International Journal For Technological Research In Engineering
Volume 2, Issue 10, June-2015 *ISSN (Online): 2347 - 4718*

DETECTION AND ELIMINATION OF BLACK HOLE ATTACK IN MANET NETWORK

Mansi Gaur[1], Asst. Prof. Ms Sonia[2]
Dept of CSE, DPGITM, Gurgaon

Abstract: A mobile ad-hoc network (MANET) is an autonomous wireless system which consists of several mobile nodes to form an arbitrary and temporary network. As the lack of infrastructure network, when the nodes want to communicate with each other, they cooperate by forwarding data packets to other nodes in the network. So, the nodes use the routing protocols to find a path to the destination node. However, due to security vulnerabilities of the routing protocols, MANETs are facing various severe security attacks. Black hole is one of these attacks and can carry great damage to the network. As a result, an efficient and simple approach for defending the routing protocol against black hole attack is very important. This paper proposed a simple approach to detect black hole attack in MANET based on Ad Hoc On-Demand Distance Vector (AODV) routing protocol. The proposed system slightly modifies AODV protocol by adding two tables and packet type alarm. This method removes black hole node and chooses a reliable node by using these two tables. When the black hole node is detected, the system is automatically sending out the Alarm message to all neighbouring nodes.
Keywords: MANET, AODV, Black Hole, NS2, Alarm (detection of malicious node)

I. INTRODUCTION

Mobile Ad-Hoc Networks (MANETs) are the collection of mobile nodes that can communicate with each other via the radio waves without fixed infrastructure. The mobile nodes may be personal digital assistance (PDA), laptop, mobile phone and any devices that are mobile. The mobile device or node can easily join and leave to the network. They can form arbitrary topologies depending on their connectivity with each other in the network. They have the ability to configure themselves and they can be deployed urgently without the need of any infrastructure. When the nodes want to communicate with each other via a wireless channel, they provide the connectivity by forwarding packets over themselves. So, these nodes may be router or host or both at the same time. MANET have the basic characteristics such as open medium, self-organization, dynamic mobile nodes and topology, limited resources, lack of infrastructure network and lack of defence mechanisms. Because of these factors, MANET often suffers from various security attacks [2]. Moreover, the nodes in the MANET communicate with each other based on the mutual trust. This characteristic makes MANET more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANET more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication. Mobile nodes present within the range of wireless link can overhear and even participate in the network. As increasing threats of attack on the Mobile Networks, the security of transmission and communication in MANET is a challenging and vital issue. In order to provide secure communication and transmission in networks, the different types of attacks and their effects on the MANET is understanding. There are different kinds of attacks to harm MANET. They are wormhole attack, black hole attack, sybil attack, flooding attack, routing table overflow attack, denial of service (DoS), selfish node misbehaving, impersonation attack and so forth. A MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes. In the black hole attack, the malicious node sends the counterfeit reply that it has the freshest and shortest path to the destination node. Then, it absorbs all data packets to the destination. Hence, it disturbs the network and becomes data lost and affects the performance of network. In this paper, the defense mechanism is presented to identify and remove black hole attack and a feasible solution is proposed to find a safe route to the destination. The proposed method concentrates on the Ad Hoc On Demand Distance Vector (AODV) routing protocol that is widely used in MANET. It gives dynamic link conditions, low network utilization, low control message overhead, low memory overhead, and so on. However, the protocol was not considered security mechanisms to ensure that the packets have reached the destination [1]. There is no acknowledgement procedure in present and hence no delivery validation. Hence, it is defenseless various types of attacks. The proposed method slightly modifies the AODV protocol to detect and prevent black hole intruder.

II. RELATED WORK

There indeed have been numerous attempts published in the literature that aim at countering the black hole attacks. Some of the research papers are reviewed in this regard. The proposed architecture AODVR [3] has introduced several modules such as Packet Classifier, Extractor, Blacklist Tester, RREP sequence number Tester, Threshold Tester and ALARM broadcaster. As the packet arrives in the system, Packet Classifier classifies it to be RREQ, RREP secure, RERR, ALARM and HELLO packet. AODVR modifies the content and format of RREP and includes a new type of packet ALARM. Extractor extracts required contents of all types of packets other than HELLO. However, the procedure of formulating the threshold is a bit overwhelming, hence it results network delay. Formulations of correct threshold range keep black holes from intrude;

while a wrong formulation may restrict an authentic node thereby disgrace it to be a black hole. Lalit Himral et al. [5] have proposed a method to find the secured routes and prevent the black hole nodes in the MANET by checking whether there is large difference between the sequence number of source node or intermediate node who has sent back RREP or not. In AODV protocol, Destination Sequence Number is a 32-bit integer associated with every route and is used to decide the freshness of a particular route. The larger the sequence number, the fresher is the route. Generally the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely that node is the malicious node, immediately remove that entry from the RR-Table. The proposed method cannot find multiple black hole nodes. Nital Mistry et al. [4] modifies the original AODV routing protocol by using a new Cmg_RREP_Tab table, a MOS_WAIT_TIME timer and a field Mali_node. The RREP_WAIT_TIME is a time period during the source node sends first RREP packet until receive the RREP control messages. The MOS_WAIT_TIME is half the value of RREP_WAIT_TIME. The RREP packets are stored in the Cmg_RREP_Tab. The Mali_node is utilized to record the malicious node in the network. The source node analyzes all the stored RREPs from the Cmg_RREP_Tab table and discards the RREPs having a very high destination sequence number. Every node in the network maintains a table called Mali_node for storing the malicious node details to isolate the malicious node in the network. Comparing with original AODV routing protocol, this solution achieves a higher packet delivery ratio in the simulation results. However, it has high processing delay and the end-to-end delay is increased unavoidably. Kamarularifin Abd et.al. [6] have designed an ERDA solution to improve AODV protocol with minimum modification to the existing route discovery mechanism recvReply() function. There are three new elements introduced in modified recvReply() function namely: table rrep_table to store incoming RREP packet parameter mali_list to keep the detected malicious nodes identity and parameter rt_upd to control the process of updating the routing table. When RREQ packet is sent out by the source node S to find a fresh route to the destination node D. RREP packet received by node S will be captured into rrep_tab table. Since the malicious node M is the first node to response, the routing table of node S is updated with RREP information from node M Since the value of parameter rt_upd is "true", node S accepts the next RREP packet from other node to update the routing table although it arrives later and with a lower destination sequence number than the one in the routing table. The current route entry in routing table will be overwritten by the later RREP coming from other node. ERDA method offers a simple solution by eliminating the false route entry and replaced the entry with later RREP. However, it has high processing delay.

III. OVERVIEW OF AODV ROUTING PROTOCOL

The Ad Hoc on Demand Distance Vector (AODV) routing protocol [7] is intended for use by the mobile nodes for routing data in Ad Hoc networks. AODV is the most widely adopted and well known reactive routing protocol for MANET [9]. It is an extension of Destination Sequenced Distance Vector (DSDV) routing protocol [8] to improve the performance characteristics of DSDV in the creation and maintenance of routes. The routing of AODV is accomplished in two processes: route discovery and route maintenance.

A. Route Discovery Process

Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. A RREQ (Route Request) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route Reply) packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbours. If its routing table does contain an entry to the destination, then the next step is the comparison of the 'Destination Sequence' number in its routing table to that present in the RREQ packet. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREQ packet, then the node relays the request further to its neighbors. If the number in the routing table is higher than the number in the packet, it denotes that the route is a 'fresh route' and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route.

B. Route Maintenance Process

During the operation, if any node identifies a link failure it sends a RERR (Route Error) packet to all other nodes that uses this link for their communication to other nodes. The Hello message is periodically sent for maintaining the route information. AODV is a prominent on-demand reactive routing protocol for MANET. But in existing AODV, there is no security mechanism against the types of attack. Thus, a malicious node can carry out many attacks against AODV.

IV. BLACK HOLE ATTACK

Black hole attack is a kind of Denial of Service (DoS) attacks [10] in MANET. The black hole attack [11, 12] occurs when a malicious node advertise itself for having the shortest and best path to the destination node or forging route

reply message that is sent to the source node, with no effective route to the destination. This malicious node advertises its availability of fresh routes without checking its routing table. It is always used the highest sequence number value and the lowest hop count value. As an example, consider the following scenario in Figure 1. In this figure, node 'S' is the source node and 'D' is the destination node. When the source node 'S' wishes to transmit a data packet to the destination node 'D', it first broadcasts the RREQ packet with destination sequence number 10 to the neighboring nodes. So, the neighboring node 'C', 'E' and 'F' receive it. When the neighboring nodes check up with its routing tables, they send back RREP packet with their destination sequence numbers to the source node 'S'. The node 'S' receives the RREP from 'F' ahead of the RREP from 'C' and 'E'. When the source node 'S' compare its sequence number with the sequence number of 'F', the sequence number is high. So, the node 'S' assumes that the route through 'F' is the freshest route and sends any packet to the destination through it. This is a typical scenario of the AODV protocol packet exchanges.

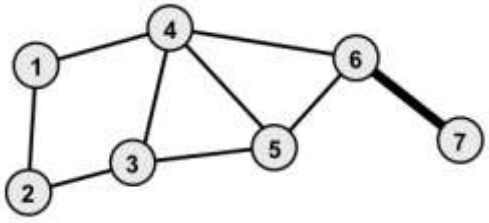

Figure 1. Packet Exchanges of AODV without Black Hole Attack

However, consider the scenario that the malicious node participates in this network in Figure 2. 'M' is assumed malicious node. When the source node 'S' wishes to transmit a data packet to the destination node 'D', it first broadcasts the RREQ packet to the neighboring nodes. So, the neighboring node 'C', 'E' and the malicious node 'M' receive it. Since the node M is a malicious node, it does not check up with its routing table for the requested route to node 'D'. Hence, it immediately sends back a RREP packet with highest sequence number, claiming a route to the destination. The node 'S' receives the RREP from 'M' ahead of the RREP from 'C' and 'E'. The node 'S' assumes that the route through 'M' is the freshest route and sends any packet to the destination through it. However, the node 'M' absorbs all the data and thus behaves like a 'Black hole'.

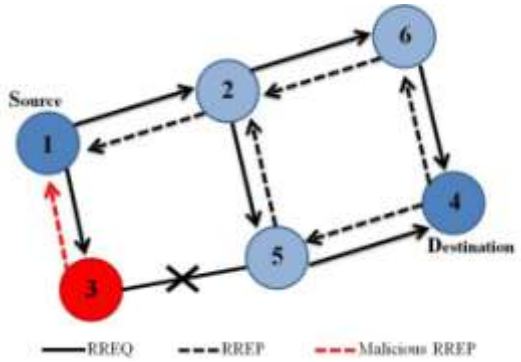

Figure 2. Packet Exchanges of AODV With Black Hole Attack

V. IMPLEMENTATION OF DETECTION AND PREVENTION MECHANISM

In this module, we have implemented a modified version of the AODV routing protocol (MAODV) to find a secure route between the source and destination node and isolate the malicious black hole nodes in MANETs. The mechanism of detection and prevention of black hole attack on the context of AODV protocol is developed by considering the working of AODV and behavior of black hole attack with intention of detecting black hole node and mitigating its effect on network.

A. Route Reply Record Table and Malicious Node Table

The proposed system tries to modify the process of source node by introducing two tables and alarm packet into existing AODV protocol. These tables are Route Reply (RREP) Record Table (RRT) and Malicious Node Table (MNT). The RRT table stores all RREP packets from the neighbor's node and the MNT table stores the information of malicious node. The examples of these two tables are shown in Table 1 and Table 2. The RRT table is stored only by the source node and the MNT table is stored by all nodes in the network.

Table 1. Route Reply (RREP) Record Table (RRT)

Time	Destination Node ID	Destination Node Seqno	Next Hop	Hop Count	Reply Source Address	Life time	Time stamp
5.203	C	100	M	1	M	9	20.4855
5.247	C	12	E	2	A	10	20.4855
5.301	C	10	D	3	B	9	20.4855
5.302	C	11	G	1	H	9	20.4855

Table 2. Malicious Node Table (MNT)

Node ID	Time
E	5.0143
M	10.6542
D	50.4968

B. Threshold Value Calculation

Threshold value is the average of difference between the destination sequence number from RRT table and the destination sequence number from routing table in each time interval (t) for destination. Threshold value is used to detect and eliminate the black hole node. β is control parameter and variable. The value of β is based on number of connection. β is used to avoid the authentic node disgrace to be a malicious node.

$$\text{Threshold} = \frac{\sum(\text{RREP}_{\text{Seqno }t} - \text{RT}_{\text{Seqno }t})}{\text{Total Number of Packets}} + \beta$$

C. Extension to Routing Table

The proposed system has implemented to yield a strong method for detecting black hole attack in MANETs. For the design of our scheme, the routing table field of AODV protocol is modified as follows. The reply initiator filed is added to the routing table. This field is stored the ID of node that the route reply send initially. When the malicious node is detected compared with the threshold value, we can find the malicious node ID by seeing this field. So, the fields of the routing table of our proposed protocol are as follows:

- Destination IP Address
- Destination Sequence Number
- Valid Destination Sequence Number flag
- Other state and routing flags
- Network Interface
- Hop Count
- Next Hop
- List of Precursors
- Lifetime
- Reply Initiator (extended field)

D. Alarm Packet

In the original AODV protocol, it uses four different types of packets to communicate among each other. They are

- Route Request (RREQ) Packet
- Route Reply (RREP) Packet
- Route Error (RERR) Packet and
- HELLO Packet Format.

The RREQ packet and RREP packet is used in the route discovery process when the nodes want to find the route to the destination. The RERR packet is used in route maintenance process in order to notify earlier nodes down the path of such a breakage when a link failure is detected along a route. The HELLO packet is used to detect and monitor links to neighbors. In the proposed system, the new ALARM packet is added to the packet types of AODV protocol. The ALARM packet is used to notify all neighboring nodes in the network about the malicious node when the black hole node is detected. The format of ALARM packet type is shown in Table 3.

Table 3. ALARM Message Format

Type	Reserved	Hop Count
Broadcast ID		
Malicious Node IP Address		
Originator IP Address		

E. Detection and Prevention Algorithm

The following terms are used to express the proposed algorithm.

- SN - Source Node
- IN - Intermediate Node
- MN - Malicious Node
- RT - Routing Table in AODV
- Seqno - Destination Sequence Number
- RREQ - Route Request Packet
- RREP - Route Reply Packet
- MNT - Malicious Node Table
- RRT - RREP Record Table

The proposed detection and prevention algorithm are as follows:

Begin
1. SN broadcasts RREQ to neighbours.
2. Store RREPs into RRT when SN receives RREP message from IN until the waiting time.
3. Retrieve the Seqno from RRT and calculate the Threshold value.
4. Detect and remove the malicious node from RRT.
while (RRT is not NULL)
if ((rep_seqno – rt_seqno) > Threshold) then
assume IN is MN
discard entry from RRT and store this IN as MN to MNT
send Alarm message
end
end
5. Select the reliable packet from the rest packets and continue the normal operation of AODV protocol.
6. Flush the RRT after completing step 4-5.
End

F. Working Principle of the Proposed System

When the source node wants to construct the route to the destination node, the source node starts broadcasting RREQ message to all neighbors. In the original AODV protocol, by default, the source node accepts the first fresh enough RREP message coming to it. Generally, the malicious node with high destination sequence number always sends the route reply ahead of other neighbour node to the source node during black hole attacks. As compared, in our approach, the source node keeps all the RREP from neighbour nodes in RRT until the waiting time. The waiting time is the time period that identifies by the source node after receiving the first RREP message. Then, the source node waits other RREP from neighbours till this time. We used 0.1 second as the value of waiting time. Then, the source node retrieve the destination sequence number from RRT table and routing table and calculate the Threshold value using the above equation. To detect the malicious node, we calculate the difference of destination sequence number from RRT and the destination sequence number from routing table. If the value of the difference is greater than the Threshold value, this intermediate node is assumed as the malicious node. The source node stores this malicious node ID in MNT and immediately removes that entry from the RRT. Then, the source node broadcasts ALARM message to all neighbouring nodes in the network to notify about this malicious node. Then, the source node chooses the reliable node from the resting node and continues the normal operation of AODV protocol. After choosing the reliable node and removing the malicious node, the RRT table must be clear all data.

VI. SIMULATION ENVIRONMENT

We have implemented the black hole attack in AODV protocol using NS-2.34 [13]. For our simulation, we use the IEEE 802.11 Mac at the physical and data link layer. The channel is Wireless Channel based on Two Ray Ground radio propagation model. AODV is used at the network layer as the routing protocol. Finally, UDP is used at the transport layer. The main traffic generator used in this simulation is the Constant Bit Rate (CBR). Each of these CBR applications uses 512-byte data packets at the rate of 2 packets per second. The overall simulation parameters are presented in Table 4. We have evaluated the performance of the AODV protocol and the proposed MAODV protocol with the black hole attack. The following performance metrics are used to analyze the performance of our solution.

Packet Delivery Ratio (PDR)

The packet delivery ratio is defined as the ratio of the total number of data packets received by the destinations over the total number of data packets transmitted by the sources. PDR shows how successful a protocol performs delivering packets from source to destination. Higher value means the better the results [14]. It measures the loss rate as seen by transport protocols and as such, it characteristics both the correctness and efficiency of ad hoc routing protocols. It represents the maximum throughput that the network can achieve. A high packet delivery ratio is desired in a network. As the calculation,

Routing Overhead

The routing overhead means that the number of routing packets transmitted for every data packet sent. Each hop of the routing packet is treated as a packet. Normalized routing load are used as the ratio of routing packets to the data packets.

End-to-End Delay

The end-to-end delay is the average delay between the sending of the data packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays at the MAC layer, etc that is the total amount of delays encountered in the whole network at every hop going to its destination. It is measured in milliseconds.

Table 4. Simulation Parameters

Parameter	**Value**
Simulator	NS-2.34
Area	600m x 600m
Routing Protocol	AODV, BlackholeAODV, MAODV
Simulation time	200s
Application Traffic	CBR
Number of Nodes	50-200
Malicious Node	1-4
Pause time	2s
Packet Size	512 bytes
Transmission rate	2 packets/s
Mobility speed	10 m/s
No of Connections	40
Movement Model	Random Waypoint

A. Performance Analysis on Variation of Malicious Node

We have created a network by using simulation parameters shown in Table 4. Fig. 3 illustrates the effect of the malicious nodes on the packet delivery ratio in MANET. The numbers of malicious nodes in the network are used randomly from one to four. It can be seen that AODV heavily suffers from the black hole attack. Therefore, its packet delivery ratio decreases when the number of malicious node increases in the network as shown in Fig. 3. On the other hand, the experimental results show that the PDR of MAODV protocol is above 95% even though the malicious node is increased. MAODV has higher average packet delivery than AODV. This is due to the fact that the proposed protocol can prevent the black hole attack that occurs in the network.

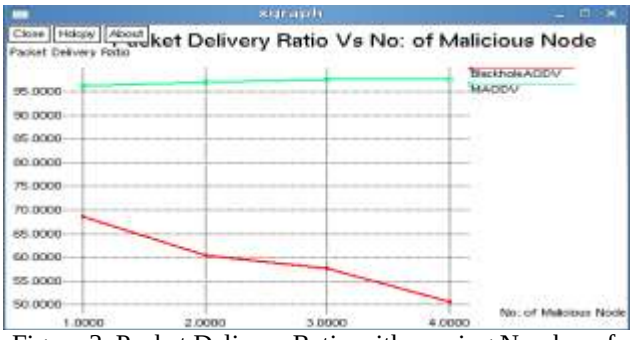

Figure 3. Packet Delivery Ratio with varying Number of Malicious Nodes

B. Performance Analysis on Variation of Node

Fig. 4 to Fig. 6 shows the results of attack when network size (number of nodes) is varying. As the number of nodes in the network increases, the PDR of AODV decreases due to increase in the number of intermediate nodes on a route. This is because the increase in number of intermediate nodes on an active route increases the probability of route failure. The PDR of AODV with attack decrease even more due to the probability that the malicious node become an intermediate node on an active route. On the other hand, the PDR of MAODV is greater than AODV with attack because our detection approach is able to identify and eliminate the malicious node which greatly increases the network PDR.

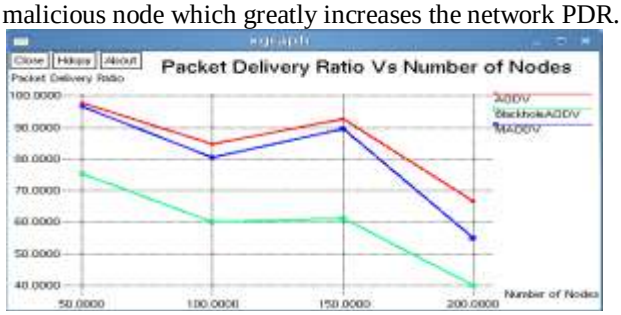

Figure 4. Packet Delivery Ratio with varying Number of Nodes

The effect of the number of nodes on the routing overhead ratio is depicted in Fig.7. The routing overhead ratio for all protocols increases as the number of nodes in the network increases. The routing overhead of the AODV under attack is greater than the normal AODV and MAODV protocol since the presence of the black hole nodes. The overhead of MAODV is the same as the normal AODV except 200 node scenario. This is the proposed protocol generate any additional requests for finding secure routes. The impact of the number of nodes on end-to-end delay is depicted in Fig. 8. It can be observed that the delay for the MAODV protocol increases at 100 node scenario since it has to avoid the malicious node when it tries to find out secure route from source to destination.

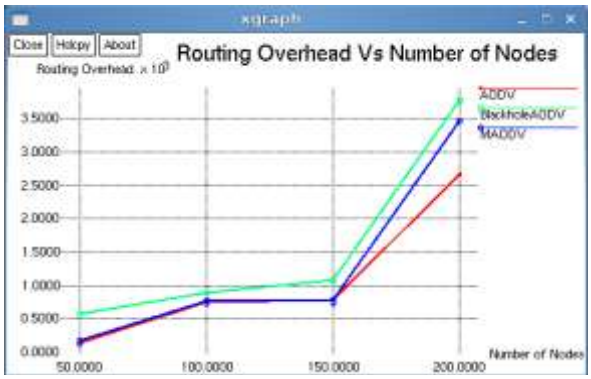

Figure 5. Routing Overhead with varying Number of Nodes

Figure 6. Average End-to-End Delay with varying Number of Nodes

VII. CONCLUSION AND FUTURE WORK

In this paper, a simple approach for defending the AODV protocol against Black Hole attack is proposed. The proposed solution can be applied to identify and remove black hole node and to discover a secured route form source to destination in the MANET. In this system, the process of source node in AODV protocol is modified by introducing two tables. These tables are Route Reply (RREP) Record Table (RRT) to store RREP from neighbour's nodes and Malicious Node Table (MNT) to store the information about the malicious nodes. The black hole node can be removed and the reliable node can be chosen by using these tables. The new ALARM packet type is also proposed to inform the intruder node to all neighbouring nodes when the black hole node is detected. To evaluate the applicability of this routing algorithm, we simulated different scenarios using AODV protocol and proposed protocol and also simulated the same scenarios after introducing the black bole node into the network. We considered the performance metrics packet delivery ratio, routing overhead and average end-to-end delay on the scenarios with number of malicious nodes and number of nodes as variable parameters. Having simulated the black hole attack in AODV protocol, it can be seen that the packet loss is increased in the ad-hoc network. This also shows that black bole attack affects the overall network connectivity and the data loss can show the existence of the black hole node in the network. If the number of black hole nodes is increased then the data loss would also be expected to increase. Simulation results show that the proposed scheme has a better result in terms of packet delivery ratio and routing overhead on different scenario over different parameters. There is an increase in the average end-to-end delay in the proposed protocol as compared to AODV protocol because the proposed protocol takes more time to detect and eliminate the malicious node.

REFERENCES

[1] Ramaswami, S. S. and Upadhyaya, S., "Smart Handling of Colluding Black Hole Attacks in MANETs and Wireless Sensor Networks using Multipath Routing", Proceedings of the 2006 IEEE Workshop on Information Assurance, (2006).

[2] Luo, J., Fan, M. and Ye, D., "Black Hole Attack Prevention Based on Authentication Mechanism", IEEE, (2008).

[3] Mohammad Abu Obaida, Shahnewaz Ahmed Faisal, Md. Abu Horaira, Tanay Kumar Roy, "AODV Robust (AODVR): An Analytic Approach to Shield Ad-hoc Networks from Black Holes", International Journal of Advanced Computer Sciences and Applications, vol. 2, issue 8, 2011, pp. 97-102.

[4] Mistry, N., Jinwala, D. C. and Zaveri, M., "Improving AODV Protocol against Black Hole Attacks", International Multi Conference of Engineers and Computer Scientists, 2 (2010).

[5] Himral, L., Vig, V. and Chand, N., "Preventing AODV Routing Protocol from Black Hole Attack", International Journal of Engineering Science and Technology, 3(5) (2011).

[6] Jalil, K. A., Ahmad, Z. and Manan, J. A., "Mitigation of Black Hole Attacks for AODV Routing Protocol", Society of Digital Information and Wireless Communications, 1(2) (2011).

[7] Perkins, C. E., Royer, E. B. and Das, S., "Ad-Hoc on Demand Distance Vector (AODV) Routing", IETF RFC 3561, (2003).

