Avoiding Black Hole Attack In Mobile Ad Hoc Networks Using Aomdv Routing Protocol

K.Divya[1], Dr.B.Srinivasan[2]
[1]*Ph.D Research Scholar, Department of Computer Science, Gobi Arts & Science College, Gobichettipalayam, INDIA*
[2]*Associate Professor, Gobi Arts & Science College, Gobichettipalayam, INDIA*

Abstract - A mobile ad-hoc network (MANET) is very receptive to security attacks due to its open medium, dynamically changing network topology, lack of centralized monitoring. These vulnerabilities are nature of MANET structure that cannot be removed. As a consequence, attacks with malicious intent have been and will be devised to exploit these vulnerabilities and to cripple MANET operations. One of the well known attack on the MANET is the Black Hole attack which is most common in the on-demand routing protocols such as AODV. This paper represents an enhanced AOMDV routing protocol for avoiding black hole attack in MANET. This routing protocol uses Ad hoc On-demand Multipath Distance Vector (AOMDV) to form link disjoint multi-path during path discovery to provide better path selection in order to avoid malicious nodes in the path using legitimacy table maintained by each node in the network.

Keywords - Attack, Black hole attack, MANET, Routing protocols, AODV, AOMDV, NS-2.34, Security, delay

I. INTRODUCTION

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 there by 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. In MANET, nodes also perform the role of routers that discover and maintain routes to other nodes in the network. The major concern of routing protocols of MANET is to establish an efficient and optimal route between the communicating entities. Any attack in routing phase may disrupt the overall communication and the entire network can be paralyzed. These attacks can be categorized as active and passive attacks. A passive attack is one in which the information is snooped by an intruder without disrupting the network activity. An active attack interrupts the normal operation of a network by modifying the packets in the network. Attacks can be further classified as external and internal attacks. External attacks are accomplished by nodes that do not form part of the network. Internal attacks are from compromised nodes that were once legitimate part of the network. Among these one of the most important security issues is the protection of the network layer from different active routing attacks. 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.

II. OVERVIEW OF MOBILE AD HOC NETWORKS

Ad hoc network can be considered as a special type of wireless mesh networks which is a collection of mobile wireless nodes formed without any infrastructure or any standard services. Mobile Ad hoc Networks (MANETs) are decentralized and mobile nodes act as router and also as host. Mobile nodes can transmit the packets to the node which are in its proximity. If a mobile node has to send the packet to other mobile nodes which are out of its range then the nodes within its range forwards packets to the next hop until packets reaches intended destination. Thus MANETs are also called mobile multihop wireless networks. MANETs can be setup between few nodes or can be expanded by connecting to fixed network.

The fundamental difference between fixed networks and MANET is that the nodes in a MANET are mobile nodes. Due to the mobility of these nodes there are some characteristics that are only applicable to MANET.

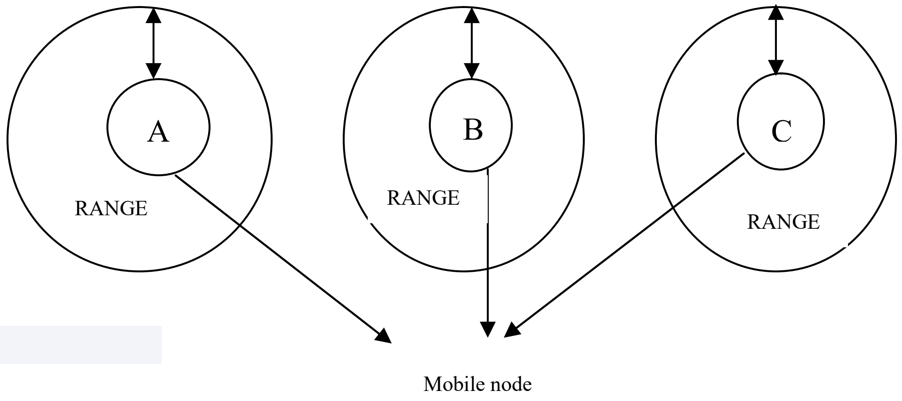

FIGURE 1 Mobile ad Hoc Network

A Security Issues for Mobile Ad Hoc Network (MANET)

Security is much more difficult to maintain in the mobile adhoc network than in the wired network. Following are the various security issues that exist in the mobile adhoc networks.

- Lack of secure boundaries
- Compromised nodes
- Lack of Centralized Management Capability
- Restricted Power Supply
- Scalability
- Wireless Links:
- Dynamic topology

2.1 Applications of Mobile Ad Hoc Network

In this section we present some general applications of mobile ad hoc networking as seen in a day-to-day life or otherwise.

- Tactical networks
- Sensor Networks
- Emergency Services
- Commercial Environments
- Educational applications
- Home and Enterprise Networking
- Location aware service

2.2 Characteristics of Mobile Ad Hoc Networks

MANETs acquire common features found in wireless networks in common and add characteristics specific to adhoc networking:

- Mobility
- Multi hopping
- Self-organization
- Energy conservation

- Scalability
- Security

III. ATTACKS IN MANET AND BLACK HOLE ATTACK

Security is an essential requirement in mobile ad hoc network (MANETs). Attacks on ad hoc networks can be classified primarily in two types such as active and passive attacks.

Active attacks: Those attacks which attempt to alter, inject, delete or destroy the data being exchanged in the network. Intention of such an attack is to damage the network or disrupt the network operations. Example: Fabrication or masquerading attacks, message modifications, message replays and DOS attacks.

Passive attacks: Those attacks which attempt to learn or make use of information but do not affect the system resources. Such an attack has no intention to damage the network & network operations because it does not modify the contents of the packets.

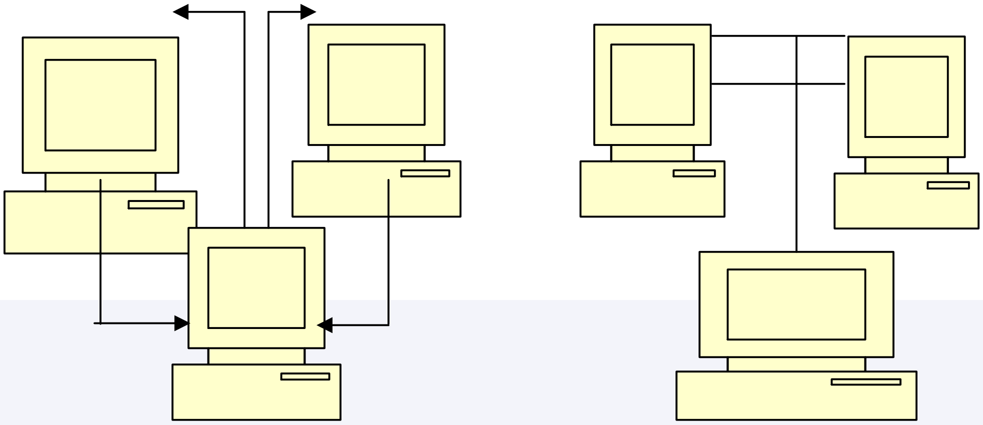

Figure 2 Active and Passive Attacks in MANET'S

3.1Black Hole Attack

Routing protocols are exposed to a variety of attacks. Black hole attack is one of the possible attacks in MANET routing protocols. In black hole attack, a malicious node sends the route reply message to the source node with the intention of advertise itself for having the shortest path to the destination node. Before the reception of the any other node in the network the malicious node reply will be received by the requesting node. When this route is created, malicious node receives the data packet, now it is up to the malicious node whether to drop all the data or forward it to the unauthenticated nodes.

3.2 Black Hole Attack in AODV Protocol

In black hole attack a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. This attack targets at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. During the Route Discovery process of AODV routing protocol when a source node wishes to communicate with the other nodes or transmits the data packets to the destination.

If there is one or more malicious node (black hole node), it receives the RREQ 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 malicious node does this by including false routing information such as 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 selects the 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.

AODV considers RREP having 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 choose the route that passes 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.

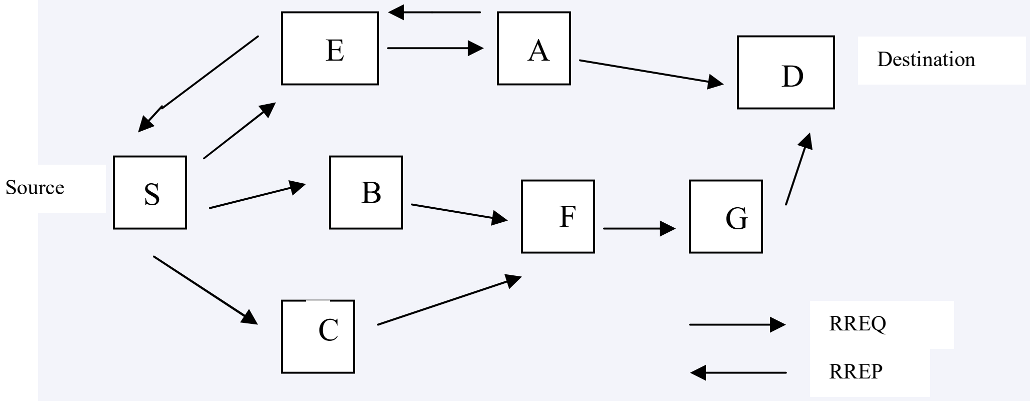

FIGURE 3 BLACK HOLE ATTACK ON AODV

IV. AODV OVERVIEW

It provides a rapid, dynamic network connection with low processing load sand low memory consumption. Nodes in the network exchange routing information only when they intend to communicate and keep this information updated only as long as the communication lasts

A node intending to send a packet to another node starts a route discovery process in order to establish discovery process in order to establish a route to the destination node, by sending a route request message (RREQ) to its neighbor nodes. Neighboring nodes increment the hop count on receiving the RREQ, and similarly forward (broadcast) the message to their neighbors using a flooding approach. This continues until the destination node is found. The RREQ message forwarding has the side effect of making the rnodes learn the reverse route to the source node. The RREQ message will eventually reach the destination node, which will respond with a route reply message (RREP). The RREP is sent as a unicast to the source node along the *reverse route* established during the RREQ broadcast. Similarly, the RREP message allows intermediate nodes to learn a *forward route* to the destination node. Hence, at the end of the route discovery process, packets can be delivered from the source node to the destination node and vice versa. Every mobile node would periodically send Hello messages (HELLO), thus, each node knows which nodes are its neighboring nodes within one-hop. Routing messages are either path discovery (RREQ and RREP) or path maintenance (RERR and HELLO) messages. All routing information expires after a timeout incase of an inactive route, and is removed from the routing table.

AODV is a collaborative protocol, permitting nodes to share information about each other. RREQ messages do not necessarily need to reach the destination node during the route discovery process. That is to say, an intermediate node having a route to the destination simply generates the RREP without any further forwarding of the RREQ. This enables a quicker response to route availability, eliminating unnecessary further flooding of RREQs.

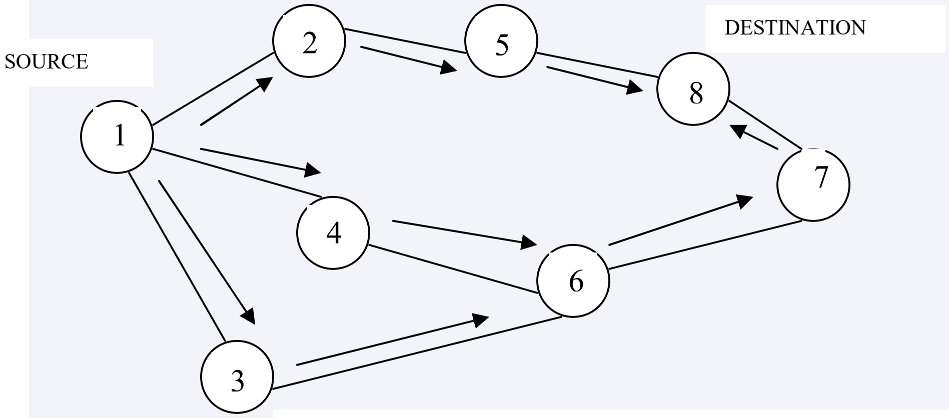

FIGURE 4 PROPAGATION OF RREQ PATH TO SOURCE

Sequence numbers are used by AODV to identify fresher routing information. Every node maintains its own sequence number, incrementing it before sending either a new RREQ or RREP message. The sequence numbers are included in routing messages and recorded in routing tables. AODV favors newer information, thus nodes update their routing table whenever they receive a message with a higher sequence number (a larger number refers to newer information) or a smaller hop count (smaller hop count refers to shorter path) than what exists in the routing table for a given destination. However, a sequence number is given a higher priority than a hop count.

However, the security of AODV is compromised by the Black Hole nodes, as it accepts the received RREP having fresher route. The standard AODV routing protocol cannot fight the threat of Black Hole attacks, because during the phase of route discovery, malicious nodes may counterfeit a sequence number and hop count in the routing message thereby, acquiring the route, eavesdropping or/and dropping all the data packets as they pass.

V. AOMDV OVERVIEW

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. 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. 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.

5.1 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 as follows: 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. For the similar destination sequence number,

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

2) 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.

5.2 Disjoint Paths

Two types of disjoint paths are considered: link disjoint and node disjoint. Link disjoint set of paths between a pair of nodes have no common links, whereas node-disjointness additionally precludes common intermediate nodes.

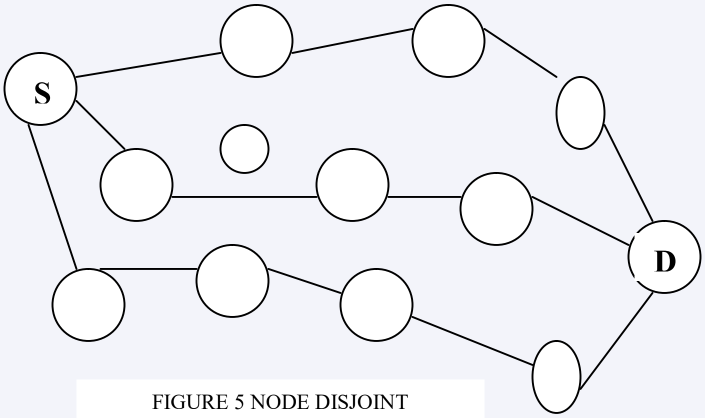

FIGURE 5 NODE DISJOINT

The following simple and straightforward observation is the basis of our mechanism to find link disjoint paths: If two paths from a node P to a destination D are link disjoint, then they must have unique next hops as well as unique last hops. Note that the converse of this observation is not necessarily true.

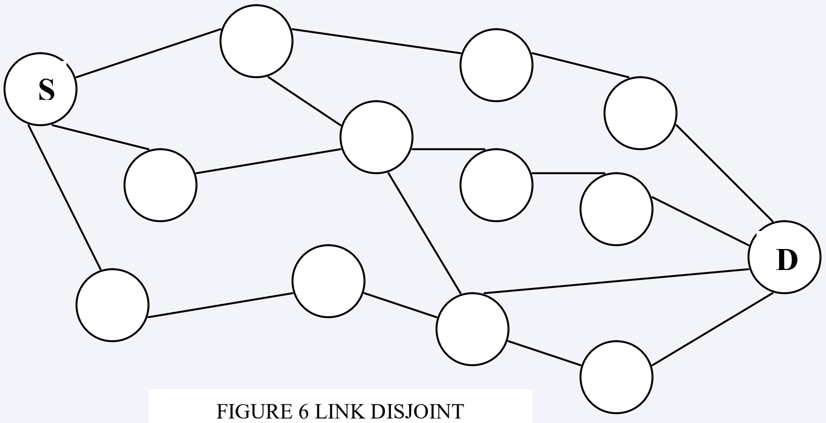

FIGURE 6 LINK DISJOINT

Though, the converse also holds true in general with an additional restriction: if every node on a path ensures that all paths to the destination from that node differ in their next and last hops.

VI. RELATED WORK

The first category is of those which modify specific well known routing protocols such as AODV, DSR and OLSR to avoid or detect black hole attack during route reply. The second category is of those which adopt an extra monitoring system such as a watchdog, confidant protocol or intrusion detection system. They propose a approach to black hole problem by using one more route to the intermediate node that replays RREQ messages to check whether the route from intermediate node to destination node exists or not. This method avoids the black hole problem and prevents the network from further malicious behavior but the routing overhead is greatly increased.

First, the sender node verify the authenticity of the node that initiates the RREP packet by utilizing the redundancy of the network. Second, each node store the last and received sent packet sequence number. If there is any mismatch then an ALARM indicates the existence of a black hole node. However, this approach unable to detect multiple black hole attack.
The watchdog identifies misbehaving nodes by listening promiscuously to the next node transmission whereas the path rater uses the knowledge from the watchdog to choose a path that is most likely to deliver packets. This technique is imperfect due to limited transmit power, collision and partial dropping.

The RREPs are 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.

VII. THE PROPOSED ENHANCED AOMDV ROUTING PROTOCOL

This approach uses AOMDV concept to form link disjoint multipath during path discovery. When a source node wishes to communicate with any specific destination node, it will send RRQP 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 few 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.
If a node whose legitimacy 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 BA-AOMDV. Thus, malicious nodes will be gradually avoided by other non-malicious nodes in the network.
The proposed BA-AOMDV has the following differences in message format and type, in comparison with AODV protocol.

7.1 RREQ PACKET

RREQ packet in BA-AOMDV has additional first hop field. This field is used to store the IP address of the first hop after it left the originator. The RREQs which has the same first_hop field value would not be processed by intermediate node.

TYPES	J	R	D	G	U	RESERVED	HOP COUNT
First_hop						RREQ ID	
Originator IP Address							
Originator sequence Number							
Destination IP Address							
Destination Sequence Number							

FIGURE 7 RREQ PACKET IN BA-AOMDV

7.2 RREP PACKET

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.

TYPES	R	A	RESERVED	PREFIX SIZE	HOP COUNT
SOURCE IP ADDRESS					
DESTINATION IP ADDRESS					
DESTINATION SEQUENCE NUMBER					
LIFETIME					
ORIGINATOR					

FIGURE 8 RREP PACKET IN BA-AOMDV

7.3 ROUTING TABLE

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.

DESTINATION SEQUENCE NUMBER
DESTINATION IP ADDRESS
FIRST_HOP
COUNT
HOP COUNT
NEXT HOP

FIGURE 9 ROUTING TABLE

7.4 LEGITIMACY TABLE

This table is used to select the most legitimate node (among the multiple backward disjoint link to source node and next hop to destination) while sending RREP back to source node. Legitimacy table includes three fields:

- Node ID
- Path count
- Sent count

Node ID: - this field stores the IP address of the node whose legitimacy is being recorded.

Path count field: - it specifies the number of times the node has been chosen in the route and

Sent count field: - it describes the number of times connection to destination have been successful node through the Node ID.

7.5 Process for Receiving RREQ in BA-AOMDV

In BA-AOMDV, each node uses three fields: source IP, sequence number and First_hop to determine whether an RREQ is duplicity or not whereas AODV uses only first two fields. For an intermediate node, if the hop count in the RREQ is larger than the hop count of the entry in the routing table which has the same sequence number and source IP, then RREQ is directly dropped. A node would create multiple entries (multiple link disjoint path) when the sequence number is same; hop count is smaller and the First_hop field value is different from the existing reverse entries. However, thedestination node replies to each RREQ in spite of the values in hop count and First_hop field of RREQ when the sequence number is equal or larger than the existing entry.

7.6 Process for Receiving RREP in BA-AOMDV

In spite of the number of RREQs received, the destination node will reply to each RREQ unless the sequence number of RREQ is not smaller than the existing sequence number in the routing entry. Intermediate nodes will reply to RREQ only when they have an entry to the destination node in the routing table. Node receiving an RREP from any of its neighbor will first check the legitimacy ratio of the neighbor node. If the legitimacy ratio crosses the lower threshold level than the node will drop the RREP, otherwise will forward it to the neighbor which has the highest legitimacy ratio among multiple backward entries and delete the other backward entries.

VIII. SIMULATION RESULTS AND PERFORMANCE ANALYSIS

8.1 Simulation Tool

The simulation is done with the help of NS-2 (v-2.34) network simulator. NS-2 provides faithful implementations of the different network protocols. The implementation of the protocol has been done using C++ language in the backend and tcl language in the front end on the Ubuntu Linux 11.04 operating system.

Whole simulation study is divided into two part one is create the node (that may be cell phone, internet or any other devices) i.e. NS-2 output. It's called NAM (Network Animator) file, which shows the nodes movement and communication occurs between various nodes in various conditions or to allow the users to visually appreciate the movement as well as the interactions of the mobile nodes.

8.2 Performance Evaluation Metrics

We choose the following parameter [24] to give an idea of behavior and reliability of the enhanced AOMDV protocol: 1 Route Formation Delay: It is the time taken to form a candid path from source to destination. 2 Packet Loss: This metric informs us about the amount of packets fails to reach its destination in a timely manner. 3 Nodes Speed: It is the speed of nodes moving in the network and we shall check the performance of BAAOMDV on different node speed. 4 Packet delivery ratio (PDR): The percentage of data packets delivered to destination with respect to the number of packets sent.

8.3 SIMULATION RESULTS

8.3.1 Performance Evaluation Metrics

We choose the following parameter [24] to give an idea of behavior and reliability of the enhanced AOMDV protocol: 1 Route Formation Delay: It is the time taken to form a candid path from source to destination. 2 Packet Loss: This metric informs us about the amount of packets fails to reach its destination in a timely manner. 3 Nodes Speed: It is the speed of nodes moving in the network and we shall check the performance of BAAOMDV on different node speed. 4 Packet delivery ratio (PDR): The percentage of data packets delivered to destination with respect to the number of packets sent.

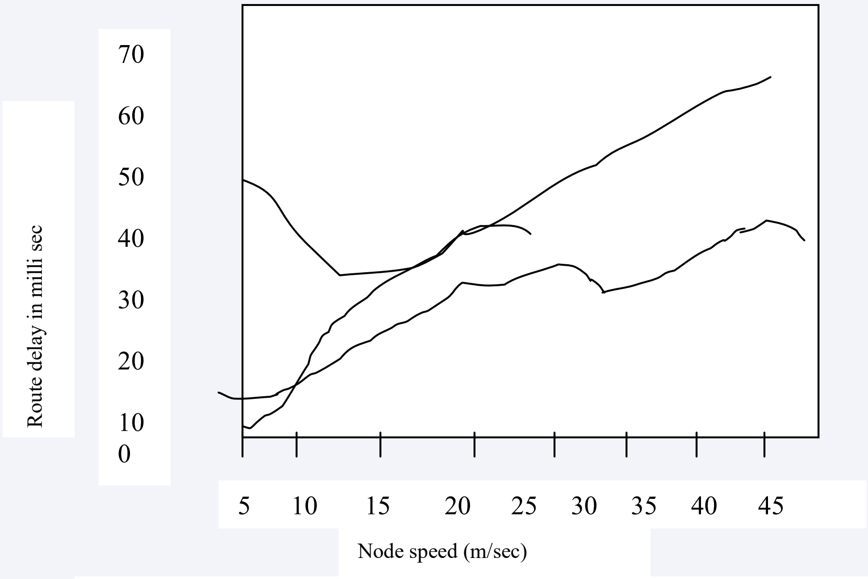

FIGURE 10 ROUTE FORMATION DELAY AGAINST NODE SPEED

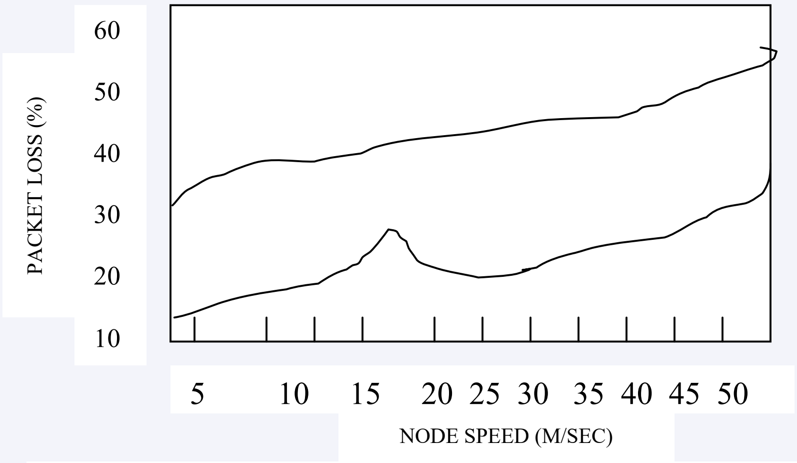

FIGURE 11 PACKET LOSS WITH VARIATION IN NODE SPEED

8.3.2 Packet Delivery Ratio

Packet Delivery Ratio is the ratio of the number of data packets received by the destination to the number of data packets sent by the source. The Fig. 16 shows that PDR of AODV is heavily affected by the malicious nodes whereas the PDR of proposed AOMDV are immune to it. According to our result, the proposed AODV is secure against black hole attacks.

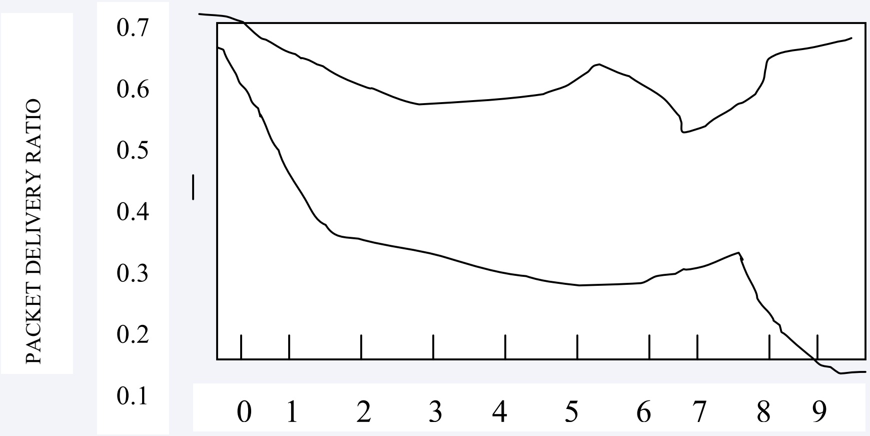

FIGURE 12 PACKET DELIVERY RATIO

IX. CONCLUSION AND FUTURE WORK

In this paper we analyzed the security system with our proposed AOMDV protocol. This approach is very simple and efficient for defending the AODV and AOMDV protocols against Black Hole attacks. This enhanced AOMDV protocol also does not require significant changes in the working of existing AOMDV protocol; however it uses an additional Legitimacy table for avoiding malicious node to grab the path between source and destination. Simulation results are showing that proposed protocol gives 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.

As future work, research work intend to develop simulations to analyze the performance of the proposed solution based on the various security parameters like mean delay time, packet overhead, memory usage, increasing number of malicious node, increasing number of nodes and scope of the black hole nodes and also focusing on resolving the problem of energy constraint related to mobile nodes against AODV.

REFERENCES

[1] Marina M.K, Das S.R, “Ad hoc on-demand multipath distance vector routing”, in Proceeding IEEE Wireless Communication and mobile computing, vol. 6, pp. 969-988, 2006.

[2] T. Clausen, P Jacquet, “Optimized Link State Routing Protocol (OLSR)”, IETF RFC 3626, October 2003.

[3] M-Y. Su, K L. Chiang and W.C. Lio, “Mitigation of black-hole nodes in mobile ad hoc networks”, Intl. Symposium on Parallel and Distributed Processing with Applications, pp.162-167, 2010.

[4] Charles E. Perkins, “Ad Hoc Networking”, Addison Welsey, Pearson education Jan 2001.

[5] Charles E. Perkins, P. Bhagwat, “Highly dynamic destination- sequenced distance-vector routing (DSDV) for mobile computers”, SIGCOMM (1994).

[6] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing", Proceedings of IEEE workshop on Mobile Computing Systems and Applications, pp. 90-100, 1999.

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

[8] David, Cerry and A. Ghioni, “Securing AODV: The A-SAODV Secure Routing Prototype”, IEEE Communications Magazine, February 2008.

[9] 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.

[10] M. A. Shurman, S. M Yoo and S. Park, “Black hole attack in wireless ad hoc networks”, In Proceedings of the ACM 42nd South east Conference (ACMSE’04), pp 96-97, Apr. 2004.

[11] M-Y Su, “WARPA Wormhole-avoidance routing protocol by anamoly detection in mobile ad hoc networks”, Computers & Security, Vol. 29 (2), pp. 216-219, 2010.