Modified AODV Routing Protocol to Improve Security and Performance against Black Hole Attack

Houda Moudni, Mohamed Er-rouidi
Faculty of Sciences and Technology
Sultan Moulay Slimane University
Beni Mellal, Morocco
{h.moudni, m.errouidi}@usms.ma

Hicham Mouncif, Benachir El Hadadi
Faculty Polydisciplinary
Sultan Moulay Slimane University
Beni Mellal, Morocco
{hmouncif, benachirelhadadi}@yahoo.fr

***Abstract*— A Mobile Ad hoc NETwork (MANET) is a collection of autonomous nodes that have the ability to communicate with each other without having fixed infrastructure or centralized access point such as a base station. This kind of networks is very susceptible to adversary's malicious attacks, due to the dynamic changes of the network topology, trusting the nodes to each other, lack of fixed substructure for the analysis of nodes behaviors and constrained resources. One of these attacks is black hole attack. In this attack, malicious nodes inject fault routing information to the network and lead all data packets toward themselves, then destroy them all. In this paper, we propose a solution, which enhances the security of the Ad-hoc On-demand Distance Vector (AODV) routing protocol to encounter the black hole attacks. Our solution avoids the black hole and the multiple black hole attacks. The simulation results using the Network Simulator NS2 shows that our protocol provides better security and better performance in terms of the packet delivery ratio than the AODV routing protocol in the presence of one or multiple black hole attacks with marginal rise in average end-to-end delay and normalized routing overhead.**

Keywords—Mobile Ad Hoc networks; AODV routing protocol; security; Black hole attack.

I. INTRODUCTION

A Mobile Ad Hoc network is a self-configuring network that is formed automatically by a collection of mobile nodes without any fixed infrastructure. These wireless devices communicate with each other directly if they are in the same radio communication range. If they are out of the radio range, the communication will require the cooperation of other nodes. Consequently, each mobile node must operate not only as a host but also as a router. Due to these characteristics they are used in many critical applications such as disaster relief, emergency operations, vehicular computing, situational information in the battlefield, mobile offices and many more.

In MANETs, one of the most challenging tasks is the security. According to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, and constrained capability, MANETs become susceptible to the security attacks. Hence, various attacks [1-3] of different layers may affect the network.

One of the most famous attacks in MANETs is the Black Hole attack [4], which can be easily launched on reactive routing protocols like AODV [5] or Dynamic Source Routing (DSR) [6]. In this attack, a malicious node can attract all data packets by falsely claiming a fresh route or shortest route to the destination, without having any active route to the specified destination, and then absorbs them without forwarding it to the destination node.

The aim of this paper is to overcome the black hole attack. Therefore, we propose a new approach to eliminate one or multiple black hole nodes on AODV routing protocol. In our approach, the intermediate node forwards the valid route reply to the next node. The invalid routes replies are avoided by intermediate nodes in the overall network.

The rest of this article is organized as follows: In Section 2, the previous works for black hole attack in reactive routing protocols are discussed. The basic concepts and preliminaries including AODV routing protocol and black hole attack are provided in Sections 3 and 4, respectively. The proposed method is given in Section 5. In section 6, we discuss the methodology of evaluating our solution and the metrics used to compare our proposed solution to the AODV routing protocol. Section 7 discusses the experimental data and analysis using the NS2 network simulator, and conclusions are given in Section 8.

II. RELATED STUDIES

Mobile Ad Hoc network is threatened by a lot of security attacks such as denial of service attack, modification, IP spoofing, fabrication attack, etc. As a result, a lot of research has been done in this area [7–12].

The black hole attack has a serious impact on reactive routing protocols. Therefore, in this section, we only present the contributions done in the field of the black hole attacks in the AODV routing protocol.

Many of researches have been conducted to design methods and intrusion detection systems to identify the black hole attack [13–17]. However, here we are interested in methods that used to mitigate the black hole attack.

In [18], the authors were proposed an approach to detect black hole nodes in the MANET. In the proposed method, the detecting node calculates the ratio of the number of packets dropped to total number of packets forwarded successfully. This ratio is checked with a predefined threshold value to detect any malicious behavior. If any misbehavior is found, the

978-1-4673-7689-1/16/$31.00 ©2016 IEEE

detecting node tries to avoid the misbehaving node. In [19], a scheme for the routing protocol AODV is proposed to detect and remove Gray Hole and Black Hole Attacks. In this scheme, the intermediate node detects the malicious node sending false routing information by calculating a PEAK value, where the PEAK value is the maximum possible value of the sequence number that any RREP can have in the current state. Then, when this intermediate node receives a RREP having sequence number higher than the calculated PEAK value; it is marked as DO_NOT_CONSIDER. The authors in [20] proposed a scheme (so-called DCBA) to identify and mitigate black hole/collaborative black hole attacks in MANETs. In their proposed method, each node has its own suspicious value, which is based on the abnormal difference observed between the routing messages transmitted from the node. Furthermore, when the source node receives the route reply (RREP) packet in reply to the route request (RREQ) packet, they verify the suspicious value of the node that initialized the RREP packet. As a verification, if this value is higher than the threshold level, then the node is considered as malicious and its address is stored in a blacklist table, preventing that node to further participate in the routing process. The proposed method in [21] project a novel automatic security mechanism using Support Vector Machine (SVM) to defend against malicious attack occurring in AODV. This method uses three metrics PDER (Packet Delivery Ratio), PMOR (Packet Modification Rate) and PMISR(Packet Misroute Rate), to decide the behavior of a node. The information required by the metrics is collected from all the nodes in the network. These metrics are compared to a threshold, according to which the node is considered malicious or not. The authors in [22] propose a defense mechanism against a cooperative black hole attack in a MANET that relies on AODV routing protocol named as SSP-AODV Protocol. They have incorporated two techniques: A* search algorithm and Floyd-Warshall's algorithm in the AODV routing process. And they have used the value of hop count and the estimate time as input in this two algorithm to decide the shortest secure path. A modified algorithm to improve security and performance of the AODV protocol against black hole attack was proposed in [23]. In this algorithm, the authors used a number of new rules to identify the destructive nodes according to node's behaviors in an Ad Hoc network and delete them from routing. The authors in [24], present a method called Code Division Security Method (CDSM) in order to prevent Black hole attack in MANETs. They consider an additional field of one byte in the packet header to represent the node's code. The approach of Route Reply caching mechanism is used in [25] to overcome the problem of black hole attack. In their approach, they count the RREP received by the source node and then the source chooses the suitable path by ignoring the first RREP.

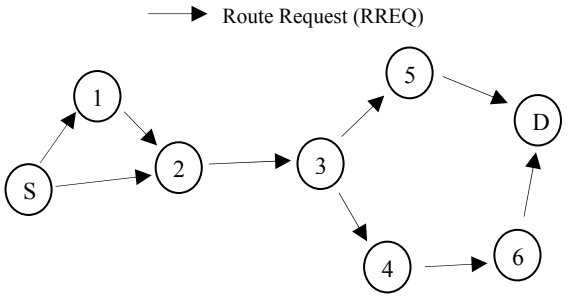
Our proposed technique differs from the techniques cited above in that it focuses on forwarding only the valid route reply to the next node, even in the case of one or more black hole attacks, by sending twice the same packet reply with the difference of plus one in the sequence number to determine whether the second packet corresponds to the first.

III. AD HOC ON DEMAND DISTANCE VECTOR (AODV)

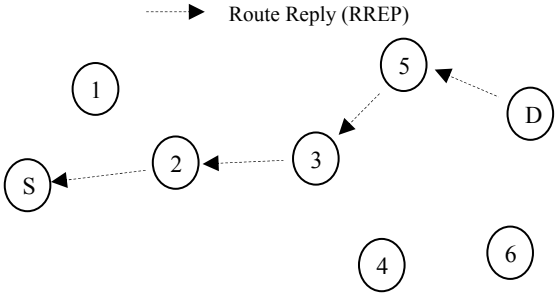
The Ad Hoc On-Demand Distance Vector (AODV) [5] routing protocol is based on the Destination-Sequenced Distance-Vector (DSDV) [26] and DSR [6] algorithm. It is a reactive protocol, since the routes were discovered at the time when a source node needs to send data packets to a destination node for which it has no cached route.

AODV has two main functionalities: (1) Route Discovery (see Fig. 1) and (2) Route Maintenance (see Fig. 2). The basic approach of this protocol during the route discovery phase is to establish a route by broadcasting Route REQuest (RREQ) packets in the network. When the neighboring node receives the request packet, first it checks if it is the destination node for that packet and if so, the node sends back an RREP (Route REPly) packet. If it is not the destination node, then it checks in its routing table to determine if it has a fresh enough routing to the destination node. If not, it relays the RREQ packet by flooding it to its neighbors. Moreover, if it has a route to the destination, it can send the RREP back to the source node by reversing the route information stored in the RREQ packet.

In the route maintenance phase, if a node detects a broken link, it sends a Route ERRor (RERR) message to the source node informing it that the link is broken. Then the source node either tries an alternate path available or initiates the route discovery process again. A link is broken when any intermediate node that involves in the packet forwarding process moves out of the transmission range of its upstream neighbor.



(a) Network Flooding of RREQ Packet



(b) Unicasting of RREP Packet

Fig. 1. Route discovery process of AODV

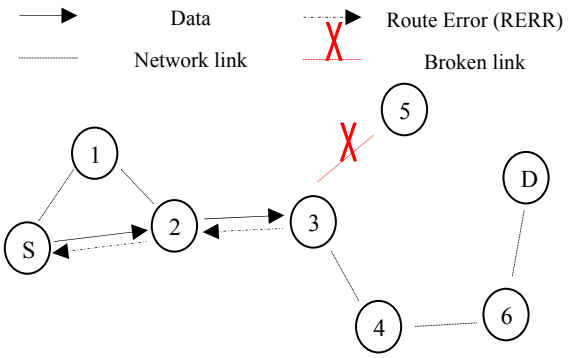


Fig. 2. Route maintenance process of AODV

IV. BLACK HOLE ATTACK

The black hole attack concerns the network layer of MANET. This kind of attack deletes all the data packets instead of sending them and consequently it makes the result of packet delivery ratio really low. The black hole attack can be divided into two groups: single black hole attack and cooperative black hole attack; it depends on the aims of the attacker. In the first kind of black hole attack, the attack is applied via one of the existing nodes in the network, and in the other kind, the malicious nodes act in coordination with other attackers.

During the Route Discovery process, the source node broadcasts the RREQ message to its neighboring nodes to find a fresh path to the intended destination. The black hole node immediately responds the source node with a RREP without checking its routing table for a fresh route to the destination packet. This packet reply includes the highest sequence number and is perceived as if it is coming from the destination node or from an intermediate node which has a fresh enough route to the destination node. The source node assumes that the process of the route discovery is done and discards the other RREP packets coming from other nodes, then selects the path through the malicious node to route the data packets. Therefore, the source node starts to send its data packets to the black hole node trusting that these packets will reach the destination node. The attacker now can drop the received data instead of relaying them as the protocol requires. The process of the black hole attack is schematized in Fig. 3.

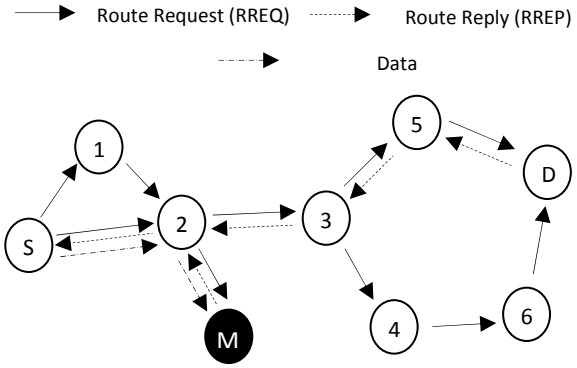


Fig. 3. Black hole attack in AODV

V. PROPOSED SOLUTION

In this section, we will describe in details our proposed solution to prevent the black hole attack that we have integrated in the AODV routing protocol. Therefore, we slightly modify the recvReply(Packet *p), recvRequest(Packet *p) procedures and the Route Reply (RREP) message as shown in the Fig. 4. Table 1 illustrates the fields of RREP message.

According to the original AODV routing protocol, the source node has to broadcast the RREQ packet to find a path to reach the destination node. The destination node, or any intermediate node having the path, can send back the reply to the source node. Then, by default, the source node accepts the first fresh enough RREP packet coming to it. In our approach, like the standard AODV routing protocol, the destination node or intermediate node generates the RREP packet, but it also generates another RREP packet. It is a kind of confirmation of the first packet with a sequence number incremented by one. Therefore, we have two RREP messages from the destination node or an intermediate node that has the route to the destination; one with the normal sequence number and the

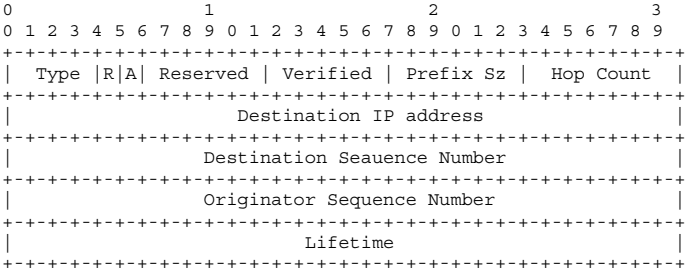


Fig. 4. Format of the modified Route Reply (RREP) Message

TABLE I. FIELDS OF RREP MESSAGE

Type	Forced to 2.
R	Repair flag; used for multicast.
A	Acknowledgment required.
Reserved	Sent as 0; ignored on reception.
Verified	One bit specifies the packet Route Reply if it is valid or not as illustrated below: 0 refer to the invalid RREP 1 refer to the valid RREP
Prefix Sz	If nonzero, the 5-bit Prefix Size specifies that the indicated next hop may be used for any nodes with the same routing prefix (as defined by the Prefix Size) as the requested destination.
Hop Count	The number of hops from the Originator IP Address to the Destination IP Address. For multicast route requests this indicates the number of hops to the multicast tree member sending the RREP.
Destination IP address	The IP address of the destination for which a route is supplied.
Destination Sequence Number	The destination sequence number associated to the route.
Originator Sequence Number	The IP address of the node which originated the RREQ for which the route is supplied.
Lifetime	The time in milliseconds for which nodes receiving the RREP consider the route to be valid.

other with the normal sequence number + 1, and both have the field VERIFIED set to 0. When the intermediate node receives the RREP packet it stores the information about the packet reply, then it checks our appended field VERIFIED if it is set to 0 or 1. If it is 0, that means that our packet is not yet verified or it is an invalid packet. Otherwise the packet is verified and valid and it must be forwarded to the next node. In case of the field VERIFIED is 0 and the intermediate node receives a second route reply message, it must verify if the first route reply's sequence number is the second reply's sequence number minus one; if the verification is true, it sets the field VERIFIED to 1 and forward the packet. Also, when the intermediate node receives another route reply from the malicious node which performs black hole attack with a very high destination sequence number. The same procedure explained will be repeated; and in this case the verification will be false, therefore, the intermediate node leaves the field VERIFIED set to 0 and ignores the packet.

Our solution avoids the black hole attack and also a multiple black hole attack. In addition, the control messages from the malicious node, are not forwarded in the network.

Our approach based on the four steps detailed below:

Step 1: (Initialization Process)
Start the route discovery phase with the source node S.

Step 2: (Generation of RREPs)
The destination node or the intermediate node generates two route reply with two different destination sequence number, the second one must be incremented by one.

```
sendReply( seqno,    // Dest Sequence Num
           VERIFIED = 0, );     // Appended field
sendReply( seqno+1,    // Dest Sequence Num
           VERIFIED = 0, );     // Appended field
```

Step 3: (Verification of RREPs)

```
if ( intermediate node receives RREP ){
      if ( the first time the node receives RREP ){
            Store the IP address and seqno of the node;
            if ( RREP is valid){
                  Forward RREP; }
      } else if (the node receives more than one RREP ){
            Store the IP address and seqno of the node;
            if ( RREP is invalid){
                  if ( new RREP's seqno == old RREP's seqno + 1){
                        VERIFIED = 1;    //( Mark RREP as valid)
                        Forward RREP;
                  } else {
                        Ignore RREP; }
            } else {
                  Forward RREP; }
      }
}
```

Step 4: (Continue default process)

The source node sends data to the destination node from the selected route reply packet.

VI. METHODOLOGY OF EVALUATION

A. Simulation Environment

The simulations are done using NS-2 (v-2.35) network simulator [27] to analyze the performance of our proposed solution against black hole nodes. In an area of 500x500 m, 25 nodes are randomly distributed, they execute once the standard AODV and another time the M-AODV (Modified AODV) routing protocol for comparing the two protocols under the black hole attack. For the malicious nodes are also randomly distributed. Five pairs were randomly chosen for data communication, each sending 512 bytes per second. All nodes were moved in a Random-way point model, with random speeds ranging between 0 and 30m/s. In addition, the pause time of nodes is 10s. The simulation parameters are summarized in table 2. Therefore, each data point represents an average of twenty runs.

B. Metrics used for Simulation

In order to evaluate the performance of our approach, we have used the following metrics:

1) Packet Delivery Ratio (PDR): It is the ratio of the total number of data packets received by the destination nodes and the total number of data packets generated by the source nodes. Hence, the packet delivery ratio shows the total number of the data packets that reach destination successfully. Higher packet delivery ratio shows higher protocol performance.

2) Average End-to-End Delay: It can be defined as the time elapsed between the moment of sending of a bit by the source node and the moment of its reception by the destination node. it includes all possible delays taken by router to seek the path in the network such as buffering during route discovery latency, queuing at the interface queue, propagation, re-transmission delays at the MAC and transfer times. The average end to end delay is measured in milliseconds.

3) Normalized Routing Overhead: This metric denotes the number of routing control packets generated per data packets transmitted. It is called Normalized Routing Overhead or Normalized Routing Load.

TABLE II. SIMULATION PARAMETERS

Parameter	Value
Coverage Area	500x500 m
Number of nodes	25
Simulation time	200s
Transmission range	50m
Mobility model	Random way point
Data Rate	0.25
Packet Size	512 Bytes
Routing Protocol	AODV / Modified-AODV
Mobility speed	0-30 m/s
No of black hole nodes	1 and 5
Connections	5
Traffic type	UDP–CBR
Pause time	10s

VII. Simulation results and analysis

A. Packet Delivery Ratio

The Fig. 5 and the Fig. 6 show the packet delivery ratio of AODV, our solution and AODV under one black hole node and under five black hole attackers when node mobility increases. It is clear from the figures that the performance of our approach is superior over AODV under black hole attack either for one or multiple attackers. The PDR of AODV under one attack was approximately 15%, while the PDR of Modified AODV in the presence of one attack was approximately 60%, increased by 45%. Similarly the PDR of AODV under multiple attacks was approximately 7%, which was increased by 43% when compared to our scheme also under multiple attacks. Moreover, the PDR of AODV routing protocol without any attacks is around 64%, which is due to congestion in the network.

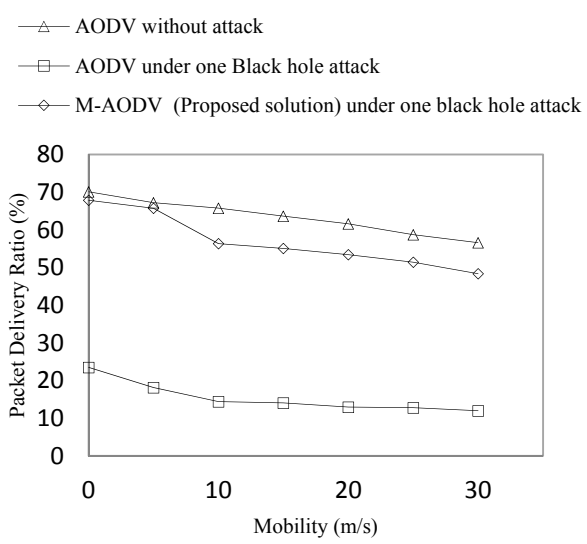


Fig. 5. Packet delivery ratio vs. mobility with one attacker

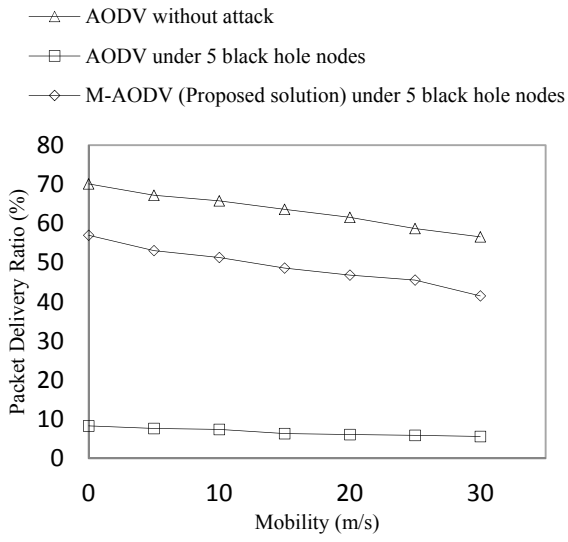


Fig. 6. Packet delivery ratio vs. mobility with five attackers

B. Average End-to-End Delay

From the Fig. 7 and Fig. 8, it can be observed that, when the Modified AODV protocol is used, there is an increase in the average end-to-end delay, compared to the standard AODV routing protocol without attack. Also, we observe that our approach under one attack is slightly increased in the average end-to-end delay, compared to under multiple attackers. This is due to the additional waiting time in each intermediate node before sending the reply, and when there is a multiple attack our approach need more time to calculate the right route reply than when one attack exists. The end to end delay in the presence of attackers in the AODV is the fewer in the two cases, either in the presence of one black hole node or in the presence of multiple attackers. This is because the immediate reply from the malicious node, which doesn't check its routing table for the route availability.

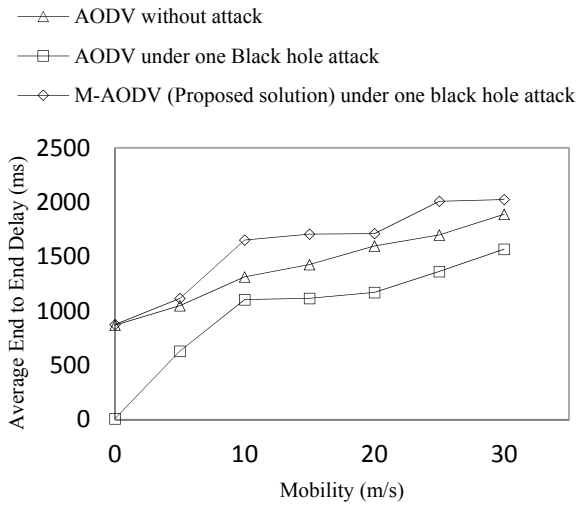


Fig. 7. Average end to end delay Vs. mobility with one attacker

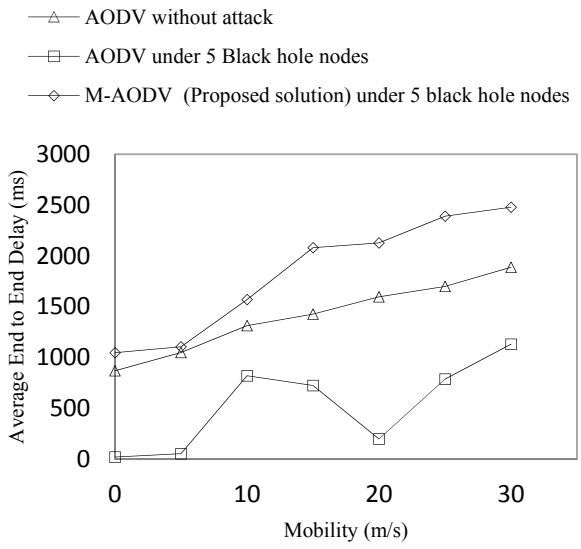


Fig. 8. Average end to end delay vs. mobility with five attackers

C. Normalized Routing Overhead

The normalized routing overhead is shown in Fig. 9 and Fig. 10 while varying the mobility. In our modified AODV, the routing overhead under one or multiple malicious nodes is slightly higher compared to the standard AODV because of the additional process involved to avoid the selection of malicious nodes. The normalized routing overhead for AODV under black hole attack, whether one or multiple attacks is very high compared to the AODV without attack. This is due to the black hole nodes that send false replies to the route request packets which compromise the routing protocol then the protocol starts misbehaving and generating additional routing packets.

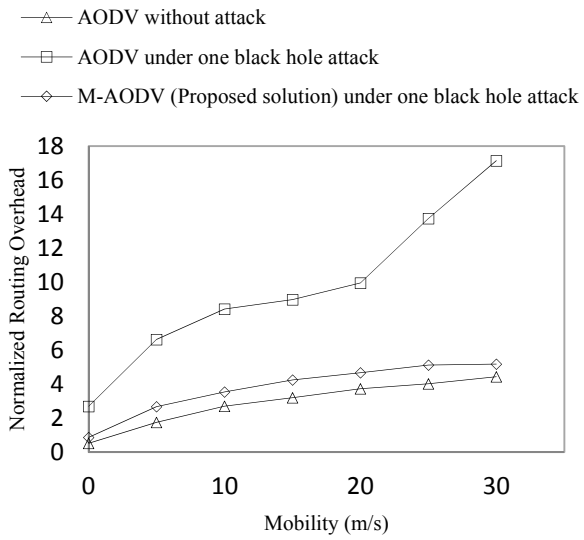


Fig. 9. NRL vs. mobility with one attacker

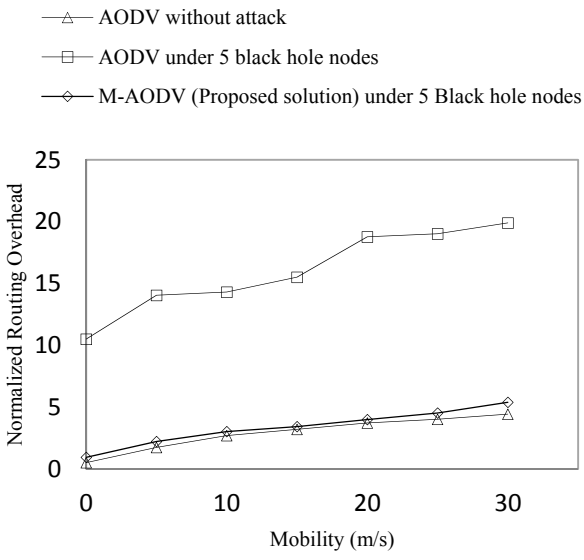


Fig. 10. NRL vs. mobility with five attackers

D. Evaluation of the Number of the Dropped Packets by the Black Hole Attack in AODV and M-AODV

We have calculated the rate of the number of packets sent, dropped and received in both cases with one black hole attack and five attackers in the standard AODV routing protocol and also in our modified AODV, as shown in Fig. 11 and Fig. 12. In this simulation, 25 nodes are moving randomly with maximum speed at 10 m/s, 10s for pause time, the number of connections is 5 and the number of packets flowing through the network is 2849 packets. From the simulation, we definitely assert that our proposed scheme overcame the black hole attack when there is a single black hole attack and even when there are multiple attackers. For the difference between sent packets and the sum of the packets dropped and received packet is due to the packets dropped in case of collision or buffering or other reasons.

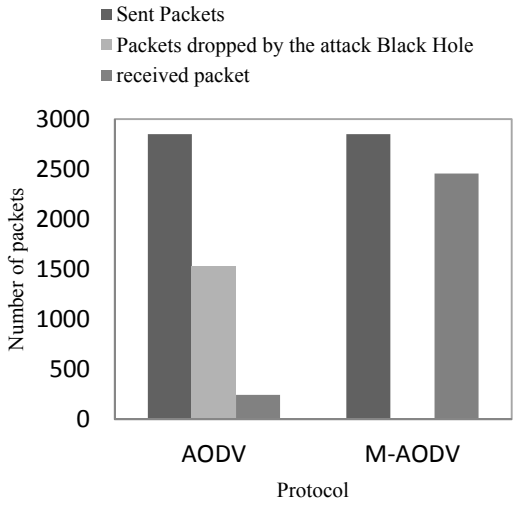


Fig. 11. Number of packets flowing through the network vs. protocols with one attacker

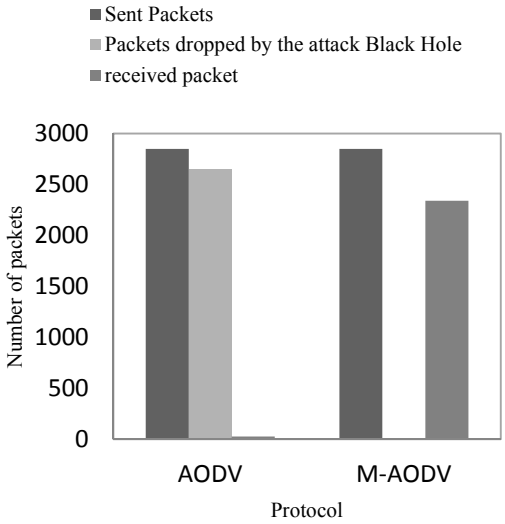


Fig. 12. Number of packets flowing through the network vs. protocols with five attackers

VIII. Conclusion

Ad hoc routing protocols are prone to various attacks due to the ignorance of the security aspect during their designs. A black hole attack disrupts normal network functionality by sending bogus routing information during route discovery phase. In this paper, we proposed a solution to avoid the black hole and the multiple black hole attackers on the AODV routing protocol in MANETs. According to the simulation results, the modified AODV gives significant improvement in packet delivery ratio with acceptable average end-to-end delay and normalized routing overhead when the mobility of nodes increases. Consequently, we concluded that our proposed approach shows superior performance than the AODV in the presence of one or multiple black hole nodes.

References

[1] Wu, B., Chen, J., Wu, J., & Cardei, M. (2007). A survey of attacks and countermeasures in mobile ad hoc networks. In *Wireless Network Security* (pp. 103-135). Springer US.

[2] Jhaveri, R. H., Patel, S. J., & Jinwala, D. C. (2012, January). DoS attacks in mobile ad hoc networks: A survey. In *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on* (pp. 535-541). IEEE.

[3] Khatri, S., Sharma, P., Chaudhary, P., & Bijalwan, A. (2015). A Taxonomy of Physical Layer Attacks in MANET. *International Journal of Computer Applications*, *117*(22).

[4] Al-Shurman, M., Yoo, S. M., & Park, S. (2004, April). Black hole attack in mobile ad hoc networks. In *Proceedings of the 42nd annual Southeast regional conference* (pp. 96-97). ACM.

[5] Perkins, C., Belding-Royer, E., & Das, S. (2003). *Ad hoc on-demand distance vector (AODV) routing* (No. RFC 3561).

[6] Johnson, D. B., & Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. In *Mobile computing* (pp. 153-181). Springer US.

[7] Patel, A. D., Jhaveri, R. H., & Shah, S. N. (2015). I-EDRI Scheme to Mitigate Grayhole Attack in MANETs. In *Intelligent Computing, Communication and Devices* (pp. 39-43). Springer India.

[8] Marttinen, A., Wyglinski, A. M., & Jantti, R. (2014, October). Moving-target defense mechanisms against source-selective jamming attacks in tactical cognitive radio MANETs. In *Communications and Network Security (CNS), 2014 IEEE Conference on* (pp. 14-20). IEEE.

[9] Gharehkoolchian, M., Hemmatyar, A. A., & Izadi, M. (2015). Improving Security Issues in MANET AODV Routing Protocol. In *Ad Hoc Networks* (pp. 237-250). Springer International Publishing.

[10] Dorri, A., & Nikdel, H. (2015, May). A new approach for detecting and eliminating cooperative black hole nodes in MANET. In *Information and Knowledge Technology (IKT), 2015 7th Conference on* (pp. 1-6). IEEE.

[11] Patel, A., Patel, N., & Patel, R. (2015, April). Defending against Wormhole Attack in MANET. In *Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on* (pp. 674-678). IEEE.

[12] Gharehkoolchian, M., Hemmatyar, A. A., & Izadi, M. (2015). Improving Security Issues in MANET AODV Routing Protocol. In *Ad Hoc Networks* (pp. 237-250). Springer International Publishing.

[13] Usha, G., & Mahalakshmi, K. (2015). Cross Layer Based Intrusion Detection in MANET Using Intelligent Paradigms. *Networking and Communication Engineering*, *7*(8), 355-360.

[14] Bhandare, A. S., & Patil, S. B. (2015, February). Securing MANET against Co-operative Black Hole Attack and Its Performance Analysis-A Case Study. In*Computing Communication Control and Automation (ICCUBEA), 2015 International Conference on* (pp. 301-305). IEEE.

[15] Nadeem, A., & Howarth, M. P. (2013). A survey of MANET intrusion detection & prevention approaches for network layer attacks. *Communications Surveys & Tutorials, IEEE*, *15*(4), 2027-2045.

[16] Nadeem, A., & Howarth, M. (2013). Protection of MANETs from a range of attacks using an intrusion detection and prevention system.*Telecommunication Systems*, *52*(4), 2047-2058.

[17] Nadeem, A., & Howarth, M. P. (2014). An intrusion detection & adaptive response mechanism for MANETs. *Ad Hoc Networks*, *13*, 368-380.

[18] Jaisankar, N., Saravanan, R., & Swamy, K. D. (2010). A novel security approach for detecting black hole attack in MANET. In Information Processing and Management (pp. 217-223). Springer Berlin Heidelberg.

[19] Jhaveri, R. H., Patel, S. J., & Jinwala, D. C. (2012, January). A novel approach for grayhole and blackhole attacks in mobile ad hoc networks. In *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on* (pp. 556-560). IEEE.

[20] Woungang, I., Dhurandher, S. K., Peddi, R. D., & Traore, I. (2013). Mitigating collaborative blackhole attacks on DSR-Based mobile ad hoc networks. In*Foundations and Practice of Security* (pp. 308-323). Springer Berlin Heidelberg.

[21] Patel, M., & Sharma, S. (2013, February). Detection of malicious attack in manet a behavioral approach. In *Advance Computing Conference (IACC), 2013 IEEE 3rd International* (pp. 388-393). IEEE.

[22] Ghathwan, K. I., & Yaakub, A. R. B. (2014). An Artificial Intelligence Technique for Prevent Black Hole Attacks in MANET. In *Recent Advances on Soft Computing and Data Mining* (pp. 121-131). Springer International Publishing.

[23] Shahabi, S., Ghazvini, M., & Bakhtiarian, M. (2015). A modified algorithm to improve security and performance of AODV protocol against black hole attack.*Wireless Networks*, 1-7.

[24] Ahmad, S. J., Reddy, V. S. K., Damodaram, A., & Krishna, P. R. (2015, January). Detection of Black Hole Attack Using Code Division Security Method. In *Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2* (pp. 307-314). Springer International Publishing.

[25] Jain, A. K., & Tokekar, V. (2015, January). Mitigating the effects of Black hole attacks on AODV routing protocol in mobile ad hoc networks. In *Pervasive Computing (ICPC), 2015 International Conference on* (pp. 1-6). IEEE.

[26] Perkins, C. E., & Bhagwat, P. (1994, October). Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In *ACM SIGCOMM computer communication review* (Vol. 24, No. 4, pp. 234-244). ACM.

[27] Issariyakul, T., & Hossain, E. (2011). Introduction to network simulator NS2. *Springer Science & Business Media.*