Novel Scheme for Isolation of Distributed Denial of Service Attack in VANETs

Krishna pal singh solanki[1], Anurag Sharma[2]
[1]Mtech Scholar, [2]Assistant Professor
[12]Sobhasaria engineering college, Sikar

Abstract- The vehicular adhoc networks are the decentralized type of network in which vehicle nodes join or leave the network when they want. In the network two type of communication is possible which is vehicle to vehicle and vehicle to infrastructure. This research work is based on the detection and isolation of DDOS attack in VANETs. The DDOS is the distributed denial of service attack in which malicious node select the nodes which flood the victim node with the rough packets. In this research work, technique will be proposed will detect and isolate malicious nodes from the network which are responsible to trigger DDOS attack in the Network. The technique which is proposed in this research is based on the two step verification. In the two steps verification technique, when the network performance is reduced to threshold value then the traffic is monitored that which node is sending data on such high rate. The proposed technique is implemented in NS2 and results are analyzed in terms of throughput, delay and routing overhead. It is analyzed that proposed technique performs well in terms of throughput, delay and routing overhead parameters as compared to existing approach.

Keywords- DDOS, Threshold, Monitor mode, VANETs

I. INTRODUCTION

A self-configuring type of network that provides vehicle to vehicle and vehicle to roadside communications is known as vehicular ad hoc network. The information is shared across the network through the nodes that represent themselves as servers or clients. The computerized system comprises of various components such as computers, communications, and management technologies as well as the sensor and control innovations [1]. The functioning of a transportation system can be improved by integrating these functions. The warnings related to environmental hazards, traffic and road conditions, and transmitting local information amongst vehicles is provided by using the VANETs. If there is any such condition present where there is traffic jam, road closure or accident casualty the information can be spread across the network. This might help the drivers in avoiding the specific routes as well as saving the time. The vehicles spread the warnings across other vehicles through proper communication. The basic ad hoc routing protocols cannot be used adequately within the VANETs because of the change is configurations, the mobility patterns, the entering and leaving of various vehicles and various other reasons [2]. The utilization of least communication time while using minimum amount of network resources, is the major objective of routing protocols in VANETs. On the basis of the position accusation and route update technique, the VANETs routing protocols can be categorized. There is a limited connection between the RSUs and the vehicles. This problem can be solved using the data dissemination technique. Due to continuous topology changes as well as the limited range provided for wireless communication, the data dissemination in VANETs is a very challenging task. On the basis of global Channel State Information (CSI) there cannot be optimized scheduling decisions be provided by the distributed data dissemination techniques. This is due to the absence of the central controller in the architecture [3]. As per the pre-determined rules the data is transmitted by the nodes across the network due to the fact that there is very little knowledge of the complete network. This will provide only certain level of local optimum within the network. Within the denser networks, there might be chances of collisions which will further result in causing delay in transmission of data. Due to this reason, the time cost for each data retransmission will increase for the complete network. The process of spreading information across the distributed networks is known as data dissemination [4]. The efficiency of traffic systems within the VANETs is enhanced through the involvement of data dissemination which further improves the quality of driving. Due to the fact that there are large numbers of vehicles available on the road, the communication amongst vehicles is not as easy as it seems to be. So, the transmission of data across the network is a very important issue The high mobility as well as the frequent disconnection of the topology at various regions in an area is the major challenge here. In the night as well as in the suburban areas, the traffic density is very low. The other major issue here is ensuring data transmission across the network which has less delay and before any disconnection occurs amongst the vehicles. The disconnection is not such a big issue when the target vehicles are in the closer range of the roadside unit within the dense network [5]. An attempt made by an attacker from different locations to stop legitimate users from accessing the required objects from the system is known as DDOS attack. The distributed arrangement adds “many to one” algorithm which creates difficulty to prevent entry of intruder in the network. The denial of service attacks consists of four parts namely; firstly, it has a victim that is a target host which is attacked by the interference of the attack. Secondly, it has attack daemon agents. They are specially designed to conduct the attack on the target victim. They are generally present in the host computers [6]. The daemon affects the working of target as well as host computers. The purpose to deploy these attack daemons is to gain access and infiltrates the host computers. Control master program is the third component of denial of service attack and the presence of real attacker, the master mind behind every attack, is the fourth component of denial of service attack. By using this master mind program, the attacker will remain off camera that is will become invisible.

II. LITERATURE REVIEW

Wesam Bhaya et al. (2017) [7] introduced in this paper the combination of unsupervised data mining methods. The Clustering Using Representative (CURE) method was a data mining method which helped in providing an entropy concept within the windowing of incoming packets. This helped in identifying the DDOS attack present within the network. Amongst the various approaches which already existed this proposed method was evaluated and compared in order to check what kind of enhancements have been made. The evaluation was done with respect to various parameters which helped in determining the performance of the proposed method. As per the results, it was seen that the proposed method outperformed all other existing approaches by providing higher level of accuracy.

Surendra Nagar et al. (2017) [8] proposed in this paper a secure routing protocol which could be applied in scenarios where DDOS attack was possible. The proposed algorithm was used to scan the infected nodes. The identified infected nodes were blocked in such a manner that they could not participate within the further activities. The intrusion prevention mechanism was used in order to protect the network. The neighbors were scanned by these nodes in regular manner. When a misbehavior node was identified by the IPS node from the frequently passing message the IPS node blocks it in such a manner that the information was sent to all the sensor nodes. Here, the routes were changed within this method. The network was protected against the DDOS attack as seen within the simulation results achieved by applying proposed method.

Munazza Shabbir et al. (2016) [9] presented a mobile Adhoc network which transformed into a mainstream and most promising technology of the modern time. Any time of information moving around the network is very important. The free movement of nodes and unpredictable path of the associated network degrades the working of VANET. DDOS is one of the dangerous attack present in the VANET, it exhaust the network working by using its greater part as its assets. In this attack, the attacker forges the identity of another node and uses spoof IP address to degrade the network circulation. So, before the proper working of the VANET all the security based requirements should be fulfilled.

Nirav J.Patel et al. (2015) [10] studied in this paper that there was vehicle to vehicle communication provided over the vehicular ad hoc networks. There is a continuous change within the locations of the vehicles within VANETs. During the routing process, there was a need to provide secure routing in order to provide a mutual trust amongst the nodes present in the network. Due to the presence of malicious nodes within the networks, the fake information can be transmitted to other nodes in order to cause attacks. In order to provide trust-based techniques within these networks, various researchers have proposed many studies. The enhancement of various ad hoc routing protocols had been reviewed in this paper, in order to study the secure the routing processes. On the basis of this review, the various enhancements to be made within the trust-based techniques were also understood.

Kirti A. Yadav et al. (2016) [11] reviewed in this paper the different types of routing protocols that are being applied in vehicular ad hoc networks. The security related scenario was to be generated through the presence of routing techniques within these systems. There was also a need to identify the need of providing security applications to the users involved here. The various security measures being provided in VANET are also studied in this paper. Within the security scenarios, there was a need to provide a future scope which could help in ensuring the security, availability as well as non-repudiation of the techniques. It was analyzed through this study that there was a need to provide enhancement in the intelligent transport system in order to provide higher level of secure environment within these networks.

Mohamed Nidhal Mejri et al. (2015) [12] proposed a new detection mechanism which was known as Greedy Detection for Vehicular ad hoc Networks (GDVAN). This mechanism was proposed in order to detect the greedy behavior attacks that occur within the VANETs. There were mainly two phases involved within this proposed mechanism which were the suspicion phase as well as the decision phase. The proposed technique was executed by any node present in the network which was a major benefit of this proposed technique. There was no need to modify the IEEE 802.11p standard within this mechanism. With the help of various simulations and experiments the effectiveness and efficiency of the proposed method was computed which showed that the proposed algorithm outperformed the already existing techniques in terms of various performance parameters.

III. RESEARCH METHODOLOGY

Phases of Proposed Flowchart:

Following are the various phases of the proposed flowchart:-

1. Network Deployment and pre-processing:- The VANET is deployed with the finite number of Vehicles. The DDOS attack is trigger by the malicious node. In the previous year, various techniques are proposed for the detection of malicious nodes. The technique which is proposed in this research work is based on the technique of the threshold. The technique which is proposed in this work, will calculate the threshold value of data rate. The formula which define threshold data rat for the detection of malicious node is given below

$$P = Pb * max\_p;$$

The average data rate that is utilized in simulations is denoted by variable called "avg". There is 1 packet/0.5 second of average data used here. The lower bound value of data rate is represented by "min" whereas the upper bound is represented by "max". The average data rate is denoted by "Pb" and the threshold data rate is achieved when Pb is multiplied by the upper bound value.

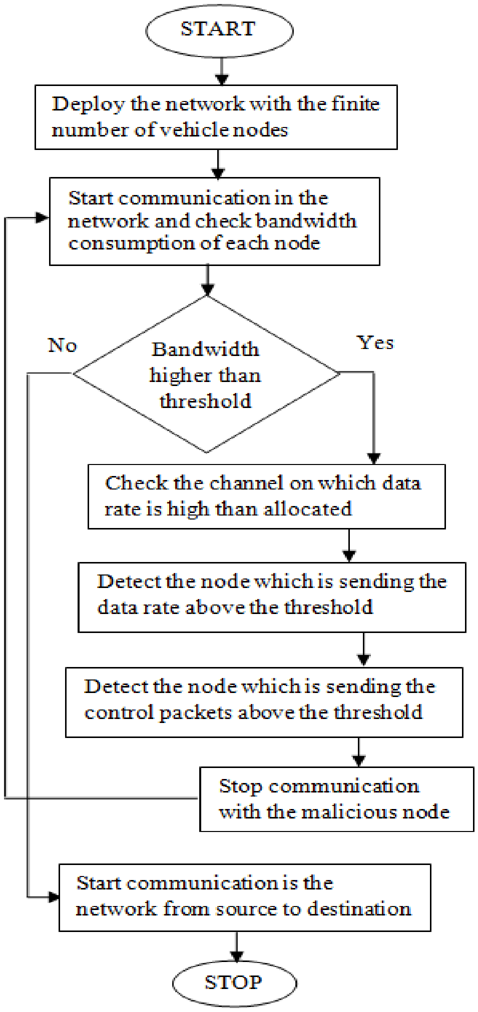
START
Deploy the network with the finite number of vehicle nodes
Start communication in the network and check bandwidth consumption of each node
Bandwidth higher than threshold
No
Yes
Check the channel on which data rate is high than allocated
Detect the node which is sending the data rate above the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

Fig.1: Proposed Flowchart

2. Detection of Malicious nodes: - The nodes are deployed randomly in the fixed area. The proposed technique is based on the per hop delay method for the identification of malicious nodes. The non-malicious nodes will forward the large number of packets and those nodes which will flood maximum number of nodes in the packets are identified as IDS nodes. These IDS nodes are the malicious nodes which are responsible for ruining the smooth working of VANET. When the network throughput reduced to threshold value, then the monitor mode technique is applied in which each node watch its adjacent node. The node which is sending the data packets above the threshold value is the marked as the malicious nodes. On the same time, if the nodes which are marked as malicious receive control packets, the nodes which send control packets is marked as malicious nodes.

3. Isolation of Malicious nodes: - The data rate is already calculated in the network and node which is increasing the data rate than defined value is detected as the malicious node. When the malicious node is identified by the network then the source node will transmit alert message to every node in the network. When the node receives the alert message, it will remove the malicious node from the path. The technique which is proposed in this research work is efficient in terms of complexity and also various congestion values are included for the detection of malicious nodes. In this phase, the malicious nodes get isolated from the network with the approach of multipath routing. When any node is identified as malicious node, it will send the alert message to all other nodes in the network. The nodes which receive the alert message stop communicating with the other nodes with the multipath routing. The node which is not able to prove its identification is isolated from the network.

IV. EXPERIMENTAL RESULTS

This research work is implemented in NS2 and the results are evaluated by making comparisons against proposed and existing techniques in terms of different performance parameters.

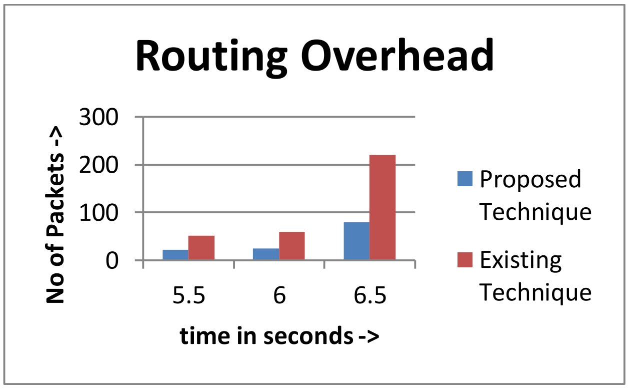

Fig.2: Comparison of Routing Overhead proposed vs existing technique

Figure 2 shows the comparison between the routing overhead of the proposed and existing technique. It is found from research that due to the presence of DDOS attack in the network, the routing protocol is very high. When the network detects the malicious node then the routing overhead is reduced.

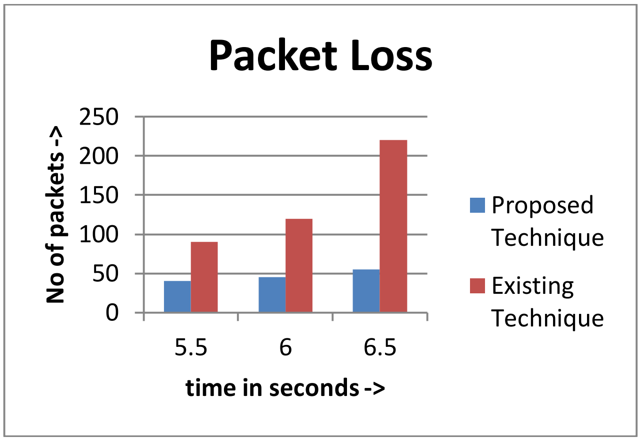

Fig.3: Comparison of Packet loss proposed vs existing technique

As shown in figure 3, 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

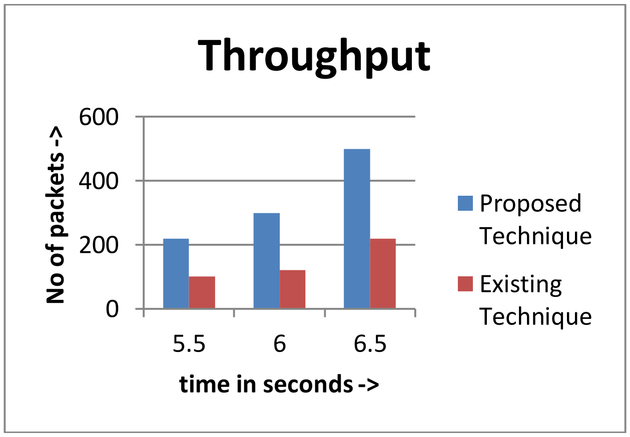

Fig.4: Comparison of Throughput proposed vs existing technique

As shown in figure 4, 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.

V. CONCLUSION

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. 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 identified as the malicious nodes. The improvement leads to increase network performance and detection of malicious nodes from the network. The proposed algorithm is implemented in NS2 and it is seen that the network's performance is improved in terms of throughput, packet loss and delay.

VI. REFERENCES

[1]. Navneet Kaur, Er. Sandeep Kad, "Data Dissemination In VANETS- A Review", International Journal of Engineering and Technical Research (IJETR), Volume-6, Issue-4, pp. 33-42 2016.

[2]. 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.

[3]. 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, , pp. 38-44, 2012.

[4]. 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.

[5]. 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.

[6]. 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.

[7]. 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.

[8]. 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.

[9]. 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.

[10]. 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.

[11]. 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.

[12]. 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.