International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 10 | Oct 2018 www.irjet.net p-ISSN: 2395-0072

Secure Framework for Isolating Smurf and Blackhole Attack in VANET

Tanjot Singh [1], Dr. Bikrampal Kaur [2]

[1] *Research Scholar, Dept. of Information Technology, Chandigarh Engineering College, Landran, Mohali, Punjab, India*

[2]*Professor, Dept. of Information Technology, Chandigarh Engineering College, Landran, Mohali, Punjab, India*

Abstract - *In vehicular ad hoc network, every moving vehicle is referred as nodes and these nodes establish connection with every passing by nodes and with the RSUs (Road Side Units) to share information through communication between them. VANET is one of the types of ITS (Intelligent Transportation System) and due to the emergence in the VANET technology, it is becoming more vulnerable due to connection establishment with every passing by node. Some hackers perform security attack to steal the information which is being transferred from one node to another node. Some attacks dropped the whole data packets from the communication, so no information or data packets reached at the destination node. Some attacks steal the data packets form communication and some take control over the control packets of the data stream and divert the whole traffic to a particular node to flood the target in the network. Any attacker or malicious node can join the network in VANET and trigger any kind of attack. In this research, our technique detects and isolate these types of malicious node which are responsible for triggering of such attacks. In Blackhole attack, when source node sends the data packets to the destination node, attacker or malicious node dropped the whole data packets from the data stream which results in zero packets delivered at the destination node. In Smurf attack, attacker node or malicious node spoofs the IP address of the target node or the destination node and broadcast the ICMP message to the broadcast IP of the router which then sends the data packet request to all the connected nodes or devices in the network and those nodes replies to the received request back to the source node to establish the connection for data communication but the whole data traffic from all node diverted to the target node whose IP was stored in the control packet by the attacker node which results in the flooding of data packets to the target node which make it non-responsive. In this study, a secure framework is designed on the proposed technique of backtracking and threshold techniques to isolate the Smurf and Blackhole attacks from VANET to secure the communication between the source node and the destination node and to any problem or traffic related issues from VANET.*

Key Words: VANET, ITS, Smurf, Blackhole, ICMP, Routing Protocol.

1.INTRODUCTION

Vehicular Adhoc Network (VANET) is part of ITS in smart city and almost as similar as MANET (Mobile Adhoc Network) which is vital part of ITS (Intelligent Transportation System) technology. VANET turns into the rising innovation with the progression in remote system correspondence and this system is produced for the vehicles that are proceeding onward the streets. VANET has the capacity that improve the proficiency and the wellbeing of the vehicular transportation.

VANET provides the facilities which helps in managing and controlling of the congestion of traffic on the roads and helps in the location tracking of vehicles based on their GPS location and ensures the safety of people and vehicles[1].

In vehicular ad hoc network, this technology allows the motor vehicles to communicate in the VANET. This communication is between the motor vehicles and the installed infrastructure (which installed on road sides called RSUs).

The different type of communication method are V 2 V and V 2 I (road side units), where 'V' represents as the motor vehicles nodes and 'I' represents as the RSU or Infrastructure in the vehicular ad hoc.

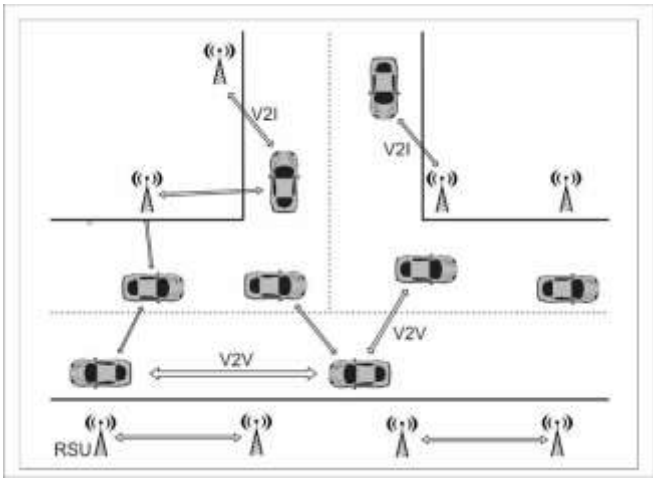

Fig -1.1: Architecture of VANET

In vehicular ad hoc network, the vehicles moving on the roads are the nodes and act as a sender and receiver. Every node is communicating with the nearby nodes. The nodes are communicating by sending data packets to the other nodes and also to the road side units that are installed on the sides of the roads. Every moving vehicle communicates with the RSU while passing from the RSU and the vehicles. These RSU's share information which is received from the nodes or vehicles with each other and also with the base station [2].

1.1 *Routing Protocols in VANET*

Routing protocol was first used for MANET and later the routing protocol was implemented and tested on VANET infrastructure. These routing protocol decreases the network load, latency and these are also reliable and robust routing protocols. These routing protocols are of three types.

First, reactive routing protocol is otherwise called the on-demand routing protocol. When the host or the node start sending data or information packets, the routing in the reactive protocol begins. The preferred standpoint is that the bandwidth wastage can be diminished with the use of reactive routing protocol. The drawback of this protocol is that it experiences the suffering because of the packet loss. AODV and DSR are usually the different types of reactive protocol [3].

Second, proactive routing protocol which is also known as the table-driven protocol. In proactive, the node presents its routing data to their neighbor nodes intermittently. Every node needs to manage their own table themselves. Every node ought to keep up the records or data of neighbor nodes until the change of topology in the network. DSDV, ZRP, DBF and OSLR are usually types of the proactive routing protocols [3].

Third, hybrid routing protocol, in which the reactive and proactive protocols are merged together to form the hybrid routing protocol. The limitations of both protocols are overcome in this hybrid protocol. This hybrid protocol creates a layered and hierarchical network. At the first step, proactive routing is utilized and accumulates the unfamiliar data. At that point, to keep up the routing data, the reactive protocol is being utilized. TORA and ZRP are the types of hybrid routing protocol [3].

1.2 *Security Attacks in VANET*

VANET network has the vulnerability from different types of attacks. These are mainly divided into two classifications.

In active attacks, attacker breaks the integrity of data as they send the data to the receiver or the user after modifying the data.

In passive attacks, the attacker compromises the confidentiality of the data. The attacker infiltrates into the network and snoops around while exchanging of data without modifying and altering any data. It is non-authorized access and the attackers only snoops around the network and hard to find.

Security of the Vehicular ad hoc network is very important as in VANET any node can join or leave the network at any time which increases the vulnerability and allow attacker to attack the network at any time. So, it is very important to secure such network as in VANET many vehicles are moving on the road and any wrong instruction lead to some accident or wrong route for the vehicle, which may cause problem in the network. In VANET, every individual node is communicating with each other node which makes the network. An attacker may spoof the identity of existing node or may perform the DDoS attack. This study is based on detecting and isolating the attacker node from the network so, they cannot send false or wrong information or data into the network or to any individual node.

2. LITERATURE SURVEY

Hanin Almutairi, et.al.,[2] author explained address a key point in the field of PC organizing security which is the location of dark gap hubs in VANETs that are helpless against security assaults because of its infrastructure less nature. The black hole assault is a type of a refusal of administration assault that influences a hole for information to movement in a VANET. their solution is appropriate for a low thickness organize where every auto moves in a straight line and conveys parcels to other neighboring autos utilizing a geographic directing convention. Street side units are set in the crossing point of streets and may acknowledge to exchange parcels when an auto experiences an issue of bundle conveyance. The black hole assault is considered at the system layer and every auto keeps up a trust table with a specific end goal to assess the unwavering quality of neighboring autos. Every sender refreshes the trust estimation of each neighbor as per the affirmation got by the goal and uses together this incentive with the advance to choose the best neighbor. All the more particularly, IEEE 802.11 is the correspondence standard that is utilized and ensures the elements of the physical and the information interface layers and takes care of the basic issues of remote correspondence between the autos since our concentration is identified with the system layer. Omnet++ is the reproduction instrument which is utilized to plan and recreate our proposed conspire. the outcomes exhibit the steering and the recognition procedure and the effect of the thickness on the required time for the location.

Mehak Kaushal and Mr. Gunjan Gandhi[3] explained Wireless sensor networks are made up out of hubs which are sent in a subjective positions and the correspondence between these hubs are done through the remote channels. The information is send through these hubs. In WSN the security is the principle issue which happens through the natural impediments of energy use and computational limit. The system layer is in charge of steering parcels, so author can state that this layer is the essential spot for the programmers and gatecrashers. The fundamental assault on this layer is Black Hole assault which implies dissent of administration and this assault upset the administration of this specific layer. Transmission benefit is likewise influenced by this kind of dropping assaults. In this paper author examined the black hole impact which is the regular assault amid the steering procedure. In this assault, noxious hubs attempt to imitate it as a goal hub by sending incorrectly course answer parcel to the source hub. This is the means by which the pernicious hubs catch the information from the

source hub. of sending there information the malignant hub drop the bundles. In this paper they examine different interruption plans and tries to relieve the impact of black hole assault.

Sharndeep Kaur, Dr. Anuj Gupta [4] explained that MANET is an accumulation of different portable hubs which imparts over generally data transmission through the remote connections. In MANETs, the hubs are versatile in nature consequently the system topology may change quickly and unusually finished time. With the expansion in the utilization of MANETS security turned into a crucial necessity to give communicational insurance and change of system presentation. The most conceivable assault in MANET is black hole assault. In which, a vindictive hub gives counterfeit directing data by promoting itself having most brief way to the source hub and afterward deny the activity from the source hub or can drop the bundles later. Here in this paper a novel approach is proposed to recognize and avert black hole assault in MANET. For this a meta heuristic pursuit composition presented by incorporating the min and max variations of ACO with DRPI check tables in view of AODV directing convention. At last the NS2 re-enactment demonstrates that this strategy recognizes and disconnect the vindictive hub and in addition decreases the parcel misfortune rate while expanding the information sending limit of hubs.

Barleen Shinh[5] explained that The mobile hubs can build up the course from source to goal when they need. In DSR steering conventions many provisos are there, these loop holes can offer emerge to various kind of dynamic and detached assaults which are activated by different inside and outside malignant hubs. Among all the sort of assaults, black hole assault is the most widely recognized of assault which is conceivable in DSR convention. black hole assault is the foreswearing of administration assault. Numerous calculations had been proposed to keep this assault. In this paper, author proposed adjustments in conventional DSR convention to avoid black hole assault

Sunil Kumar Jangir and Naveen Hemrajani[6] addressed A mobile ad hoc network (MANET) is an infrastructure less system of different cell phones and for the most part known for its self configuring conduct. MANET can convey over moderately data transfer capacity obliged remote connections. Because of restricted data transfer capacity battery power and dynamic system, topology steering in MANET is a testing issue. Communitarian assaults are especially major issues in MANET. Assaults are obligated to happen if steering calculations neglect to recognize inclined dangers and to find and additionally expel noxious hubs. Our goal is to analyze and enhance the execution of system lessened by assortment of assaults. The execution of MANET organize is inspected under Black opening, Wormhole and Sybil assaults utilizing Performance networks and after that significant issues which are identified with these assaults are tended to.

Vimal Bibhu, et.al.,[7] black hole attack in Vehicular Ad Hoc Network is real issue related with the field of PC organizing. In this paper author displayed the execution investigation of the dark gap assault in Vehicular Ad Hoc Network. they expound the diverse sorts of assaults and their profundity in specially appointed system. The execution metric is taken for the assessment of assault which relies upon a parcel end to end delay, organize throughput and system stack. The postponement, throughput and load are recreated by the assistance of OPNET 14.5 modeler. The reenactment setup contains 30 Vehicular hubs moving with consistent speed of 10 meter for every second. The information rate of Vehicular hubs is 11 Mbps with default transmitting energy of 0.005 watts. With On Demand Distance Vector Routing and Optimized Link State Routing the pernicious hub cradle estimate is brought down to a level which increment bundle drops.

Sanjeev Kumar[8], research the elements that add to the amplification the traffic of smurf attack and comprehend the connection among the actual attack flood, transitional unprotected system or network and the last enhanced attack flood. They likewise characterize another term called attack amplification factor which speaks to the level of amplification that actual attack flood experiences during the transmission to the target machine. It is likewise appeared in this paper using this enhanced attack, it is feasible for an aggressor to simply utilize a dial-up modem and unprotected delegate network system to debilitate even ultra-rapid optical line, for example, OC-192 of the target network.

Benamar Bouyeddou et.al., [9], used an approach which they proposed to detect the flooding attach which are ICMP based DoS and DDoS attacks based on the Kullback-Leibler Divergence (KLD) technique. This is spurred by the high limit of Kullback-Leibler divergence to quantitatively segregate between two circulations. Here, the rule of three-sigma is connected to the Kullback-Leibler divergence distances to detect an anomaly. They assessed the adequacy of this plan by using the evaluation dataset of 1999 DARPA Intrusion Detection.

3. PROBLEM FORMULATION

The vehicular adhoc network is the type of network in which vehicle nodes can change its location any time. Due to decentralized nature of the network, vehicle nodes join or leave the network when they want. The malicious nodes join the network which are responsible for triggering various type of active and passive attacks. This research is based on isolating active type of attacks which are blackhole and Smurf attacks. In the blackhole attack, malicious node forces the source node to select path through it which leads to reduction in network throughput and delay. In the Smurf attack, malicious node spoofs the IP address of the legitimate node and communicates on behalf of the legitimate node. In this work, proposed techniques are used to isolate the malicious

or selfish node from the network responsible for triggering of blackhole and Smurf attacks in the network.

3.1 *Routing Protocols in VANET*

The objectives related to this research are as following:

1. To study and analyze various security techniques for vehicular ad hoc network.
2. To propose technique for the isolation of Smurf and blackhole attacks in vehicular ad hoc network.
3. Implement proposed techniques and analyze results in terms of certain parameters.

4. METHODOLOGY & IMPLEMENTATION

In the proposed methodology, this technique works in two phases for detecting and isolating the smurf and blackhole attacks in VANET, where in the first phase smurf attack is detected and isolating the malicious node from the network and in second phase, selfish node which is responsible for triggering of blackhole attack is detected and isolated from the network.

In the process, first of all a network is deployed in with finite number of nodes in the network as shown in figure 4.1.

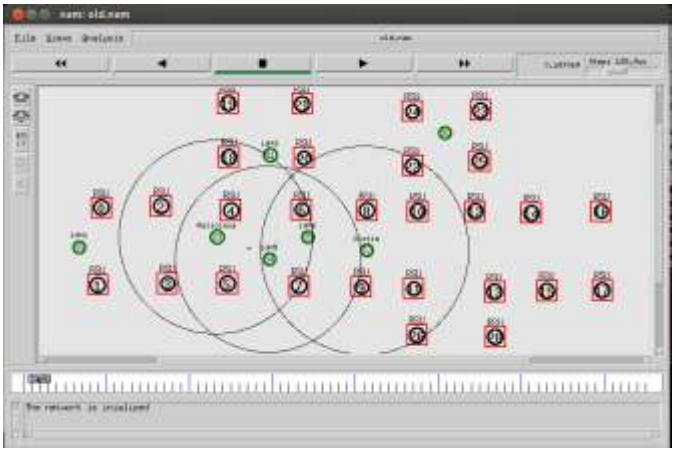

Fig -4.1: Network Deployment

A connection or path must be established for the data transfer between the source node and destination node, best path is selected between the source and destination to start the communication.

Source node sends the Route Request packets in the network and other nodes in the network replies to the route request by sending Route Reply packets. On the basis of the received request, a route is established for the data transfer between the source and destination as shown in the figure 4.2.

In figure 4.2, path is established from the source node to the destination node and starts communicating through that route. Shortest path algorithm is used to select the best route for data transfer.

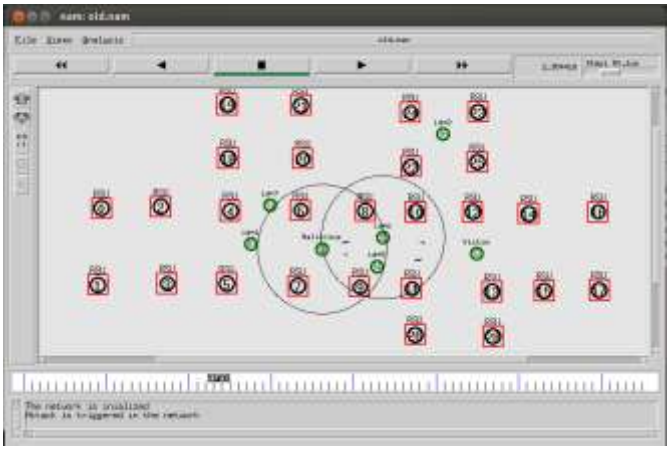

Fig -4.2: Attack is Triggered by the Malicious Node

When route is selected for the data transfer a selfish node or malicious node start jamming the network and also starts dropping the whole data packet from the data stream which is being transferred. As in the figure 4.3, node 33 acts as selfish node which dropping the data packets with high rate.

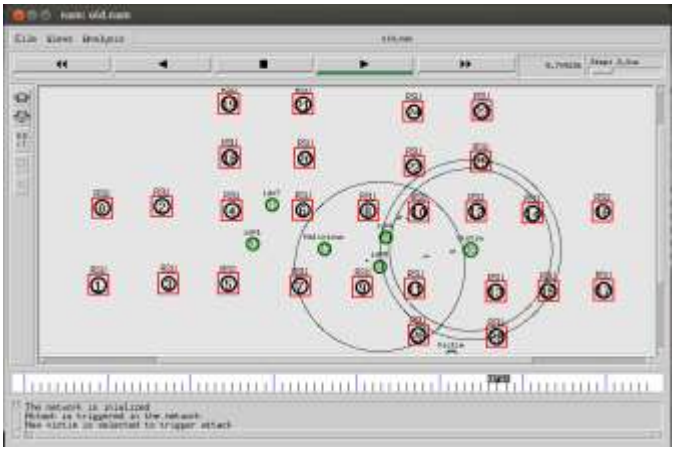

Fig -4.3: Jamming Network and Packet Loss

With these network attacks a lot of data packets has lost and not delivered to the destination. To detect these attacked a technique is proposed which detect the malicious node and isolating them from interfering between the data communication. Here IDS node is created in the network which has least mobility. These IDS nodes create the profiles of each node on the basis of number of packets forwarded by the nodes.

It then starts checking the route request packets initiated by the nodes. If nodes are forwarding least packets then time of route request packet is being checked and if no then it starts establishing the path from source to destination.

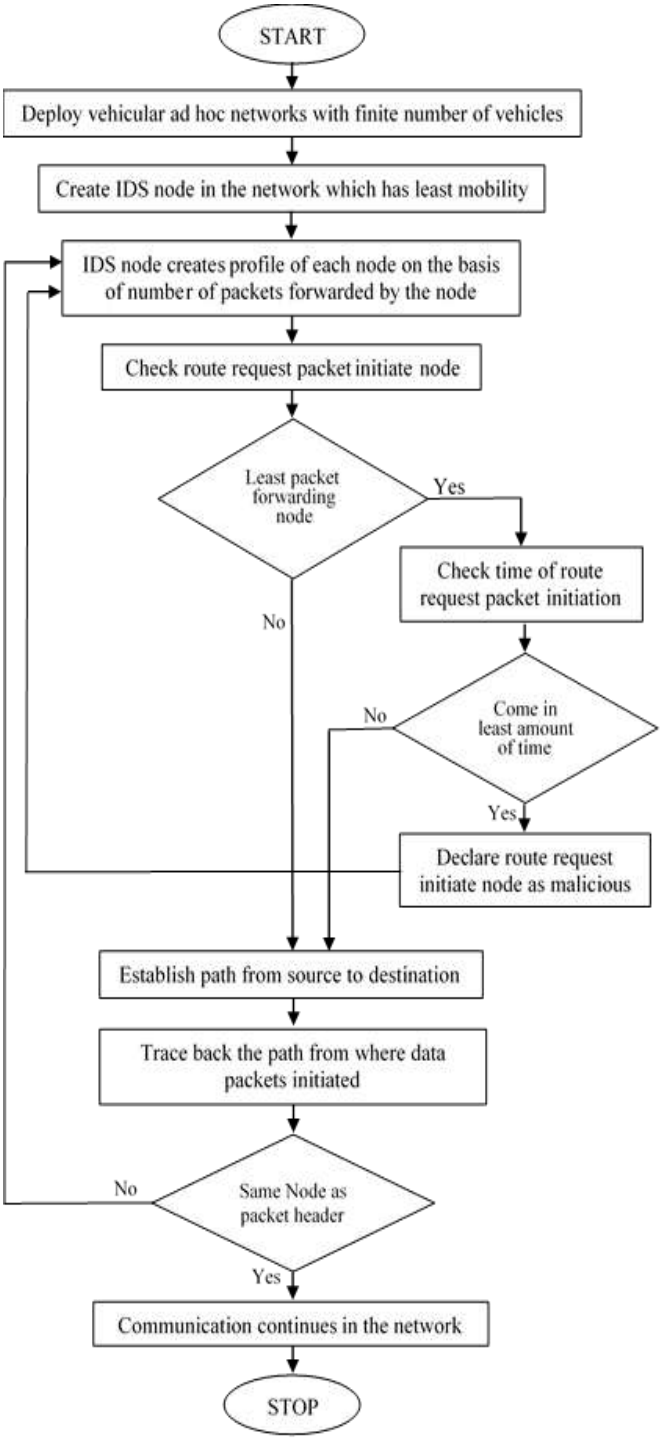

Fig -4.4: Flowchart of Detecting and Isolating Malicious Node

After checking the time, if it comes in least amount of time then the node is declared as the malicious node due to their abnormal behavior. Otherwise, it then establishes the connection for data transfer from source to destination. Now, again it is checked by tracing the path back from where data packets was initiated, if same node is detects as the source node then data transfer is started otherwise it starts again by checking the profiles of the nodes created by the IDS node.

In figure 4.5, destination node starts sending back the negative acknowledgement packets to detect the malicious node from the network

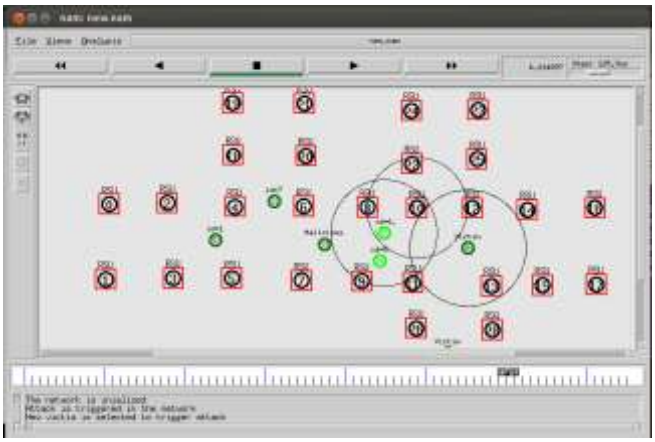

Fig -4.5: Negative Acknowledgement by Destination

IDS nodes create the profiles of each node based on the number of data packets forwarded by the node. With the backtracking the threshold techniques both smurf attack and blackhole attacks are detected and isolating from the network. Malicious node is detected as shown in the figure 4.6 and isolated and stop all the communication from the network.

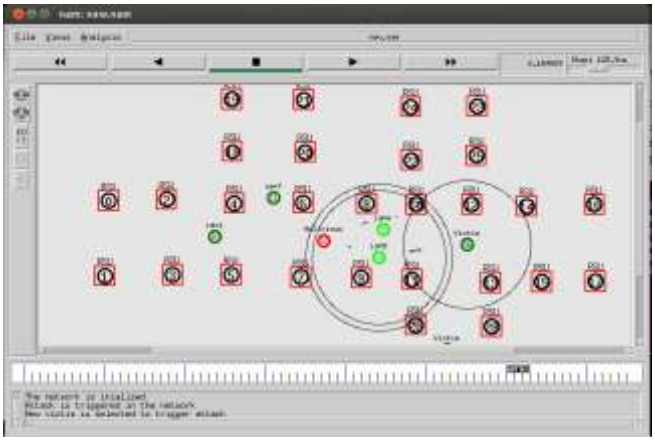

Fig -4.6: Malicious Node is Detected

5. RESULTS & DISCUSSIONS

The outputs were taken from the simulation of the network and represented in the graphs. The results of various parameters are drawn in the graphs such as throughput, packet loss and routing overhead. The results from these parameters drawn and represented in the graph to show the comparisons between the previous and proposed techniques.

The various parameters used in the network simulation with results and conclusion are as follows:

1. Throughput: The throughput is defined as the fraction of all the received data packets at the destinations over the number of data packets sent by the sources. This is an important metric in networks. If the application uses TCP as the layer 2 protocol, high packet loss at the intermediate nodes will result in retransmissions by the sources that will result in network congestion. The equation of throughput is as following:

$$Throughput = \frac{Total\ Data\ Packets\ Recieved}{Total\ Data\ Packets\ Sent}\ X\ Time$$

--- Equation (5.1)

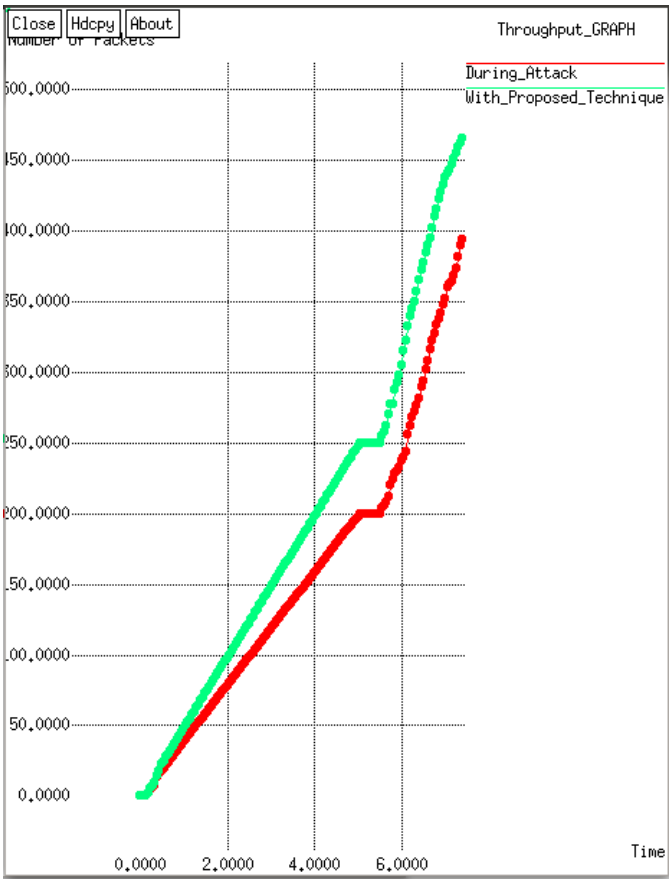

Fig. 5.1: Throughput Graph

In figure 5.1, throughput graph is displayed comparing the proposed techniques with the previous technique. It concludes that the throughput of network is increased due to the isolating of malicious node as this malicious node dropping the data packet from the transmission.

2. Packet Loss Comparison: In packet loss comparison, the analysis displays the results that the packet loss is decreased with elimination of the malicious node from the network. The equation of packet loss is as following:

$$Packet\ Loss = Number\ of\ Packets\ Sent - Number\ of\ Packets\ Received$$

--- Equation (5.2)

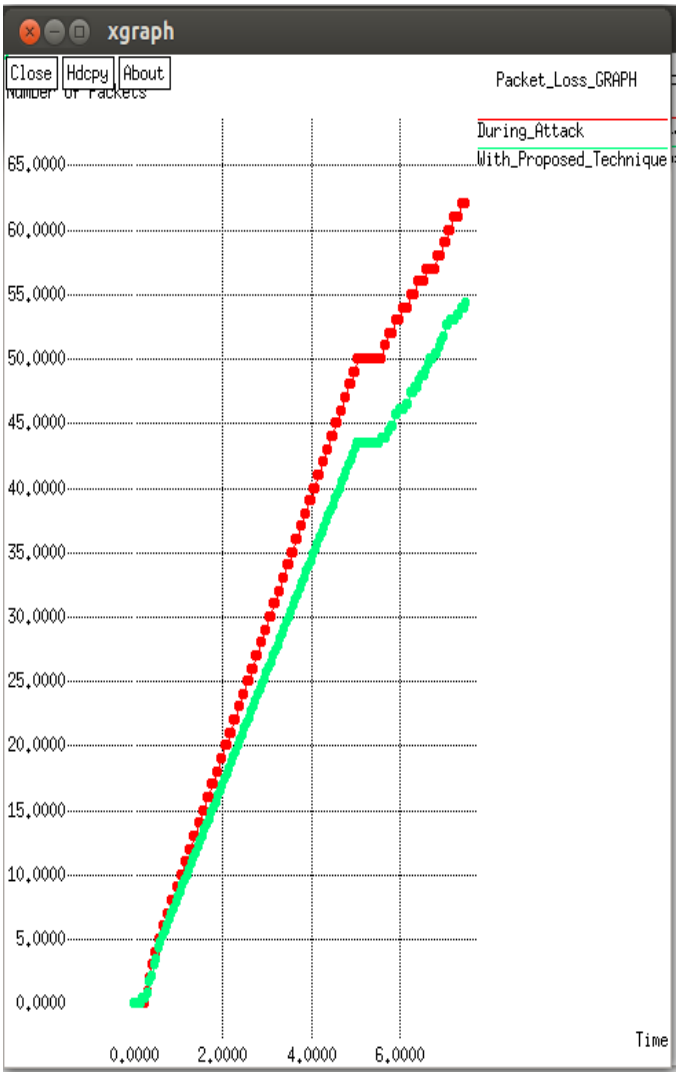

Fig. 5. 2: Packet Loss Graph

In figure 5.2, result clearly shows that the packet loss decreases and provides more efficiency to transfer of the data packet through the communication path.

3. Routing Overhead: The number of the routing packet which are required for communication in the network.

$$R.O. = \frac{Routing\ Sent\ Packets}{Total\ Sent\ Packets}$$

--- Equation (5.3)

In figure 5.3, it is shown as the results are analyzed using the proposed technique the routing overhead is also

improved from the previous technique and displays the difference in the previous and proposed technique.

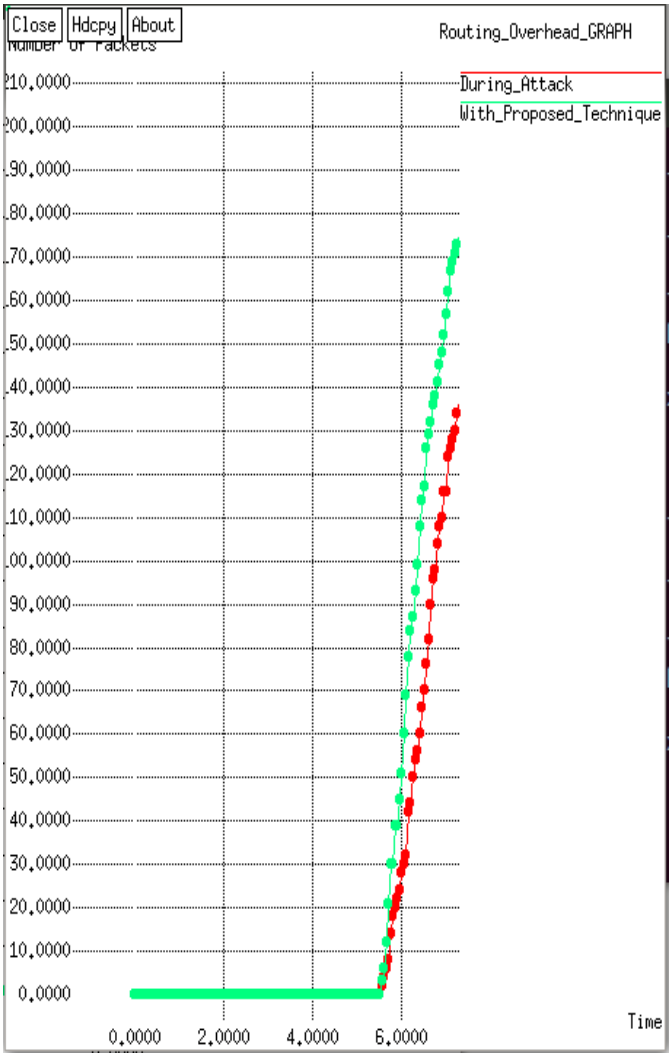

Fig. 5. 3: Routing Overhead Graph

Below in the table, comparison of the result data is displayed in the format show the variance in previous and proposed techniques.

Table -1: Results Comparison

Parameters	Previous Technique	Proposed Technique
Throughput	408	473.5
Packet Loss	62	54.34
Routing Overhead	160	189

6. CONCLUSION

VANET architecture is advancing day by day as the advancement of the new technologies. It is also important to make the VANET architecture is secure enough so that attacker cannot be able to breach the security of the network and does not create any nuisance which may cause the catastrophic events or the accidents on the roads. In this study, we implemented the secure framework which is being used to detect the malicious node from the network by monitoring their activities and isolate them from the network and communication so that they cannot further set up the communication or disturbs the network and make sure that the network is secure from the vulnerable attacks like smurf and blackhole attacks. This way performance of the network cannot be reduced with these types of attacks.

REFERENCES

[1] Aravendra Kumar Sharma, Sushil Kumar Saroj, Sanjeev Kumar Chauhan, Sachin Kumar KumarSoni, "Sybil Attack Prevention and Detection in Vehicular Ad hoc Network", International Conference on Computing, Communication and Automation (ICCCA 2016), IEEE, 2016.

[2] Hanin Almutairi, SamiaChelloug, Hanan Alqarni, RaghdaAljaber, AlyahAlshehri, Dima Alotaish, "A New Black Hole Detection Scheme for Vanets", ISBN 978-1-4503-2767-1, ACM, 2014.

[3] Mehak Kaushal, Mr. Gunjan Gandhi, "Detection Prevention and Mitigation of Black Hole Attack for MANET", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 4, Issue 04, April, 2015.

[4] Sharndeep Kaur, Dr. Anuj Gupta, "A Novel Technique to Detect and Prevent Black Hole Attack in MANET", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 6, June, 2015.

[5] Barleen Shinh, "Novel Technique to Detect and Isolate Black hole Attack in MANET", International Journal of Engineering and Computer Science, ISSN: 2319-7242, Vol. 3, Issue 6, June, 2016.

[6] Sunil Kumar Jangir, Naveen Hemrajani, "Evaluation of Black hole, Wormhole and Sybil Attacks in Mobile Ad-hoc Networks", ISBN 978-1-4503-3962-9, ACM, 2016.

[7] Vimal Bibhu, Kumar Roshan, Dr. Kumar Balwant Singh, Dr. Dhirendra Kumar Singh, "Performance Analysis of Black Hole Attack in Vanet", I.J. Computer Network and Information Security, MECS, 2012.

[8] Sanjeev Kumar, "Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet", Second International Conference on Internet Monitoring and Protection (ICIMP 2007), IEEE, 2007.

[9] Benamar Bouyeddou, Fouzi Harrou, Ying Sun, Kadri, "Detection of Smurf Flooding Attacks Using Kullback-Leibler-Based Scheme", 4th International Conference of Computer and Technology Applications, IEEE, 2018.