ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 5, Issue 3, March 2018

Modified AODV Protocol for Detection and Prevention of Black hole Attack in Mobile Ad Hoc Network

[1] Neelam Janak Kumar Patel, [2] Dr. Khushboo Tripathi

[1] Ph.D. Research Scholar, Dept. of CSE, ASET, Amity University, Haryana, India, [2] Assistant Professor, Dept. of CSE, ASET, Amity University, Haryana, India

Abstract: - **Mobile ad hoc network (MANET) is a special group of nodes; those are infrastructure less and wirelessly. In MANET nodes are legitimate to leave and join the network at any point of the period. MANET is vulnerable to various types of security attacks like a wormhole, black hole, rushing attack etc., so security in MANET is the most significant concern to give secured communication and transmission between mobile nodes. Black hole attack is one of the most destructive attacks in network layer against routing in MANET. A black hole is a malicious node, an attacker provides a single-hop, high-quality path on behalf of all destination beginning all nodes around it to forward packets to it. A black hole node sends bogus routing information, advertised that it has an ideal route and springs other good nodes to route data packets through one. A malicious node drops all packets that it received instead of forwarding those packets. In this research paper, we implemented IDSAODV routing protocol for improving the securities in MANETs. It is the reactive type Ad hoc On-Demand Distance Vector (AODV) routing protocol to escape black hole attack. To identify and avoid the black hole attack using a proposed routing protocol (idsAODV). It deliberated a modification of the AODV protocol. Using Network Simulator NS-2.35 we get the experimental results that show an improvement in Throughput, Packet Delivery Ratio (PDR), and End to End delay using the proposed routing protocol that is idsAODV and results are comparing with Normal AODV routing protocol in the attendance of black hole attacks.**

Keywords- **AODV Reactive routing protocol, MANETs, idsAODV protocol, Black hole Attack and NS2.**

I. INTRODUCTION

A Mobile Ad Hoc Network (MANETs), also known as wireless ad hoc network is a set of wireless mobile nodes that dynamically establishes the network in the nonexistence of predetermined communication. The nodes are communicating with each other using multi-hop routing and it can interconnect through wirelessly to each other [1]. Hence, each node in a MANET works equally as a router that forwarding of packets to destination in the network, when a route is established, MANET is more vulnerable to various kind of network attacks as it gains and loss many nodes simultaneously, and these nodes are squash into the resource limitations such as bandwidth, storage, and energy capacity[4]. In MANET attacks can be characterized into two major groups: internal and external. External attacks have not authorization information about the data packets and control. This type of attacks can only be consigned to user authentication and cryptography schemes. The most distinctive internal attacks on the network layer are a black hole, wormhole, sinkhole, denial of service, Sybil, and selective forwarding. Hence, it is necessary to design a good routing protocol for protecting against insider attacks. Using compromised node an internal attack is created on the same network. They drop, formulate, alter, or misroute data packets. The external attack is not participating in the routing process but interrupts network operations like flooding, DOS, or cut-off nodes from a network. The routing protocols generally characterized by three major types as table-driven called proactive, on-demand called reactive and hybrid. Proactive protocols are called table-driven routing protocol because it immediately learns network topology and the routing tables are updated periodically. In reactive routing protocols, the route is established whenever it is required so are called on-demand routing protocols. The hybrid protocol is a permutation of both reactive and proactive routing protocols [5]. Reactive routing protocol AODV is very efficient, simple and effective routing protocol which is used predominantly. In case of reactive AODV routing protocol, source node starts the path discovery process by broadcasting a route request packet (RREQ). Intermediate node takes part in this process by more broadcasting this RREQ [3]. A black hole node does not follow this process and sends back a fake route reply (RREP) packet to the source node proclaim that it has an optimal path to the destination[1][2][3][4][5]. Consequently, the source node starts to send data packets via this malicious node which then drops all the data packets. This paper is based on black hole attack in mobile ad hoc networks, using network simulator ns-2 (version 2.35), this paper provides an effect of black hole attack on the performance of the network. A protocol named blackholeAODV is implemented that demonstrates the black hole attack behaviour in AODV protocol; consequently, the performance of the network evaluated using with and without black holes. The result of observation shows accomplishment of the network collapse significantly in the attendance of a black hole.

II. PROPOSED METHODOLOGY

The normal AODV protocol that is implemented in NS2 but it does not simulate a network topology with a malicious node or black hole behavior. In this research paper, we implemented a modified AODV protocol that is capable of simulating a network topology with a black hole behavioral a malicious node that drops all packets that pass through it. This modified AODV protocol is given an abbreviation blackholeAODV. The new routing protocol has its own folder that is blackholeAODV under the main folder ns2.35. Inside this folder, there are implementation files like blackholeaodv.h, blackholeaodv.cc, blackholeaodv.tcl, blackholeaodv_rqueue.h, blackholeaodv_rqueue.cc etc. of the modified blackholeAODV routing protocol. The main purpose of a black hole attack is to instantaneously reply to any RREQs without forwarding the data packet to an original destination; it drops all the received packets. An attacker node proceeds that it provides a high-quality path to the destination, so an attacker node that receives route request packet from source node it sends immediately route reply packet. Black hole attack that increases the sequence number using compromise node in the network, highest sequence number is 4294967295 which is 32-bit unsigned integer value of AODV protocol [3]. The hop count is situating to 1 and the sequence number is located to 4294967295. The black hole attack that provides a false RREP message is sendReply (rq->rq_src, (IP destination), index (Dest IP Address), 1 (HOP count), 4294967295 (Highest Dest Sequence Num), My_route_timeout (Lifetime), rq->rq_timestamp (timestamp).

The RREP sent by this black hole node is the fastest and the first to be received by the source node. Upon receiving the first RREP message from the malicious node, the source node will establish the communication link and starts transmitting data packets to the malicious node. We have implemented idsAODV like a solution against black hole attack and it will observe its particular effects on AODV concert faces with single and multiple cooperative black hole attack. We use to select the secure path between the source and destination using an idsAOVD protocol which is using RREP accumulating mechanism. To implement idsAODV to enable existing AODV routing protocol in NS2, it was necessary to modify the recvReply function of the aodv.cc file. The RREP message entries are taken as analysis data for alteration detection. The recvReply was modified in such a way that it has to check every single RREP message against an audit data that has already been collected to categorize anomaly detection. False RREP messages from a black hole node usually contain a maximum destination sequence number. Hence, it can be taken as an entry for audit data. To prevent such poor decision making by a source node or to avoid false positive alarms in detecting intruders, checking RREP messages with a given audit data involves multiple entries of possible anomaly detection parameters before reaching to a conclusion that an RREP message is sent from an intruder. RREP messages that are sent from a black hole node are generated exactly at the same time the RREQ message is received by the replying malicious node. This gives us timestamps of RREP messages as an additional audit data to be collected in addition to maximum destination sequence numbers. To assure the perfection of a decision made by a source node that an RREP message is received from a black hole node, all entries of RREP messages can be checked against a set of predefined audit data for possible inconsistency conditions.

III. PSEUDO CODE - PROPOSED ALGORITHMS

```
ReceiveReply (Packet P)
    Replyingnode = Null
    Reply counter = 0
Initiate Route Discovery ()
Set time (RREP_WAIT_TIME)
Set Max_seq_No = 4294967295
While (received _RREP)
{
IF Blacklist _table Contain (recived_RREP_nodeID)
{discard RREP }
else {
IF ((dest_seq_no in RREP >node_seq_no in source routing table) || (dest_seq_no in RREP = node_source_Seq_No) && (hop_count in RREP <node_hop_count in source routing table))
Add this RREP massage into RRT
Reply_count= Reply_count+1
}
IF ((Reply_count> 1) && (dest_seq_no in RREP < max_seq_no))
{
Update entry of P (Packet) in routing table
Unicast data packets to the route specified in RREP
}
else {
Add this RREP massage into Blacklist _table
Remove this RREP massage from RRT
Broadcast_Alarm ()
}
}
// End of ReceiveRREP
```

IV. SIMULATION RESULTS AND ANALYSIS

The implemented work for the AODV protocol has been categorized into three phases: In first phase the AODV protocol is implemented without black hole attack, in second phase the AODV protocol is implemented with black hole attack and in third phase it is implemented intrusion detection and prevention mechanism which help to detect and avoid the black hole nodes. We used ns2 (ns2.35) simulation to prepare investigation to modify AODV protocol. The experiments are shown on different parameters are throughput, packet delay, and packet loss to find out the best precise results. The execution is done by NS2 simulator. In order to get precise results from the simulations, we did our research in three states, first, we used AODV without any malicious in MANETs. Then we implemented MANETs with a black hole attack. Finally, we implemented MANETs under intrusion detection and prevention solution using RREP Accumulating Mechanism. Table I summarizes the used simulation parameters.

Parameter	Value
Simulator	NS-2 (Ver. 2.35)
Simulation Time S	80.0 sec
Number of mobile nodes	8 and 15
Simulation area	500 m X 500 m
Routing Protocol	AODV, blackholeAODV and idsAODV
Packet Size	512 byte

Table I: Simulation Parameters

Figure 1 shows the nam file for the Normal AODV routing protocol. In this scenario use number of mobiles nodes which communicate with each other. In this figure, it shows use of Normal AODV without any black hole attack. We can see how nodes are relocated and some packets are dropped because we used UDP protocol which is unreliable.

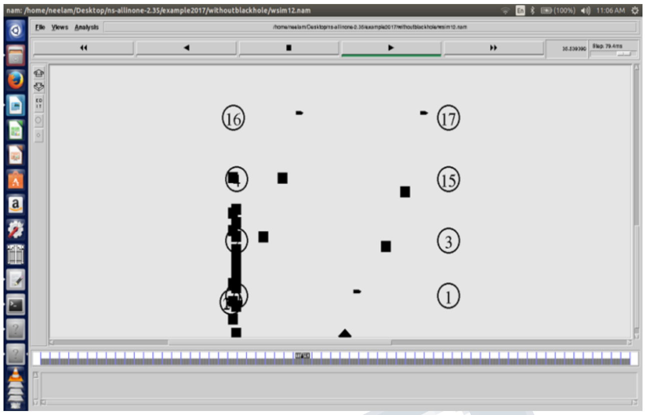


Figure 1: The nam file for without black hole Attack

Figure 2 shows the graph for average throughput in Xgraph using transfer size in bit Vs. transfer time of Normal AODV without black hole attack. As we see average throughput gives the high result because there is a normal situation.

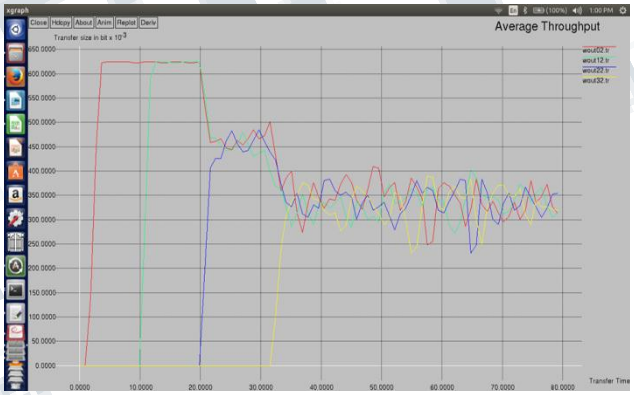


Figure 2: Average Network Throughput without black hole Attack

Figure 3 shows the graph for Packet loss in Xgraph using a number of packet loss Vs. routing time of normalAODV without black hole attack. The number of packets lost at the beginning of the simulation is less than the number of packets which are delivered at the end.

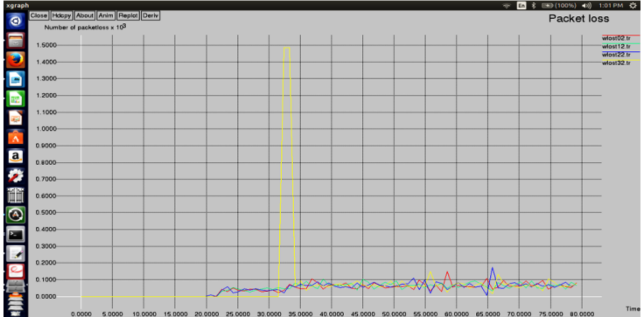


Figure 3: Packets Loss without black hole Attack

Figure 4 shows the graph for Packet Delay in Xgraph using a number of packets vs. last packet time of normalAODV without black hole attack. The packet delay will decrease because of using AODV without any hacking problem.

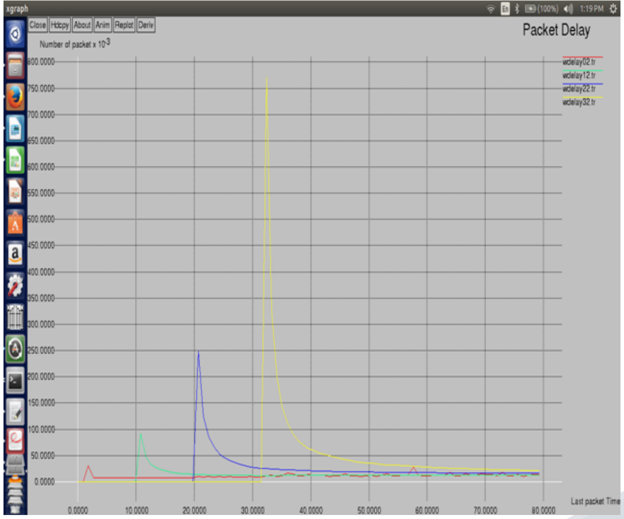


Figure 4: Packet Delay without black hole Attack

Figure 5 shows the nam file for the blackholeAODV routing protocol. In this scenario, Suse of number of mobiles nodes which communicate with each other which are affected by black hole attack. This figure shows the use of new blackholeAODV added with black hole attack. We can see that large number of packet drop or lost when the black hole attack is activated in the ad-hoc network.

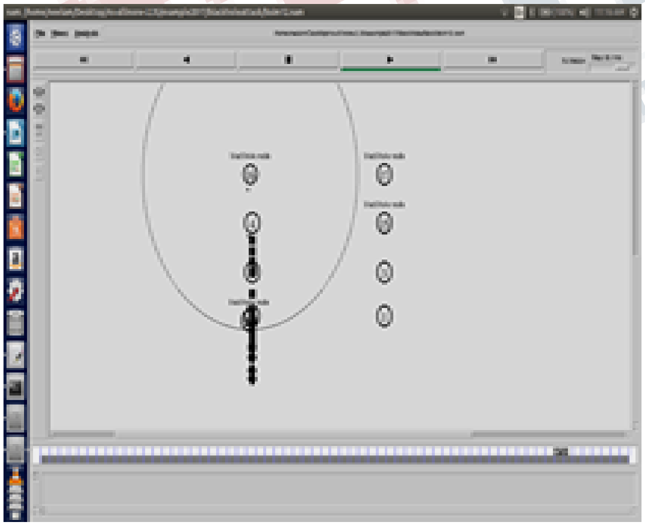


Figure 5: The nam file for black hole attack

Figure 6 shows the graph for average throughput in Xgraph using transfer size in bit Vs. Transfer time of black hole AODV with black hole attack. As we see that the average throughput which is less than normal AODV as it decreases in this situation. Because sending and receiving mechanism under black hole attack.

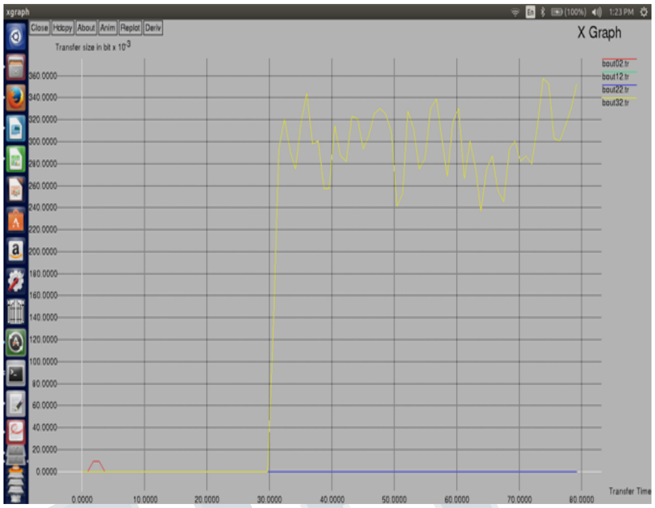


Figure 6: Average Throughput under black hole attack

Figure 7 shows the graph for Packet loss in Xgraph using a number of packet loss Vs. routing time of blackholeAODV with black hole attack. We can see that the number of packets lost increases at the time. This refers to some of the packets absorb in the black hole node without reaching the destination.

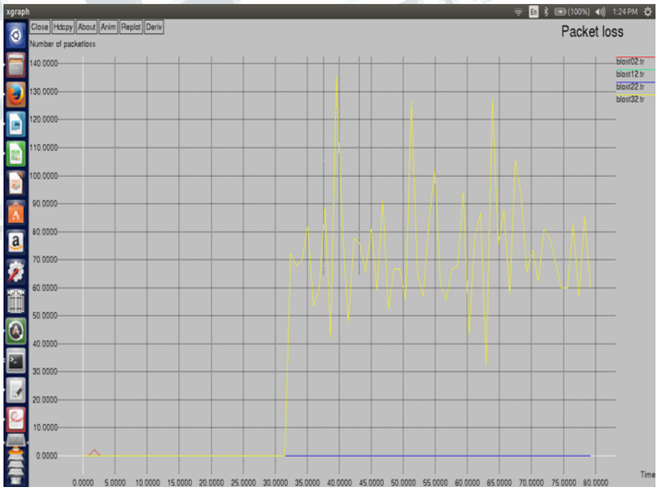


Figure 7: Packet loss under black hole Attack

Figure 8 shows the graph for Packet Delay in Xgraph using a number of packet Vs. Last packet time of blackholeAODV with black hole attack. The packet delay will increase because of a large number of packet losses as the black hole nodes absorb it.

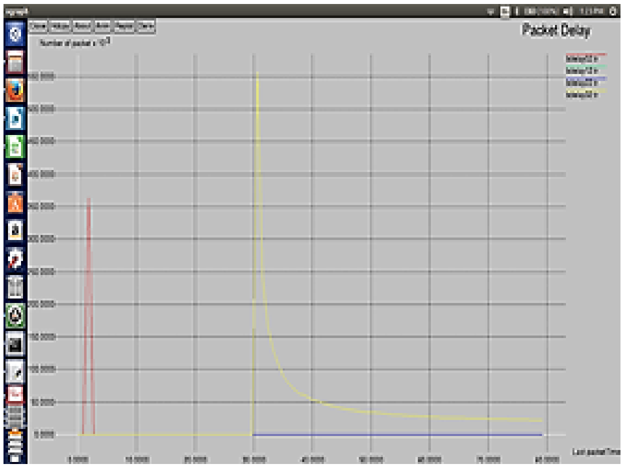


Figure 8: Packet delay under black hole Attack

Figure 9 shows the nam file for the idsAODV routing protocol. In this scenario, we improved and modified AODV routing protocol to detect and prevent intrusion and the malicious node, which causes attacks the network so we use a chasing mechanism. We show this in idsAODV, ids stands for (intrusion detection solution). This figure shows that we have black hole node in the MANETs but packets can deliver from the source to destination.

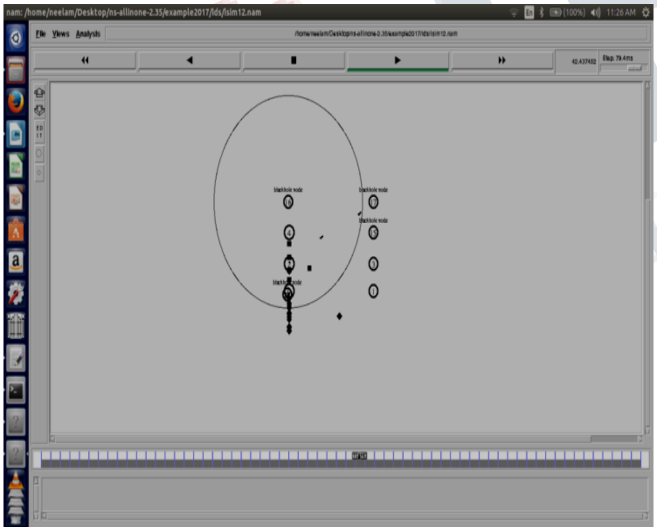


Figure 9: The nam file for idsAODV

Figure 10 shows the graph for average throughput in Xgraph using transfer size in bit Vs. Transfer time of ids AODV with black hole attack. As we see that the average throughput which is less than normalAODV and higher than blackholeAODV under the same situation, because of sending and receiving mechanism under black hole attack.

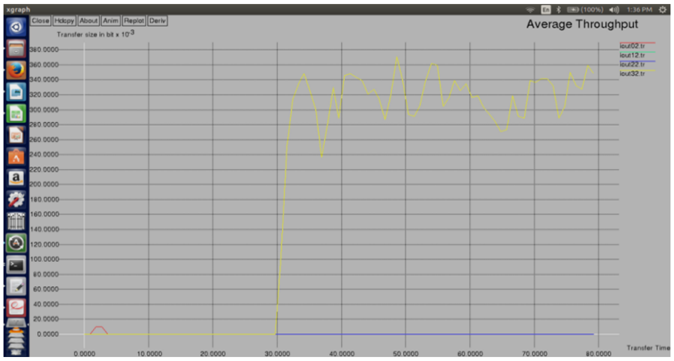


Figure 10: Average Throughput with idsAODV

Figure 11 shows the graph for Packet loss in Xgraph using a number of packet loss Vs. Routing times of idsAODV with black hole attack. We can see that the number of packets lost decrease within the time compare to blackholeAODV. Most of the packets are reaching to destination without any loss.

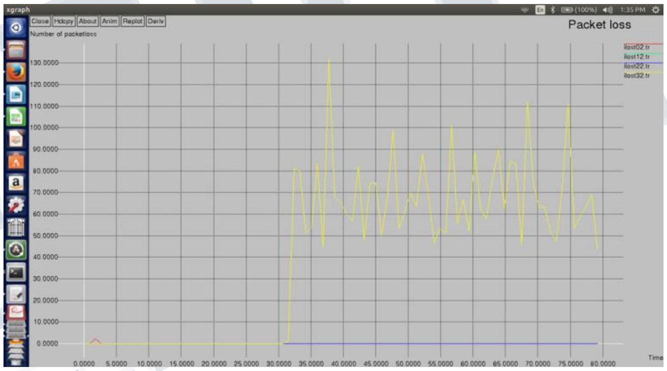


Figure 11: Packet loss with idsAODV

Figure 12 shows the graph for Packet Delay in a graph using a number of packet Vs. Last packet time of idsAODV with black hole attack. The packet delay will decrease because of a large number of packets are reaching to destination without delay

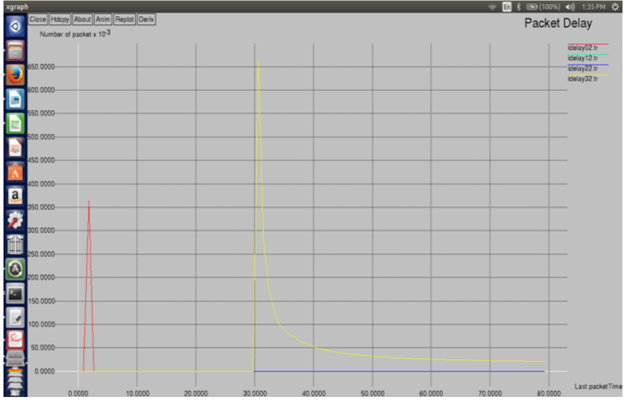


Figure12: Packet delay withidsAODV

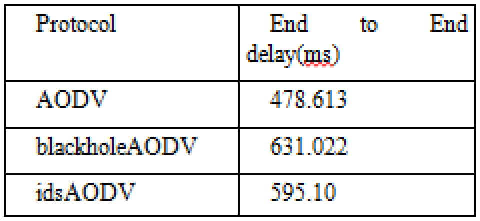
Table II shows a comparison between AODV, blackholeAODV and idsAODV protocols using average throughput, which represent that an intrusion detection solution idsAODV come in between more than black hole AODV and less than normal AODV.

Table: II Average Throughput for protocols

Protocol	Average Throughput
AODV	1185.49
blackholeAODV	187.98
idsAODV	199.91

Table III shows a comparison between AODV, blackholeAODV, and idsAODV protocols using end to end delay, which represents that an intrusion detection solution idsAODV come in less than black hole AODV, and more than normal AODV.

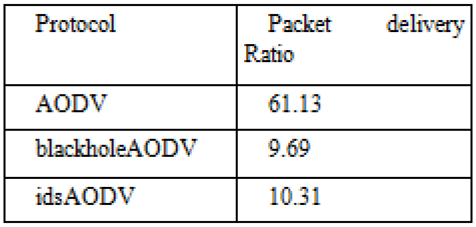
Table III: End to End delay for protocols



Protocol	End to End delay(ms)
AODV	478.613
blackholeAODV	631.022
idsAODV	595.10

Table IV shows a comparison between AODV, blackholeAODV, and idsAODV protocols using packet delivery ratio, which represents that an intrusion detection solution idsAODV come in between more than black hole AODV and less than normal AODV.

Table IV: Packet delivery Ratio for protocols



Protocol	Packet delivery Ratio
AODV	61.13
blackholeAODV	9.69
idsAODV	10.31

V. CONCLUSION

In this research paper, we discuss the MANETs securities issues. Various types of attacks are easily deployed against the MANETs. Here we introduce a black hole attack in the various scenario and compared the performance metrics with and without a black hole attack. We also introduced a prevention of black hole attack using IDSAODV routing protocol. The observation and results show that throughput increases in the presence of IDS. The PDR in the attendance of black hole attack is 9.69 but when we used IDS to prevent the system from attack, the value rises 10.31. The value of End to End delay for black hole attack is 631.022ms but when we used IDS the delay has reduced that is 595.10ms. The advantage of using this method is that idsAODV does not require any supplementary overhead and require minimum modification in AODV protocol and it does not make any changes in the packet format.

REFERENCES

[1] Yibeltal Fantahum Alem and Zhao Hheng Xaun, "Preventing Black Hole Attack in Mobile Ad-hoc in Networks Using Anomaly Detection," from Tainjin, China, IEEE Vol.2 (6), 2010.

[2] Soo Young Shin, Eddy Hartono Halime et al., “Wormhole Attack Detection in MANETs using Route Redundancy and Time-based Hop Calculation,” IEEE, pages 781 – 786, 2012.

[3] Seryvuth Tan and Keecheon Kim, “Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs,” IEEE International Conference on High-Performance Computing and Communications & IEEE International Conference on Embedded and Ubiquitous Computing, IEEE, 2013.

[4] Ume-Hani Syed, Dr. Arif Iqbal Umar et al., “Avoidance of Black Hole Affected Routes in AODV Based MANET,” IEEE International Conference on Open Source Systems and Technologies (ICOSST), IEEE, 2014.

[5] Vimal Kumar and Rakesh Kumar, “An Adaptive Approach for Detection of Black hole Attack in Mobile Ad hoc Network,” International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015), elsevierprocedia computer science 2015, pp. 472-479

[6] Nidhi Choudhary and Dr. Lokesh Tharani, “Preventing Black Hole Attack in AODV using Timer-Based Detection Mechanism,” Signal processing and communication engineering systems (SPACES), International Conference on IEEE, 2015.

[7] Ashish Kumar Jain and Vrinda Tokekar, "Mitigating the effects of Black hole attacks on AODV routing protocol in Mobile Ad hoc Networks,” Pervasive computing (ICPC), 2015 International conference on IEEE, 2015.

[8] Tarek M Mahmoud, Abdelmgeid A. Aly et al., “A Modified AODV Routing Protocol to Avoid Black Hole

Attack in MANETs," International Journal of Computer Applications, Volume 109 –No. 6, January 2015.

[9] Chitra Gupta and Priya Pathak., "Movement-Based or Neighbor Based Technique For Preventing Worm hole Attack in MANET," IEEE Symposium on Colossal Data Analysis and Networking (CDAN), IEEE, 2016.

[10] Upendra Singh, Makrand Samvatsar et al., "Detection and Avoidance of Unified Attacks on MANET using Trusted Secure AODV Routing Protocol", IEEE Symposium on Colossal Data Analysis and Networking (CDAN), IEEE, 2016.

[11] Deepak Kumar Verma, Renu Jain et al., "Intrusion Detection using RREP Messages Of AODV Routing Protocol," International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 9, pp. 1956-1961,2017.