ISSN No. 0976-5697

Volume 4, No. 8, May-June 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Performance Evaluation of Modified AODV Protocol with DSR routing protocol In Presence of Black Hole Attack in Mobile Ad-hoc Network

Romina Sharma
SRIT Jabalpur Jabalpur, India
sharmaromina@gmail.com

Rajesh Shrivastava
SRIT Jabalpur Jabalpur, India
rajesh_5479@rediffmail.com

***Abstract*—** A mobile ad-hoc network (MANET) is a non-infrastructure network that consists of self configuring mobile nodes connected by wireless links. In this network, mobile nodes are free to move in an open environment. Two nodes can communicate directly as long as they are within the radio communication range of each other, but when the two nodes are far apart, they require the help of other intermediate nodes to relay their traffic. The mobile nodes can receive and forward packets as a router. The characteristics of self-organization and wireless medium make Mobile Ad hoc Network (MANET) easy to set up and thus attractive to users. The open and dynamic operational environment of MANET makes it vulnerable to various network attacks .So routing is a critical issue in MANET. Many applications today, especially military and emergency ones, are based upon *ad hoc* wireless networks, where security requirements are harder to enforce than in traditional networks .Hence the focus of this research paper is to evaluate the performance of our proposed algorithm with DSR routing protocols in presence of black hole attack. Our simulation tool will be OPNET modeler. The performance of these routing protocols is analyzed by three metrics: delay, network load and throughput.

Keywords- Wireless Ad-hoc Network, Black Hole Attack, Simulation, Security, AODV, DSR, OPNET, MANET

I. INTRODUCTION

Mobile Ad-hoc network is a set of wireless devices called wireless nodes, which energetically connect and transport information. Wireless nodes can be personal computers (desktops/laptops) with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices **[1]**. A Mobile Ad hoc Network (MANET) is a set of wireless mobile nodes which form a self-motivated independent network. Nodes talk with each other without the interference of centralized access points or base stations. In such a network, each node acts both as a router and as a host. Due to the restricted transmission range of wireless network, multiple hops are needed to swap data between nodes in the network .In MANET a wireless node can be the source, the destination, or an intermediate node of data transmission. When a wireless node plays the role of intermediary node, it serves as a router that can collect and promote data packets to its neighbor closer to the destination node. Due to the character of an ad-hoc network, wireless nodes are inclined to keep moving rather than stay still. Therefore the network topology changes from time to time. In a mobile ad hoc network, all the nodes work together with each other to forward the packets in the network, and hence each node is effectively a router. Thus one of the most important issues is routing **[2].**

II. AD-HOC ON DEMAND ROUTING (AODV) PROTOCOL AND DYNAMIC SOURCE ROUTING PROTOCOL

a. The Ad Hoc On-Demand Distance Vector (AODV) routing protocol is a version of the DSDV protocol for dynamic link conditions. Each node in an Ad-hoc network maintains a routing table, which stores information about the route to a particular destination. At whatever time a packet is to be sent by a node, it initially checks its routing table to decide whether a path to the target is already accessible or not. If so, it uses that path to send the packets to the target. If a path is not accessible or the previously entered path is inactivated, then the node initiates a path discovery process. A RREQ (Route Request) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route Reply) packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbors. If its routing table does contain an entry to the destination, then the next step is the comparison of the 'Destination Sequence' number in its routing table to that present in the RREQ packet. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREQ packet, then the node relays the request further to its neighbors. If the number in the routing table is higher than the number in the packet, it denotes that the route is a 'fresh route' and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route Error) packet to all other nodes that uses this link for their communication to other nodes. This is

illustrated in figure 1. Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. A malicious node M can carry out many attacks against AODV. This paper provides routing security to the AODV routing protocol by eliminating the threat of 'Black Hole' attacks **[3].**

Figure 1 Route discovery in AODV

Figure 2 Route Maintenance in AODV

b. Dynamic Source Routing (DSR) Protocol is an on-demand routing protocol developed at Carnegie Mellon university Pittsburgh USA for use of multi-hop wireless mobile ad hoc networks. DSR routing protocol is designed for mobile ad hoc network to keep features of both on-demand routing protocol and source routing protocol. DSR protocol performing as on-demand routing establishes a route between source and destination node when source node wants to send data packets, routing of data packets in DSR protocol between mobile nodes of ad hoc network is based on request/reply method.DSR control the wastage of bandwidth by eliminating need of periodic table updating. As discussed earlier that DSR protocol can establish a route to destination through source routing, therefore it does not require transmission of periodic hello message by a node to inform its neighbor about his presence. Attractive point of DSR source routing protocol is that intermediate nodes of ad hoc network do not need to keep route information. The path is clearly defined in data packet of source node. DSR routing protocol supports unidirectional communication between mobile nodes. In mobile wireless ad hoc network communication between mobile nodes through DSR routing protocol is achieved by two phases: Route establishment and maintenance **[4]** .In order to discover a route between two nodes, DSR floods the network with a Route Request packet. This packet is forwarded only once by each node after concatenating its own address to the path. When the targeted node receives the Route Request, it piggybacks a Route Reply to the sender and a route is established. Each time a packet follows an established route, each node has to ensure that the link is reliable between itself and the next node. DSR provides three successive steps to perform this maintenance: link layer acknowledgment, passive acknowledgment and network layer acknowledgment. If a route is broken, then the node which detects the failure sends a Route Error packet to the original sender **[5]**.

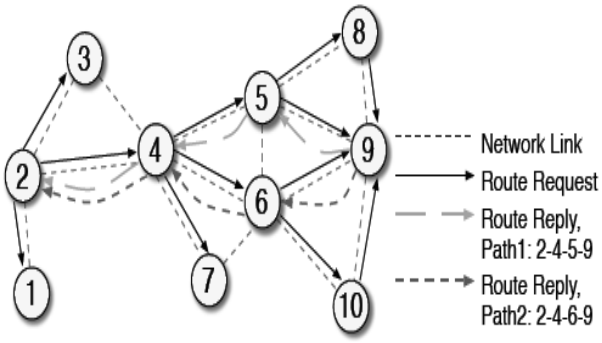

Figure 3 Route discovery in DSR

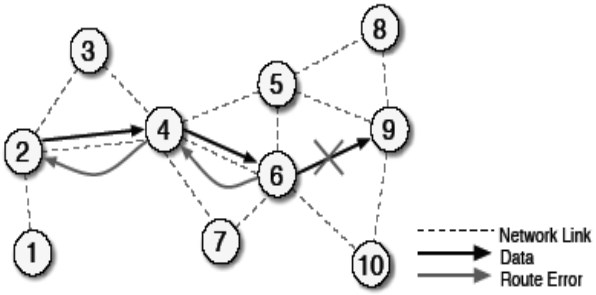

Figure 4 Maintenance for Error Route in DSR

III. BLACK HOLE ATTACK IN MANET

Route discovery is a vulnerability of on-demand ad-hoc routing protocols, especially AODV, which an adversary can exploit to perform a black hole attack on mobile ad-hoc network. A malicious node in the network receiving an RREQ message replies to source nodes by sending a fake RREP message that contains desirable parameters to be chosen for packet delivery to destination nodes. After promising (by sending a fake RREP to confirm it has a path to a destination node) to source nodes that it will forward data, a malicious node starts to drop all the network traffic it receives from source nodes. **This deliberate dropping of packets by a malicious node is what we call a black hole attack.** A malicious node sends RREP messages without checking its

routing table for a fresh route to a destination. As shown in Fig. 1 above, source node 0 broadcasts an RREQ message to discover a route for sending packets to destination node 2. An RREQ broadcast from node 0 is received by neighboring nodes 1, 3 and 4. However, malicious node 4 sends an RREP message immediately without even having a route to destination node 2. An RREP message from a malicious node is the first to arrive at a source node. Hence, a source node updates its routing table for the new route to the particular destination node and discards any RREP message from other neighboring nodes even from an actual destination node. Once a source node saves a route, it starts sending buffered data packets to a malicious node hoping they will be forwarded to a destination node. Nevertheless, a malicious node (performing a black hole attack) drops all data packets rather than forwarding them on **[6].**

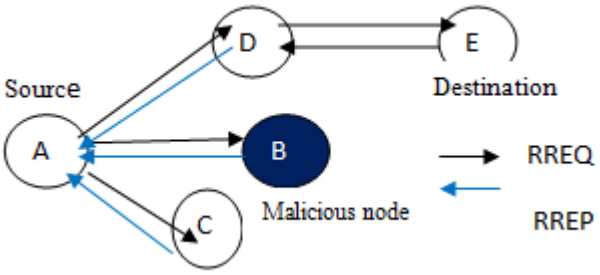

Figure 5 RREQ broadcast

IV. RELATED WORK

Marti *et al.* proposes two techniques that improve throughput in an ad hoc network in the present of misbehaved nodes .The ***watchdog*** method is used for each node to detect misbehaving nodes in the network. When a node sends a packet to next hop, it tries to overhear the packet forwarded by next hop. If it hears that the packet is forwarded by next hop and the packet matches the previous packet that it has sent itself, it considers the next hop behaves well. Otherwise it considers the next hop misbehaves .The ***pathrater*** uses the knowledge about misbehaving nodes acquired from watchdog to pick the route that is most likely to be reliable. Each node maintains a trust rating for every other node. When watchdog detects a node is misbehaving, the trust rating of the node is updated in negative way. When a node wants to choose a safe route to send packets, pathrater calculates a path metric by averaging the node ratings in the path .Marti et al implemented the solutions on DSR protocol using ns2 as simulation environment.

The simulation result shows the throughput of the network could be increased by up to 27% in a network where packet drop attack happens. However routing overhead is also increased by up to 24% **[3].**In a black hole attack, several malicious nodes falsely claim a new route to the destination in order to absorb all packets coming from the source. To combat this kind of routing protocol attack, **Hongmei et al.** proposed a solution that revolved around waiting and checking the replies from all other neighbouring nodes and then deciding on the safe route. In Robust Routing by **Lee, Han, Shin**, the intermediate node requests its next hop to send a confirmation message to the source. After receiving both route reply and authentication message, the source verifies the legitimacy of path according to its policy **[7]**. **Juwad and Al-Raweshidy** presents an experimental performance comparison between Secure-AODV (SAODV) and AODV. They claim that there has been a lack of performance and security analysis in real network test-beds. A quantitative performance comparison between routing protocols AODV and SAODV is presented in an experimental test-bed and using the OPNET network simulator. These results show that SAODV is more effective in preventing two types of attacks (control message tampering and data dropping attacks) than AODV. **Chen *et al*.** quantitatively evaluate an approach detailing network survivability in wireless ad-hoc networks. They define network survivability as a combination of network failure impacts and failure durations and use a performance metric called excess packet loss due to failures **[8].**

V. MODIFIED AODV PROTOCOL TO PREVENT BLACK HOLE ATTACK

In our proposed work we modify the AODV protocol to prevent black hole attack. The solution that we propose here, basically, modifies the working of AODV protocol by adding next hop information in the RREP message and two other control messages including further route request (FRREQ) and Further route reply (FRREP).Once the source receives RREP with next hop information it broadcasts Further RREQ message to next hop nodes to the received RREPs and then next hop nodes reply back with Further RREP message to source node. After receiving FRREP source node routes data packets to the destination with the shortest path. If the node is black hole node the next hop of its does not exists so it never receives FRREQ and not reply FRREP to the source node so source node never send data to path suggest by black hole node.

Steps of the proposed algorithm

a. Source node broadcasts RREQ
b. Source node receives RREPs with next hop information from nodes
c. Source node fetch next hop information from RREPs received
d. Source node send further route request (FRREQ) to all next hop nodes
e. if (next hop node is of black hole)
   {
   FRREQ will not reach to next hop node and no FRREP will send to source
   }
   else
   {
   FRREQ will reach to all reliable next hop nodes and FRREP is send to source by these reliable next hop nodes
   }
f. Source node now receives FRREPs from reliable nodes; it will update its routing table
g. Source node routes data packets to the destination

VI. EXPERIMENTAL SETUP

The evaluation is carried out with the OPNET Modeler 14.0. It is a useful research tool for achieving good simulation results. The simulation parameters like number of nodes, terrain range etc. as given in table 1 along with their respective values are used to examine the performance of the network **[9].**

Table: 1

Parameter	Value	Description
Simulation time	2 mins	Maximum execution time
Terrain Dimensions	1000 * 1000	Physical area in which the nodes are placed in meters
Number of nodes	20	Nodes participating in the network
Mobility model	Random way point	Mobility model used
Node placement	uniform	Node placement policy
Mobility	0-10 m/s	Speed of node
Routing protocol	AODV,DSR	Routing protocol used

In this research paper we have evaluating the performance of MAODV protocol with DSR routing protocol in presence of black hole node. There are two scenarios in this research paper -.In first scenario we have 20 reliable nodes with Modified AODV routing protocol with one blackhole node. In second scenario again we have 20 nodes with DSR routing protocol and one black hole node. All scenarios are run under identical mobility and traffic conditions. The performance metrics chosen for the evaluation of MAODV and DSR were traffic sent and received, wireless end to end delay, network throughput and network load.

The network topology graph for 20 nodes is shown below follow with two scenarios simulation result.

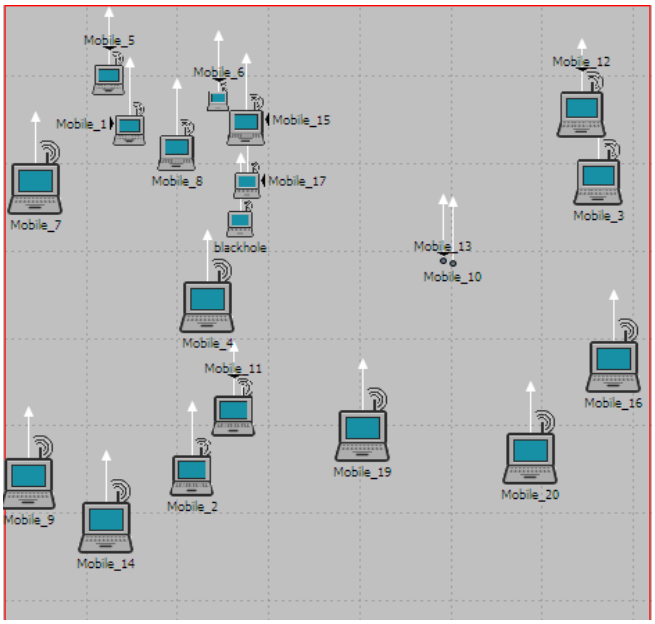

Figure 6. Network topology of our scenario

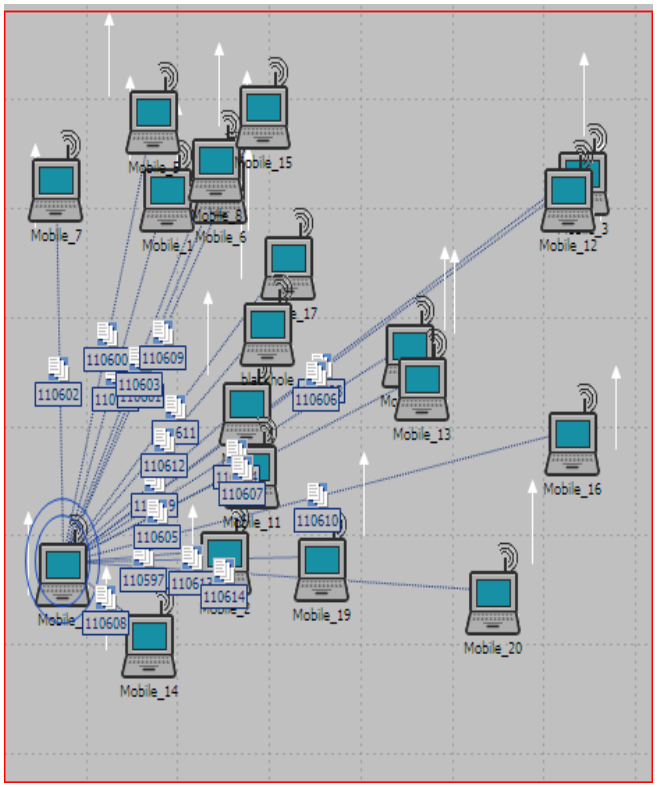

Figure 7 Simulation Animation Graph

VII. RESULTS

The performance metrics used for evaluation are:

a) Total traffic sent
b) Total traffic received
c) Throughput
d) End-to-end delay
e) Network load

a. ***Total traffic sent:*** Total number of MANET packets sent per second by this node to other MANET nodes in the network.

b. ***Total traffic received:*** Total number of MANET packets received per second by this node from all other MANET traffic sources in the network**.**

c. ***End to end delay:*** It represents the end-to-end delay of all the data packets that are successfully received by the WLAN MAC and forwarded to the higher layer.

d. ***Throughput:*** Throughput is the average rate of successful message delivery over a communication channel. Throughput is the ratio of total amount of data which reaches the receiver from the sender to the time it takes for the receiver to receive the last packet. It is calculated according to this formula: Throughput = Packets Received / Packets Sent.

e. ***Network load:*** It is the total traffic received by the entire network from higher layer of MAC which is accepted and queued for transmission. It indicates the quantity of traffic in entire network. It represents the total data traffic in bits per seconds received by the entire network from higher layer accepted and queued for transmission.

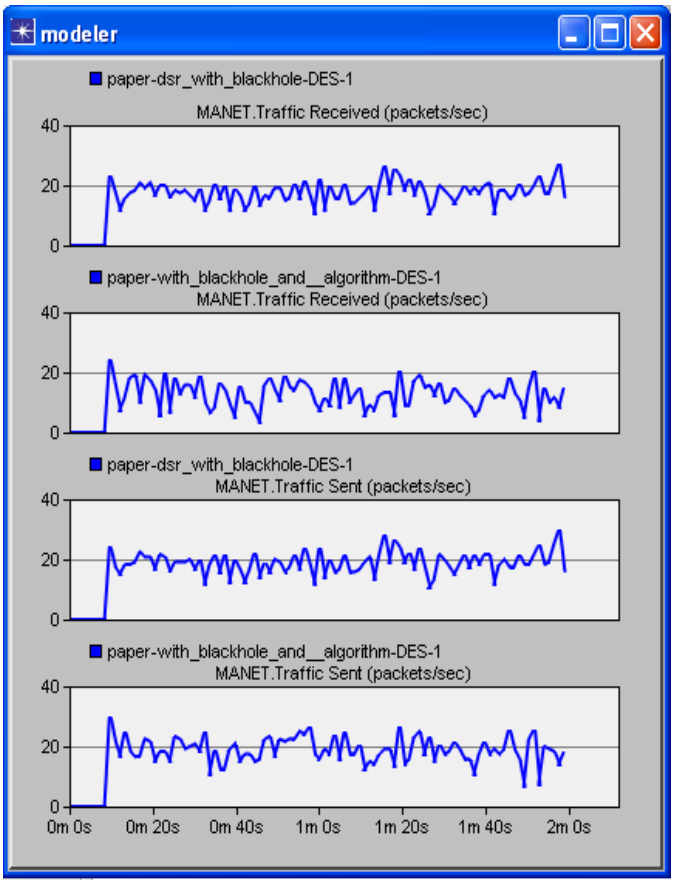

Figure 8 traffic received and sent

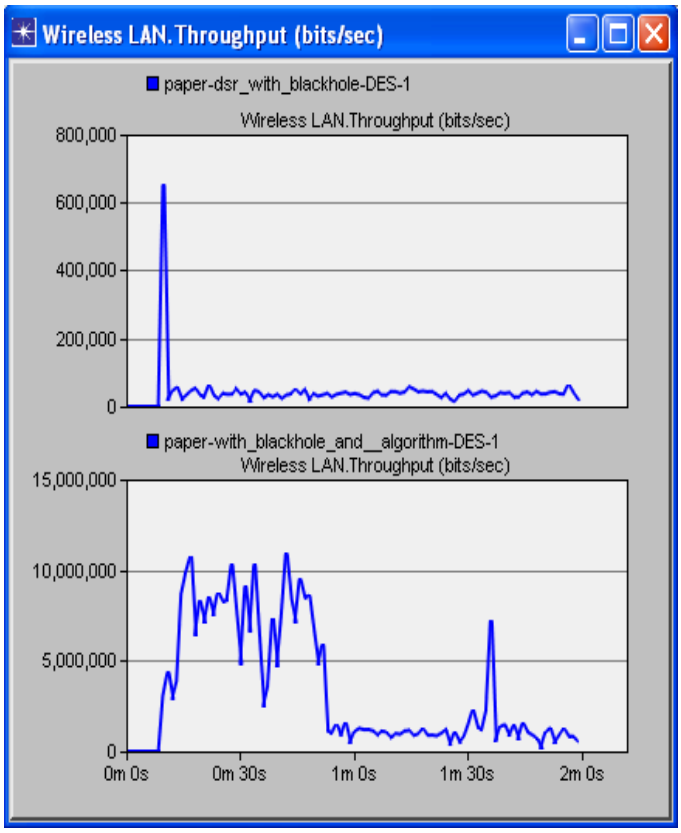

Figure 9 Throughput

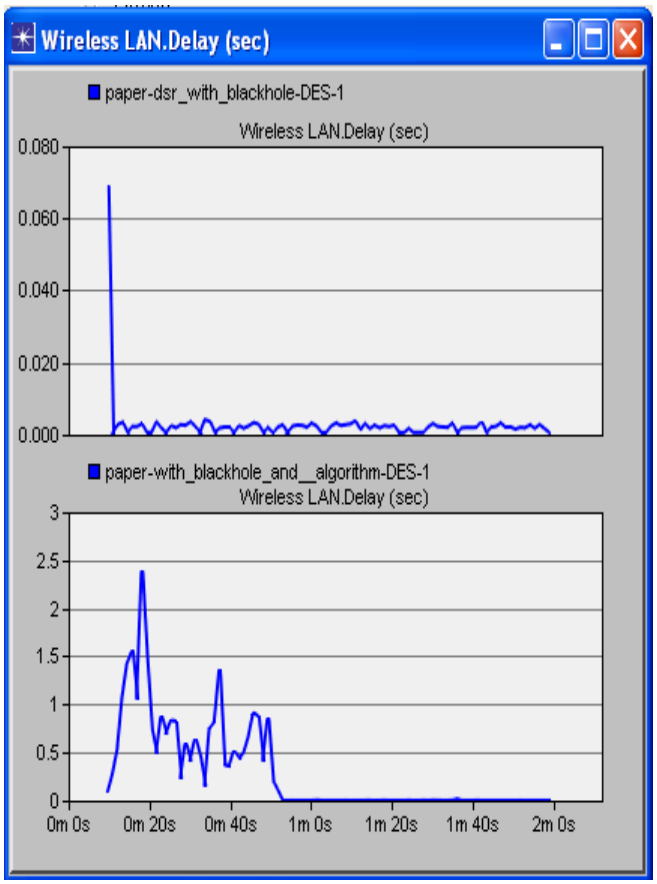

Figure 10 end-to-end delay

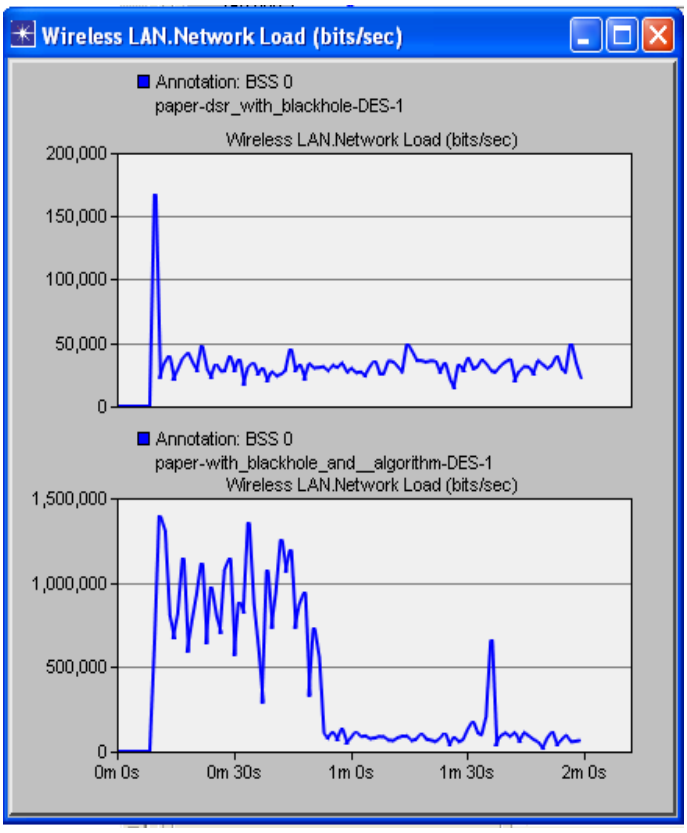

Figure 11 Network Load

VIII. CONCLUSION

IN this research paper we discussed two routing protocols and the vulnerabilities associated with them. One type of attack, the black hole, which can easily be deployed against the MANET, is described. In this research paper we evaluate the performance of our proposed modified AODV with the DSR routing protocol. Routing protocols comparison has been done on the basis of three different performance metrics i.e. Average throughput, packet delivery ratio and end-to-end delay. Throughput and Delay is more in Modified AODV as compared to DSR routing protocol. The solution is simulated using the OPNET Simulator and is found to achieve the required security with minimal delay & overhead. Future works may be concentrated on ways to reduce the delay in the network.

IX. ACKNOWLEDGMENT

I express my heartfelt gratitude to all the staff members of computer science engineering department SRIT Jabalpur and my family and friends and also to each and every individual who was associated with my project work, including those whom I may have inadvertently failed to mention.

X. REFERENCES

[1]. Irshad ullah , Shoaib Ur Rehman, Analysis of Black Hole attack On MANETs Using different MANET Routing Protocols, Master Thesis ,Electrical Engineering Blekinge Institute of Technology

[2]. Abdalla Ahmed Fekry Mahmoud, Reputed Authenticated Routing for Ad Hoc Networks Protocol (Reputed-ARAN). M.S. Thesis, Department of Computer Science, The American University in Cairo School of Sciences and Engineering May, 2005

[3]. Mehdi Medadian , Ahmad Mebadi, Elham Shahri " Combat with Black Hole Attack in AODV Routing Protocol" Proceedings of the 2009 IEEE 9th Malaysia International Conference on Communications 15 -17 December 2009 Kuala Lumpur Malaysia

[4]. Jahangir khan, Syed Irfan Hyder, Syed Malek Fakar Duani syed Mustafa, "Modeling and Simulation Of Dynamic Intermediate Nodes And Performance Analysis in MANETS Reactive Routing protocols" International Journal of Grid and Distributed Computing Vol. 4, No. 1, March 2011

[5]. Razan Al- Ani , " Simulation and Performance Analysis Evaluation for Variant MANET Routing Protocols" International Journal of Advancements in Computing Technology , Volume 3 , Number 1 , February 2011

[6]. Yibeltal Fantahun Alem , Zhao Cheng Xuan ,"Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection" 2010 2nd International Conference on Future Computer and Communication.V3-672

[7]. Mohammad Abu Obadiah, Shahnewaz Ahmed Faisal, Md. Abu Horaira, Tanay Kumar Roy "AODV Robust AODVR): An Analytic Approach to Shield Ad-hoc Networks from Black Holes" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 8, 2011

[8]. Malcolm Parsons, Peter Ebinger "Performance Evaluation of the Impact of Attacks on Mobile Ad hoc Networks"

[9]. Yudhvir Singh ,Yogesh Chaba ,Monika Jain, Prabha Rani ," Performance Evaluation of On-Demand Multicasting Routing Protocols in Mobile Adhoc Networks " 2010 International Conferenceon Recent Trends in Information, Telecommunication and Computing.

