# Improved AODV Protocol to Detect and Avoid Black Hole Nodes in MANETs

Muneer Bani Yassein, Yaser Khamayseh, Bahaa Nawafleh
Department of Computer Science
Jordan University of Science and Technology
22110, Irbid, Jordan
Email: {masadeh, yaser}@just.edu.jo, nawafleh_bahaa@yahoo.com

***Abstract*— Security in Mobile Ad Hoc Networks (MANETs) is difficult to achieve because of the different attacks that might occur in the network, such as black hole attacks. In black hole attacks, the malicious node tries to attract most of the network traffic by advertising it has the best routing paths to the destination nodes, once the traffic is received by the black hole node, it simply drops the packets. This paper proposes an enhancement to Ad hoc On-Demand Distance Vector (AODV) routing protocol by employing effective policies to detect and avoid black hole nodes. The performance of the proposed scheme is evaluated using simulation. The obtained performance results indicate that the proposed AODV protocol achieves a significant improvement over both MI-AODV and the original AODV protocols, in terms of packet delivery ratio, dropped packets ratio, and overhead.**

***Keywords*- Black Hole; Routing Protocol; Mobile Ad hoc Networks; Wireless Network; AODV.**

## I. INTRODUCTION

A wireless ad hoc network is a network using different airwaves (such as radio waves) to connect a collection of infrastructureless nodes; it differs from wired network which uses physical connection. Due to the open nature of wireless links, wireless links face many challenges, such as security, routing, and scheduling [3][6][12][14]. A Mobile Ad Hoc Network (MANET) is a group of mobile devices that are connected through wireless links. These nodes collaborate together in order to achieve different network functionalities. Moreover, it uses a point to point transmission and each node works as a host and as a router [1][3]. Each node in the network may be sender, receiver, or intermediate node that provides contact of the other nodes, and these networks do not have any infrastructure such as Base Stations. MANETs are vulnerable to attacks and threats [4][9]. The process of transmitting data between the source and the destination nodes through the path is called routing. The determination of the best path depends on many measurements such as paths cost, and number of hops.

Routing involves two sub processes, namely, (i), determining the best routing paths from the source to the destination, and (ii), transferring the data packets using the discovered path. Security in MANETs is difficult to achieve because of different attacks that might occur in the network (e.g., black hole attacks). In black hole attacks, the malicious node tries to attract as much as possible of the network traffic by advertising the best routing paths to the destination nodes, once the traffic is received by the black hole node, it drops the data. For example, in the widely used Ad hoc On-Demand Distance Vector (AODV) [4] routing protocol in a network infected with black hole nodes, when a source node sends data packets into a destination, the black hole advertises that it has the best path to the destination node whenever it receives any Route Request (RREQ) control packet. Then, it sends the response, Route Reply (RREP) to the source node. RREP messages could arrive from a normal node or a black hole node. If the reply arrives from a normal node, the protocol works as intended. If the first replay arrives from a black hole node, the source will transmit the data through the path that contains the black hole node. Once the data is received by a black hole node, it drops the data.

The probability of black hole node replies first to the RREQ message increases if the black hole is physically closer to the destination. Moreover, the probability of a false RREP message from a black hole arriving first to the source is higher than a normal safe reply as a black hole nodes response immediately to RREQ messages without the need for waiting a responding from the destination or checking the Routing Table (RT) as in the case of normal nodes.

According to the AODV specification, once a source receives a RREP message, this makes the routing discovery process completed, and thus, it ignores all other reply messages from other nodes, and it begins sending the data packets using the received path. This work aims at improving the AODV protocol in order to detect and avoid black hole nodes to improve data packet delivery ratio, to provide secure routing, and to increase the network performance.

The rest of this paper is organized as the following: Section II presents some of the related work in the area. Section III presents the proposed scheme. Section IV presents the simulation environment and the obtained results. The paper is concluded in Section V.

## II. RELATED WORK

Different mechanisms were proposed to solve the black hole node problem. Most of researches conducted in this area can be divided into three categories: securing existing protocols, developing new secure protocols, and intrusion detection techniques. The following is a sneak review of some of the works that attempt to solve the black hole problem [8][16][17][18][20][21][22][23][25][24].

Sangi et al. [20] analyzed the performance degradation for AODV protocol, especially if the byzantine attacks are generated in a combination. In their analysis, they used

GloMoSim simulator. The authors concluded that the effects of byzantine and black hole are devastating when they are compared to a single black hole attack. In the routing protocol, route rushing or wormhole attacker maximizes the probability of malicious nodes. Also, a limited number of malicious nodes may generate wormhole attack with a combination between black/gray hole attack in which it may affect the activities of the network more than the rushing with black/gray hole attack.

Medadian et al. [21] proposed a new scheme to prevent the black hole attacks based on the discussion between neighbor nodes in the network that will participate in the communication between the source and the destination nodes. The proposed scheme provides a higher security and better performance in delivering packets than the traditional AODV. The proposed scheme restricts each node with a number of rules to identify if they are not attacker; the node activities within the network determine if it is honest or not, in order to be a participant in the transmission process, the node must proves its honesty. Firstly, every node in the network is allowed to be a participant of the transmission process between the source and destination nodes, so each node has enough time to prove its truth. Min and Jiliu [22] addressed the security issues included in the routing process in MANET networks, in addition to detecting multiple black holes that act in groups in the networks, it proposed two authentication approaches using hash functions: firstly, the Message Authentication Code (MAC), and secondly, the Pseudo Random Function (PRF). Based on these two approaches, it can be fast to verify the message and to identify the group, making it possible to determine multiple black holes that work and cooperate together, also to find the safe routing path while avoiding attack from black hole groups.

Zhang et al. [23] proposed a new approach for detecting black holes based on the process of checking a sequence number assigned to the Route Reply message based on the use of a new message generated by the destination of the route.

The proposed scheme is used to deal with malicious attacks and with the problems resulted from traditional methods, rather than using a public key as in the traditional methods in which this may result in extra problems, such as key distribution, instead, in this scheme, an intermediate node in the network unicast a message along with a defined control message to the destination to ask for up to date serial number. Khamayseh et al. [8] proposed the protocol MI-AODV to detect black hole nodes in a network. This mechanism modifies the original AODV protocol to enable the nodes of detecting black hole nodes in the network.

## III. Proposed Protocol

The security issue in MANETs is essential and even more challenging because of multiple senders, multiple receivers, and the usage of wireless links for transmitting the data. Thus, MANETs are more likely to be affected by attacks, such as the black hole attack. In general, MANET attacks can be classified into two types; external (outside) and internal (inside) attacks. The external attacks are caused by nodes that do not belong to the domain of the network, while the internal attacks are caused by the nodes which are part of the network itself.

Furthermore, a black hole attack is a type of denial of service attack where a malicious node can attract data packets by falsely advertise a fresh route to the destination and retain them without forwarding them to the destination. This work proposes a mechanism for preventing the black hole attack by modifying the operations of the AODV routing protocol. The proposed mechanism aims at detecting and avoiding black hole nodes in MANET to reduce its impact. The proposed mechanism utilizes the following observations:

- The necessity to monitor the RREP messages and to observe its history. In this work, we propose to insert a new field in the RREP message to store the address of the last node that has a path to the destination.
- The necessity to observe the behavior of other nodes. Create new two tables in each node: suspect and black list tables.
- Suspect table contains the addresses of intermediate nodes which have sent RREP message; it also includes the number of times a node failed to send data through this node. For each node *i*, the suspect table contains a list of all nodes in the network that node *i* have received a RREP message and for node *i* the number of failures. A RREP message is considered failed if it was not able to deliver the data to the destination using the specified path. If the node doses not receive an acknowledgment message it considered the data is lost and restart the routing process again to retransmit the data.
- Black list table contains a list of nodes with failed RREP message that exceeded a certain threshold.

  If node *i* receives a RREP message from node j, with invalid path, it adds node *j* to the suspect table. Once the number of failures for a particular node exceeds a certain threshold, this node is moved to the black list table and any coming RREP messages from this node will be ignored.

- Add acknowledgment message of length one bit. The message is set to 1 if the packets are delivered to the destination node; otherwise, it is set to 0. The acknowledgment message will be forwarded to the source node to acknowledge the recipient of the send data.

Moreover, the source sends a RREQ message in a standard manner as in the original ADOV protocol. In this scenario, the source node *S* sends RREQ to the destination *D* through intermediate nodes. When a RREP message is received from intermediate nodes, the following steps are performed:

- Transmit the data packets through the path received in the first route replay message. In Figure 1, the first RREP message arrives to the source node through intermediate nodes I3, I5. Figure 1 shows the first RREP arrived to the source node.

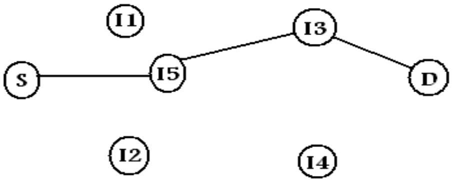

Figure 1. First RREP arrived to the source node.

- The source node waits for an acknowledgement to arrive. If the acknowledgement arrives, then the path is safe.
- If the acknowledgement does not arrive, the address of the last node that has a path to the destination node is stored in the suspect table, and retransmit the data using the second received path; go to steps (a, b).
- The nodes will exchange their suspect tables, in case of a common node is found in the exchanged lists, and the node is already in the suspect table, then it is moved to the black list table.
- Once a node is added to the black list table, RREP messages from this node are ignored.

Figure 2 depicts the procedures of the proposed algorithm that to solve a black hole problem in a consistent and sequential manner.

```
ST: Suspect Table (ST)
BLT:  Black List Table (BLT)
--------------------------------------------------------------------------------
Step 1: A RREQ packet is broadcasted by node i, wait a RREP then
send data packet, and wait an Ack packet from destination
    While (no Acknowledgement is received)
        Increment the suspect probability for node i
        If ($P_{i,j}$ >= $P_{suspect}$)
            Insert replying address in suspect table
            Resend data to other RREP

Step 2: Broadcast ST
Step 3: While (received ST is not empty)
              if( $P_{i,j}$ >= $P_{black\ hole}$)
                            Move node j from ST to BLT
              otherwise
                            Rebroadcast Received ST
Step 4: Broadcast BLT
Step 5: While (received BLT is not empty)
                            Insert in this BLT
                            Broadcast this BLT
```

Figure 2. Proposed AODV Protocol Algorithm.

## IV. Simulation and Analysis of Results

In this study, we use GloMoSim simulator [26] to evaluate the performance of three deferent protocols: proposed protocol, original AODV protocol, and MI-AODV protocol.

In order to evaluate the performance of the proposed scheme, different experiments with different number of nodes, namely, 15, 20, 25, 30, and 35 nodes, were conducted. The nodes placed randomly and move according to the random waypoint model with a speed of (0 – 20 m/s) over a square terrain area of 1000*1000 meters. Each run lasts for 800 seconds. The radio propagation range is 250 meters, and the bandwidth is 2 Mb/s. In the application layer, the Constant Bit Rate (CBR) traffic generator is used as a model of data resources in the simulations and the size of each data packet is 512 byte. In the MAC layer (i.e., Data Link Layer), we used the IEEE 802.11 communication protocol. Table 1 shows the simulation parameters for the different scenarios.

TABLE I. SIMULATION PARAMETERS

| Parameter | Value |
|---|---|
| Simulator | GloMoSim 2.03 |
| Simulation time | 800 second |
| Simulation area | 1000m × 1000m |
| Number of nodes | 15, 20, 25, 30, and 35, |
| Mobility model | Random waypoint |
| Minimum speed | 0 meter/second |
| Maximum speed | 20 meter/second |
| Pause time | 0 , |
| MAC protocol | IEEE 802.11 |
| Data packet size | 512 byte |
| Radio range | 250m |
| Bandwidth | 2 Mb/s |

The simulation evaluates the performance of the original AODV, MI-AODV and the proposed versions of AODV with the presence of 1, 2, 6 black hole nodes for each protocol. Each experiment was repeated 10 times with different random seeds to change the random simulator parameters; the average of the obtained 10 values is computed. The margin of error for each average at 95% confidence is computed. Four performance metrics were used in this study to evaluate and compare the proposed AODV to the MI-AODV and the original one. These metrics are: packet delivery ratio, dropped packets ratio, overhead, and end-to-end delay.

### A. *Results and Analysis*

In this section, we provide analysis of the results obtained from the simulation experiment that we performed to compare the performance of the three protocols in the presence of the black hole nodes. Throughout the paper, the green line with the triangular markers represents the original

AODV protocol, the red line with the square markers represents the MI-AODV protocol, and the blue line with the trapezoidal markers represents the proposed protocol.

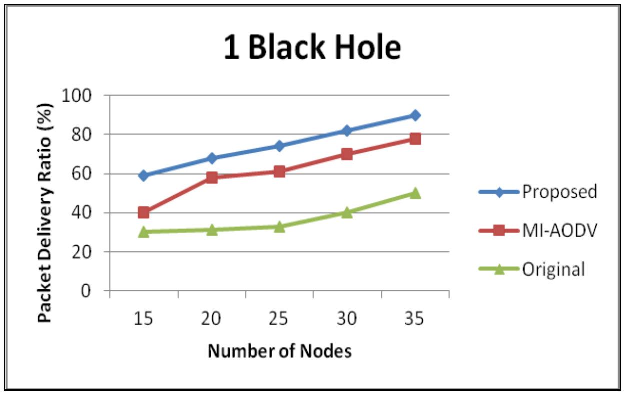

Figure 3. Delivery ratio, 1 Black hole, Pause 0.

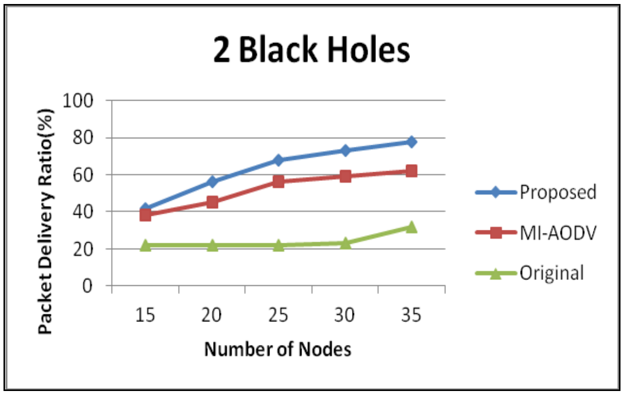

Figure 4. Delivery ratio, 2 Black holes, Pause 0.

Figure 3 shows the improvement of packets delivery ratio in the proposed AODV protocol compared to MI-AODV and original AODV protocols when the network is attacked by one black hole. Figure 4 shows the improvement of packets delivery ratio as the network is being attacked by two black hole nodes. As shown in Figures 3 and 4, the proposed AODV protocol improves the delivery ratio by 50.9% in case of 1 black hole and by 57.8% in case of 2 black holes; the MI-AODV protocol improves the delivery ratio by 38.4% in case of 1 black hole and by 48.5 in case of 2 black holes, compared to the original AODV protocol for a network attacked by one and two black hole.

Figures 3 and 4 show the results of a network attacked by one and two black holes, the packets delivery ratio for the cases of 15 to 35 nodes increases as the number of nodes increases. Within this interval, as the number of nodes decreases the effect of black hole increases, because a black hole has the chance to obtain more RREQ messages from all RREQ messages sent in the network; therefore, it drops more packets. This is the reason behind the decreasing packets delivery ratio for all protocols when the number of nodes decreases.

The packets delivery ratio increases as the number of nodes increases from 15 to 35 nodes for the original AODV, the MI-AODV, and the proposed AODV protocols. As the number of nodes increases within this interval a black hole has the chance to subscribe in more communications; however, the source node surrounded by more neighbor nodes therefore it has a greater chance to receive routes from other normal and reliable nodes.

Figures 5 and 6 show the ratio of dropped packets results for the three protocols for a network attacked by one and two black hole. The proposed AODV protocol improves the dropped packets ratio by 61.5% and 57.8% for the cases of 1 and 2 black holes respectively compared to the original AODV protocol. The MI-AODV protocol improves the dropped packets ratio by 39.7% and 48.5% for the cases of 1 and 2 black holes respectively compared to the original AODV protocol.

The proposed AODV protocol reduces the ratio of dropped packets compared to the MI-AODV and the original AODV protocols for a network attacked by one black hole. As shown in Figure 5, the ratio of dropped packets increases as the number of nodes decreases for the cases of 15 to 35 nodes. As number of nodes decreases within this interval, the black hole has the chance to drop high ratio of sent packets. This is the reason behind the increasing ratio of dropped packets.

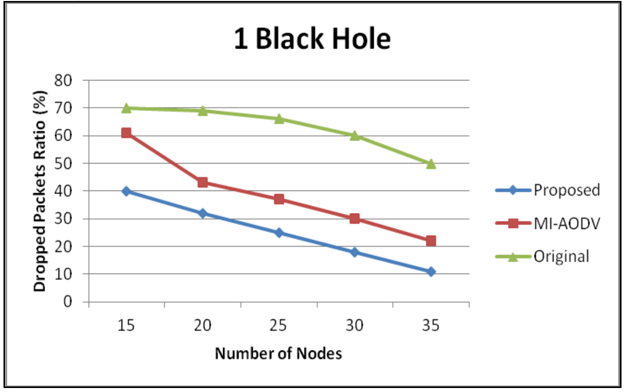

Figure 5. Dropped packets ratio, 1 Black holes, Pause 0.

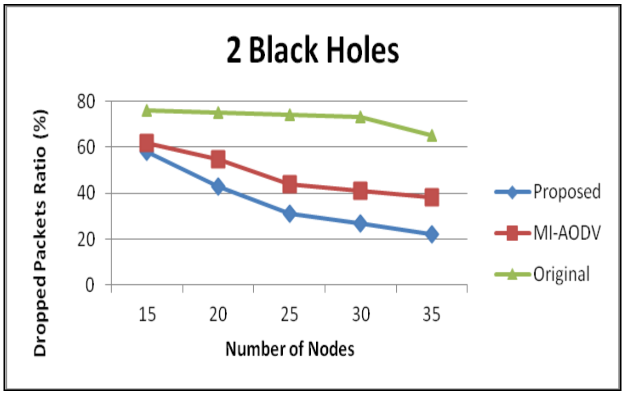

Figure 6. Dropped packets ratio, 2 Black holes.

When the number of nodes increases the source node becomes surrounded by more neighbors and has a high chance to receive more alternative routes to the desired destination and the effect of black hole nodes decreases. There is an observable agreement between the results of dropped packets ratio and delivery packets ratio for a network attacked by one and two black hole nodes. The obtained results for end-to-end delay show that the delay time is very close for the cases of 15 to 20 nodes because of the decreased number of nodes. This leads to increasing the chance of destination node to be neighbor to the source node. The original AODV protocol shows the best delay result compare to the proposed protocol by 24.3% and MI-AODV protocol by 11.6% for the case of one black hole.

Figure 7 depicts the results for delay times. The results indicate that by increasing the number of nodes, the delay increases for all protocols. Moreover, the original AODV achieves the lowest delay, while the proposed scheme achieves the highest delay; the increase in delay for the proposed scheme is due to the extra processing and resend of packets over the second discovered path to the destination. Therefore, the packet deliver ratio achieved by the proposed scheme is higher than the other 2 schemes.

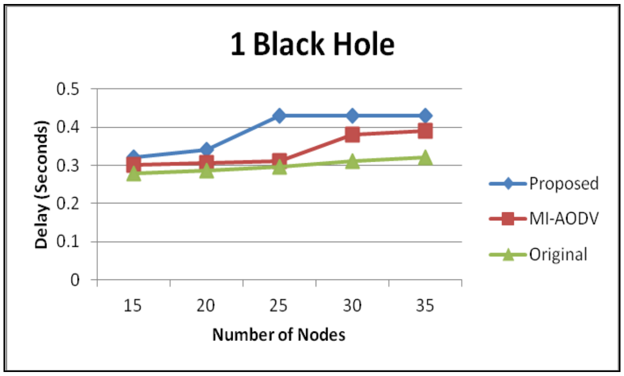

Figure 7. Delay, 1 Black hole.

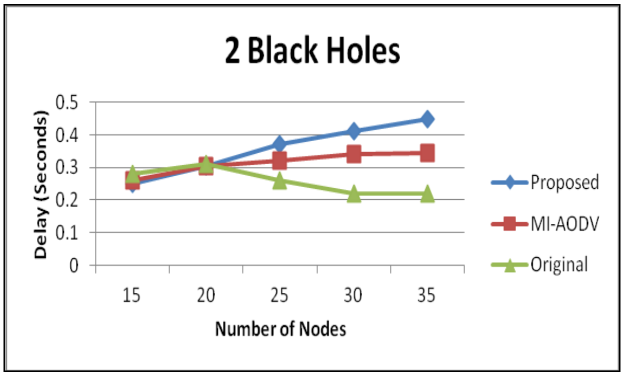

Figure 8. Delay, 2 Black hole.

In Figure 8, the network is attacked by two black holes and the delay time results are depicted. Similar behavior is depicted as in the case of 1 black hole except for the case of 15 to 20 nodes, in which the proposed scheme achieved the best results. For the case of 35 nodes, the original AODV protocol outperforms the proposed protocol by 18.3% and the MI-AODV protocol by 13.2%. Figures 9 and 10 depict the overhead results for the 3 protocols for the cases of 1 and 2 black holes, respectively. As shown in Figures 9 and 10, the proposed AODV protocol improves the additional overhead by 15.7% for the case of 1 black hole, and 15.1% for the case of 2 black holes, and the MI-AODV protocol improves the overhead by 6.9% for the case of 1 black hole, and 10.7% for the case of 2 black holes. The overhead reported by the original protocol is higher than the overhead reported by the other 2 protocols, while the proposed protocol achieved the lowest overhead.

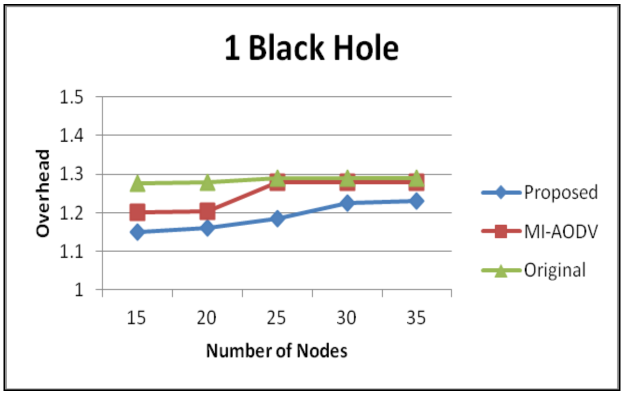

Figure 9. Overhead, 1 Black holes, Pause 0.

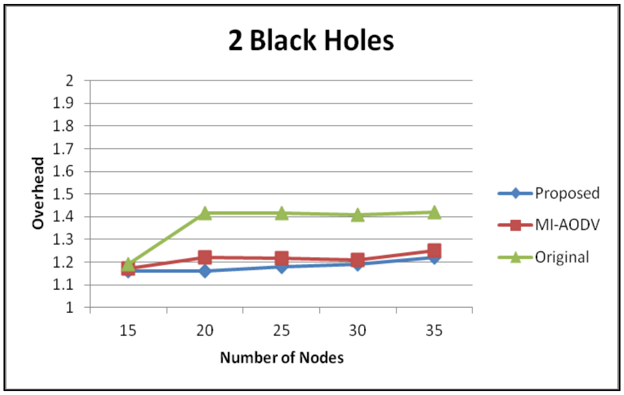

Figure 10. Overhead, 2 Black hole, Pause 0.

## V. Conclusion and Future Work

The main focus of this research is security issue in MANETs because it is essential and even more challenging as it has multiple senders, multiple receivers, and the usage of wireless links for transmitting data. Black hole problem is type of denial of service attack where a malicious node can attract data packets by falsely advertise a fresh route to the destination and retain them without forwarding them to the destination. The proposed AODV protocol modify the behavior of the original AODV to send the data packets safely, and it aims at detecting and avoiding black hole nodes in MANET to reduce the impacts of black hole nodes.

This is due to the fast response of the black hole in the original scheme to the RREQs. This leads to increase the number RREQ and RREP control messages in the network. The transmission data processes by both MI-AODV and proposed protocols needs more time than the original AODV protocol, thus, the number of the control packets in MI-AODV and proposed AODV protocols is less than the number of control packets in the original AODV protocol.

Each node has suspect and black list tables to hold the addresses of the suspicions nodes, Suspect table contains the addresses of intermediate nodes which have sent RREP message, it also includes the number of times a node failed to send data through this node, and black list table contains a list of nodes with failed RREP message that exceeded a certain threshold. RREP is overloaded with an extra field to store address of the last node reply has a path to the destination. We added a new acknowledgment message to acknowledge the recipient of the send data from the source to the destination nodes. The obtained simulation results shown that the proposed AODV protocol comprehend the ill effects of the black hole attack and outperforms both the MI-AODV, and original AODV protocols in terms of packet delivery ratio, dropped packets ratio, and overhead.

The protocol does not consider the behavior of two black hole nodes that cooperate together and work as a team. The next step is to support the protocol with a certain technique to solve the problem for more than one black hole cooperate together, and support it with a certain mechanism to deal with spoofing and reply acknowledgment from black hole.

## REFERENCES

[1] R. Rangara, R. Jaipuria, G. Yenugwar, and P. Jawandhiya, “Intelligent Secure Routing Model for MANET”. Proceedings of Computer Science and Information Technology (ICCSIT), IEEE, vol. 3, pp. 452 - 456, 2010.

[2] J. Sen, S. Koilakonda, and A. Ukil, “A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks”, Proceedings of Intelligent Systems, Modelling and Simulation (ISMS), IEEE, pp. 338 - 343, 2011.

[3] P. Tsou, J. Chang, Y. Lin, H. Chao, and J. Chen, “Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs”, Proceedings of Advanced Communication Technology (ICACT), IEEE, pp. 755 – 760, 2011.

[4] M. Medadian, A. Mebadi, and E. Shahri, “Combat with Black Hole Attack in AODV Routing Protocol”, Proceedings of First Asian Himalayas, IEEE, pp. 530 - 535, 2009.

[5] S. Lu, L. Li, K. Lam, and L. Jia, “SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack”, Proceedings of Computational Intelligence and Security, vol. 2, pp. 421 - 425, 2009.

[6] S. Umang, B. Reddy, and M Hoda, “Enhanced intrusion detection system for malicious node detection in ad hoc routing protocols using minimal energy consumption”, In ITE journal, vol. 4, 2010, pp. 2084 - 2094.

[7] S. Kannan, T. Maragatham, S. Karthik, and V. Arunachalam, “A Study of attacks, Attack Detection and Prevention Methods in Proactive and Reactive Routing Protocols”, In Medwell journal, vol. 5, 2011, pp. 178-183.

[8] Y. Khamayseh, A. Bader, W. Mardini, and Muneer BaniYasein, “A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks”, In International Journal of Communication Networks and Information Security (IJCNIS), vol. 3, 2011, pp. 36-47.

[9] N. Bhalaji and A. Shanmugam, “A Trust Based Model to Mitigate Black Hole Attacks in DSR Based Manet”, In European Journal of Scientific Research, vol. 50 no. 1, 2011, pp. 6-15.

[10] A. Sangi, J. Liu, L. Zou, “A Performance Analysis of AODV Routing Protocol under Combined Byzantine Attacks in MANETs”, Proceedings of Computational Intelligence and Software Engineering CiSE , IEEE, pp. 1 - 5, 2009.

[11] D. Mishra, Y. Jain, S. Agrawal, “Behavior Analysis of Malicious Node in the Different Routing Algorithms in Mobile Ad Hoc Network (MANET)”, Proceedings of Advances in Computing, Control, & Telecommunication Technologies, pp. 621-623, 2009.

[12] T. Manikandan and K. Sathyasheela, “Detection Of Malicious Nodes in MANETs”, Proceedings of Communication Control and Computing Technologies (ICCCCT), IEEE, pp. 788 - 793, 2010.

[13] W. Gong, Z. You, D. Chen, X. Zhao, M. Gu, and K. Lam, “Trust Based Malicious Nodes Detection in MANET“, Proceedings of E-Business and Information System Security, IEEE, pp. 1 - 4, 2009.

[14] N. Bhalaji and A. Shanmugam, “Association Between Nodes to Combat Blackhole Attack in DSR Based MANET”, Proceeding of Wireless and Optical Communications Networks, pp. 1-5, 2009.

[15] L. Tamilselvan and V. Sankaranarayanan, “Prevention of Blackhole Attack in MANET”, Proceeding of Wireless Broadband and Ultra Wideband Communications, IEEE, pp. 21, 2007.

[16] A. Saini and H. Kumar, “Effect Of Black Hole Attack On AODV Routing Protocol In MANET”, In International Journal of Computer Science and Technology, vol. 1, 2010, pp. 1 – 4,.

[17] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke, and J. T¨olle, “A Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs”, Proceeding of Local Computer Networks, IEEE, pp. 1043 - 1052, 2007.

[18] G. Mamatha and S. Sharma, “A New Combination Approach To Secure MANETS Against Attacks”, In International Journal of Wireless & Mobile Networks (IJWMN), vol. 2, 2010, pp.1-10.

[19] R. Das, B. Purkayastha, and P. Das, “Security Measures for Black Hole Attack in MANET: An Approach”, In International Journal of Engineering Science and Technology, vol. 3, 2011, pp. 2832- 2838.

[20] A. Sangi, J. Liu, and L. Zou, "A Performance Analysis of AODV Routing protocol under Combined Byzantine Attacks in MANETs" , International Conference on Computational Intelligence and Software Engineering,CiSE 2009, pp. 1-5, 2009.

[21] M. Medadian, M. Yektaie, and A. Rahmani "Combat with Black Hole Attack in AODV routing protocol in MANET", AH-ICI 2009. First Asian Himalayas International Conference on, pp. 3-5 Nov. 2009.

[22] Z. Min and Z. Jiliu, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks", In Proceedings of the 2009 International Symposium on Information Engineering and Electronic Commerce. IEEE Computer Society, Washington, DC, USA, pp. 26-30, 2009.

[23] X. Zhang,Y. Sekiya, and Y, Wakahara, "Proposal of a Method to Detect BlackHole Attackin MANET", Autonomous Decentralized Systems, International Symposium on, pp. 23-25 March 2009

[24] S. Marti, T. Giuli, K. Lai, and M. Bake, “Mitigating Routing Misbehavior”. In Proceedings of Mobile Ad hoc networks 6th MobiCom, BA Massachuestts; pp. 10-18, 2000.

[25] N. Mistry, D. Jinwala, and M. Zaveri, "Improving AODV Protocol against Blackhole Attacks", proceedings of the International Multi Conference of Engineers and Computer Scientists, vol. 2, 2010.

[26] X. Zeng, R. Bagrodia, M. Gerla, "GloMoSim: a library for parallel simulation of large-scale wireless networks," Parallel and Distributed Simulation, 1998. PADS 98. Proceedings. Twelfth Workshop on , pp. 154-161, May 199

ISBN: 978-1-61208-339-1