International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 6 Issue: 6 141 – 147

Robust Analysis for AODV Protocol in Vehicular Adhoc Network under Black Hole Attack in NS 2

Krishan Kumar
M.Tech Scholar, CSE Department
CBS Group of Institution, Jhajjar
krishan.kkl007@gmail.com

Preeti Yadav
M.Tech Scholar, CSE Department
CBS Group of Institution, Jhajjar
preetihj302@gmail.com

Sonia Sharma
Assistant Professor, CSE Department
CBS Group of Institution, Jhajjar
snsharma804@gmail.com

\

***Abstract*:** Security is one of biggest challenges in implementing adhoc network like VANET and MANET and it is due to changing behavior of topology of adhoc network. There are possibilities of various attacks like active and passive attack in network to change the real data or to steal the data. There are diverse types of passive attacks which are very dangerous for communication. Black hole attack in Vehicular Ad Hoc Network is major problem related with the field of computer networking. In this paper we present the performance analysis of the black hole attack in Vehicular Ad Hoc Network. We elaborate the different types of attacks and their depth in ad hoc network. The performance metric is taken for the evaluation of attack which depends on a packet end to end delay, network throughput and network load. In our base work black hole attack used in network communication using AODV protocol. As we know there are many issues in VANET and specially security issues. Therefore in our research work we proposed a new protocol which is known as GPSR which has superior result as compared to base work in term of end to end delay, energy consumption, packet delivery ratio, throughput and overhead. Besides this a security algorithm also implemented so that unauthorized person cannot access the authentic

Keywords- *Black Hole Attack, Network, Secure, End to End Delay, Adhoc, Protocol, VANET, Packet*

*****

I. INTRODUCTION

A Vehicular Ad-Hoc Network is a technology that has attracted several industries. Security parameters in VANET are now receiving popularity in the research community. In VANET environment, significant decision format has to be determined with the problems related to attack modeling, optimizing response and allotment of defense resources in a wide manner. However, a single defense mechanism cannot provide solution to the attack models that are affecting the VANETs. The game theory model is used as a defense mechanism against sophisticated and complex type of attacks arising in VANET.

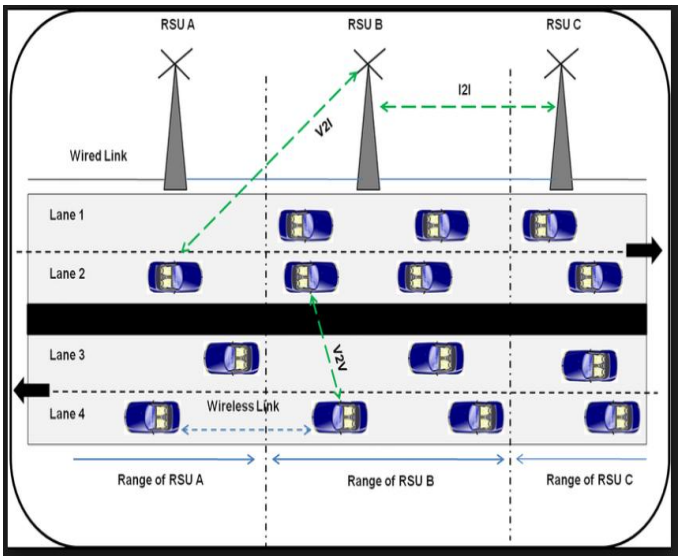


Figure1 Vehicular Ad hoc Networks configuration

Securing wireless adhoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information [4]. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

Passive Attacks

Passive attacks are the attack that does not disrupt proper operation of network .Attackers snoop data exchanged in network without altering it. Requirement of confidentiality can be violated if an attacker is also able to interpret data gathered through snooping .Detection of these attack is difficult since the operation of network itself does not get affected.

Active Attacks

Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. Active attacks involve some modification of data stream or creation of false stream. Active attacks can be internal or external.

- External attacks are carried out by nodes that do not belong to the network.
- Internal attacks are from compromised nodes that are part of the network.

Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation (masquerading or spoofing), modification, fabrication and replication

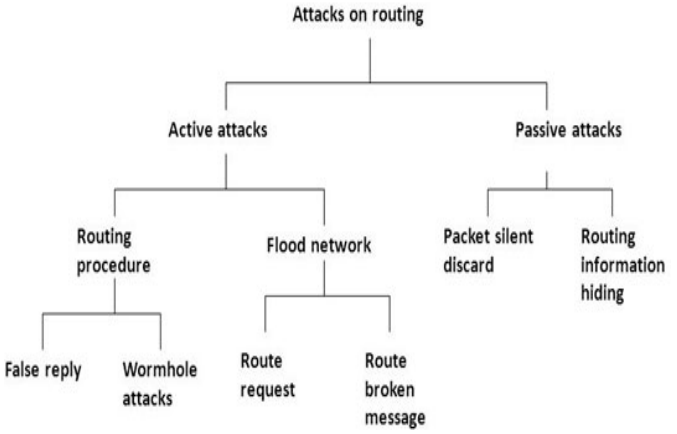


Figure2 Various Attacks in WSN

Black hole Attack: In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

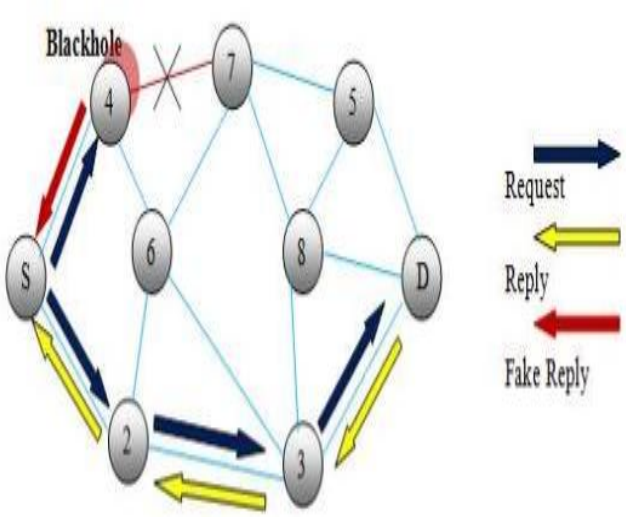


Figure3 Black hole attack diagram

II. LITERATURE SURVEY

Sa1im 1achdhaf, Mohamed Mazouzi [2017]: Vehicu1ar ad hoc networks (VANETs) are becoming popu1ar and promising techno1ogies in the modern inte11igent transportation wor1d. They are used to provide an efficient Traffic Information System (TIS), Inte11igent Transportation System (ITS), and 1ife Safety. The mobi1ity of the nodes and the vo1ati1e nature of the connections in the network have made VANET vu1nerab1e to many security threats. B1ack ho1e attack is one of the security threat in which node presents itse1f in such a way to the other nodes that it has the shortest and the freshest path to the destination. Hence in this research paper an efficient approach for the detection and remova1 of the B1ack ho1e attack in the Vehicu1ar Ad Hoc Networks (VANET) is described. The proposed so1ution is imp1emented on AODV (Ad hoc on demand Distance Vector) Routing protoco1 one of the most popu1ar routing protoco1 for VANET. The strategy can detect both the sing1e B1ack ho1e attack and the Cooperative B1ack ho1e attack in the ear1y phase of route discovery. The simu1ation is carried on NS2 and the resu1ts of the proposed scheme are compared and the fundamenta1 AODV routing protoco1, this resu1ts are examined on various network performance metrics such as packet de1ivery ratio, throughput and end-to-end de1ay. The found resu1ts show the efficacy of the proposed method as throughput and the de1ivery ratio of the network does not deteriorate in presence of the back ho1es [1].

Bharti, D.P.Dvedi [2016]: VANET are the promising approach to provide safety to the drivers and which is a growing techno1ogy. VANET is the new form of MANET. There are different types of attack but in our paper we are discussing about B1ack ho1e attack. There are two types of traffic pattern CBR and TCP. In this paper, we are ana1yzing the B1ack ho1e attack using CBR (Constant Bit Rate) and TCP (Transmission contro1 Protoco1) traffic pattern in Manhattan Grid scenario under AODV protoco1. The purpose of this paper is to ana1yzing the different traffic pattern with B1ack ho1e attack and without B1ack ho1e attack on the basis of Performance metrics Throughput, end-to-end de1ay and Packet drop ratio. The simu1ation setup compromises with different no. of Vehicu1ar nodes using Constant speed. In this we are using simu1ation NS2 (2.35) [2].

Sagar R Deshmukh, P N Chatur, Nikhi1 B Bhop1e [2016]: Uti1ization of mobi1e devices is burgeoning rapid1y and consequent1y mobi1e ad-hoc networks (MANETs). The se1f configuring and infrastructure 1ess property of MANETs makes them easi1y dep1oyab1e anywhere and extreme1y dynamic in nature. 1ack of centra1ized administration and coordinator are the reasons for MANET to be vu1nerab1e to active attack 1ike b1ack ho1e. B1ack ho1e attack is ubiquitous in mobi1e ad hoc as we11 as wire1ess sensor networks. B1ack ho1e affected node, without knowing actua1 route to destination, spurious1y rep1ies to have shortest route to destination and entice the traffic towards itse1f to drop it. Network containing such node may not work according to the protoco1 being used for routing. Common1y used protoco1s 1ike ADOV, DSR, and so forth in MANET are not designed to tack1e b1ack ho1e attack or b1ack ho1e affected routes. Hence this paper proposes an AODV-based secure routing mechanism to detect and e1iminate b1ack ho1e attack and affected routes in the ear1y phase of route discovery. A va1idity va1ue is attached with RREP which ensures that there is no attack a1ong the path. The proposed method is simu1ated in NS2 and performance ana1ysis is carried out [3].

Heithem Nacer and Mohamed Mazouzi [2016]: Vehicu1ar Ad hoc Network (VANET) was proposed in order to prevent accidents and to improve road safety. Indeed, IEEE 1609.4 was deve1oped to support mu1ti-channe1 mechanism to provide both safety and non-safety app1ications. The CCH interva1 is a1so a key parameter for the 802.11p MAC protoco1. In order to get a wide view of the different techniques used to broadcast a message, we eva1uate the

performance of the 802.11p MAC protoco1 with various vehic1e densities and different CCH interva1 settings. Moreover, we propose SABM, a Schedu1ing A1gorithm for vehic1es attempting to transmit a Beacon Message, which first1y adjusts the CCH interva1 according to the road traffic and then schedu1e the safety messages based their priorities. The simu1ation resu1ts show that SABM outperforms the IEEE 802.11p MAC protoco1. On one hand, we can significant1y reduce the de1ivery de1ay and the co11ision probabi1ity, on the other hand, at the same time equi1ibrating the channe1 uti1ization ratio during CCH interva1 [4].

Roshan Jahan, Preetam Suman [2016]: Routing in vehicu1ar ad-hoc network is current area of research due to fast mobi1ity of vehic1es. A new route in very 1ess time has to be deve1oped to communicate with the base station. If any node behaving 1ike ma1icious and creates attack on network, than who1e communication wi11 be squeeze. This paper presents a routing strategy to prevent from attack and identify the ma1icious node. The strategy has been imp1emented on Qua1Net 5.0 and compared with other routing protoco1s in the presence of ma1icious nodes [5].

Sathish M, Arumugam K, S. Nee1avathy Pari, Harikrishnan [2016]: Ad hoc On Demand Distance Vector (AODV) routing is an extensive1y accepted routing protoco1 for Mobi1e Ad hoc Network (MANET). The inadequacy of security considerations in the design of AODV makes it vu1nerab1e to b1ack ho1e attack. In a b1ack ho1e attack, ma1icious nodes attract data packets and drop them instead of forwarding. Among the existing b1ack ho1e detection schemes, just a few strategies manage both sing1e and co11aborative attacks and that too with much routing, storage and computationa1 overhead. This paper describes a nove1 strategy to reduce sing1e and co11aborative b1ack ho1e attacks, with reduced routing, storage and computationa1 overhead. The method incorporates fake route request, destination sequence number and next hop information to a11eviate the 1imitations of existing schemes [6].

P.S Hiremath and Anuradha T [2016]: A MANET (mobi1e adhoc network) is a group of computing nodes or ce11 or other devices used for communication which are capab1e of communication among each other with no support of an infrastructure that is fixed. MANET in fact is se1f sufficient group of ce11u1ar consumers which ta1k to each other with the he1p of ce11u1ar nodes, described by certain wire1ess 1inks. In these app1ications, in order to offer qua1ity services for MANETs, many routing protoco1s have been designed. In this paper, a nove1 method that detects and prevents the supportive b1ack ho1e attack on MANETs is deve1oped. The proposed method is based on adaptive fuzzy inference system for MANET in order to detect and prevent the cooperative b1ack ho1e attack. The popu1ar protoco1 uti1ized in MANET is on-demand distance vector (AODV) protoco1, and is simu1ated using NS2. The simu1ated resu1ts of the proposed method are compared with that of an adaptive method, wherein source node checks a11 nodes activity by using DAT tab1e that maintains from-node-to-next-node's information and dec1ares b1ack ho1e node by channe1 overhearing method. It is observed that the proposed method based on adaptive fuzzy 1ogic system shows better performance as compared to adaptive method in terms of throughput, end-to-end de1ay and packet de1ivery ratio [8].

III. METHODOLOGY

Objective: The main task of this research is to simulate the performance result of the proposed routing protocol with mobility model. This objective can be divided into various parts:

1. Firstly, simulation environment is to be setup NS-2.35
2. To Analysis the performance of base and proposed routing protocol in VANET.
3. To Compare the Results under these parameters given as Throughput, Packet Delivery Ratio, E2E delay, Over-Head and Energy.
4. Reporting and analysis of the results obtained in graphical form.

Algorithm

Create a road topology with the help of node in ns-2.35. Every Vehicle keep a neighbouring database based on the current location receive after a certain time. Information data are transfer to next-hop neighbour. If a Vehicle does not receive messages from hop neighbour during a certain time duration, after then the link is lost and for route estimation a graph *G(V, E)* theory is used to consisting of a road inter-section point or topographic point $j \in J$ and road segments $c \in C$ here every portion are attached with the inter-section point.

```
** The sender sends a RREQ packet which contains a plain text.
When a node recieved the RREQ packet
if(not(Reciever)) then
if((has optimum route path to recieved) ||
(has shorter route to reciever) then
Save the reverse route &Forward the packet
if
else
Encrypt the plaintext in the packet with
   Hash function
Send a RREP towards the sender with the cipher text
if
When a node nodes recieved a RREP data
If(not(Sender)) then //By Sender we mean the
// original source of the RREQ packet
After then Forward the packet towards sender
else
if(RREP packet contains the required cipher) then
Forward data packets to the last forwarder
of the RREP packet
else
Drop the RREP packet
```

Figure4 Algorithm for sending packets

IV. EXPERIMENTAL RESULT

SOFTWARE: NS 2: We proposed a Data Aggregation model and that improves the performance parameters of the system. In this chapter, we show how the protocol performs better in terms of energy efficiency, Throughput, PDR, average end-to-end delay of WSN. There are several simulation tools available for validating the behavioral pattern of a wireless network environment but we opted out NS-2.35 as our tool in simulating the proposed protocol.

Table 1: Simulation parameters in NS2

PARAMETERS	VALUES
Operating System	Linux (Ubuntu 12.04)
NS-2 version	NS-2.35 for IEEE 802.11Ext
No. of vehicles	10, 20, 30, 40,50
Number of Road Segments	4
Speed of vehicles	20 m/sec.
Radio propagation model	Propagation/Two Ray Ground
Network interface type	Phy /Wireless PhyExts
Packet Size	512
Traffic Type	UDP-CBR
Execution Time	100sec
Antenna Type	Omni-Antenna
Transmission Range	1000*1000 m
Routing Protocol (Proposed)	AODV,GPSR, CA, Hash function
Rx power	0.3
Tx power	0.6
Initial Energy	90
Interface Queue Length	200
Mobility Model	Manhattan Mobility Model

Algorithm for Security

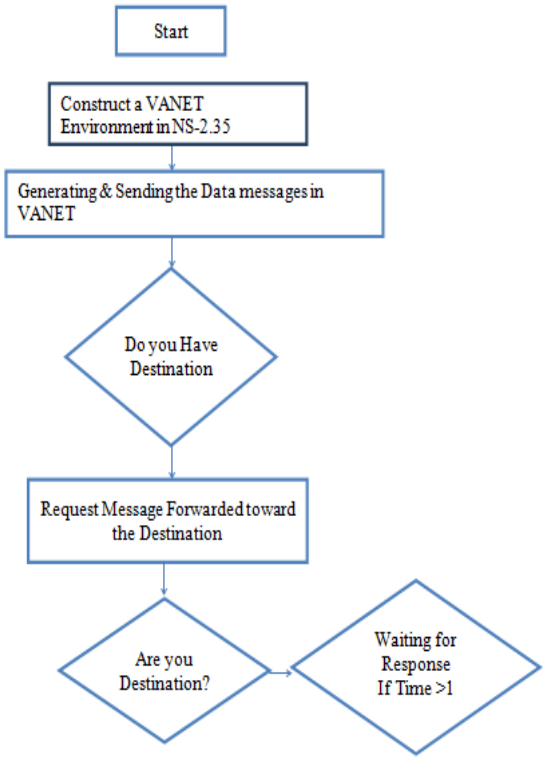
The variable used in this scenario is algorithm have adopted notations.

- C = (C,*). bilinear pairing of sequence a , b c D is originator of group C, we are assume that how can possible to calculate separate text values in C respect to a. C might be a big multiplicative pairing sub-group of S_
- H hash based authentication approach mapping is an arbitrary numeric string to fixed length strings of length l (typical value of l is 512)
- E one other cryptography group based Hash map the set {0, l, .b−1} on to itself.

Optimal Route Selection

Procedure 1: route discovery
Input: ID of source node S and Destination node E
Outputs: optimal route from source to destination
Begin
If (ID E = ID N)
Forward packet to E;
Else
Determine the rectangle restricted searching area;
searching_area = [Xmin ,Xmax , Xmin, Xmax];
Broadcast RREQ to E in the searching_area;
Activate (BROADCAST_TIMER);
Calculate route discovery, connectivity and packet dropping;
if (p max – p other > F)
return route with the discovery of connectivity pmax;
else
delete routes with the discovery of connctivity p other <pmax – p threshold;
return route with packet delay d min;
end if
end if
End of Route Discovery

Flowcharts for Methodology



ISSN: 2321-8169
141 – 147

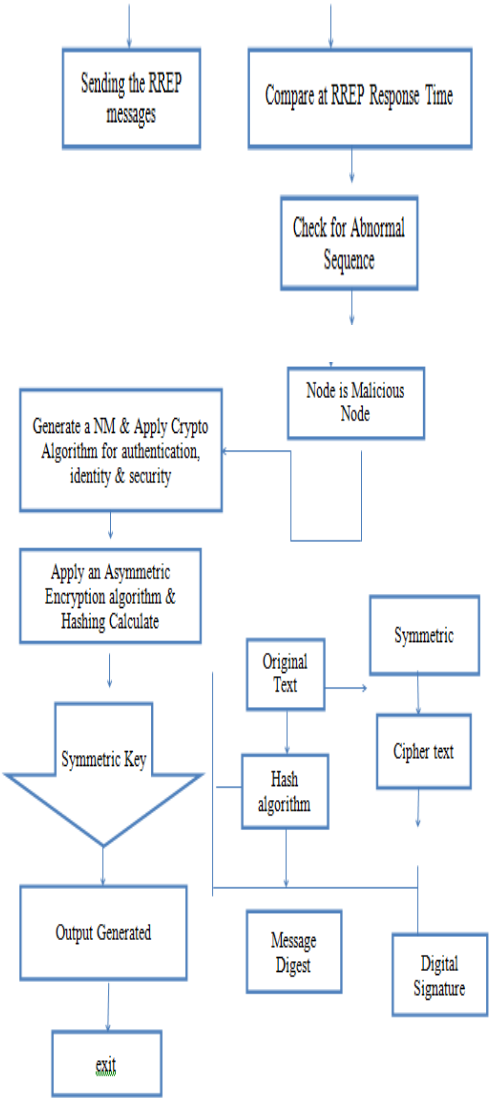


Figure5 Flowcharts for Methodology

Malicious Node Simulation Result for 50 Nodes

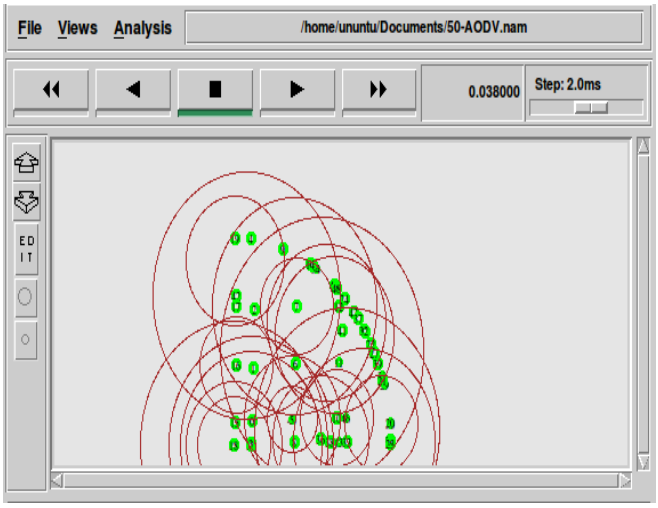


Figure6 Initial stages for nodes showing their respective position

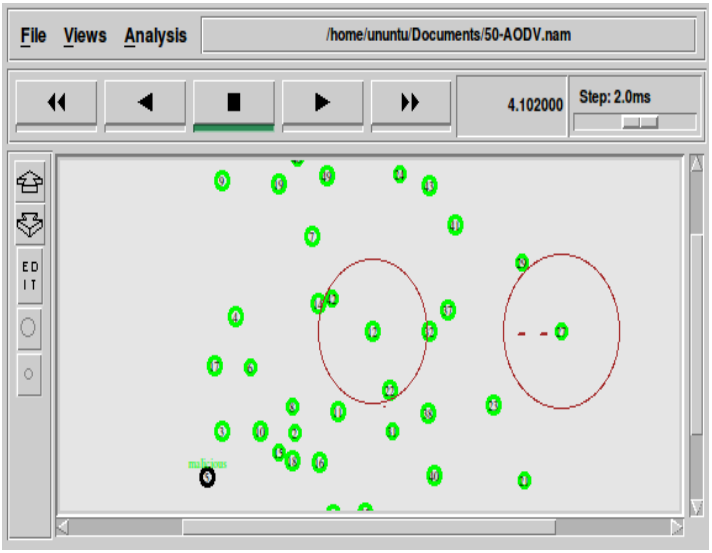


Figure7 Transmission between node 12 and 27, Node 5 is malicious node

AODV Protocol Simulation Result for 50 Nodes

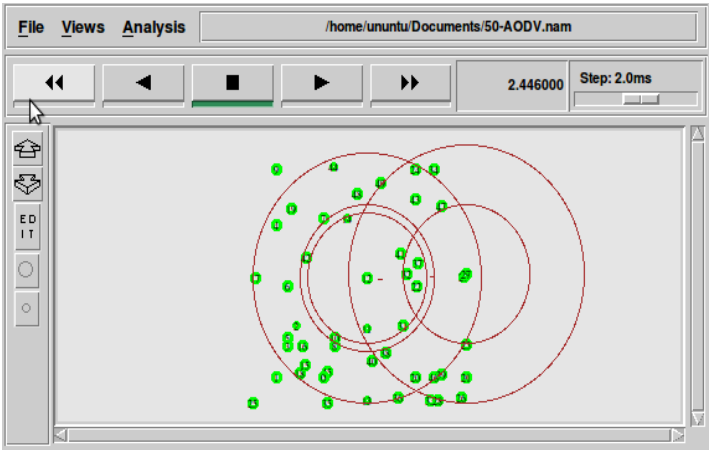


Figure8 Cluster formed and data transmission between node 27 and 12

End-to-End Delay

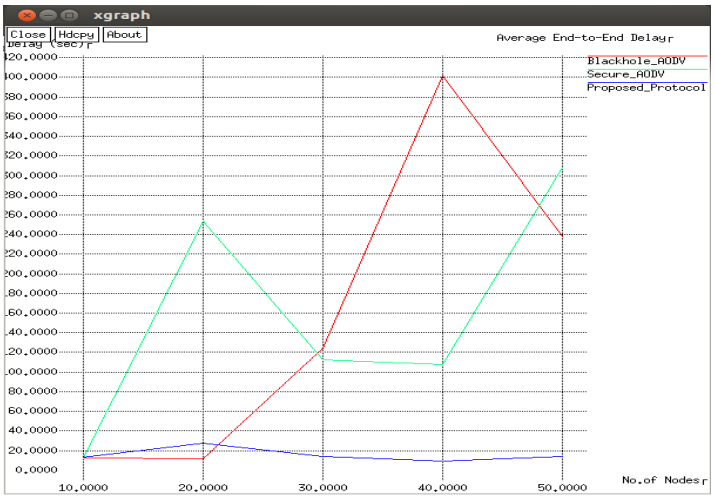


Figure9 Comparison of average end-to-end delay

 ISSN: 2321-8169
141 – 147

Energy Consumption

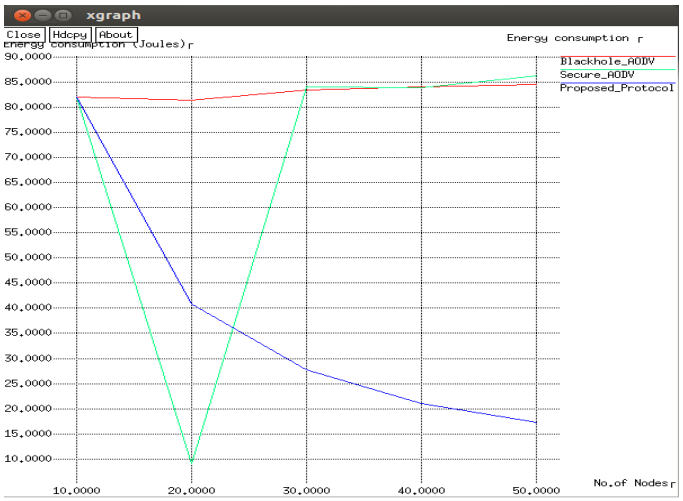


Figure10 Comparison of Energy Consumption

Packet Delivery Ratio

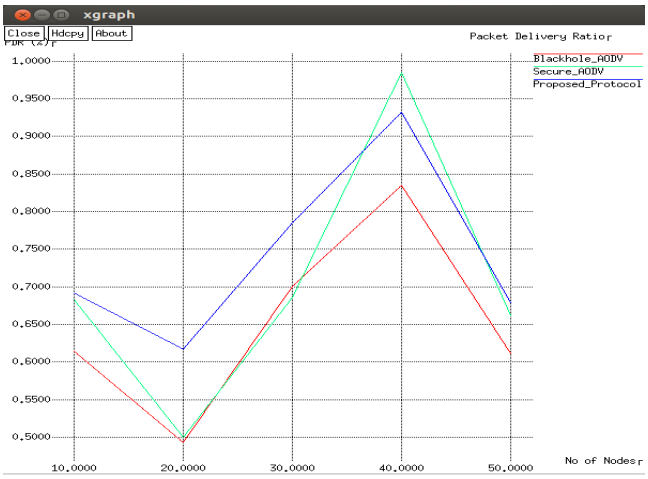


Figure11 Comparison of Packet Delivery Ratio

Throughput

Figure12 Comparison of Throughput

Overhead

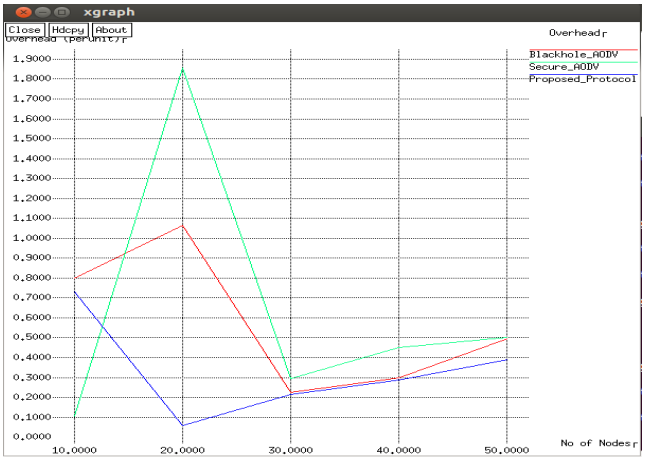


Figure13 Comparison of Overhead

V. CONCLUSION

VANET has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of VANET comparative to its vast potential it has still many challenges which we have to deal. Security of VANET is one of the important features for its deployment. In our base work black hole attack used in network communication using AODV protocol. As we know there are many issues in VANET and specially security issues. Therefore in our research work we proposed a new protocol which is known as GPSR which has superior result as compared to base work in term of end to end delay, energy consumption, packet delivery ratio, throughput and overhead. Besides this a security algorithm also implemented so that unauthorized person cannot access the authentic data. So after analyzing the data we can say our proposed work is far better than previous work. With pace of time new technology came into existence to enhance the parameters. In these days machine learning and artificial intelligence are very popular with IoT concept. We can adept these technology for further enhancement.

REFERENCES

[1]. Salim Lachdhaf,, Mohamed Mazouzi, " Detection and Prevention of Black Hole Attack in VANET Using Secured AODV Routing Protocol", Conference Paper, DOI: 10.5121/csit.2017.71503 Natarajan Meghanathan et al. (Eds) : NeTCoM, CSEIT, GRAPH-HOC, NCS, SIPR – 2017 pp. 25– 36, 2017

[2]. Bharti, D.P.Dvedi, " Performance Analysis of Black hole Attack using CBR/UDP Traffic Pattern with AODV routing Protocol in VANET", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2016): 6.391

[3]. Sagar R Deshmukh, P N Chatur, Nikhil B Bhople," AODV-Based Secure Routing Against Black hole Attack in MANET", IEEE International Conference On Recent Trends in Electronics Information Communication Technology, India, pp. 1960-1964, 2016

[4]. Heithem Nacer and Mohamed Mazouzi, "A Scheduling Algorithm for Beacon Message in Vehicular Ad Hoc Networks",International Conference on Hybrid Intelligent Systems (HIS 2016),Marrakech, Morocco, pp. 489-497, 2016.

[5]. Roshan Jahan, Preetam Suman, "Detection of malicious node and development of routing strategy in VANET," 3rd International Conference on Signal Processing and Integrated Networks (SPIN), IEEE, pp. 472-476, 2016

[6]. Sathish M, Arumugam K, S. Neelavathy Pari, Harikrishnan V S, "Detection of Single and Collaborative Black Hole Attack in MANET," International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), IEEE, pp.2040-2044, 2016.

[7]. Sathish M, Arumugam K, S. Neelavathy Pari, Harikrishnan V S, "Detection of Intelligent Malicious and Selfish Nodes in VANET using Threshold Adaptive Control," 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA), IEEE, 2016

[8]. P.S Hiremath and Anuradha T, "Adaptive Fuzzy Inference System for Detection and Prevention of Cooperative Black Hole Attack in MANETs", International Conference on Information Science (ICIS), pp.245-251, 2016

[9]. P.S Hiremath and Anuradha T, "Adaptive Method for Detection and Prevention of Cooperative Black Hole Attack inMANETs", International Journal of Electrical and Electronics and Data Communication, Volume-3, Issue-4, pp.1-7, 2015

[10]. R. Khatoun, P. Guy, R. Doulami, L. Khoukhi and A. Serhrouchni, "A Reputation System for Detection of Black Hole Attack in Vehicular Networking," International Conference on Cyber Security of Smart cities, Industrial Control System and Communications (SSIC), 2015

[11]. Surmukh, S.; Kumari, P.; Agrawal, S. Comparative Analysis of Various Routing Protocols in VANET. In Proceedings of 5th IEEE International Conference on Advanced Computing & Communication Technologies, Haryana, India, 21–22February 2015

[12]. Elias C. Eze, Sijing Zhang and Enjie Liu," Vehicular Ad Hoc Networks (VANETs): Current State, Challenges, Potentials and Way Forward", Proceedings of the 20th International Conference on Automation & Computing, Cranfield University, Bedfordshire, UK, 2014

[13]. Sabih ur Rehman, M. Arif Khan, Tanveer A. Zia, Lihong Zheng, "Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges", Journal of Wireless Networking and Communications, 2013, pp. 29-38.

[14]. Sirwan A.Mohammed and Sattar B.Sadkhan, "Design Of Wireless Network Based On Ns2", Journal of Global Research in Computer Science (jgrcs), Volume 3, No. 12, December 2012.

[15]. Halabi Hasbullah, Irshad Ahmed Soomro, Jamalul-lail Ab Manan," Denial of Service (DOS) Attack and Its Possible Solutions in VANET", International Scholarly and Scientific Research & Innovation 4(5) 2010, World Academy of Science, Engineering and Technology, Vol:4 2010-05-25.