# Performance Evaluation of Proactive and Reactive Routing Protocols against Packet Drop Attack in Mobile Ad hoc Networks (MANET)

*Muwassil Ahmed Shaikh and P. U. Dere*

**Abstract: In this paper the effect of Packet drop or Black hole attack are evaluated in MANET routing protocols namely AODV as reactive and OLSR as a proactive routing protocols by using performance metrics delay, network load, throughput and data dropped using OPNET Modeler 17.5 network simulator tool. By keeping network area 1000m x 1000m, simulation time 1800 second, IEEE 802.11g using data rate 24 mbps and mobility model Random way point are constant. In this study black hole node is a malicious node with less buffer size of 64Kb. In OPNET, simulation result show that comparatively reactive routing protocol like AODV is more vulnerable than proactive routing protocol OLSR under varying number of black hole node attack.**

**Keywords: AODV, MANET, OLSR, OPNET Modeler, Packet drop attack,.**

## I. INTRODUCTION

MANET Stands for Mobile Ad hoc network, is an autonomous decentralized and infrastructure less wireless system [1]. MANET consist of a group of mobile nodes which can acts as a host or router to receive and forward the packet to the neighbouring nodes on the basis of mutual trust. These nodes are the systems or devices such as mobile phone, laptop, MP3 player, tablet PC, personal digital assistant and personal computer. Routing protocols provide a means for wireless nodes to communicate with nodes outside their transmission range by discovering a path between the source and destination. MANET working group (WG) under the Internet Engineering Task Force (IETF) works devoted for developing IP routing protocols. MANET working group have been developed many routing protocols such as AODV, DSR, OLSR etc. Self-configuration and easy deployment features of MANETs resulted in many applications to makes it suitable for emergency, surveillance situations and rescue operations. Because of this characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Security always determined implies the identification of potential attacks, threats and vulnerability of a certain system. Present-day routing protocols do not much focus on the security and the privacy issues.

Muwassil Ahmed Shaikh and P. U. Dere are with Electronicd & Telecommunication Department, Terna Engineering College, Nerul, Navi Mumbai. Emails: muwassil@hotmail.com , pravindere@rediffmail.com )

To achieve security in MANETs is particularly difficult because of the vulnerability of links, intermittent nature of connectivity, dynamically changing topology, absence of the certification authority, the lack of centralized monitoring or management point and limited physical protection of each of the nodes. To provide secure way of communication and transmission the engineers must understand different types of attacks and their effects on the MANET routing protocols. There are various types of attacks that a MANET routing protocols can suffer from i.e. Wormhole attack, Black hole attack, Grayhole attack, Flooding attack, routing table overflow attack, Denial of Service DoS, Byzantine and Rushing attack etc. Routing protocols in MANETs are classified into two main categories according to their functionality named as proactive or table driven and reactive or on-demand algorithms.

## II. MANET ROUTING PROTOCOLS AODV & OLSR

AODV stands for "Ad hoc On Demand Distance Vector" is described in RFC3561, is a reactive routing protocol [1-3]. It is also known as on-demand routing protocols in which route is found as when desires nodes want to send a data packet to the destination node by using three control messages RREQ, RREP and RERR. When source node wants to make a connection with the destination node, it broadcasts RREQ message across the network which is propagated from the source and received by neighbors (intermediate nodes).On receiving this packet nodes update their information for the source node and setup backwards pointers in the routing tables. Intermediate nodes broadcast the RREQ message to their neighbors and this process goes on until the packet is received by destination node or an intermediate node that has a fresh enough route entry for the destination in its routing table. RREQ message contains a source IP address of node's, current sequence number and broadcast ID. On receiving RREQ message, a node sends route reply RREP if it is either destination or intermediate node with a corresponding sequence number greater than or equal to that contained in the RREQ. In this case it unicast a RREQ back to the source, otherwise it rebroadcasts RREQ. If the source node receives the RREP then it starts to forward data packets to the destination node.

OLSR stands for Optimized Link State Routing is described in RFC3626 [2-4] is a modular proactive hop by hop routing protocol. It is a proactive approach, so it continuously tries to find route, to all possible destinations in the network. Proactive and link state behavior could increase congestion in the network due to the routing traffic generated. However,

due to its proactive basis, it has the advantage of having routes immediately available whenever' they are required.

## III. PACKET DROP ATTACK IN AODV AND OLSR

In black hole or packet drop attack all network traffics are redirected to a specific node which does not exist at all. Because traffics disappear into the special node, so the specific node is named as a Black hole.

For example, in figure 1, in AODV black hole attack the malicious node "A" first detect the active route in between the sender "E" and destination node "D". The malicious node "A" then send the RREP which contains the spoofed destination address including small hop count and large sequence number than normal to node "C". This node "C" forwards this RREP to the sender node "E". Now this route is used by the sender to send the data and these data will then be dropped by malicious node. Thus sender and destination node will be in no position any more to communicate in state of black hole attack [1].

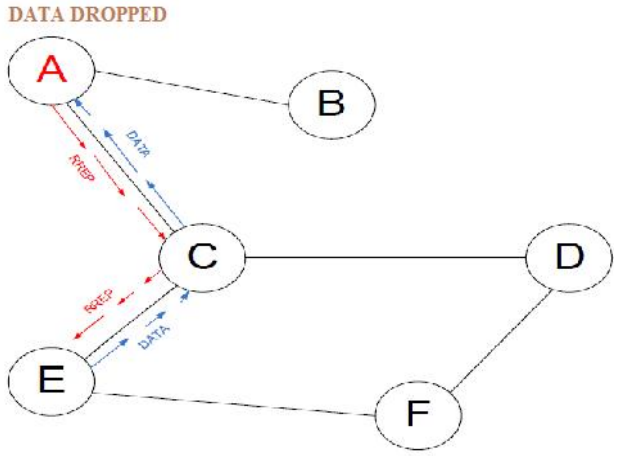


Figure 1: Black hole Attack specification

In OLSR black hole attack, a malicious node forcefully selects itself as MPR. Malicious node keep its willingness field to Will always constantly in its HELLO message. So in this case, neighbors of malicious node will always select it as MPR. Hence the malicious node earns a privileged position in the network which it exploits to carry out the denial of service attack. The effect of this attack is much vulnerable when more than one malicious node is present near the sender and destination nodes. According to OLSR protocol, when a node receives a control message, should retransmit it on condition that it has been selected as MPR by that node.

MPR-Flooding can be performed by propagating received TC messages by means of an attacker node which has not been selected as MPR. Therefore, in the next steps of propagation, it is possible that such retransmitted packets be ignored by real MPR nodes; because real MPR nodes have recently received related packets from another node (attacker node) and it leads to network routing obstacles [5].

## IV. SIMULATION ENVIRONMENT AND RESULT

This section is the major portion of the thesis, it is important to setup simulation environment to observe OLSR as proactive and AODV as reactive routing protocols behavior over MANET module. Quantitative analysis is conducted to with the help of OPNET Modeler 17.5 tool (wireless).

OPNET (Optimized Network Engineering Tools) Modeler is a discrete-event network simulator first created in 1986 by two PhDs from Massachusetts Institute of Technology and is written in C++. Commercial OPNET was established in 1987. Currently there are about 2700 OPNET users which spread all over fields including enterprises, internet service providers, device manufactures as well as military, education, banking and insurance [6]. OPNET Modeler is a software tool for network modeling and simulation. Modeler provides an open environment that allows users to create new protocols and devices, define and simulate every detail of then for the research purposes.

All the mobile nodes moving at a constant speed of 10 meter per second. Total eighteen scenarios have been developed, all of them with mobility of 10 m/s. Number of nodes were varied and simulation time was taken 1800 seconds. Simulation area taken is 1000 x 1000 sq. meters. Packet Inter-Arrival Time (sec) is taken exponential (1) and packet size (bits) is exponential (1024). The data rates of mobile nodes are 24 Mbps with the default transmitting power of 0.005 watts. Random way point mobility is selected with constant speed of 10 meter/seconds. Table 1 shows the common network simulation parameters.

Table 1: Common network simulation parameter

| Parameter | Value |
|---|---|
| Examined Routing Protocols | AODV and OLSR |
| Network Area/ Region | 1000 x 1000 sq.m |
| Network size | 16, 30 & 50 |
| Simulation Time | 1800 seconds |
| Transmission Power | 0.005 Watts |
| Mobility Speed | 10 meter/second |
| Mobility Model | Random waypoint |
| MAC Layer | IEEE 802.11g |
| Data Rate | 24 Mbps |
| Data Type | FTP |
| Packet Inter-Arrival Time (s) | Exponential (1) |
| Packet Size (bits) | Exponential (1024) |

Simulation is divided into eighteen scenarios based on network sizes on two MANET protocols AODV and OLSR. Nine scenarios for each MANET Routing protocols.

First three scenario consisting of 16 nodes with no attack, with 25% and 50% attacks of malicious node. Next three scenario consisting of 30 nodes with no attack, with 25% and 50% attacks of malicious node. And last three scenario consisting of 50 nodes with no attack, with 25% and 50% attacks of malicious node.

Comparative results for 16, 30 and 50 nodes without, with 25% and 50% black hole node attack for the MANET routing protocol AODV and OLSR are discussed.

A. Packet End-to-End Delay:

As shown in the graph in figure 2, 3, 4 and 5 average End-to-End delay of AODV and OLSR without attack and in case of Black-hole attack for 16, 30 & 50 nodes by comparing three scenarios of AODV and OLSR depends upon the network size i.e. number of nodes in the network and routing procedure of MANET protocols.

From the graph in figure 2, 3, 4 and 5, observed and investigated that, average delay for AODV with attack is low, as compare to no attack present in the network, this is due to Black-hole attack a malicious node already sends its RREQs and RREPs message immediately with less delay before Destination node reply. AODV shows more delays compare to OLSR because of its Routing nature & Route discovery mechanism. This means that OLSR protocol performs better than AODV under black-hole attack for all the scenarios.

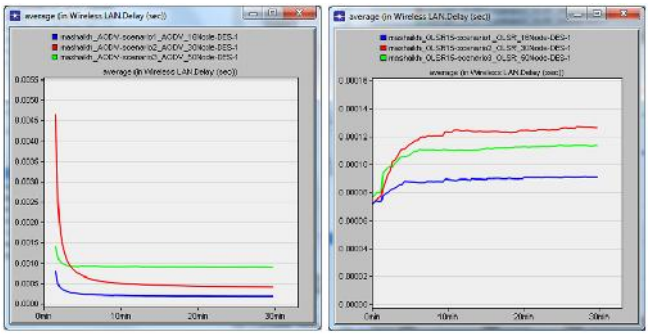

Fig 2: Average End-to-end Delay of AODV and OLSR without attack for 16, 30 & 50 nodes

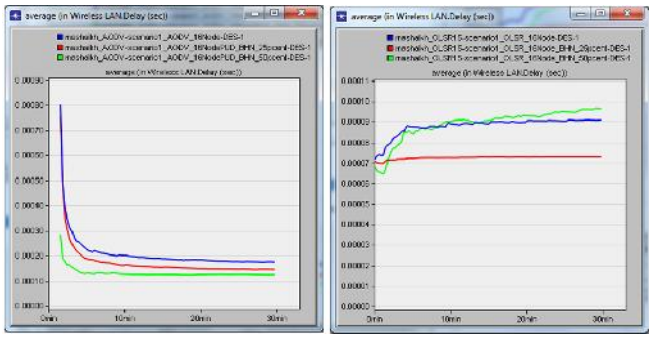

Fig 3: Avg. End-to-End Delay of AODV & OLSR without, with 25% & 50% attack for 16 nodes

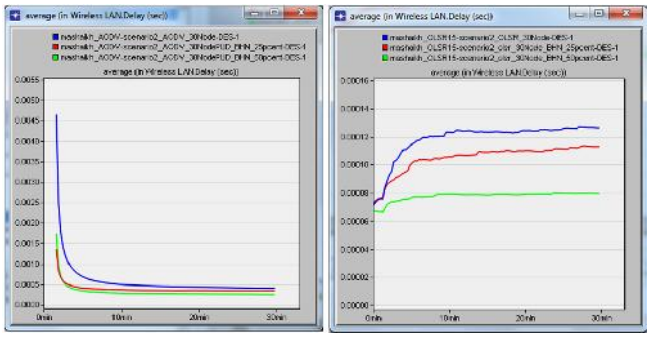

Fig 4: Avg. End-to-End Delay of AODV & OLSR without, with 25% & 50% attack for 30 nodes

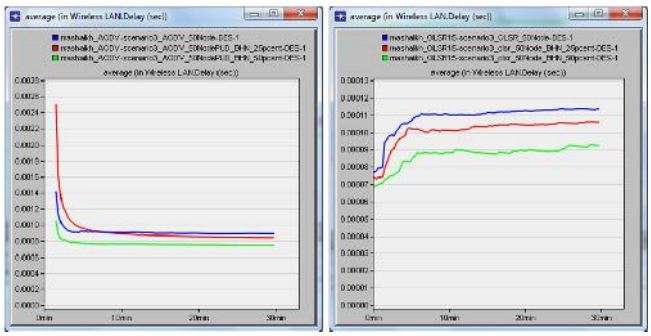

Fig 5: Avg. End-to-End Delay of AODV & OLSR without, with 25% & 50% attack for 50 nodes.

B. Network Load:

As shown in the graph in figure 6, 7,8 and 9 average network load of AODV and OLSR without attack and in case of Black-hole attack for 16, 30 & 50 nodes by comparing three scenarios of AODV and OLSR depends upon the network size i.e. number of nodes in the network and routing procedure of MANET protocols.

From the graph in figure 6, 7,8 and 9, it is investigate that as the network size increases average network load increases due to proper routing of protocols but in case of attack of BHN, it decreases. OLSR protocol offers less network load comparatively AODV protocol. This means that OLSR protocol performs better than AODV under black-hole node attack.

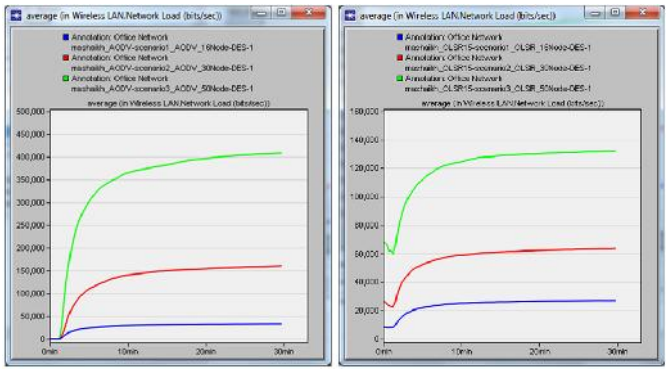

Fig 6: Avg. Network Load of AODV and OLSR without attack for 16, 30 & 50 nodes

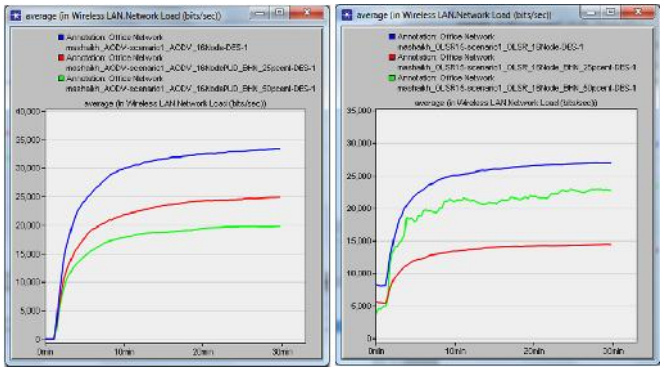

Fig 7: Avg. Network Load of AODV & OLSR without, with 25% & 50% attack for 16 nodes

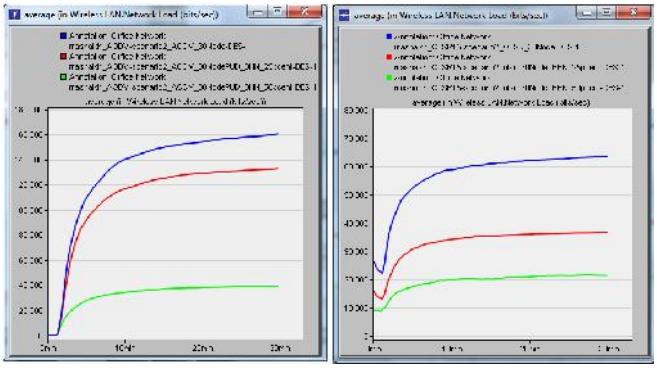

Fig 8: Avg. Network Load of AODV & OLSR without, with 25% & 50% attack for 30 nodes

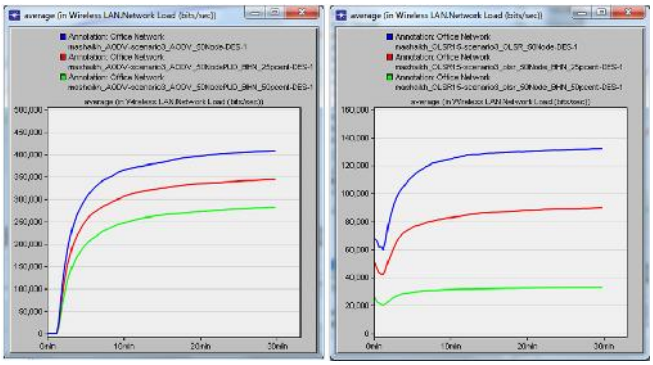

Fig 9: Avg. Network Load of AODV & OLSR without, with 25% & 50% attack for 50 nodes

C. Throughput:

As shown in the graph in figure 10,11,12 and 13 average throughput of AODV and OLSR without attack and in case of Black-hole attack for 16, 30 & 50 nodes by comparing three scenarios of AODV and OLSR depends upon the network size i.e. number of nodes in the network and routing procedure of MANET protocols.

From the graph in figure 10, 11, 12 and 13, it is investigate that as the network size increases average throughput increases but in case of attack of BHN, it decreases due to these nodes do not forward the packets and drops the packets instead of forwarding. OLSR protocol shows less throughput comparatively AODV protocol under black-hole node attack. Comparatively AODV protocol is more vulnerable under more attack of BHN in case of small and medium scaled network.

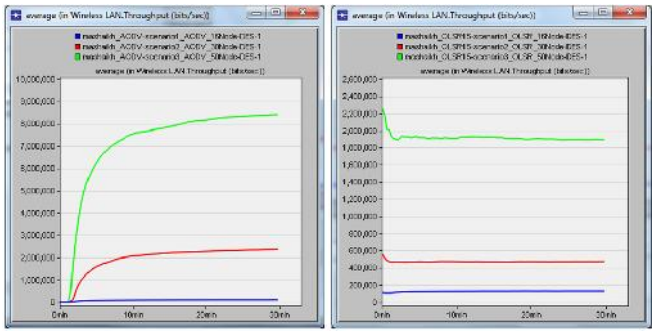

Figure 10: Average Throughput of AODV and OLSR without attack for 16, 30 & 50 nodes

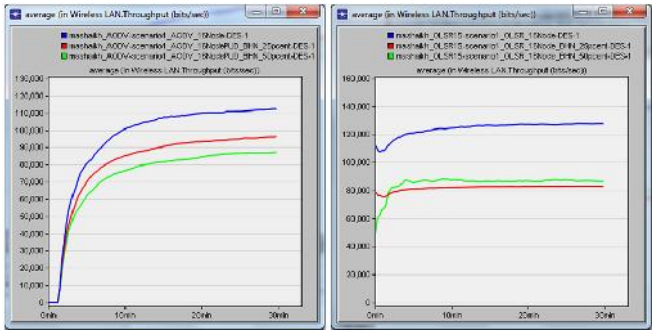

Fig 11: Avg. Throughput of AODV & OLSR without, with 25% & 50% attack for 16 nodes

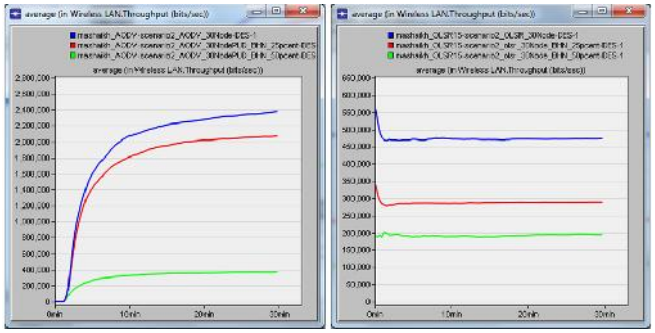

Fig 12: Avg. Throughput of AODV & OLSR without, with 25% & 50% attack for 30 nodes

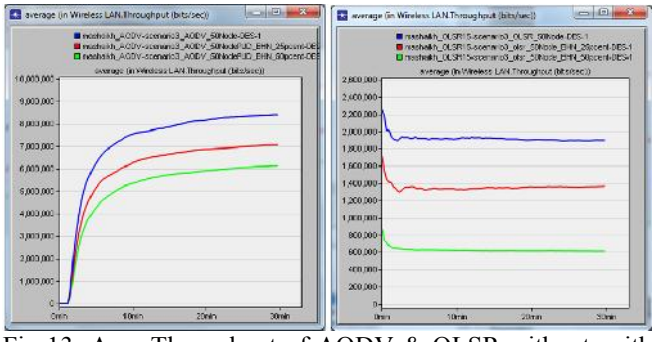

Fig 13: Avg. Throughput of AODV & OLSR without, with 25% & 50% attack for 50 nodes

D. Data Dropped (Buffer overflow)

As shown in the graph in figure 14,15, and 16 average data dropped of AODV and in case of Black-hole attack with 25% and 50% BHN for 16, 30 & 50 nodes by comparing three scenarios of AODV and OLSR depends upon the network size i.e. number of nodes in the network and routing procedure of MANET protocols.

From the graph in figure 14, 15, and 16, it is observed that as the number of black-hole node attack increases average data dropped increases because these nodes do not forward the packets and drops the packets instead of forwarding. AODV protocol shows more average data dropped comparatively OLSR protocol under black-hole node attack. Reasonably AODV protocol is more vulnerable under attack of BHN in all the scenarios.

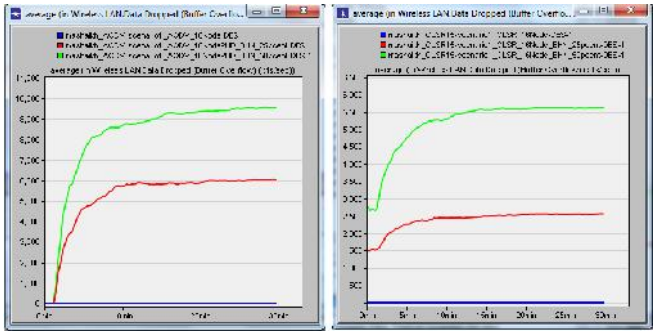

Fig 14: Avg. Data Dropped of AODV & OLSR without, with 25% & 50% attack for 16 nodes

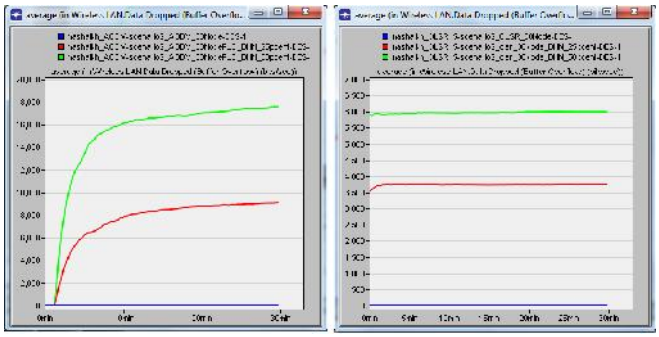

Fig 15: Avg. Data Dropped of AODV & OLSR without, with 25% & 50% attack for 30 nodes

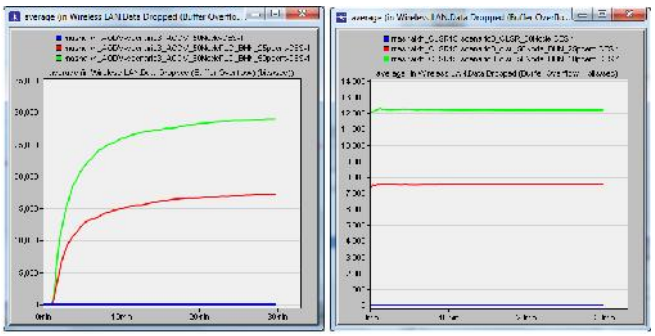

Fig 16: Avg. Data Dropped of AODV & OLSR without, with 25% & 50% attack for 50 nodes

## V. CONCLUSION

AODV shows more delays, network load and data dropped compare to OLSR for varying number of nodes in a MANET in case of packet drop or black hole attack. As per the analysis of performance parameters from the simulated result statistics End to End Delay, Network load and Data Dropped using Network Simulator, OPNET 17.5, it is found that OLSR performs the best in each case by varying the number of nodes against Packet drop attack or Black hole attack and conclude that comparing AODV as Reactive Routing algorithm is more vulnerable against Packet drop attack than OLSR as Proactive Routing algorithm.

## ACKNOWLEDGMENT

The study of performance evaluation of MANET routing protocols against packet drop attack have been possible due to the diligence of guide. Special thanks to P. U. Dere for his efforts.

## REFERENCES

[1] Irshad Ullah, Shoab Ur Rehman, "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols," [Ronneby 2010]

[2] T. Clausen and P. Jaqcquet, Optimized Link State Routing (OLSR) RFC 3626, IETF Networking Group, October 2003.

[3] C.E. Perkins, E.M. Belding-Royer, and S.R. Das, Ad Hoc On-Demand Distance Vector (AODV) Routing RFC 3561, IETF MANET Working Group, August 2003.

[4] Sajjad Ali and Asad Ali, "Performance Analysis of AODV, DSR and OLSR in MANET", Department of Electrical Engineering with emphasis on Telecommunication, Blekinge Institute of technology Sweden, MSc Thesis, 2009

[5] L. Tamilselvan, V. Sankaranarayanan, "Prevention of Blackhole Attack in MANET", Proc. of 2nd International Conference on wireless Broadband and Ultra Wideband Communications, AusWireless 2007, pp. 20-21, Aug. 2007.

[6] S. Floyd and K. Fall, "Simulation based Comparisons of Tahoe, Reno and Sack TCP", ACM Computer Communication Review, 1996, Vol. 26, No.3: 5-21.

**First Author**

Mr. Muwassil Ahmed Shaikh received his Bachelor degree from Dr BAM University Aurangabad. Currently he is pursuing hir master degree from Terna Engineering College, Nerul, Navi Mumbai. He has published his one paper in national conference. His research interest are MANET.

**Second Author**

Mr. P.U. Dere received his Bachelor degree from BAM University Aurangabad and master degree from Dr. B.A.T.U. Lonere. He has published more than 20 papers in national and internationals jornals and conference proceedings. His research interest are Mobile Communications and Wireless Networks. Currently he is working as Asst. Professor in Electronics and Telecommunication Engineering Department at Terna Engineering College, Nerul, Navi Mumbai.