I. J. Computer Network and Information Security, **2019, 4, 26-34**
Published Online April 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2019.04.04

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

Palak Shandil
Department of Computer Science & Engineering, NITTTR, Chandigarh, INDIA
E-mail: palak.cse@nitttrchd.ac.in

Rakesh Kumar
Department of Computer Science & Engineering, NITTTR, Chandigarh, INDIA
E-mail: raakeshdhiman@gmail.com

Received: 17 January 2019; Accepted: 19 February 2019; Published: 08 April 2019

***Abstract*—**A network in which the vehicular nodes are free to join or leave the network is known as vehicular ad hoc network (VANET). Either vehicle to vehicle or vehicle to infrastructure types of communication is performed in this decentralized type of network. The identification and elimination of Distributed-Denial of Service (DDoS) attacks from VANETs is the major objective of this research. The nodes that can flood victim nodes with large numbers of rough packets are chosen by the malicious nodes in this kind of attack. Identifying such malicious nodes from the network is an important research objective to be achieved. 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. NS2 simulator is used to implement the proposed technique. With respect to various performance parameters, the proposed technique is analyzed. A comparative evaluation of results achieved from proposed and existing techniques is also done to conclude the level of improvement achieved.

***Index Terms*—**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 [5]. 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 [6]. 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 [7]. 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 [8]. The architecture of VANET is separated amongst three broader domains names as Ad hoc Domain, In-Vehicle domain and Infrastructure Domain.

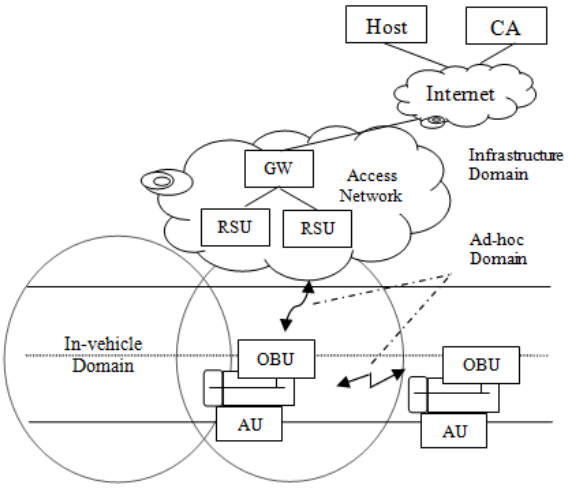

Fig.1. VANET System Architecture

A. *DDOS Attack*

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 various examples of DDOS attack involve:

1. Preventing access of legitimate network traffic by network flooding.
2. Preventing user to access a service by disrupting the connections amongst two machines [9].
3. Preventing the user from accessing a service by preventing one individual user to have access to it.

The distributed arrangement adds "many to one" algorithm which creates difficulty to prevent entry of intruder in the network [10]. 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. 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 [11]. By using this master mind program, the attacker will remain off camera that is will become invisible.

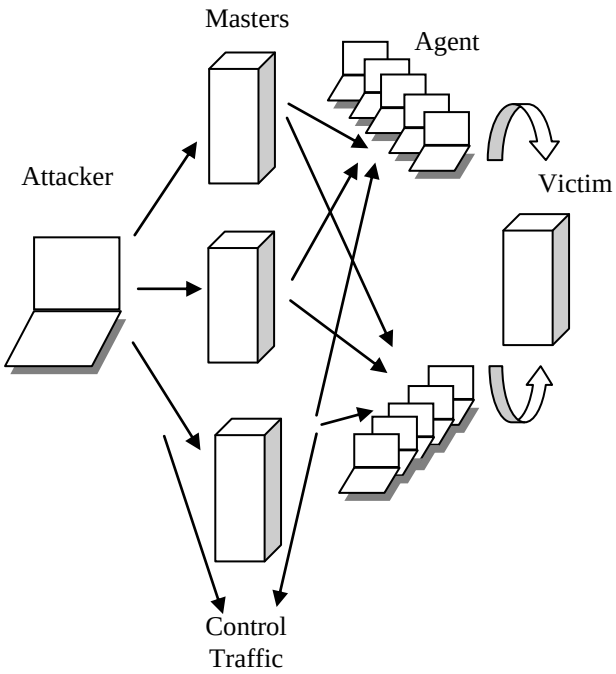

Fig.2. DDOS Attack

There are different tools utilized within the DDOS attacks. The basic structure of the tools is same even though they have different names. As shown in figure 2, the components involved here are:

- **Attacker**: The personal computer used by the hacker that is responsible for attack.
- **Master:** The commands from the attacker are directly received by this system and other agents are also controlled by it.
- **Handler:** The tasks are performed on the program master system through this program.

- **Agent**: The attack target is directly attacked by this system.
- **Demon program**: The above tasks are performed on the agent system with the help of this program.

II. Related Works

Wesam Bhaya et al. (2017) [12] 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) [13] 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) [14] 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) [15] 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) [16] 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) [17] 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 Gaps

Following are the inferences drawn from the literature review:

1. VANET is deployed with several vehicular nodes which can change their location any time due to which routing becomes challenging which needs to get resolved.
2. Since the nodes can enter or leave the network at any time, the malicious nodes easily enter network and trigger active as well as passive attacks within these networks. A security framework is required which can secure the vehicular ad hoc network.
3. The DDOS is the active attack which is very easy to identify but difficult to defend due to its dynamic

nature. In the previous research no efficient technique is proposed which can detect malicious node in minimal time.

4. Various types of techniques are required to identify the malicious nodes present in the network, which are responsible for the degradation of working of network. They are also responsible to find the nodes having spoof credentials and trigger the DDOS attack in the network.

IV. Research Methodology

The technique proposed by the author Mohamed Nidhal Mejri [12] detects malicious nodes from the vehicular ad hoc networks. In the proposed technique is based on two steps which are suspicious nodes detection and the detection of actual malicious node. In the suspicious phase, the technique of classification is applied on collected traces. In the suspicious detection phase, the intrusion detection nodes are defined in the network which collects network traces for the particular time. The correlation will be defined in the collected traces and the traffic pattern which is close to malicious traffic is put into the suspicious list. The technique of logistic regression is applied to cross check the collected traces. In the second phase, the suspicious list will be given as input to the detection phase. On the detection phase, the watchdog technique is applied on the suspicious nodes and which do not follow the rules are declared as the malicious nodes.

Following are the various steps of the existing approach which is used for the detection of malicious nodes.

Step 1: Suspicious Traffic Detection: - This is first phase of malicious node detection from the network. In this phase, the network traffic traces are collected by the intrusion detection nodes. The relationship will be derived between the collected network traces. The traffic patterns which are closed to malicious are put into the suspicions list. The data traces are verified using the logistic regression.

Step 2: Malicious node Detection: - The suspicious list will be taken as input in the malicious node detection phase. The technique of monitor mode is applied on the suspicious nodes which malicious average connection time, number of login attempts and waiting time. The vehicle nodes which do not follow regular pattern are declared as malicious.

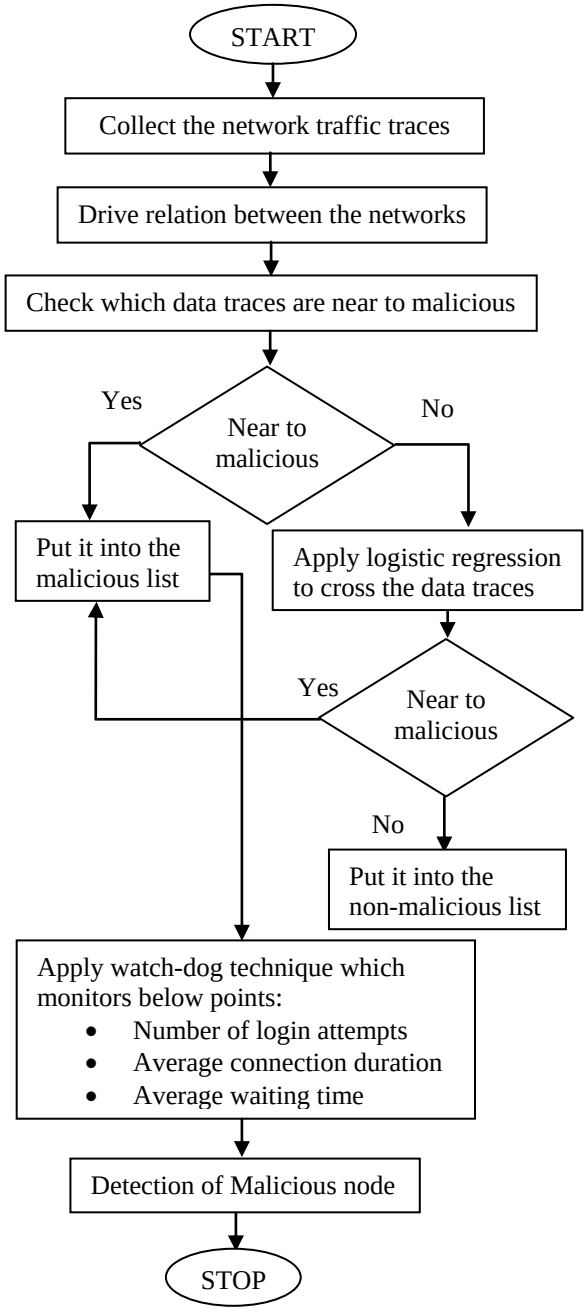

Fig.3. Existing System's Flowchart

In the work, a novel technique is presented which will detect malicious nodes from the network and to detect malicious nodes following are the steps which will be followed:-

1. In the first step, the network will be employed with the finite number of vehicle nodes. The fixed bandwidth will be allocated to each vehicle node in the network.
2. The road side units will start analyzing the bandwidth consumption of each vehicle node and node which will use the bandwidth above allocated value will be the malicious node.
3. In the third step, the road side units will check the type of packets the node is sending which is using the bandwidth above the allocated value. When the

node transfers the data packets to the victim node, then that node may or may not be the malicious node.

4. In the last step, the nodes which will send the malicious data packets, if that node will receive control packets from any node then that node will be identified as the malicious node which will be responsible to trigger DDOS attack.

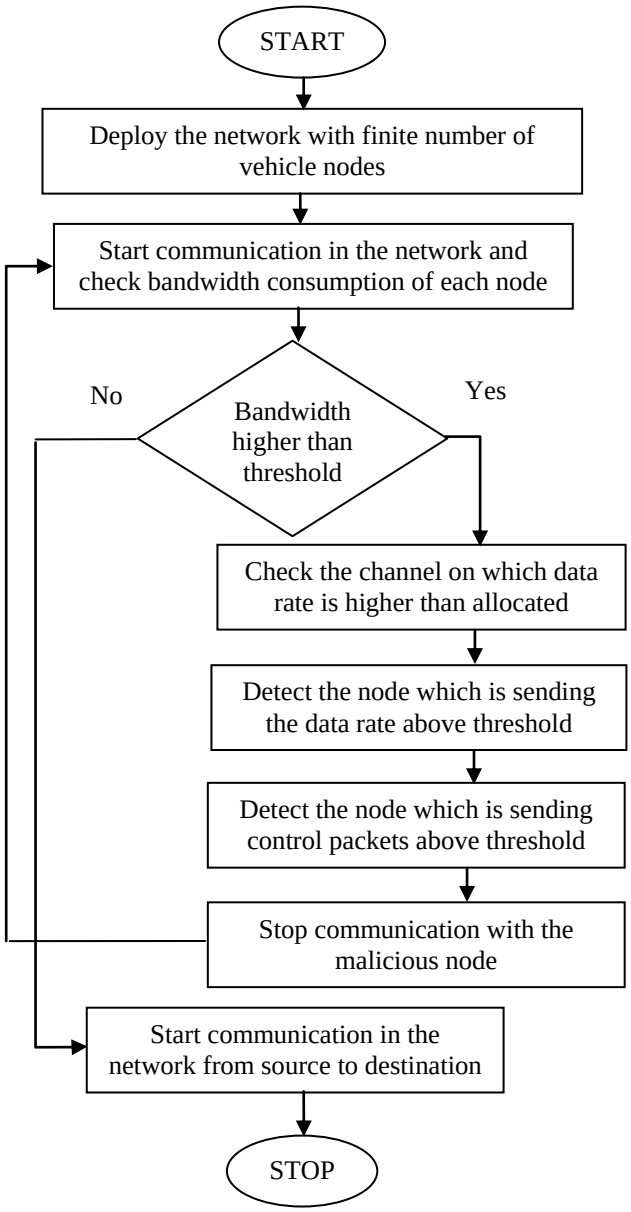

Fig.4.Proposed Flowchart

A network that is decentralized in nature which means that the vehicles are free to join or leave the network is known as VANET. Different types of active and passive attacks are generated here because of the decentralized nature of these networks as this can result in making it easy for the malicious nodes to enter the networks. The path or route from source node to destination node is generated using the routing protocols which are categorized amongst reactive, proactive and hybrid depending upon their properties. The protocols which establish the path by collecting the complete network information are known as reactive routing protocols.

The route request packets are flood in the network by source node such that the network's information can be collected. In response, the route reply packets are sent by the nodes that is adjacent to destination. Based on the hop count and sequence number of the nodes collectively, the best path possible is chosen by the source. The path that has least hop count and highest sequence number is chosen as the best. Below is the pseudo code applied to establish path in the networks:

PATH ESTABLISHMENT ALGORITHM

Input: Number of vehicle nodes
Output: Establishment of Path

1. Deploy the network with the finite number of vehicle nodes in the network
2. Source and destination nodes are defined in the network for the path establishment.
3. Source flood route request packets in the network.
4. if (node route request packets has route to destination)

   Then

   Node responds back to source node with the route reply packets

   Else

   Repeat step number 4

5. Check all the available paths from source to destination

   If (path (i) has less hop count than path (i+1)

   If (path (i) has high sequence number than path (i+1)
   Then path (i) is selected as best path
   Else
   Path (i) is selected as the best path

6. Transmit data through the selected path

The proposed technique is based on two type of message which are data packets and control packets. The vehicles and road side units are used for the detection of malicious nodes. The DDOS attack is the special type of attack in which malicious nodes select the nodes which flood the victim node. The malicious nodes which forward maximum number of packets and flood maximum number of packets are detected as the IDS nodes. The IDS nodes detect the malicious nodes. 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. The proposed technique does not require any extra hardware or software for the detection of malicious nodes from the network.

THRESHOLD BASED ALGORITHM

Input: Number of vehicle nodes
Output: Detection of malicious

1. Assign bandwidth consumption to each node in the network.
2. The source node start sending data to destination node.
3. If (bandwidth consumption >threshold)
4. Check channel on which data rate is high than threshold
5. Check the node which is sending data packets on the node
6. If (node ==detected)
7. Check the node which is sending control packets
8. Isolate detected node
9. Else
10. No malicious node
11. End
12. End

PHASES OF PROPOSED FLOWCHART**:**

The different phases followed in the proposed flowchart are explained below:

1. **Network Deployment and pre-processing:-** 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:

$$P = Pb * max\_p; \quad (1)$$

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.

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.

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

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.

V. Performance Evaluation

This research work is based on the vehicular ad hoc network for the detection and isolation of distributed denial of service attack. The technique of watchdog is implemented in the previous work for the detection of malicious nodes. The technique of threshold is proposed for the detection and isolation of malicious nodes. In the existing approach for the isolation of malicious nodes require extra hardware and also it does not pin point malicious nodes. The existing scheme does not pin point malicious due to which accuracy of malicious node detection is low. The proposed technique pin point malicious nodes from the network due to which malicious node detection accuracy is high. In this chapter, both existing and proposed techniques are implemented in Ns2 and results are analyzed in terms of various parameters.

Table 1. Simulation Parameters

Parameter	**Value**
Simulator	Ns2-2.35
Visualization Tool	Xgraph
No of Nodes	37
Transmission range	18 meter
Routing Protocol	DSRC
Mac type	802.11
Channel Type	Wireless channel
Area	800*800 meters
Simulation time	10 seconds
Traffic Type	TCP traffic
Packets Size	1000 bytes
Mobility Model	Random way point
Propagation model	Two ray ground

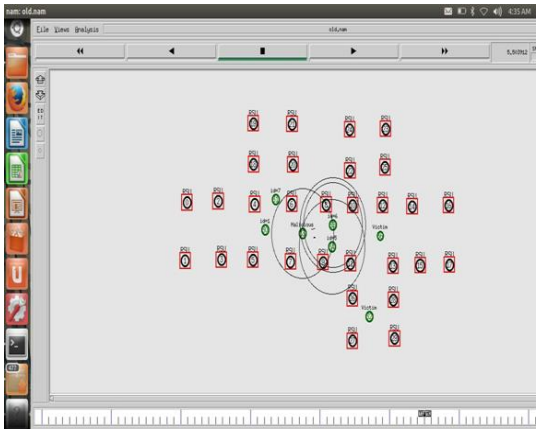

Fig.5. Attack Scenario

As shown in Fig 5, 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.

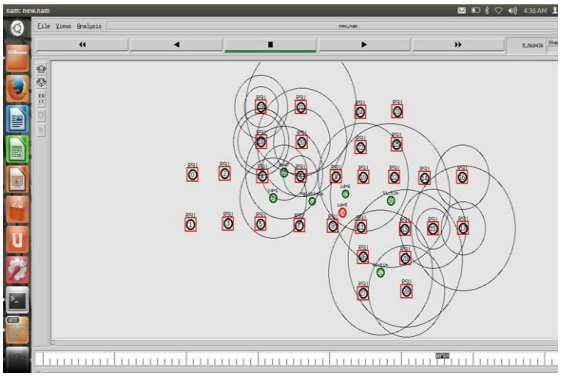

Fig.6. Marking of Nodes which are Sending Data Packets

As shown in Fig 6, 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 may be the malicious node.

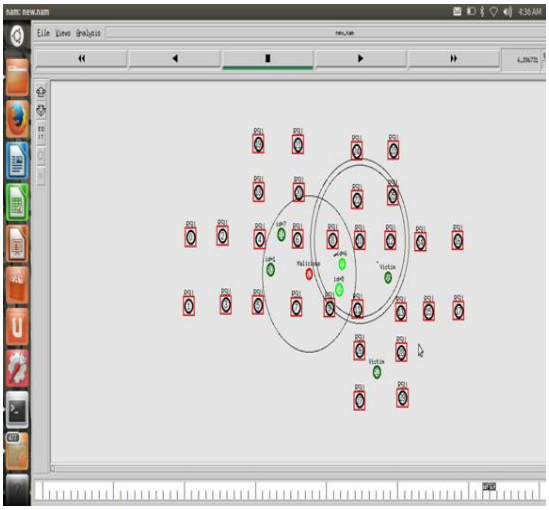

Fig.7. Isolation of Malicious Nodes

As shown in Fig 7, the node which is sending the data above the threshold value will be detected as the malicious node.

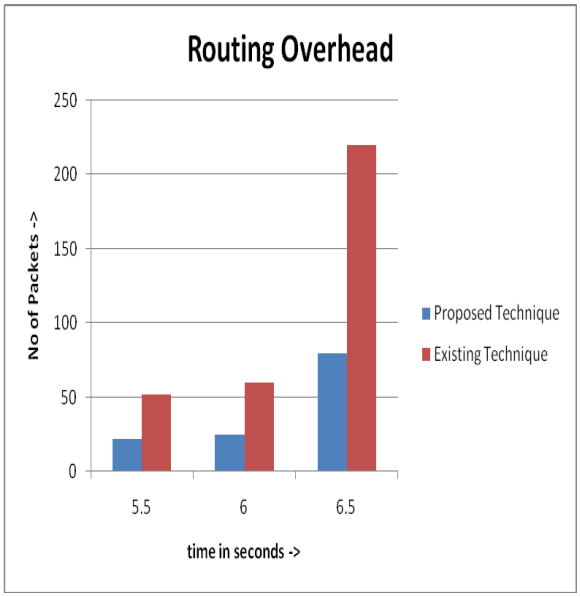

Fig.8. Comparison of Routing Overhead Proposed vs. Existing Technique

As shown in Fig 8 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 higher amount of routing overhead is achieved. When malicious node is detected and removed then the routing overhead is reduced.

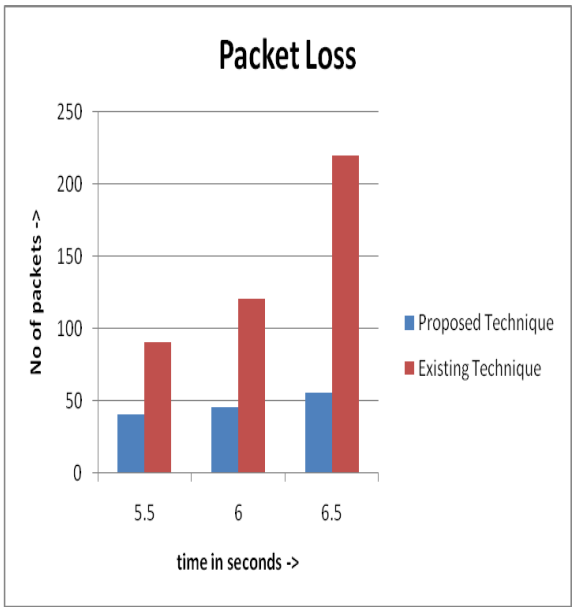

Fig.9. Comparison of Packet loss Proposed vs. Existing Technique

As shown in Fig 9, 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.

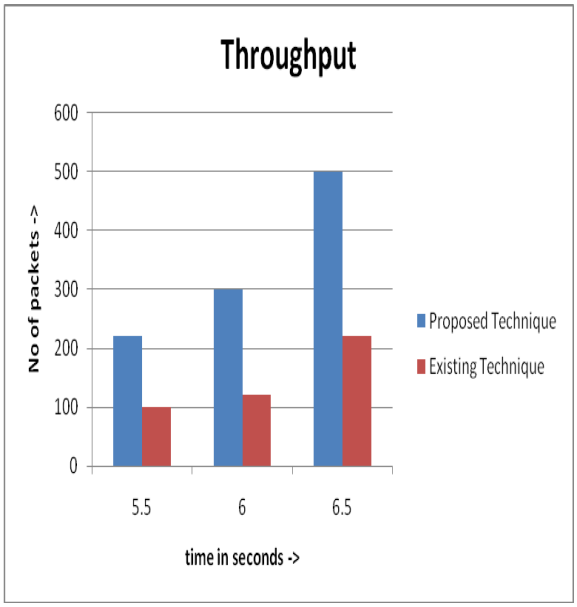

Fig.10. Comparison of Throughput Proposed vs. Existing Technique

Fig 10 shows a comparative analysis of proposed and existing techniques to analyze their performances. The throughput of the proposed technique is high due to isolation of malicious nodes from the network when compared to scenario which has malicious nodes.

Table 2. Routing Overhead

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

Table 3. Throughput Comparison

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

Table 4. Packet loss Comparison

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

VI. 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. It is seen that the performance of network is improved with respect to throughput, packet loss and delay.

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] Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, and Bertrand Ducourthial, "Sybil Nodes Detection Based on Received Signal Strength Variations within VANET," *International Journal of Network Security*, volume 9, no. 1, pp-22- 33, 2009.

[8] Mina Rahbari and Mohammad Ali Jabreil Jamali, "Efficient Detection of Sybil Attack Based on Cryptography in VANET," *International Journal of Network Security & Its Applications*, volume 3, No.6, pp-23-29, 2011.

[9] S. Roselin Mary, M. Thamaraiselvan and M. Maheshwari, "Early Detection of DDOS attacks in VANET by Attacked Packet Detection Algorithm (APDA)," *International Conference on Information Communication and Embedded Systems*, volume 9, issue 8, pp. 230-241,2013.

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

[11] Archana S. Pimpalkar, Prof. A. R. Bhagat Patil "DDOS Attack Defense against Source IP Address Spoofing Attacks*" International Journal of Science and Research,* volume 4, issue 3, pp. 36-46, 2015.

[12] Wesam Bhaya, Mehdi Ebady Manaa, "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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

Authors' Profiles

Palak Shandil is pursuing M.Tech (Computer Science) at National Institute of Technical Teachers Training and Research, Chandigarh, India. She received B.Tech in Computer Science and Engineering from Bahra University, Solan India. Her research interest includes Wireless Communications & Networks and cyber security.

Rakesh Kumar is an Assistant Professor at the Department of Computer Science and Engineering, National Institute of Technical Teachers Training and Research, Chandigarh, India. He received his Ph.D. (Computer Engineering) from NIT Kurukshetra, M.Tech. (IT) from GGS Indraprastha University, Delhi, B.Tech. in Computer Science and Engineering from Punjab Technical University, Jalandhar. His research interest includes Cloud Computing, Mobile Adhoc Networks and Wireless Sensor Networks.

How to cite this paper: Palak Shandil, Rakesh Kumar,"A Novel Scheme for Isolation of Distributed Denial of Service Attack in VANETs", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.4, pp.26-34, 2019.DOI: 10.5815/ijcnis.2019.04.04

