International Journal of Advance Research in Science and Engineering
Vol. No. 5, Issue No. 08 , August 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

SIMULATION OF BLACK HOLE ATTACK USING OPNET ON MANETS USING DIFFERENT MANET ROUTING PROTOCOLS (AODV & OLSR)

[1]Manish Pandey, Dr. Sanjay Kumar Sharma[2]

[1] *Department of Electronics and Communication, Research Scholar, UIT-RGPV-Bhopal, M.P, (India)*

[2] *Department of Electronics and Communication, Professor, UIT-RGPV-Bhopal, M.P, (India)*

ABSTRACT

Wireless networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. It's an analogy to the black hole in the universe in which things disappear. The node presents itself in such a way to the node that it can attack other nodes and networks knowing that it has the shortest path.

The scope of this thesis is to study the effects of Black hole attack in MANET using both Proactive routing protocol i.e. Optimized Link State Routing (OLSR) and Reactive routing protocol Ad Hoc on Demand Distance Vector (AODV). Comparative analyses of Black hole attack for both protocols were taken into account. The impact of the attack on the performance of MANET is evaluated finding out which protocol is more vulnerable to the attack and how much is the impact of the attack on both protocols. The measurements were taken in the light of throughput, end to end delay and network load. Simulation is done in Optimized Network Engineering Tool (OPNET).

Keywords: MANET, Black Hole, Routing protocols.

.

I.INTRODUCTION

MANET is a wireless network that allows user to communicate and transfer information withoutusing any infrastructure and irrespective of their location. They are very useful for home uses,for military uses etc. Though they are very useful in day to day life, major threats are also thereto attack over it; some of them are wormhole attack, denial of service, eavesdropping etc. BlackHole attack is one of the major attacks on MANET. In this research paper, the effect of blackhole over the network is evaluated by varying certain values of the network like number ofnodes, pause time, area and speed. This paper shows that despite of presence of black hole inthe network, the increment and decrement of certain values also affect the performance ofMANET. For this, a table has been used which stores all the values of the parameters with andwithout black hole in the network obtaining

by variations among the several values. Before andafter values are stored which are afterwards will use for the analysis of the performance of theprotocol. The protocol used in this paper is AODV (Ad-Hoc on Demand Distance Vector)protocol.

MANET work without a centralized administration where node communicates with each other on the base of mutual trust. This characteristic makes MANET more vulnerable to be exploited by an attacker from inside the network. Wireless links also makes the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication . Mobile nodes present within the range of wireless link can overhear and even participate in the network.

MANETs must have a secure way for transmission and communication and this is quite challenging and vital issue as there is increasing threats of attack on the Mobile Network. Security is the cry of the day. In order to provide secure communication and transmission engineer must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from. MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources. Security is a prime importance in scenarios of deployment such as battlefield in an ad hoc network. Since MANET has multi hop links, it is venerable against several attacks like black hole attack, Byzantine attack, wormhole attack etc.

II BLACK HOLE ATTACK IN MANET

MANETs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the networks. These attacks are categorized in previous chapter “security issues in MANET” on the basis of their nature. In these attacks, black hole attack is that kind of attack which occurs in Mobile ad hoc networks (MANET). This chapter describes Black Hole attack and other attacks that are carried out against MANETs.

Black hole attack in AODV

Two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack.

Internal Black hole attack

This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node.

External Black hole attack

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET. External black hole attack can be summarized in following points

1. Malicious node detects the active route and notes the destination address.
2. Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
3. Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
4. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node.
5. The new information received in the route reply will allow the source node to update its routing table.
6. New route selected by source node for selecting data.
7. The malicious node will drop now all the data to which it belong in the route.

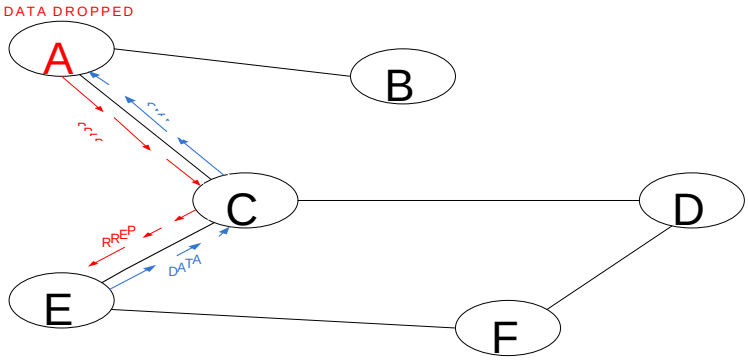

Fig. 1 Black hole attack specification

III RESEARCH METHODOLOGY

Research methodology defines how the development work should be carried out in the form of research activity. Research methodology can be understand as a tool that is used to investigate some area, for which data is collected, analyzed and on the basis of the analysis conclusions are drawn. There are three types of research i.e. quantitative, qualitative and mixed approach as defined in.

3.1 Quantitative Approach

This approach is carried out by investigating the problem by means of collecting data, experiments and simulation which gives some results, these results are analyzed and decisions are made on their basis. This approach is used when the researchers' wants verify the theories they proposed, or observe the information in greater detail.

3.2 Qualitative Approach

This approach is usually involves the knowledge claims. These claims are based on a participatory as well as / or constructive perspectives. This approach follows the strategies such as ethnographies, phenomenology and grounded theories. When the researcher wants to study the context or focusing on single phenomenon or concepts, they used qualitative approach to achieve their desired goals.

3.3 Mixed Approach

Mixed approach glue together both quantitative and qualitative approaches. This approach is followed when the researchers wants to base their knowledge claims on matter of fact grounds. Mixed approach has the ability to produce more complete knowledge necessary to put a theory and practice as it combined both quantitative and qualitative approaches.

3.4 Author's Approach

Author's approach towards the thesis is quantitative. This approach starts by studying the elated literature specific to security issues in MANETs and MANETs. Literature review is followed by simulation modeling. The results are gathered and analyzed and conclusions are drawn on the basis of the results obtained from simulation.

3.5 Research Design

The author divided the whole research thesis into four stages.

1) Problem Identification and Selection.
2) Literature study.
3) Building simulation.
4) Result analysis.

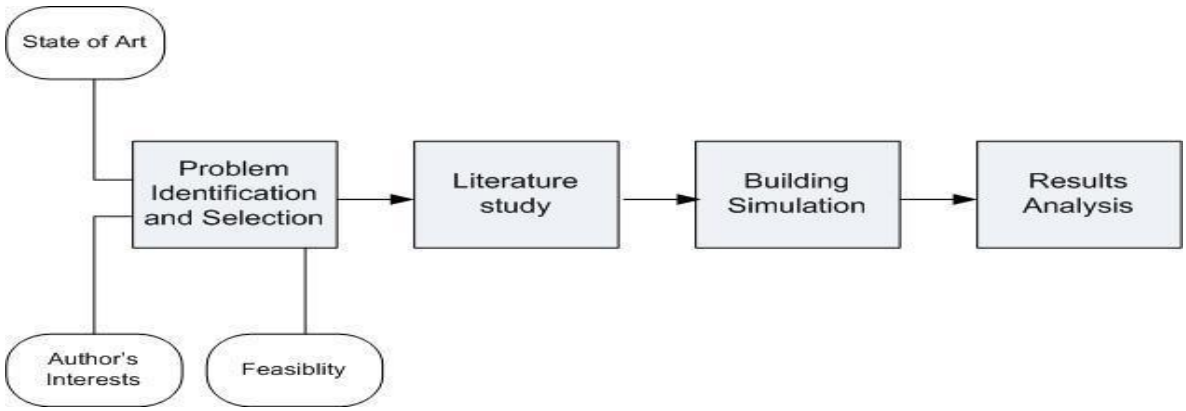

Fig. 2 Research Methodology

3.6 Simulation Tool

OPNET tool is selected to carry out the simulation. OPNET provide technologies, protocols, communication devices for academic research, assessment and improvement.It is efficient, robust and highly reliable which grant the user the ease of graphical interface, developing and running the simulation and validation of the results.

IV PERFORMANCE ANALYSIS

This chapter explains the various performance metrics required for evaluation of protocols. To reiterate the black hole attack, we begin with the overview of performance metrics that includes End to End delay, Throughput and Network load. These matrices are important because of it performance analysis of network. Furthermore implementation of the simulation setup, tools and its design are explained.

4.1 Performance Metrics

The performance metrics chosen for the evaluation of black hole attack were packet end to end delay, network throughput and network load.

The packet end-to-end delay is the average time in order to traverse the packet inside the network. This includes the time from generating the packet from sender up till the reception of the packet by receiver or destination and expressed in seconds. This includes the overall delay of networks including buffer queues, transmission time and induced delay due to routing activities.

4.2 Modeling of Network

At first network is created with a blank scenario using startup wizard. Initial topology is selected by creating the empty scenario and network scale is chosen by selecting the network scale. In our case we have selected campus as our network scale. Size of the network scale is specified by selecting the X span and Y span in given units. We have selected 1000 * 1000 meters as our network size. Further technologies are specified which are used in the simulation. We have selected MANET model in the technologies. After this manual configuration various topologies can be generated by dragging objects from the palette of the project editor workspace. After the design of network, nodes are properly configured manually.

4.3 Collection of Results and Statistics

Two types of statistics are involved in OPNET simulation. Global and object statistics, global statistics is for entire network's collection of data. Whereas object statistics involves individual nodes statistics.

4.4 Simulation Setup

Figure 1 employs the simulation setup of a single scenario comprising of 30 mobile nodes moving at a contact speed of 10 meter per seconds. Total of 12 scenarios have been developed, all of them with mobility of 10 m/s. Number of nodes were varied and simulation time was taken 1000 seconds. Simulation area taken is 1000 x

1000 meters. Packet Inter Arrival Time (sec) is taken exponential (1) and packet size (bits) is exponential (1024).

SIMULATION PARAMETERS	
Examined protocols	AODV and OLSR
Simulation time	1000 seconds
Simulation area (m x m)	1000 x 1000
Number of Nodes	16 and 30
Traffic Type	TCP
Performance Parameter	Throughput,delay,Network Load
Pause time	100 seconds
Mobility (m/s)	10m/s
Packet Inter-Arrival Time (s)	exponential(1)
Packet size (bits)	exponential(1024)
Transmit Power(W)	0.005
Mobility Model	Random waypoint

V. RESULTS

This chapter focuses on result and its analysis based on the simulation performed in OPNET modeler 14.5. Our simulated results are provided in Figures (6.1-6.12) gives the variation in network nodes while under Black Hole attack. To evaluate the behavior of simulated intrusion based black hole attack we considered the performance metrics of packet end to end delay, throughput and network load. These parameters are already defined in chapter 6 “Performance analysis”.

5.1 Packet End-to-End Delay

International Journal of Advance Research in Science and Engineering
Vol. No. 5, Issue No. 08 , August 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

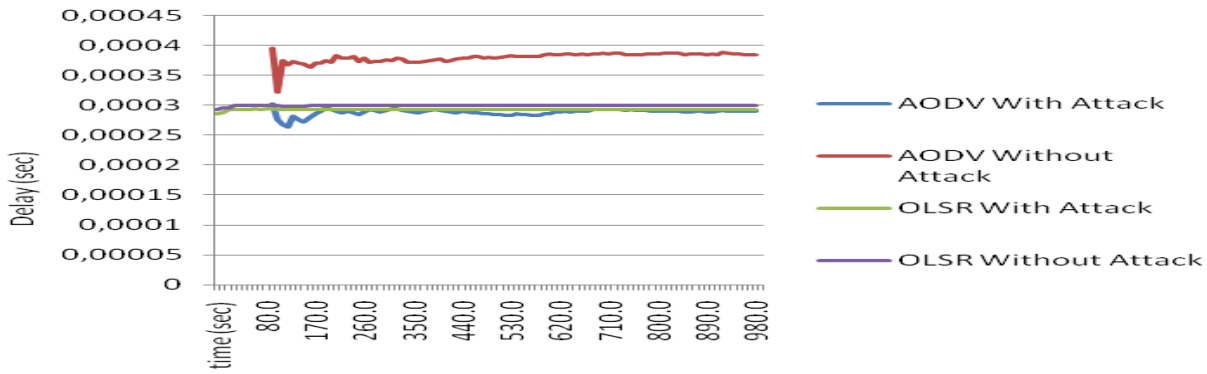

Fig. 3 End to End delay of OLSR and AODV with vs. without attack for 16 nodes

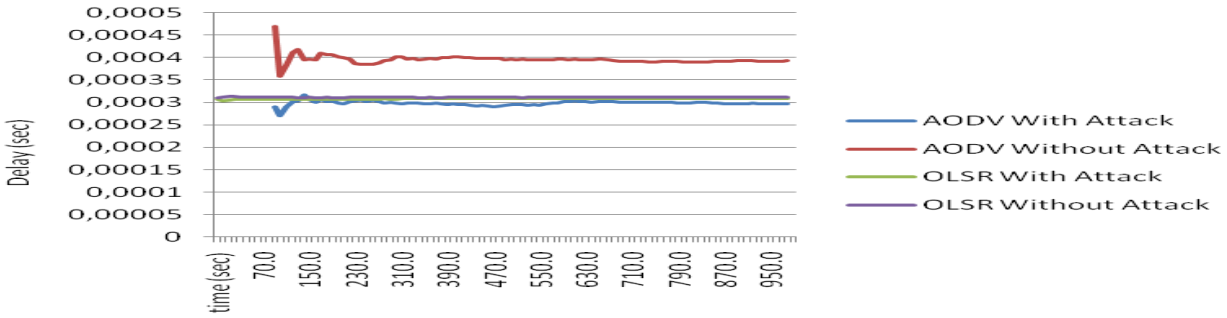

Fig. 4 End to End delay for OLSR with vs. without attack for 30 nodes

Fig. 3 and Fig. 4 show the average packet end-to-end delay in presence of a malicious node only.

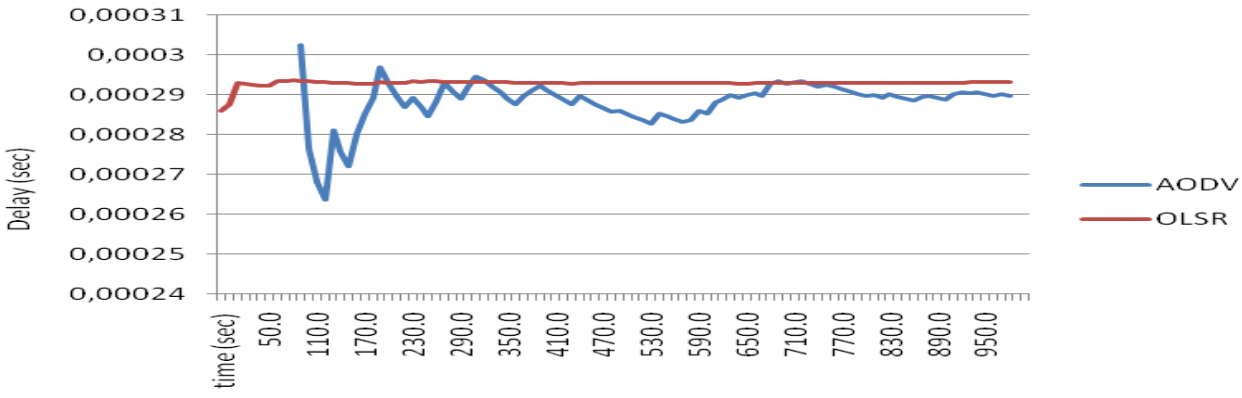

Fig. 5 End to End delay 16 nodes AODV vs. OLSR with attack

International Journal of Advance Research in Science and Engineering
Vol. No. 5, Issue No. 08 , August 2016
www.ijarse.com
IJARSE
ISSN 2319 - 8354

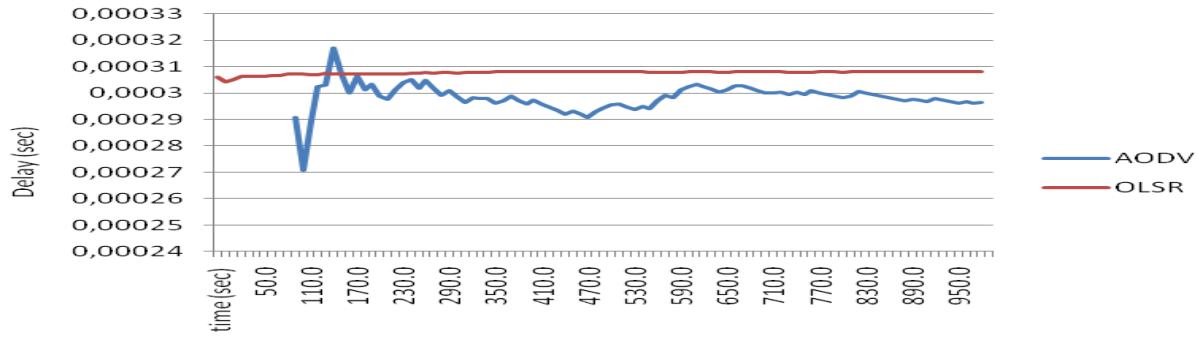

Fig. 6. End to End delay 30 nodes AODV vs. OLSR with attack

5.2 Throughput

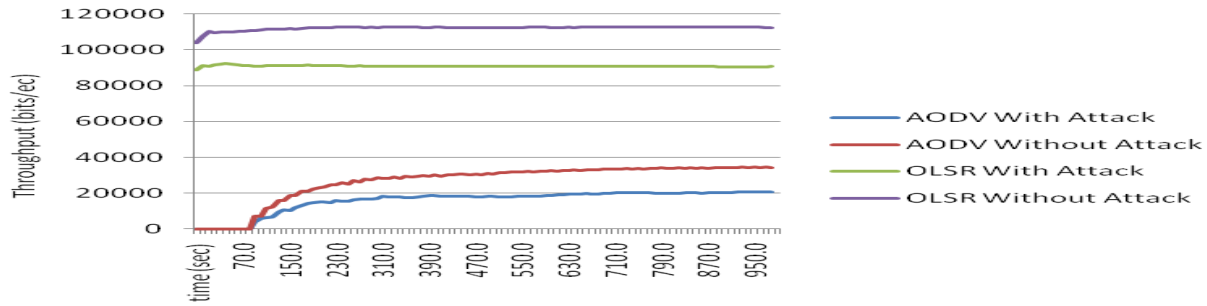

Fig. 7 Throughput of OLSR and AODV with vs. without attack for 16 nodes

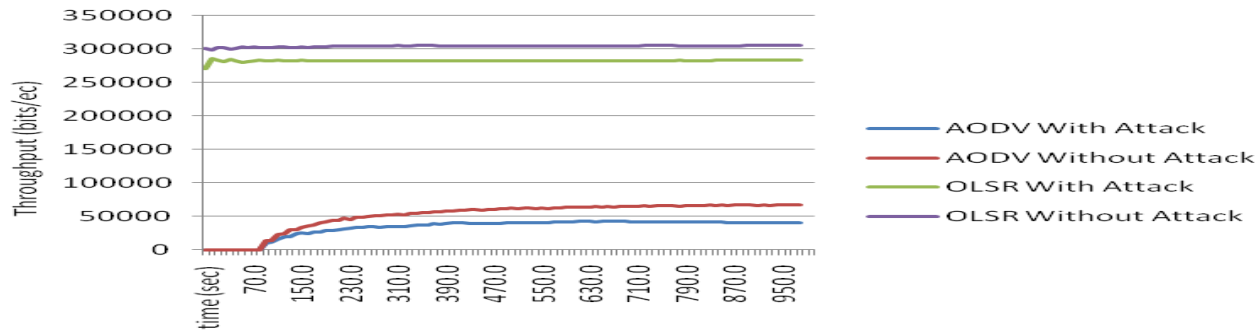

Fig. 8 Throughput of OLSR and AODV with vs. without attack for 30 nodes

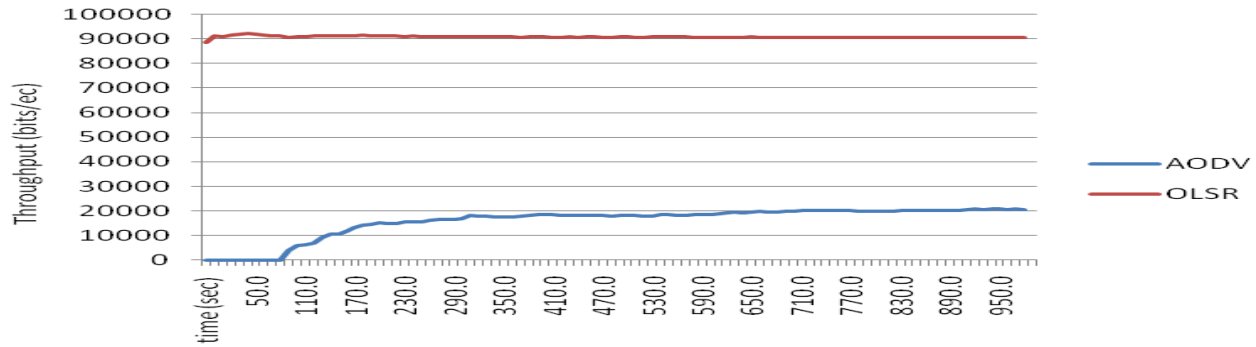

Fig. 9Throughput 16 nodes AODV vs. OLSR with attack

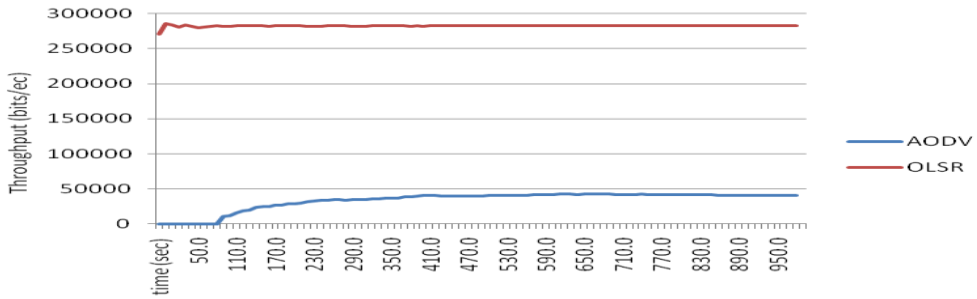

Fig. 10 Throughput 30 nodes AODV vs. OLSR with attack

5.3 Network Load

The network load of OLSR is much high as compare to AODV. In case of attack OLSR has less network load as compare to without attack. In case of 16 nodes the network load of OLSR is 3 times higher in case of without attack which implies that it is actually routing its packet to the entire destination properly. But under attack it cannot send its packet i.e. packet discarding leads to a reduction of network load.

In case of 30 nodes there is a slight variation in between OLSR with and without attack. This is due to the high number of nodes which leads to more increase in routing traffic. However AODV show no changes in both cases of 16 and 30 number of nodes.

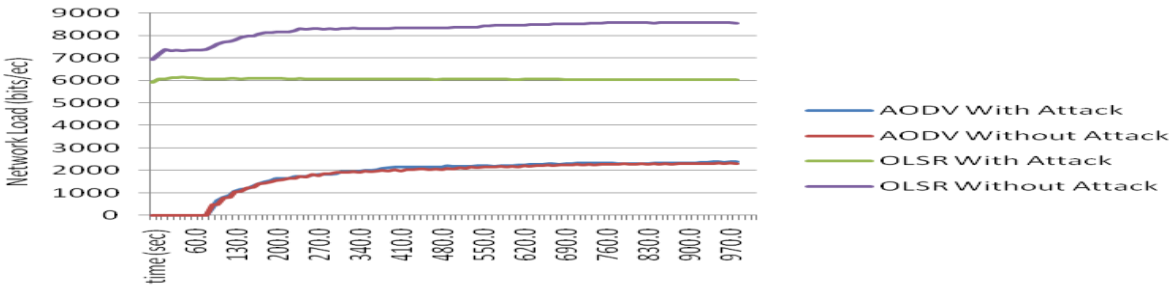

Fig. 11 Network Load of OLSR and AODV with vs. without attack for 16 nodes

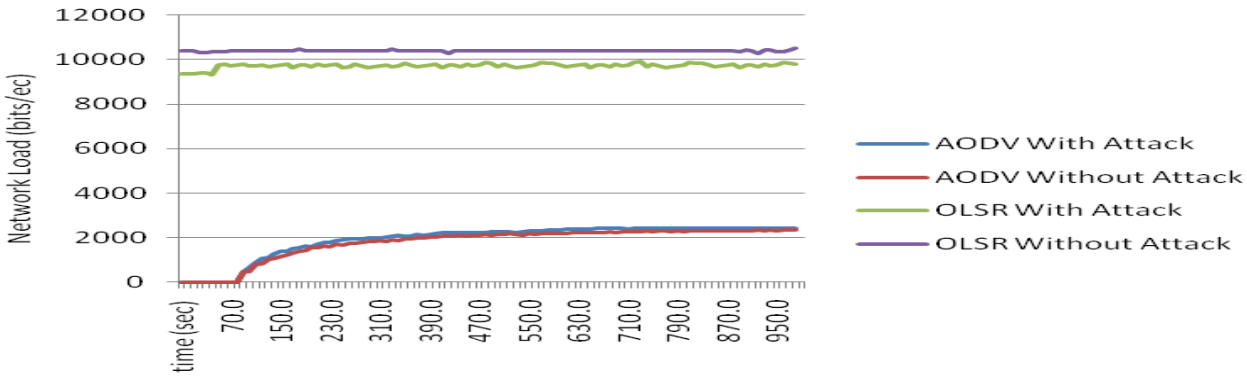

Fig. 12Network Load of OLSR and AODV with vs. without attack for 30 nodes

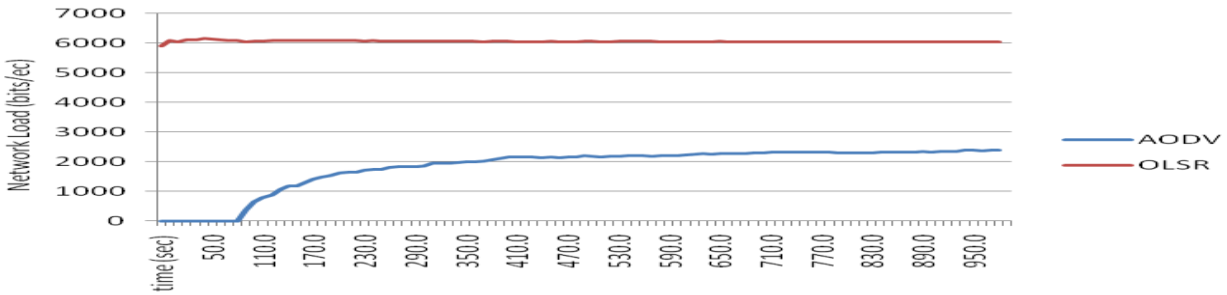

Fig. 13 Network load 16 nodes AODV vs. OLSR with attack

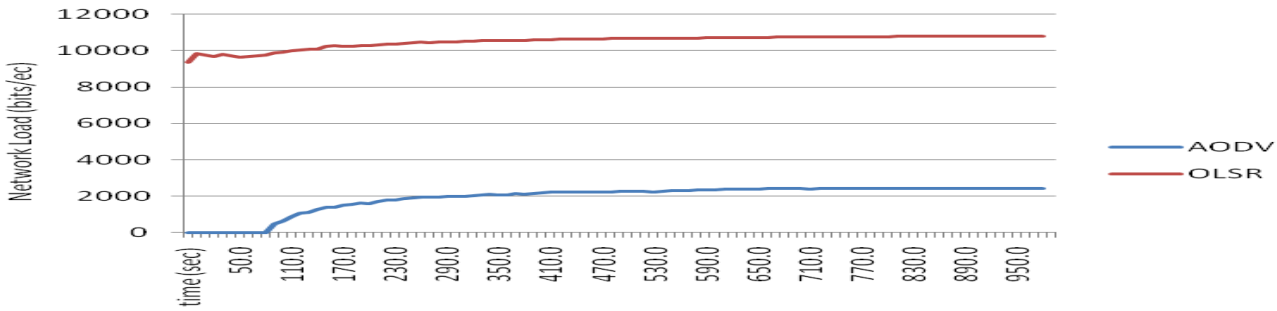

Fig. 14 Network load 30 nodes AODV vs. OLSR with attack

VI CONCLUSIONS

Mobile Ad Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of MANET comparative to its vast potential it has still many challenges left in order to overcome. In our study we analyzed that Black Hole attack with four different scenarios with respect to the performance parameters of end to end delay, throughput and network load. In a network it is important for a protocol to be redundant and efficient in term of security. We have analyzed the vulnerability of two protocols OLSR and AODV have more severe effect when there is higher number of nodes and more route requests. The percentage of severances in delay under attack is 2 to 5 percent and in case of OLSR, where as it is 5 to 10 percent for AODV. The throughput of AODV is effected by twice as compare of OLSR. In case of network load however, there is effect on AODV by the malicious node is less as compare to OLSR. Based on our research and analysis of simulation result we draw the conclusion that AODV is more vulnerable to Black Hole attack than OLSR.

REFERENCES

[1]http://en.wikipedia.org/wiki/Personal_area_network , last visited 12, Apr, 2010.

[2]http://en.wikipedia.org/wiki/Mobile_ad_hoc_network, last visited 12, Apr, 2010.

[3]C.E.Perkins and E.M.Royer, “Ad Hoc on Demand Distance Vector Routing,” Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applictions, pp.90-100, Feb, 1999.

[4]C.M barushimana, A.Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad Hoc Networks," Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684, May, 2003.

[5]http://www.faqs.org/rfcs/rfc3561.html .