issue 9, pp- 559-567, 2009.

[20] Neha Goel,Gaurav Sharma, " A Study of Position Based VANET Routing Protocols", International Conference on Computing, Communication and Automation (ICCCA), volume 12, issue 3, pp. 541-550, 2016.

[21] Navneet Kaur, Er. Sandeep Kad, "Data Dissemination In VANETS- A Review", International Journal of Engineering and Technical Research (IJETR), Volume-6, Issue-4, 2016.

[22] Nivraj J.Patel, Rutvij H.Jhaveri, " Trust based approaches for secure routing in VANET: A Survey", ELSEVIER, volume 19, issue 71, pp- 194-203, 2015.

[23] Pooja. B, Manohara Pai M.M, Radhika M Pai, Nabil Ajam, Joseph Mouzna, " Mitigation of the Insider and Outsider DOS attack against the Signature Based Authentication in VANETs", IEEE Computer Aided System Engineering , volume 15, issue 2, pp- 639-645, 2014.

[24] P. Muhlethaler and A. Laouiti, "Vehicle Ad Hoc Networks: Applications And Related Technical Issues", IEEE Communications Surveys & Tutorials , volume 4, issue 15, pp- 231-240, 2008.

[25] Ravendra Kumar Sharma , Sushil Kumar Saroj, "Sybil attack prevention and detection in vehicular ad hoc network", IEEE International conference on Computing Communication and Automation , volume 4, issue 2, pp-152-163, 2016.

[26] Raksha Upadhyay, Salman Khan, Harendra Tripathi, Uma Rathore Bhatt, "Detection and Prevention of DDOS

Attack in WSN for AODV and DSR using Battery Drain", International Conference on Computing and Network Communications, volume 19, issue 2, pp- 732-745, 2015.

[27] Rakesh Kumar and Mayank Dave, "A Review of Various VANET Data Dissemination Protocols", International Journal of u- and e- Service, Science and Technology ,Volume 5, issue 3, 2012.

[28] Surendra Nagar, Shyam Singh Rajput, Avadesh Kumar Gupta, Munesh Chandra Trivedi, "Secure Routing Against DDoS Attack in Wireless Sensor Network", 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" volume 3, issue 9, pp- 114-128, 2017.

[29] Seyed Amir Ali Ghafourian Ghahramani , Ali Mohammad Afshin Hemmatya, "A Network Model for Vehicular Ad Hoc Networks: An Introduction to Obligatory Attachment Rule," IEEE Transactions on Network Science and Engineering, , volume 3, issue 2, pp. 32–41, 2016.

[30] Subir Biswas, Jelena Misic, Vojislav Misic, "DDOS Attack on WAVE-enabled VANET Through Synchronization", IEEE Global Communications Conference (GLOBECOM) ,volume 10,issue 8,pp-131-154,2012.

[31] S.Panichpapiboon, W.Pattara-atikom,"A Review of Information Dissemination Protocols for Vehicular Ad Hoc Networks", IEEE Communications Surveys & Tutorials ,volume 13, issue 99, pp- 1–15, 2011.

[32] Surya Nepal, Julian Jang, John Zic, "Anitya: An Ephemeral Data Management Service and Secure Data Access Protocols for Dynamic Collaborations", IEEE computer society, volume 7,issue 23, pp-219-226,2007.

[33] Tracey Ho, Muriel Médard, Ralf Koetter, David R. Karger, Michelle Effros, Jun Shi, and Ben Leong," A Random Linear Network Coding Approach to Multicast", IEEE Transactions On Information Theory, Volume 52, issue 10,pp-261-281,2006

[34] Uzma Khan, Shikha Agrawala, Sanjay Silakari, " Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks," Procedia Computer Science ,volume 22, issue 46, pp- 965–972, 2015.

[35] Vinh Hoa La, Ana Cavalli, "Security Attacks And Solutions In Vehicular Ad Hoc Networks: A Survey", International Journal on AdHoc Networking Systems, volume 4, Issue 6, pp- 48-55, 2014.

[36] Varsha Nigam, Saurabh Jain, Dr. Kavita Burse, "Profile based Scheme against DDOS Attack in WSN", Fourth International Conference on Communication Systems and Network Technologies, volume 11, issue 7, pp- 251-267, 2014.

[37] Wesam Bhaya, Mehdi EbadyManaa, "DDoS Attack Detection Approach using an Efficient Cluster Analysis in Large Data Scale", Annual Conference on New Trends in Information & Communications Technology Application, volume 16, issue 3, pp- 236-241, 2017.

[38] Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Shenling Wang, and Rongfang Bie, "Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends", International Journal of Distributed Sensor Networks, volume 16, issue 3, pp- 819-824, 2015.

[39] Xia Shen, Xiang Cheng, Liuqing Yang, Rongqing Zhang, and Bingli Jiao," Data Dissemination in VANETs: A Scheduling Approach", IEEE Transactions On Intelligent Transportation Systems, Volume 15,issue 5,pp-110-132,2014.

[40] Xia Shen, Xiang Cheng, Rongqing Zhang, and Bingli Jiao," Distributed Congestion Control Approaches for the IEEE 802.11p Vehicular Networks", IEEE Intelligent transportation systems magazine,volume 5,issue 4,pp-234-256,2013.

[41] Xiang Cheng, Qi Yao, Cheng-Xiang Wang, Bo Ai, Gordon L. St¨uber, Dongfeng Yuan, and Bing-Li Jiao," An Improved Parameter Computation Method for a MIMO V2V Rayleigh Fading Channel Simulator Under Non-Isotropic Scattering Environments", IEEE Communications Letters, Volume 17,issue. 3,pp-231-254,2013.