OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

AOMDVBased Security Mechanism for Black Hole Attack in MANET

Shruti Srivastava&Hari Mohan Singh
Department of Computer Science & I.TSHIATS, Allahabad-211007

ABSTRACT: A mobile ad-hoc network is an autonomous system of mobile nodes connected by wireless links in which nodes cooperate by forwarding packets for each other. Security is an essential requirement in mobile ad-hoc networks to provide protected communication between mobile nodes. Due to unique characteristics of MANETS, it creates a number of consequential challenges to its security design. As a consequence, attacks with malicious intent have been and will be devised to exploit the vulnerabilities and to cripple MANET operations. One of the well-known attacks on the MANET is the Black Hole attack which is most common in the on demand routing protocols such as AODV. In a black hole attack, the malicious node presents itself as containing the shortest path to the node it is impersonating, making it easier to intercept the message. This paper represents an enhanced AOMDV routing protocol for avoiding black hole attack in MANET and provide its security. The simulation results demonstrate that this protocol not only prevents black hole attack but consequently improves the overall performance of (normal) AODV in presence of black hole attack. It is observed that the packet loss is less initially but it increases substantially as the mobility of node increases. The proposed enhanced AOMDV (BDA-AOMDV) approach has lesser packet loss when node speed is increases. Similarly, In the case of route delay performance metric, on the increment of node speed (mobility of node) the route delay of packets is very high for the AOMDV than the proposed approach under the presence of black hole nodes.

Keywords:Attack, Black hole attack, MANET, Routing protocols, AODV, AOMDV, Security, delay.

I. INTRODUCTION

Mobile ad hoc network (MANET) is one of the recent active fields and has received spectacular consideration because of their self-configuration and self-maintenance. Early research assumed a friendly and cooperative environment of wireless networkthereby enabling communication beyond direct wireless transmission range. Security in wireless ad-hoc networks is a complex issue. This complexity is caused by various factors like insecure wireless communication links, dynamic topology, and absence of a fixed infrastructure, node mobility, and resource constraints.MANETs are more susceptible to security attacks caused by the lack of a reliable centralized authority and limited resources and mobility/wireless links. Attacks on mobile ad hoc networks can be categorized as passive and active attack as well as external and internal attack, based on whether the common operations of the network is disrupted or not. A black hole attack is one such type of severe active routing attack in which a malicious node advertises itself as having the shortest path to a destination in a network. This can cause Denial of Service (DoS) by dropping the received packets [2].MANETs are also called mobile multihop wireless networks. MANETs are defined as "A Mobile Ad hoc Network is an autonomous organization of mobile nodes or computers."

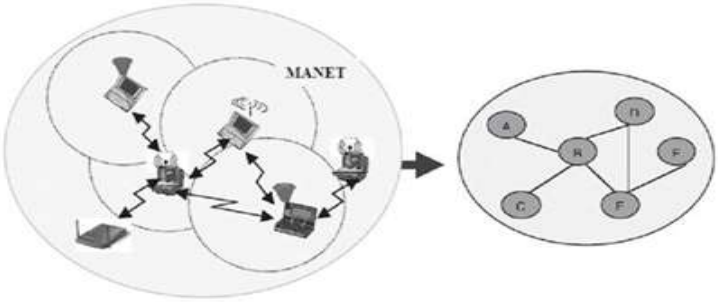


Figure 1: Mobile Ad Hoc Network

Attacks in Manet

Attacks on ad hoc networks can be classified primarily in two types such as active and passive attacks [1].

Passive Attacks In passive attacks, attackers don't disrupt the operation of routing protocol but only attempt to discover valuable information by listening to the routing traffic. The attacker only looks and watches the transmission and does not try to modify or change the data packets.

Active Attacks In the active attacks, the malicious nodes introduce false information to confuse the network topology. They can either attract traffic to them and then drop or compromise the packets. They can also send false information and lead packets to the wrong node and cause congestion in one area.

Black Hole Attack

A black hole attack occurs when a malicious node impersonates the destination node or forging route reply message that is sent to the source node, with no effective route to the destination. The malicious node may generate unwanted traffics and usually discards packets received in the network. When this malicious node (black hole node) has effects on one or more nodes, making them malicious as well, then this kind of attack can be referred to as multiple node attack or collaborative attack [1]. In a black hole attack, the malicious node presents itself as containing the shortest path to the node it is impersonating, making it easier to intercept the message [10].

Routing in MANET

Many different types of routing protocols have been developed for ad hoc networks and have been classified into two main categories by Royer and Toh (1999) as Proactive protocols and Reactive (on-demand) protocols. In a proactive routing protocol, nodes periodically exchange routing information with other nodes in an attempt to have each node always know a current route to all destinations. In a reactive protocol, on the other hand, nodes exchange routing information only when needed, with a node attempting to discover a route to some destination only when it has a packet to send to that destination. In addition, some ad hoc network routing protocols are hybrids of periodic and on-demand mechanisms.

II. AD HOC ON-DEMAND DISTANCE VECTOR ROUTING

AODV is a reactive routing protocol that does not lie on active paths .The nodes do not have to discover and maintain a route to another node until the two needs to communicate, unless former node is offering its services as an intermediate forwarding station to maintain connectivity between other nodes. AODV has borrowed the concept of destination sequence number from DSDV, to maintain the most recent routing information betweennodes [15]. Whenever a source node needs to communicate with another node for which it has no routing information, Route Discovery process is initiated by broadcasting a Route Request (RREQ) packet to its neighbours. Each neighbouring node either responds the RREQ by sending a Route Reply (RREP) back to the source node or rebroadcasts the RREQ to its own neighbours after increasing the hop_count field. If a node cannot respond by RREP, it keeps track of the routing information in order to implement the reverse path setup or forward path setup.

The destination sequence number specifies the freshness of a route to the destination before it can be accepted by the source node. Eventually, a RREQ will arrive to node that possesses a fresh route to the destination. It determines whether the route is fresh by comparing the destination sequence number in its route table entry with the destination sequence number in the RREQ received. The intermediate node can use its recorded route to respond to the RREQ by a RREP packet, only if, the RREQ's sequence number for the destination is greater than the recorded by the intermediate node. Instead, the intermediate node rebroadcasts the RREQpacket. If a node receives more than one RREPs, it updates its routing information and propagates the RREP only ifRREP contains either a greater destination sequence number than the previous RREP, or same destination sequence number with a smaller hop count. It restrains all other RREPs it receives. The source node starts the data transmission as soon as it receives the first RREP, and then later updates its routing information of better route to the destination node. As the routing protocols typically assume that all nodes are cooperative in thecoordination process, malicious attackers can easily disrupt network operations by violating protocol specification. If there is oneor more malicious node (black hole node), it receives theRREQ then Malicious nodes respond immediately by sending a fake RREP to the source node as these nodes do not refer the routing table, which shows malicious node already has a fresh path to the destination. The maliciousnode does this by including false routing information suchas higher sequence number and lower hop count that shows it is a fresh path. The source node receives the RREP, it assumes that the route discovery process is complete; it ignores other RREP messages from other nodes and selectsthe path through the malicious node to route the data packets. The attacker now drops the received messages instead of relaying them as the protocol requires.

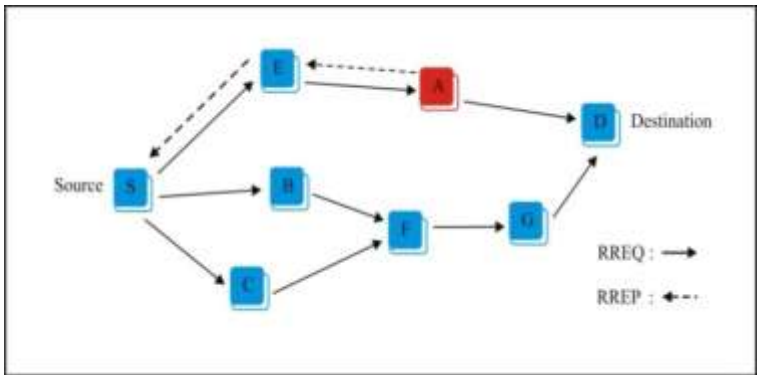


Figure 2: Black hole Attack on AODV

Figure 2 shows an example of a black hole attack, in which malicious node A sends a false RREP packet to the source node S without performing standard AODV operations, declaring that it has a adequately fresher route than other nodes. Since AODV thinks about RREP packet containing higher value of destination sequence number and lower hop count to be fresh, the RREP sent by the malicious node A is treated fresh. The source node S will select the route that goes through node A. Thus, malicious nodes succeed in injecting Black Hole attacks. . The received data packets by the Black Hole node will then be eavesdropped or dropped. Therefore, source and destination nodes are unable to communicate with each other

AOMDV

Ad-hoc on-demand multipath distance vector (AOMDV) routing protocol (Marina and Das, 2006) is an extended version of AODV. AOMDV provides multiple paths to reach the destination while AODV only has a unipath to the destination. Despite of their difference, both protocols share the same behavior in several things such as reactive route discovery mechanism and route maintenance [3]. AOMDV also has similar kind of routing packets such as RREQ,RREP, RERR and Hello messages. However, AOMDV in particular has extra RREP and RERR for multipath discovery and maintenance along with few extra fields in routing control packets. Thus it costs more routing overhead than AODV. However, instead of responding to one RREQ, the destination will respond to several numbers of RREQs by sending unicast transmission of multiple RREPs back to the source. Thus it creates the multipath between the source and the destination. The challenge of how to ensure the loop free and disjoint path is the issue that needs to be considered in AOMDV.

LOOP FREEDOM

A set of sufficient conditions for loop-freedom is formulated below. These conditions allow multiple paths to be maintained at a node for a destination. Sufficient Conditions are-

1. Sequence number rule: Maintain routes only for the highest known destination sequence number. For every destination, we restrict that multiple paths maintained by a node have the same destination sequence number. Once a route advertisement containing a higher destination sequence number is received, all routes corresponding to the older sequence number are discarded. However, as in AODV, different nodes (on a path) may have different sequence numbers for the same destination.

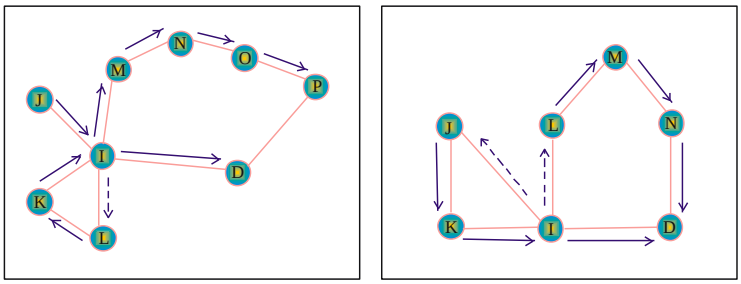
2. for the Similar Destination Sequence Number-

(a)Route advertisement rule: Never advertise a route shorter than one already advertised.

(b) Route acceptance rule: Never accept a route longer than one already advertised. AOMDV uses the concept of an "advertised hop count", to keep up multiple paths for the same sequence number. Every node maintains a variable called advertised hop count for each destination. This variable is set to the length of the longest available path for the destination at the time of first advertisement for a particular destination sequence number. The advertised hop count remains unchanged until the sequence number changes. Advertising the longest path length permits more number of alternate pathsto be maintained.

Disjoint Paths

Besides maintaining multiple loop-free paths, AOMDV try to find disjoint alternate paths. Two types of disjoint paths are considered: link disjoint and node disjoint. Link disjointset of paths between a pair of nodes have no common links, whereas node-disjointness additionally precludes common intermediate nodes.



(a) (b)

Figure 3: Examples of potential routing loop scenarios with multiple path computation.

III. RELATED WORK

The black hole attack is one of the eminent security dangers in wireless mobile ad hoc networks (MANETs). The intruders utilize the loophole to perform their malicious behaviors because the route discovery procedure is necessary and unavoidable. Many researchers have conducted different detection and prevention techniques to propose different types of detection/prevention schemes or approaches. In this section, we survey the existing solutions for single black hole attack and cooperative black hole attack and analyze or study them properly and discuss the up to date routing methods.

Zaid Ahmad et al. (2011)proposed that the problem of black hole attack and its effect on the AODV-based routing protocol has been discussed. ERDA is designed to isolate and alleviate the effect of black hole attacks in MANET. ERDA improves recvReply () function in the AODV protocol to enhance the network performance by improving routing update condition. The improvementonly involves a smallest modification anddoes not change the existing AODV protocol technique. The solution is also simple and appropriate for most resource constraint devices.

Ming-Yang Su (2011), attempts to detect and separate malicious nodes, which preferably perform black hole attacks by deploying IDSs inMANETs. All IDS nodes perform an ABM (Anti-Black hole Mechanism), which estimates the suspicious value of a node, in accordance with the amount of abnormal differencebetween RREQs and RREPs transmitted from the node. With the deployment of the proposed IDSs, the total packet loss rate can be greatly improved.

E. A. Mary Anita, V. Vasudevan et al. (2010) have proposed a solution for black hole attack by authenticatingnodes using localized certificate chains. Simulations show that BHS-ODMRP is as effective as ODMRP in discovering and maintaining routes additionally to providing the required security. The suggested protocol decreases the packet loss due to black holes to about 20% which is about 15% higher compared to ODMRP protocol. Also, the proposed mechanism protects the network through a self-organized, completely distributed and localized process. The additional certificate publishing happens only for a short period of time throughout which almost all nodes in the network make certified by their neighbor nodes. Later on some duration of time each node has a catalog of certificates and hence the overhead incurred in this process is reasonable with a good network performance regarding security. The proposed method can also be applied for securing the network from other routing attacks by altering the security parameters according to the nature of the attacks.

In paper [16, 18]authors proposed an improvement of the AODV protocol by introducing fidelity table. The RREPsare collected in the response table and the fidelity level of each RREP is checked and one is selected having the highest level. After acknowledgement is received, the fidelity level of the node is updated proving it safe and reliable. However, updating the fidelity table of each node by broadcasting it to other nodes results in congestion and also the selection of wrong RREP from the response table cause another route request flooding.

IV. BLACK HOLE DETECTION & AVOIDANCE BASED ON AOMDV

The routing protocol (BDA-AOMDV) Black hole Detection & Avoidance Ad-hoc on Demand Multipath Distance Vector, which is proposed to avoid multiple black hole attacks during path setup (route discovery phase) between source and destination. This approach based on Ad hoc On Demand Multipath Distance Vector (AOMDV) and uses its concept to build link disjoint multipath during path detection and it does an additional check to find whether the RREP_Seq_no is higher than the threshold value. The threshold value is dynamically updated as in every time interval. As the value of RREP_Seq_no is found to be higher than the threshold value, the node is suspected to be malicious and it adds the node to the black list. As the node detected an anomaly, it sends a new control packet, TERROR to its neighbours.TheTERRORpacket has the black list node as a parameter so that, the neighbouring nodes know that RREP packet from the node is to be discarded. Further, if any node receives the RREP packet, it looks over the list, if the reply is from the

blacklisted node, no processing is done for the same. It simply ignores the node and does not receive reply from that node again. So, in this way, the malicious node is isolated from the network by the TERRORpacket. The continuous replies from the malicious node are blocked, which results in less Routing overhead. Moreover, unlike AODV, if the node is found to be malicious, the routing table for that node is not updated, nor the packet is forwarded to another node. The threshold value is dynamically updated using the data collected in the time interval. If the initial training data were used, then the system could not adapt the changing environment. The threshold value is the average of the difference of dest_seq_no in each time slot between the sequence number in the routing table and the RREP packet. The time interval to update the threshold value is as soon as a newer node receives a RREP packet. As a new node receives a RREP for the first time, it gets the updated value of the threshold. So our design not only detects the black hole attack, but tries to prevent it further, by updating threshold which reflects the real changing environment. Other nodes are also updated about the malicious act by a TERROR packet, and they react to it by isolating the malicious node from network.

Threshold Value= {avg (Destination_seq_noin Routing table - Destination_seq_no. in RREP)}

When a source node wishes to communicate with any specific destination node, it will send RREQ packets to its intermediate nodes to find out a shortest and fresh path to the destination through using these nodes. When intermediate nodes reply to source node then only some nodes in the path may have multiple paths to the destination but it ultimately chooses only one path to the destination node for transmits its data packets. In this proposed solution (BDA-AOMDV), each node maintains the compatibility of their neighbor nodes to create the correct path to destination node. If a node whose compatibility ratio crosses the predefined lower threshold level, it will not be attempted by an intermediate node to create a path that goes through with this node, during path discovery of BDA-AOMDV. Thus, malicious nodes will be steadily avoided by other non-malicious nodes in the network. The proposed BDA-AOMDV has the following message formats.

RREQ Packet: RREQ packet in BDA-AOMDV has additional $first_hop$field. This field is used to store the IP address of the first hop after it left the originator. In path discovery phase, BDA-AOMDV creates link disjoint multiple paths using $first\_hop$ field but during path setup (RREP) it selects only single link which has the higher compatibility ratio among multiple links towards source and destination.

RREP Packet:RREP packet in BDA-AOMDV has one extra field called. This field is used to store the identity of the node (can be intermediate or destination node) who is declaring a path to the destination. When the node receives RREP packet, this field value (of node) is being stored in the field of routing table.

Routing Table: Routing table in enhanced AOMDV (BDA-AOMDV) has following fields: First_hop it is used to store the value of First_hop field of RREQ to avoid loop in the path formation. However, when a node receives an RREP, this field is used to store the value of Originator field of RREP. Count field denotes the number of RREPs received with same sequence number for the entry but its value would be-1 if the entry has been created after RREQ arrival.

Compatibility Table: In BDA-AOMDV protocol, each node maintains a compatibility table that is shown in Table 1 this table is used to pick the most compatible node (among the many backward disjoint link to source node and next hop to destination) while transmitting RREP packet back to source node. Compatibility table includes three fields: Node ID, Pathcount and Sentcount.
Node ID: - this field keeps the IP address of the node whose compatibility is being listed.
Pathcount field: - it denotes the number of times the node has been selected in the route.
Sentcount field: - it explains the number of times connection to destination node have been successful node through the Node ID.
The compatibility ratio of a node is calculated as follows:
(CR) = ((Sentcount) / (Pathcount +1))

Table1: Compatibility Table

Node ID	Pathcount	Sentcount
B	4	7
-	-	-
C	6	4
E	5	9

The compatibility ratio of a Node ID which signifies the confidence of node in accomplishing its intended function of accurate routing. If a node contains higher compatibility ratio means it has higher possibility of being non-malicious.

Threshold Levels

Black hole node cannot cause BDA-AOMDV to lose its security functions because each node traces the compatibility ratio of other nodes in its compatibility table which black hole node cannot access in any case. Sometime later, when non-malicious nodes in the network get high compatibility ratio value in other nodes compatibility table then black hole node will not be chosen in the path because of its low compatibility ratio. The node which has the higher compatibility ratio will be chosen for the data transmission. We have set three threshold level of compatibility ratio namely lower, middle and upper which description is given below-

1. Lower threshold level is used to discover the black hole activity (drops all the incoming packet, therefore *Sentcount* field of these nodes are always zero that is Compatibility Ratio=0) of the node in the network.
2. Middle threshold level is used to detect the gray hole activity (selective dropping i.e. Compatibility Ratio≠0) of the node. When the compatibility ratio of a node crosses either lower or middle threshold level, then an RREP from such node will be dropped by their neighbors. However we have simulated BDA-AOMDV only for avoiding black hole.
3. Upper threshold level indicates a high confidence node.

V. SIMULATION & RESULTS

Simulation Environment

The simulation parameters chosen for the experiments are only for illustration purposes and given as -

Parameter	Value
Channel Type	Channel/Wireless Channel
Propagation	Propagation / Two way
MAC Type	MAC/802.11
Antenna Type	Antenna /Omni Antenna
Network Layer	LL
Queue	Queue/ Drop Tail/Pri Queue
Queue Length	50
Range of Each Node	50
Network Interface Type	Phy/wireless Phy
No. of Nodes	30
Protocol	AODV, AOMDV
Value (x)	1000
Value(y)	1000
Packet size	512 bytes
Traffic Size	Constant Bit Rate (CBR)
Node Mobility	5 to 40
Number of Malicious nodes	5
Simulation Tool	Network simulator-2.34

Simulation Evaluation Methodology

Nodes Speed: It is the speed of nodes moving in the network and we shall check the performance of BDA-AOMDV on different node speed.

Number of packets dropped: The total number of routing packets dropped during the simulation.

Packet Loss: packet loss is the difference between the number of data packets delivered and the number of data packets obtained. It is calculated as follows

Packet Loss= Number of data packets sent− Number of data packets received.

Packet loss percentage: percentage of data packets dropped in the network either at the source or at intermediate nodes;

Average route delay: This comprises all possible delays caused by buffering throughout route detection, waiting in line at the interface queue, retransmission delays,and propagation and transfer times.

Packet Delivery Ratio: The ratio of the data delivered to the destination to the data sent out by the source.

Throughput: It is the measure of how fast we can actually send packets through network. It is the total amount of data a receiveractually receives from the sender divided by the time it takes for receiver to get the last packet.

The performance of AODV, AOMDV and enhanced AOMDV(BDA-AOMDV) against the black hole attack is compared according to the performance metrics and simulation results which are shown in below with tables and figures.

Figure 4 and Figure5 shows the percentage of packet loss in BDA-AOMDV against node mobility in comparison with AOMDV protocol in presence of black hole attack.

Figure4: Comparison of AOMDV and BDA-AOMDV on basis of Packet Loss

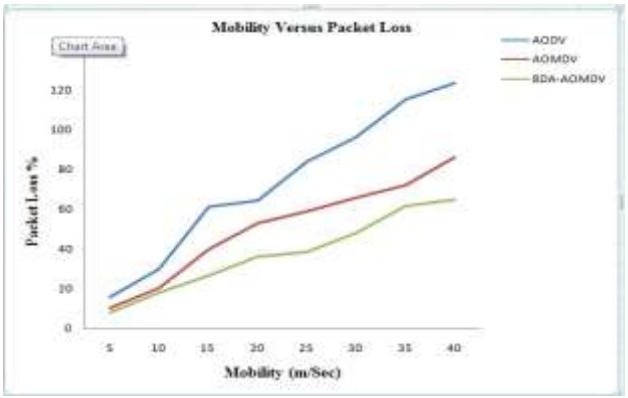


Figure5: Comparison of AODV,AOMDV and BDA-AOMDV on basis of Packet Loss

Figure 6 shows the percentage of packet delivery ratio in BDA-AOMDV against node mobility in comparison with AOMDV and AODVprotocol.

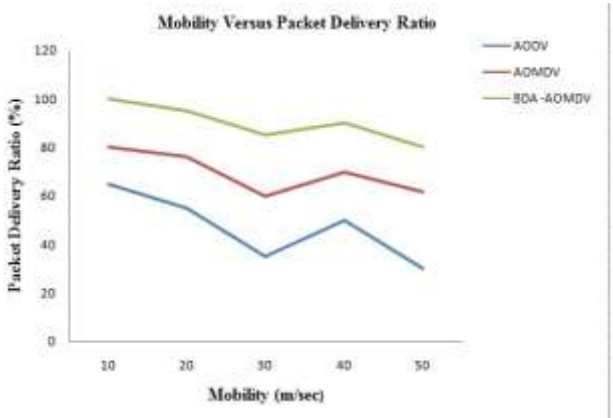


Figure6: Comparison of AODV,AOMDV and BDA-AOMDV on basis of Packet Delivery Ratio

AOMDV being a multipath routing protocol, even if the current link breaks due to black hole attack, the network will find an alternate path from the source to the destination node and have a better chance of packet delivery without any block hole attack, hence less number of packets will be dropped for BDA-AOMDV.

From the figure 7and Figure8it is confirmed that BDA-AOMDV has comparatively low average route delay than AOMDV due to the fact if a link break occurs in the current topology, BDA-AOMDV would try to find an alternate path from among the backup routes between the source and the destination node pairs resulting

in additional delay to the packet delivery time. In comparison, if a black hole attack occurs in AODV, the packet would not reach the destination another path from source to destination, since only singular paths exist in AODV between a source and destination node.

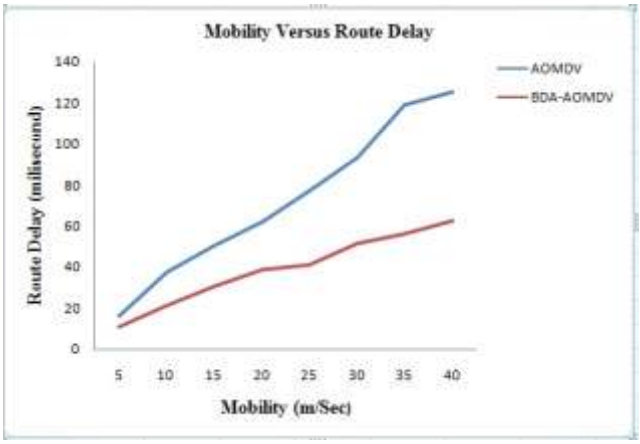


Figure 7: Comparisons of AOMDV and BDA-AOMDVon basis of Route delay

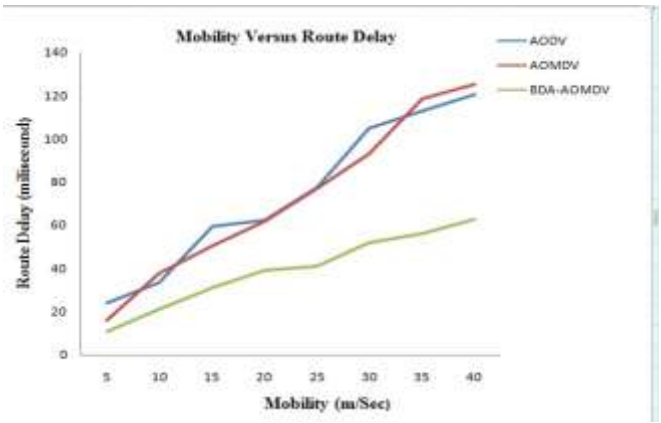


Figure 8: Comparison of AODV, AOMDV and BDA-AOMDV on basis of Route delay

From the Figure9and Figure10 it is confirmed that BDA-AOMDV has better throughput and packet delivery ratio in presence of attack.

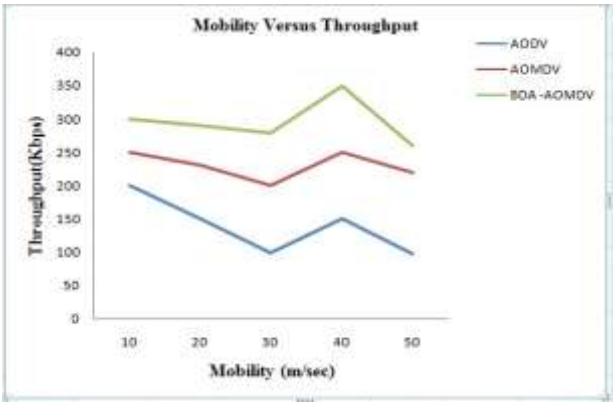


Figure 9: Comparison of AODV, AOMDV and BDA-AOMDV on basis of Throughput

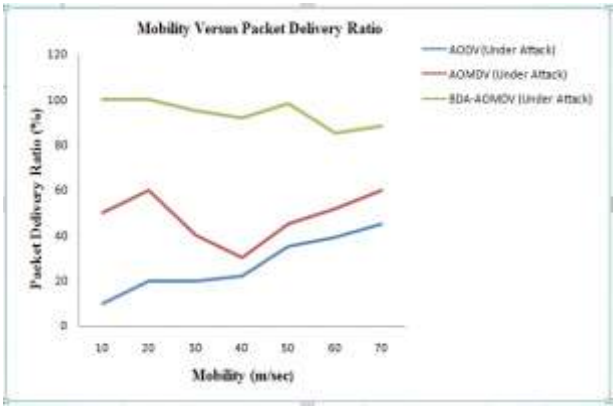


Figure 10: Comparison of AODV, AOMDV and BDA-AOMDV under attack on basis of PDR

VI. CONCLUSION

Black Hole Attack is a main security threat that affects the performance of the AODV routing protocol. Its recognition is the major subject of concern. Due to the intrinsic design drawbacks of routing protocol in MANETs, many research workers have performed various techniques to propose different types of avoidance techniques for black hole issue.

So we can conclude by receiving simulated results that the proposed approach has shown better performance results with respect to performance parameters such as route delay and loss of packet in the presence of black hole nodes in the network. It also shows that throughput of the network is increased in the proposed approach in comparison of AOMDV.

REFERENCES

[1] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks", *Proceedings of the ACM Conf. on Mobile Computing and Networking (Mobicom), pp. 255-265, August 2000.*

[2] M. K. Marina and S. R. Das,"On-demand multi-path distance vector routing in ad hoc networks", *Proceedings of the IEEE Intl. Conf. on Network Protocols (ICNP), pp.14-23, 2001.*

[3] Bhargava, S.; Agrawal, D.P, "Security enhancements in AODV protocol for wireless ad hoc networks", *IEEE VTS 54th Vehicular Technology Conference (VTC), Vol. 4, pp. 2143 – 2147, 2001.*

[4] H. Deng, W. Li, and D. P. Agrawal," Routing Security in Ad hoc Networks", *In IEEE Communications Magazine, Vol. 40, No. 10, pp. 70-75, Oct. 2002.*

[5] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding Royer, "Secure routing protocol for Ad-Hoc networks," *In Proc. of 10th IEEE International Conference on Network Protocols, Dept. of Computer. Sci., California Univ., Santa Barbara, CA, USA. Pp.78- 87, ISSN: 1092-1648, 12-15 Nov. 2002.*

[6] S. Buchegger, and J. Le Boudec, "A test bed for misbehaviour detection in mobile ad hoc network show much can watchdogs really do", *Technical Report IC/2003/72 EPFL-DI- ICA, pp. 32-41, 2003*.

[7] J. Schiller, "Mobile Communications", *Addison- Wesley, Pearson education August 2003.*

[8] Yi-Chun Hu, Adrian P., David B. Johnson ,"Rushing Attacks and Defence in Wireless Ad Hoc Network Routing Protocols", *WiSe 2003, September 19, 2003, San Diego, California, USA.*

[9] Li. Zhou, Zygmunt J. Haas,"Securing Ad Hoc Networks", *IEEE network, special issue, November/December 1999.*

[10] Perkins, E. Belding-Royer, and S. Das, "Ad-hoc on-demand distance vector (AODV) routing",*Internet Draft, RFC 3561, July 2003.*

[11] Yi-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", *IEEE Security andPrivacy May/June 2004.*

[12] C. E. Perkins and E. M. Royer, "The Ad hoc On-demand distance vector protocol", *In C. E. Perkins, editor, ad hoc Networking, Addison-Wesley, pp. 173-219, 2004.*

[13] M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks", *In Proceedings of the ACM 42nd Southeast Conference (ACMSE'04), pp 96-97, Apr. 2004.*

[14] M.A. Shurman, S.M. Yoo, and S. Park, "Black hole attack in mobile ad hoc networks*", 42nd ACMSoutheast Regional Conf., pp. 11-14, 2004.*

[15] Latha Tamilselvan, V Sankaranarayanan, "Prevention of Black hole Attacks in MANET", *In Proceedings of the 2nd InternationalConference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007), pp. 21-21, Aug. 2007.*

[16] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", *Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007*

[17] L. Tamilselvan, and V. Sankaranarayanan, "Prevention of cooperative black hole attack in manet", *Journal of Networks, Vol. 3 (5), pp.13-20,2008.*

[18] Davide Cerri and A. Ghioni, "Securing AODV: The A-SAODV Secure Routing Prototype", *IEEE Communications Magazine, February 2008.*