Performance Analysis of Black Hole Attack in MANET using OPNET

Vijay Kumar Kalakar[1], Syed Tariq Ali[2], Hirdesh Chack[3]
[1,2]*Government Women's Polytechnic College, Lecturer, Department of Electronics and Telecommunication, Bhopal, MP*
[3]*Government Polytechnic College, Lecturer, Department of Electronics and Telecommunication, Jatara, MP*

***Abstract*- The growing popularity of wireless networks, and the peak in the present era, so as to attract the wireless user, regardless of their geographical location. There is more and more mobile ad hoc network (MANET) the risk of security threats. One of these security thread is Black hole. In this type of attack a malicious node falsely advertised itself have a short and a fresh route to a destination and absorbs the all packets itself. In this paper we see the effect of black hole attack node under the AODV routing protocol. Protocols consider a comparative analysis of the black hole attack. Manet Black hole attack performance evaluation, agreements for exploration of the effects are more vulnerable to attack. Measurement of end-to-end throughput, latency and load optical network, packet loss. Simulation is done by the optimized network engineering tools (OPNET). The extent of this postulation is to contemplate the impacts of Black hole assault in MANET utilizing both Proactive routing protocol for example Advanced Link State Routing (OLSR) and Reactive routing protocol Ad Hoc on Demand Distance Vector (AODV). Near investigations of Black hole assault for the two protocols were considered. The effect of the assault on the execution of MANET is assessed discovering which protocol is progressively powerless against the assault and what amount is the effect of the assault on the two protocols. The estimations were taken in the light of throughput, start to finish deferral and network stack. Reproduction is done in Optimized Network Engineering Tool (OPNET).**

***Index terms*- MANET, Black Hole, Routing protocols, AODV, OLSR, OPNET**

I.INTRODUCTION

A MANET consists of various mobile nodes which is joint by wireless connections. A router to establish a route and each mobile as a host. Each and every mobile node act as a transmitter router or transmitter. MANET routing protocols are ordered into three various kinds of protocols are as subsequent proactive, pre active and Hybrid protocols. Nodes in MANET function both as a host as well as a router for routing data between the nodes in the network. When the source node is sending data and if in this case the destination node is not in the collection of the source node, in such circumstance routing technique is used to ensure that the forwarded packet touches the destination node. The following figure 1 explain about the structure of Mobile ad hoc network. In MANET, the information which is exchanging routing details [1] and also save the data's into the routing tables in correct way and true manner. It is called proactive routing protocols. These MANETs such is used to military application and some emergency resave operations.

Figure 1. Mobile ad hoc network

1.1 Routing Protocols in MANET

MANETs are typically infrastructure-less and autonomous networks [2] where a set of mobile nodes are connected by wireless adhoc links. The design of routing protocols for MANETs is complex because of several constraints. These routing protocol aim to provide paths that are not only optimum in terms of some standards (minimum distance,

maximum bandwidth, and shortest delay) but also in satisfying some constraints, for example, the limited power of mobile nodes and the limited capacity of wireless links.

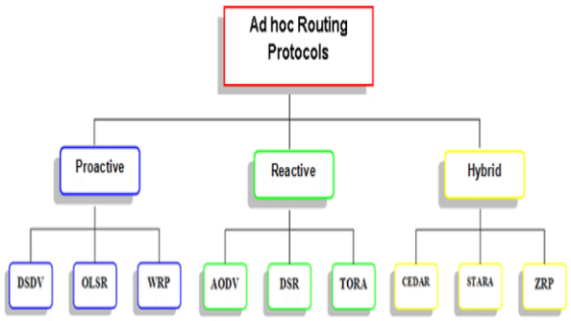

Figure 2. Classification of MANETs Routing Protocols.

Pro-active routing protocols: These are also known as table-driven routing protocols. Each mobile node maintains a separate routing table which contains the information of the routes to all the possible destination mobile nodes. Since the topology in the mobile ad-hoc network is dynamic, these routing tables are updated periodically as and when the network topology changes. It has a limitation that is doesn't work well for the large networks as the entries in the routing table becomes too large since they need to maintain the route information to all possible nodes.

Reactive routing protocols: These are also known as on-demand routing protocol. In this type of routing, the route is discovered only when it is required/needed. The process of route discovery occurs by flooding the route request packets throughout the mobile network. It consists of two major phases namely, route discovery and route maintenance.

Hybrid routing protocols: It basically combines the advantages of both, reactive and pro-active routing protocols. These protocols are adaptive in nature and adapts according to the zone and position of the source and destination mobile nodes. One of the most popular hybrid routing protocol is Zone Routing Protocol (ZRP).

The whole network is divided into different zones and then the position of source and destination mobile node is observed. If the source and destination mobile nodes are present in the same zone, then proactive routing is used for the transmission of the data packets between them. And if the source and destination mobile nodes are present in different zones, then reactive routing is used for the transmission of the data packets between them.

The most widely used MANET routing protocols are AODV (Ad hoc On-Demand Distance Vector), OLSR (Optimized Link State Routing), and DSR (Dynamic Source Routing) [3].

AODV Protocol: Ad hoc On-demand Distance Vector Routing (AODV) is a novel algorithm for the operation of ad hoc networks [3]. Each mobile node operates as a specialized router and routes are obtained as needed i.e. on-demand with little or no reliance on periodic advertisements. The new routing algorithm is quite suitable for a dynamic self-starting network as required by users wishing to utilize ad hoc networks. AODV provides loop free routes even while repairing broken links. Because the protocol does not require global periodic routing advertisements, the demand on the overall bandwidth available to the mobile nodes is substantially less than in those protocols that do necessitate such advertisements.

AODV can be called as a pure on-demand route acquisition system, in this nodes do not lie on active paths neither maintain any routing information nor participate in any periodic routing table exchanges. Further, a node does not have to discover and maintain a route to another node until it needs to communicate. To maintain the most recent routing information between nodes the concept of destination sequence numbering will be used. Each ad hoc node maintains a monotonically increasing sequence number counter which is used to supersede stale cached routes.

The advantage of AODV is that it creates routes only on demand, which greatly reduces the periodic control message overhead associated with proactive routing protocols. The disadvantage is that there is route setup latency when a new route is needed, because ADOV queues data packets while discovering new routes and the queued packets are sent out only when new routes are found. This situation causes throughput loss in high mobility scenarios, because the packets get dropped quickly due to unstable route selection.

Optimized Link State Routing Protocol (OLSR): OLSR is a proactive or table driven, link-state routing protocol [4]. Link-state routing algorithms choose best route by determining various characteristics like link load, delay, bandwidth etc. Link-state routes are more reliable, stable and accurate in calculating best route and more complicated than hop count. To update topological information in each node, periodic message is broadcast over the network. Multipoint relays are used to facilitate efficient flooding of control message in the network. Route calculations are done by multipoint relays to form the rout from a given node to any destination in the network. The OLSR protocol is developed to work independently from other protocols. Conceptually, OLSR contain three generic elements: a mechanism for neighbour sensing, a mechanism for efficient flooding of control traffic, and a specification of how to select and diffuse sufficient topological information in the network in order to prove optimal routes [5], [6].

In OLSR, neighbor nodes related information are gathered with HELLO messages which are send over network periodically [7]. These HELLO messages detect changes in neighbor nodes and related information such as interface address, type of link symmetric, asymmetric or lost and list of neighbors known to the node. Each node update and maintain an information set, describing the neighbor and two-hop neighbor periodically after some time.

1.2 Black-hole Attack

A black hole attack is [9] used by a malicious node which makes all the traffic travel through it by claiming to have the shortest route to all other nodes in the network. Then, instead of forwarding the packets, the malicious node simply drops it. In a black hole attack, a malicious node impersonates a destination node by sending a spoofed root reply packet to a source node that initiates a route discovery. The source node traffic can be deprived by malicious node. A variant of this black hole is the gray hole, attack, which selectively transmits some packets and drops others. Other attacks towards an adhoc network include partitioning and replay attacks.

1.2.1 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.

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 in this way data will arrive at the malicious node. These data will then be dropped. In this way sender and destination node will be in no position any more to communicate in state of black hole attack.

II. LITERATURE REVIEW

Ayesha Siddiqua et al. [1] proposed a secure knowledge algorithm to avoid the black hole attack in MANETs. In which, every node display other all adjacent nodes, and nodes compare information of its neighbor node with its knowledge table. In knowledge table have information about fm & rm morals of node. If nodes fm value does match with rm value, that node declare as a malicious node by using this algorithm, finds packet drop reason before requesting node as a black hole node.

Haque Nawaz Lashari et al. [2] going to calculate the power attribute from various MANET routing protocols. At the same time, calculating the transmission range and protocols performance observed from AODV, DSR, and TORA. In various protocols they are examining the physical characteristics 802.11a or 802.11g by exploiting individual metrics of protocols. Also denoting the the power values decreasing or increasing manner and how it will be affected into that particular MANET routing protocols.

Ayanwuyi T. Kolade et al. [3] analyzed the presence of black hole attack in different scenarios into the AODV MANET routing protocol. They find the routing protocols using different simulator parameters with and without loads in that working environment. How the black hole attack will destroy the data while send to destination end. Also calculate the packet delivery ratio, end to end delay, and throughput what they are deployed in the present network. Measuring the end to end delay into that destination node without any packet loss. Able to send the data to other end without any malicious node attack and may be the slight change will happen in that end to end delay.

Mohammad Al-Shurman and Seong-Moo Yoo et al. [4] purposed two systems to detect the black hole attack. First system is based on RREP packet reaches from more than two nodes. This method is sheltered but longer time delay. Second method is based on send RREP with record of Last-packet sequence numbers. Second method is fast, reliable and reduces the overhead in network. But this method is not secure because from time to time malicious node can listen to channel and inform their tables.

III. SIMULATION SETUP

The tool used for the simulation study is OPNET 14.5 modeler. OPNET is network and application based software used for network management and analysis [24]. OPNET models communication devices, various protocols, architecture of different networks and technologies and provide simulation of their performances in virtual environment. OPNET provides various research and development solution which helps in research of analysis and improvement of wireless technologies like WIMAX, Wi Fi, UMTS, analysis and designing of MANET protocols, improving core network technology, providing power management solutions in wireless sensor networks.

In our case we used OPNET for modeling of network nodes, selecting its statistics and then running its simulation to get the result for analysis.

3.1 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.

3.2 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. After the selection of statistics and running the simulation, results are taken and analyzed. In our

case we have used global discrete event statistics (DES).

3.3 Simulation Setup

Figure 3 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). The data rates of mobile nodes are .5 Mbps with the default transmitting power of 0.005 watts. Random way point mobility is selected with constant speed of 10 meter/seconds and with pause time of contact 100 seconds. This pause time is taken after data reaches the destination only. Our goal was to determine the protocol which shows less vulnerability in case of black hole attack. We choose AODV and OLSR routing protocol which are reactive and proactive protocols respectively. In both case AODV and OLSR, malicious node buffer size is lowered to a level which increase packet drop. Furthermore the simulation parameters are given in Table I.

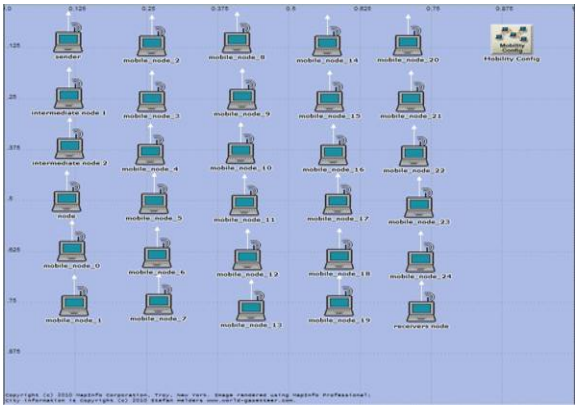

Figure 3. Simulation Environment for 30 nodes

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

Implementing a Routing Protocol in OPNET to Simulate Black Hole Behaviours:

To give a node the characteristics of black hole node we need to implement a new routing protocol in OPNET. Implementation of a New MANET unicast Routing Protocol in OPNET is described. All routing protocols in OPNET are installed in the directory of "OPNET". We first duplicate the AODV protocol in the OPNET directory and change the name of this directory as "blackholeaodv". In this blackholeaodv directory the name of all files that are labeled as "aodv" are changed to "blackholeaodv" such as blackholeaodv.cc,blackholeaodv.h, blackholeaodv.tcl etc. All classes, functions, variables, and constants names in blackholeaodv directory have changed but struct names that belong to AODV packet.h file have not changed.

Adding the "blackholeaodv" protocol agent in the "\tcl\lib\opnet-lib.tcl" file:-

```
blackholeaodv
{
set ragent [$ self-create – blackholeaodv-agent $node]
}
Simulator instproc create-blackholeaodv-agent {node}
{
Set ragent [new Agent /blackholeaodv [$node node-addr]]
$self at 0.0 "$ragent start"
$node set ragent _ $ragent
Return $ragent
}
```

To integrate the new blackholeaodv protocol in OPNET simulator, we have changed two files that are used globally in this simulator. In "\tcl\lib\ opnet-lib.tcl" file we first add the lines shown above, for the agent procedure for blackholeaodv.

Addition in the "\makefile" at the opnet directory

blackholeaodv/blackholeaodv_logs.o

blackholeaodv/blackholeaodv.o\

blackholeaodv/blackholeaodv_rtable.o
blackholeaodv/blackholeaodv_rqueue.o\
In aodv.cc, the "recv" function process the packet based on the type of the packet. If packet type is AODV route conducting packet such as RREQ, RREP, RERR, it sends the packet to the "recvAODV" function .When the received packet type is data packet type then AODV protocol sends it to the destination address.

```
if ( (u_int32_t)ih->saddr() = = index ) // if destination address itself forward (( blackholeaodv_rt_entry*) 0,p,NO_DELAY);
else
drop (p,DROP_RTR_ROUTE_LOOP);
```

//For blachole attack in the wireless adhoc network, after taking the path over itself, misbehaving node drops all packets.
First "if" condition provides the node to receive data packets if it is the destination and the "else" condition consume all remaining packets as a Black Hole node.
To generate the black hole behaviour we need to make change in blackholeaodv.cc file by adding the false RREP. The false RREP message show that it has the highest sequence number and the sequence number is set to 4294967295 and hop count is set to 1.The Highest sequence number of AODV protocol is 4294967295, 32 bit unsigned integer value .The lines in are added to aodv.cc file to generate the characteristics of black hole node. After changing the files then we compiled the "make" in the terminal window (Cygwin window) to create object files.

```
Sendreply
(rq - > rq_src,          //IP Destination
1,                       // Hop Cou
index                    // Dest IP Address
429496729                // Highest Dest Sequence Num
MY_ROUTE_TIMEOUT, //Lifetime
rq - > rq_timestamp;  //timestamp
```

To detect the blackhole attack the "Blackhole Detection System" checks the RREPs that come from multiple paths. As the blackhole node immediately send RREP message to the source without checking its routing table, it is more likely that the first RREP comes from the blackhole node. Then the solution will discard the first RREP packet using the route reply saving mechanism that come from malicious node and choose the second RREP packet.

Algorithm for Black Hole Detection System

- Step1: Source node broad cast route Request (RREQ) packet.
- Step2: Multiple Route Reply of corresponding Route Request comes to Source node.
- Step3: The Route Reply that comes first set as the response from malicious node and removes from the table by using the RREP saving mechanism.
- Step4: The second Route Reply is choose by RREP saving mechanism and set it as reply from corresponding destination node. Then the source node delivers the data to the path through which the second RREP came.
- Step5: Stop.

Implementing the Black Hole Detection System in OPNET against the Black Hole Attack

To implement solution against Blackhole, we duplicated the "AODV" protocol, changing it to "bdsAODV" as we did in "blackholeaodv". Here for the solution, we had to change the receive RREP function (recv Reply) and create RREP saving mechanism. This RREP saving mechanism counts the second RREP message. At first, we have changed all files name in the cloned "aodv" directory to bdsAODV. To integrate the new bds AODV protocol in OPNET simulator, at First the file "\tcl\lib\ opnetlib. tcl" is modified where protocol agents are coded that is presented.

```
bdsAODV{
set ragent [$self create-bdsaodv-agent $node]
}
Simulator instropc create –bdsaodv-agent {node}
{create bdsAODV roting agent
Set ragent [new Agent /bdsAODV [$node node-addt]]
$self at 0.0 "$ragent start"
$node set ragent_$ragent
return $ragent
}
```

Second file which is in the opnet directory named "\makefile" where we add the lines that is given below. To detect blackhole attack we create RREP saving mechanism in recv Reply function of bdsAODV.cc file that is presented below. In the RREP saving mechanism the "rrep_insert" function is used for adding RREP messages, "rrep_lookup"

function is used for looking any RREP message up if it is exist,"rrep_remove" function removes any record for RREP message that arrived from defined node and "rrep_purge" function is to delete periodically from the list if it has expired.

```
bdsaodv/bdsaodv_logo.o bdsaodv/bdsaodv.o\
bdsodv/bdsaodv_rtable.o bdsaodv/bdsaodv_rqueue.o\

void
bdsAODV::rrep_insert{opnetaddr_t id)
{bdsBroadcastRREP *r = new bdsbrodcast
RREP(id);
assert (r);
r - > expire = CURRENT_TIME +
BCAST_ID_SAVE;
r - > count ++;
LIST_INSERT_HEAD(&rrephead,r,link);
}
bdsbroadcastRREP *
bdsAODV::rrep_lookup(opnetaddr_t id)
{bdsBroadcastRREP *r =rrephead.lh_first;
for(; r; r= r - > link.le_next)
{
if (r - >dst == id)
return r;
}
return NULL ;
}
void
bdsAODV::rrep_remove(opnetaddr_t id)
{bdsBroadcastRREP *r=rrephead.lh_first;
for(;r; r=  r -> link.le_next)
{
if (r-> dst==id)
LIST_REOVE(r,link);
delete r;
break;
}
}
void
bdsAODV::rrep_purge()
{
bdsBroadcastRREP *r =rrephead.lh_first;
bdsBroadcastRREP *rn;
Double now =CURRENT_TIME;
for(; r; r=rn)
{
Rn = r-> link.le_next;
if(r-> link.le_next;
if(r->expire <=now)
{
LIST_REMOVE(r,link);
delete r;
}
}
}

bdsAODV::recvReply(packet*p)
{
bdsBroadcastRREP *r =rrep_lookup(rp->rp_dst);
If (ih-> daddr()==index)
{
If ( r = = NULL)
{
rrep_insert(rp->rp_dst);
packet::free(p);
return;
}
else
rrep_remove(rp->rp_dst);
}
If (r = = NULL)
{
count= 0;
rrep_insert (rp-> rp_dst);
}
else
{
r-> count++;
count = r-> count;
}
```

IV. RESULTS AND DISCUSSIONS

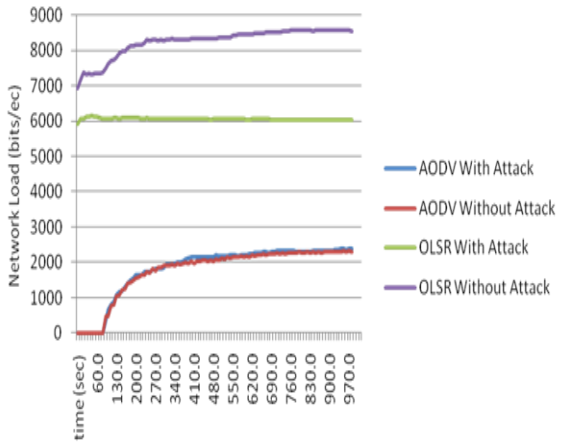

Figure 4. Network Load of OLSR and AODV with vs. without attack for 16 nodes

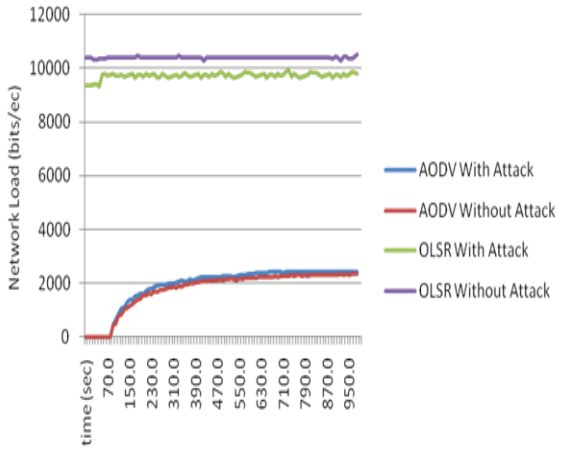

Figure 5. Network Load of OLSR and AODV with vs. without attack for 30 nodes.

The network load graph of OLSR and AODV with and without presence of a malicious node has been shown in the Fig. 4and 5. 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.

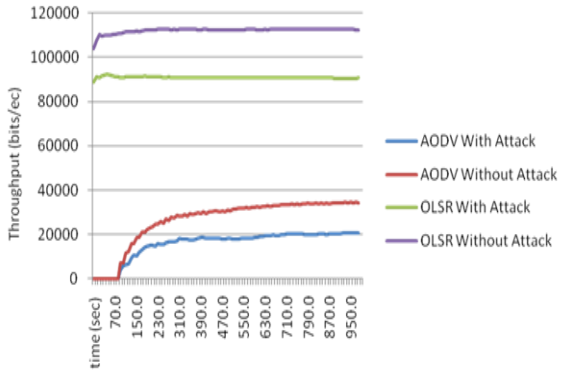

Figure 6. Throughput of OLSR and AODV with vs. without attack for 16 nodes.

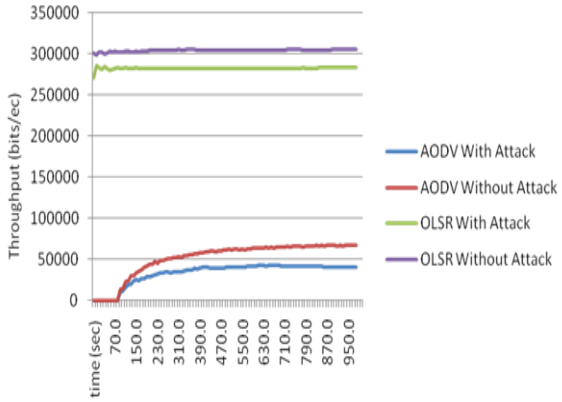

Figure 7. Throughput of OLSR and AODV with vs. without attack for 30 nodes.

From Fig. 6, for 16 nodes, it is obvious that the throughput for OLSR is high compared to that of OLSR. Also in OLSR throughput for the case with no attack is higher than the throughput of OLSR under attack. This is because of the fewer routing forwarding and routing traffic. Here the malicious node discards the data rather than forwarding it to the destination, thus effecting throughput. The same is observed in the case with AODV, without attack, its throughput is higher than in the case with under attack because of the packets discarded by the malicious node. Similarly in Fig. 7 for 30 nodes, the throughput is high because of the higher number of nodes but the trend of throughput with attack and without attack remains the same as in 16 numbers of nodes.

V. CONCLUSIONS

In present work 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] Siddiqua, A., Sridevi, K., & Mohammed, A. A. K. (2015, January). Preventing black hole attacks in MANETs using secure knowledge algorithm. In 2015 International Conference on Signal Processing and Communication Engineering Systems (pp. 421-425). IEEE.

[2] Nawaz, H., Ali, H. M., & Nabi, G. (2014). Simulation based analysis of reactive protocols metrics in manet using opnet. Sindh University Research Journal-SURJ (Science Series), 46(4).

[3] Kolade, A. T., Zuhairi, M. F., Yafi, E., & Zheng, C. L. (2017, January). Performance analysis of black hole attack in MANET. In Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication (p. 1). ACM.

[4] Al-Shurman, M., Yoo, S. M., & Park, S. (2004, April). Black hole attack in mobile ad hoc networks. In Proceedings of the 42nd annual southeast regional conference (pp. 96-97). ACM.

[5] Esmaili, H. A., & Shoja, M. R. (2011). Performance analysis of AODV under black hole attack through use of OPNET simulator. arXiv preprint arXiv:1104.4544.

[6] Prashant Kumar Varma, Rajesh Upadhyay, Gulshan Katara, Performance Analysis of Black Hole Attack in MANET NETWORK. International Journal of Research and Scientific Innovation, Volume III, Issue III, March 2016.

[7] Jing Deng, Richard Han, Shivakant Mishra, INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks. University of Colorado, Department of Computer Science Technical Report CU-CS-939-02.

[8] Abdel-Moniem, A. M., Mohamed, M. H., & Hedar, A. R. (2010, November). An ant colony optimization algorithm for the mobile ad hoc network routing problem based on AODV protocol. In 2010 10th International Conference on Intelligent Systems Design and Applications (pp. 1332-1337). IEEE.

[9] Naga Srinivasu S.V, Dr.I.Ramesh Babu, Performance evaluation of AODV under the black hole attacks using the OPNET, International Journal of Computers Electrical and Advanced Communications Engineering Vol.1 (2), 2012.(pp. 204-207).

[10] Mahmood K. Ibrahem , Ameer M. Aboud, A Secure Routing Protocol for MANET , International Journal of Computer Science Engineering and Technology(IJCSET) | July 2014 | Vol 4, Issue 7,223-230.

[11] B.Padminidevi."Anonymity,Unlinkability,Unobservability for routing protocol in MANETs." International Journal of Emerginf trends in Science and Technology (IJETST), Vol.01, Issue 01, 2014.

[12] T. T. Manikandan, Rajeev Sukumaran, M. R. Christhuraj, M. Saravanan, "Performance Evaluation of MANET Routing Protocols under Pulse Jammer Attack". International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-8 Issue-5 March, 2019.

[13] Rajaram, A., & Palaniswami, D. S. (2010). Malicious node detection system for mobile ad hoc networks. International Journal of Computer Science and Information Technologies, 1(2), 77-85.

[14] Tseng, F. H., Chou, L. D., & Chao, H. C. (2011). A survey of black hole attacks in wireless mobile ad hoc networks. Human-centric Computing and Information Sciences, 1(1), 4.

[15] Garg, A., & Juneja, D. (2012). A Comparison and analysis of various extended techniques of query optimization. International Journal of Advancement in Technology, 3.