IMPROVING AD HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL AGAINST BLACKHOLE ATTACKS FOR MOBILE AD HOC NETWORK

Eden Teshome Dr.-IngTowfikJemal Mohammed Muntaz

ECE. Jimma Institute of Technology
Jimma, Ethiopia
edenethio1@gmail.com towfik.jemal@ju.edu.et mohammedmuntaz@yahoo.com

***Abstract* -A mobile ad hoc network (MANET) is a non-organized structure, decentralized monitoring and dynamic changing network topology of mobile devices connected by wireless for transmission of data from source to destination. In MANET, security of routing protocol is a basic requirement to provide protected communication between mobile nodes. The vulnerability of MANET creates a number of challenges on securing this routing protocol. In order to overcome these challenges, it is essential to improve the routing technique and achieve secure data communication as well as desirable network performance. MANETs are susceptible to various attacks. Among these black hole attack is one of the common ones, which affects ad hoc on demand distance vector (AODV) routing protocol.**
In this paper, a new modified AODV protocol is proposed to identify single as well as multiple black hole nodes in networks. Our technique identifies the black hole node based on computing each received route reply(RREPs) from intermediate node which is monitored at the source node. The simulation of the proposed algorithm demonstrates that the solution detects black hole node and allow source node to avoid it and also improves the overall performance of AODV in the presence of black hole attack.

Keywords-AODV, Black hole attack, MANET, Routing Protocol, RREP

1. INTRODUCTION

The fast growingof number of wireless mobile computers and communication devices is driving a revolutionary change in the way we communicate the digital age. The collection of this wireless mobile computers and communication devices forms a network called mobile ad hoc network.

A Mobile Ad hoc Network is self-organizing network of wireless mobile computers in which nodes cooperate to communicate beyond direct transmission range by forwarding packets to one another [1]. Communication among nodes in ad hoc network is achieved by implementing routing protocols.

MANETs can be used in applications such as military communications, commercial applications, and rescue operation. However, due to the absence of any fixed infrastructure, ensuring the security of this network becomes very difficult using the existing routing technique [2]. There are different routing techniques used in MANET. Among thesead hoc on demand distance vector (AODV) is one of the common one which is easily compromised by black hole attack.

Therefore, in order to minimize the effect of black hole attack in AODV protocol, this paper:

1. Clearly identify which part of the AODV protocol is affected by the black hole attack

2. Modify the protocol so that it could not be affected by black hole attack

3. Improve the performance of packet delivery ratio

The rest of this paper is organized as follows. Section 2 describes operation of AODV. Section 3 describes black hole attack. Section 4 described solutions for blackhole attack. Section5 describes the proposed algorithm for detection of black hole attack. Section 6, describes Pseudo code for detection of black hole nodes.Section 7, simulation result is discussed. Section 8, simulation metrics is discussed. Finally, in section 9, conclude the paper.

2. OPERATION OF AODV

The AODV is an on demand routing protocol designed for ad hoc mobile networks [3]. When we say AODV is an on demand routing protocols, it means that routes are only created whenever a node requested it.AODV incorporate routes using a route request (RREQ) and route reply (RREP) query cycle.

Route Discovery process will be initiated by source node to establish a new route towards the destination node by broadcasting a RREQ packet to its neighboring node. Whenever source node needs to communicate with another node for which it has no routing information it broadcast RREQ.Each neighboring node that received RREQ sending a RREP back to the source node or rebroadcasts the RREQ to its own neighboring node after increasing the hop count field for every received RREQ. The RREQ will arrive to node that possesses a fresh route towards the destination [5]. Therefore the intermediate node checks whether the route towards the destination is fresh or not by comparing the destination sequence number in its route table entry with that of the destination sequence number in the received RREQ. If the received RREQ's sequence number for the desired destination is greater than the recorded by the intermediate node, the intermediate node responds by sending RREP to source node otherwise the intermediate node rebroadcasts the RREQ packet. The source node after receiving the RREP form intermediate node starts to transmit data through that node, and then later updates itsrouting information of better route to the destination node. Figure. 1 clearly shows route discovery process in AODV.

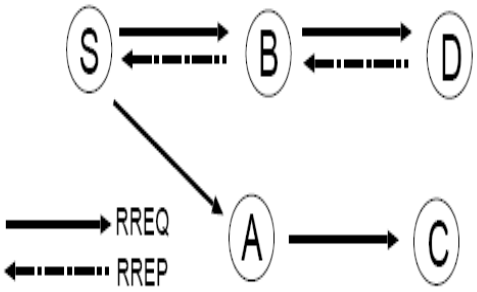

Figure1. AODV Route Discovery Process [4]

MANETs are designed that all nodes are cooperative in the coordination process to forward data packet toward the destination node, however some malicious node such as blackhole node can easily disrupt network operations by violating the protocol specification.

3. BLACKHOLE ATTACK

Black hole attack is a kind of Denial of Service (DoS) attack in which a black hole node advertise itself as having the shortest and valid path to the destination, with the intention of intercepting data packets. Then the blackhole node consumes the intercepted packets [6].

The source node sends RREQ packets to the intermediate nodes during the Route Discovery process to find fresh path to the intended destination. Black hole nodes respond immediately to source node without referring to their routing table by assigning high sequence number to the reply packet. The black hole node does this to make look like it has fresh route to the intended destination. The source node assumes that the route reply is from legitimate node, selects the path through the black hole node to route the data packets. The black hole node drops the received messages instead of forwarding to the destination as the protocol requires.Figure. 2 shows black hole attack in AODV protocol.

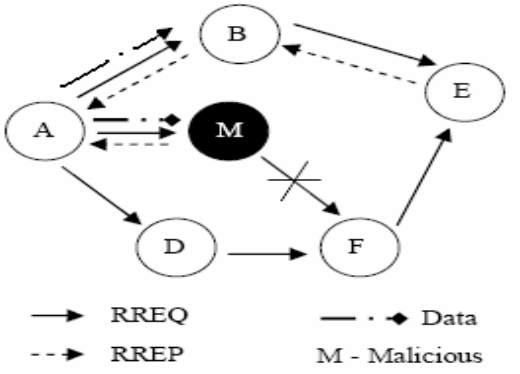

Figure. 2. Black hole attacks in AODV[10]

Figure. 2 shows that source node A broadcasts an RREQ message to discover a route for sending packets to destination node E. However, malicious node or blackhole node M sends an RREP message immediatelywithout even having a route to destination node E.

source node assume the received RREP is form legitimate node and starts sending data packet using the route which is provided by the malicious node or

blackhole node M. Nevertheless, a Black hole node drops all data packets rather than forwarding them on.

4. SOLUTIONS FOR BLACKHOLE ATTACK

1. In [4] count_drop_packet approach isintroduced in order to avoid black hole attack. In this approach, a source node broadcasts the RREQ packets in order to search the path towards the destination and all nodes that have an entry for the destination in its routing table will give RREPs. One table *drop_ table has* been createdwhich stores address of all the intermediate nodes that sends RREP packets as well as number of packet drop by each node. When intermediate node drops the packet, the value of count_ drop_packet is incremented in the drop_table. If the value of count_drop_packet incremented beyond threshold, that node is suspected to be a Black hole node and then it is stored in malicious table. The Source node stops sending the packets through that path and start the route discovery again. The advantage of this approach is that it increases 40-45% packet delivery ratio for modified AODV as compared to AODV with blackhole attack.

2. In [7] the,proposed approach for the detection of the black hole attack is based on the Intrusion Detection Systems (IDS). The proposed technique uses host based Intrusion detection system for detecting anomaly activities in the network. In this approach the activity of a user is monitored therefore anomaly activities of a malicious node are identified easily from normal activities. To detect a black hole node the system compares every activity with audit data which pre-collected set of anomaly activities generated by each node in the network. If any activity of a host is found out to be out of the activity provided in the audit data, the system assumes that black hole node exists in the network so it isolates that particular node from the network.

3. In [8], the authors discuss an approach which follows, basically the working principle of the source node, using an additional function Pre_ReceiveReply(Packet P). In this approach, the source node after receiving the first RREP control message waits for duration of MOS_WAIT_TIME then the source node will save all the coming RREP control messages in Cmg_RREP_Tab table. Using Cmg_RREP_Tab table the source node analyses all RREPs, and discard the RREP having presumably very high destination sequence number. The node that sent RREP having high destination sequence number is suspected to be the malicious node and discard any control messages coming from that node. This approach increases 25-95% packet delivery ratio for modified AODV as compared to AODV with black hole attack.

5. PROPOSED SOLUTION

The proposed solution modifies the operation of the source node without changing intermediate nodes as well as destination node. The algorithm is implemented in a popular reactive routing protocol, called AODV. In this proposed algorithm every route RREPs from intermediate nodes as well as destination node is computed at the source node. The source node compares each incoming route RREP destination sequence number with that of the RREQ destination sequence number which is stored at source node in order to ascertain the information about destination sequence number in RREP are received from legitimate node or not. The comparison is done based on whether the incoming RREPs destination sequence number beyond the predefined threshold value or not, where this threshold value is obtained from incrementing the RREQ destination sequence number by one (Dst-Seq-No.rt + 1). If the RREP's destination sequence number greater than threshold value, then the informationrelated to that destination in the AODV message must be discarded.

6. PSEUDO CODE FOR DETECTION OF BLACK HOLE NODES

Step 1:route discovery process

Source node broadcast RREQ (route request) message to discover a secure route towards the destination node.

Step 2: storing process

If intermediate node generate RREP for RREQ

{

Source nodes route entry destination table is updated

}

Step 3:identify black hole node and removed

If RREP destination sequence number is much greater than threshold valueDiscard RREP and put it in black list table

If (RREP DSN>Th)

{

Malicious-node=MNode-ID

Discard RREP

m-blacklist.update(new entry)

}

Step 4:continue normal AODV process

If RREP destination sequence number is lower than threshold value The RREP is assumed to be from legitimate node soroute table entry to the destination is updated and source node starts to send data packet trough the legitimate node.

If (RREP DSN <Th)

{

Node=Node-ID

m_routingTable.Update (newEntry)

}

7. RESULTS AND ANALYSIS

All Simulations performed using Network Simulator-2 or ns2 (v-2.29). NS-2 provides faithful implementations of the different network protocols. The IEEE 802.11 standard has been used at the physical and data link layer to provide the interconnection between the devices to the wireless transmission media. The channel used is Wireless Channel with Two Ray Ground radio propagation model. This propagation model is used because it gives accurate prediction of a received signal at a long distance compared to other models. At the network layer, AODV is used as the routing algorithm. The function of this routing algorithm is:

1. Path determination using route discovery procedure
2. Forwarding the data if secure path is found

Finally, TCP is used at the transport layer for guarantee delivery of data by keeping the track of the acknowledgment.On the top of TCP, FTP (file transfer protocol) application has been used to determine the kind of traffic that has simulated. The size of the packet is 2000bytes. The connection model is generated using cbrgen.The random positions of the nodes in the network and mobility in the network are generated by mobility model called Setdest. The terrain area is 500m X 400m with number of nodes varying from minimum 1 to maximum 100 nodes and among those nodes 12 nodes are considered to be malicious, which performs blackhole attack.

Table 1: Simulation Parameter

Parameters	Values
Simulator	Ns-2.29
Simulation time	320sec
Number of node	100
Number of black hole nodes	12
Routing protocol	AODV
Traffic type	FTP
Environment size	500×400
Packet size	2000 byte
Send rate of traffic	1packet/sec
Pause time	10sec
Mobility Model	Random waypoint
Propagation Model	Two Ray ground
Channel type	Wireless channel

8. SIMULATION METRICS

The metrics used to evaluate the performance are given below.

Packet delivery ratio (PDR): it is ratio between number of packets received by destination and number of packet originated by application [9].

PDR = (Data Packet Received / Data Packet Sent) * 100

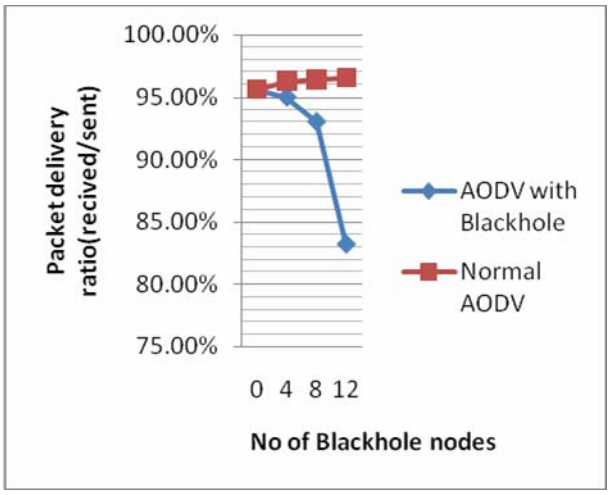

Figure. 3.Comparison of Normal AODV with AODV with Black hole attack

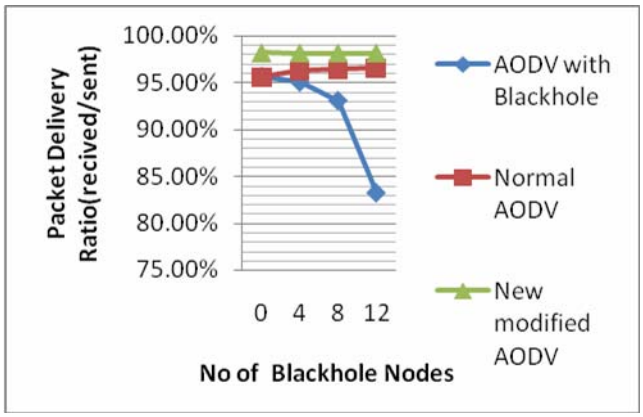

Figure. 4. Implementation of New Modified AODV for Blackhole attack

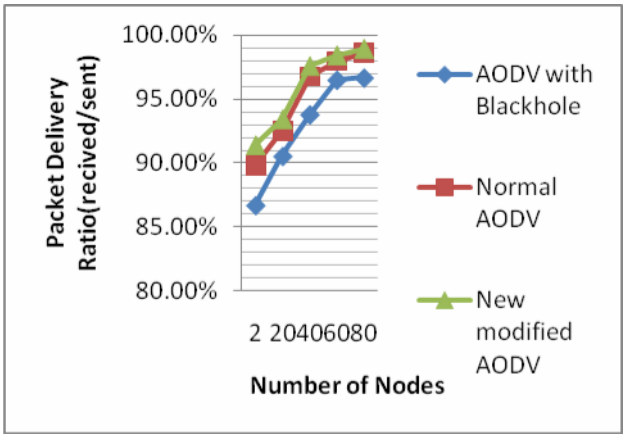

Figure. 5.Comparison of New Modified AODV with Normal AODV by varying network size

Figure.3 depicts the comparison of Normal AODV with that of AODV with Black hole attack. The simulation of the network using AODV routing protocol has been done. As number of Black hole nodes increases, Packet Delivery Ratio of AODV with Blackhole decreases drastically. This is due to the fact that the data did not reach the destination node on account of blackhole node data loss occurs. Therefore PDR of the network decreases due to blackhole effect as compared to without the effect of black hole attack.

Figure.4 shows the Implementation of New Modified AODV for Blackhole attack. The total number of node used in the network is hundred. From the above graph of packet delivery ratio (PDR) v/s Number of black hole nodes it can be seen that, The PDR drop from 98% to 83% due to the blackhole node for AODVconsidering twelve number of black hole node in the network. With the New modified AODV protocol the PDR value is higher as compared to AODV with Blackhole as well as Normal AODV protocol.This is because of the New modified AODV protocol detects the black hole node and allow source node to avoid the black hole node. By avoiding the black hole node that exist in the network, the New modified AODV protocol finds the shortest paths towards the destination as a result it delivers more data packets which in turn results high data delivery ratio. Therefore on applying the solution there is a 15% increase in Packet Delivery ratio.

Figure.5 shows theComparison of New Modified AODV with Normal AODV having the network size varying from two to eighty number of node. In this figure the performance of Normal AODV and the new modified AODV are almost identical for higher number of nodes in the network. This is because there is no blackhole node which intercepts the data packet; the data will reach to the destination node without being altered by blackhole node. Therefore the data packet is delivered to the destination node as a result the Normal AODV as well as the New modified AODV has identical PDR value.
The figure indicates that PDR of Normal AODV and New modified AODV routing protocol increases with increase in the number of nodes. As the number of node increased the probability of the source node finding the shortest and alternative path to forward the data packet towards the destination node is higher, as a result more data packet delivered to destination node which in turn results in higher PDR value both for Normal AODV as well as in New Modified AODV protocol. In AODV with one blackhole attack the PDR is lower due to blackhole node that exists in the network that drops the data packet. The new Modified AODV improved the PDR by increasing from 91% to 99% compared to an increase of 87% to 97% when simulation without implantation of the solution was conducted. AODV drops more packets under blackhole attacks as compared to new modified AODV under varying number of nodes.

9. CONCLUTIONS

Different solution has been proposed in the past to secure the routing protocol of MANET; but solutions are not perfect in terms of producing desirable or intended results. Some of the proposed solution works well in the presence of single malicious node or black hole node, its performance degrades in case of multiple black hole nodes. For this purpose, multiple Black hole nodes in the network have been added. Five scenarios where each one has 100 nodes that use AODV protocol and also simulated the same scenarios after introducing multiple Black Hole Node into the network. Finally, the results of solution were compared with normal AODV under attack by varying different network parameters using same scenarios in NS -2. From the results obtained one can conclude that the New Modified AODV gives better performance compared to a normal AODV under black hole attack.

In future this approach can be extended to analyzing the performance based on end to end delay and throughput.

ACKNOWLEDGMENT

We would like to thank MrAshenafiNegussie for his assistance during the research work.

References

[1]N.Dixit.S, S.Agrawal and N.V.Singh, "A proposed solution for security issues in MANETS", Vol.2, pp. 1409- 1412,2013.

[2]A.Adoghe,A.Olujimi,U.D.Lke and O.Olukayode"Security issues in MANET and counter measures",InternationalJournal Data and Network Security (IJDNS), vol.3, 2013.

[3] N.Khemariya and A.Khuntetha,"An efficientalgorithm for detection of blackhole attack in AODV based MANETs.",International Journal of Computer Applications, vol. 66, pp. 18-24, 2013.

[4] D.Thakarand N.Prajapati,"A modified AODV algorithm for prevention of black hole attack in mobile adhoc Networks", International Journal of Conceptions on Electrical and Electronics Engineering, vol. 1, 2013.

[5] A.Sharma,R.Singh and G.Pandey, "Detection and prevention from black hole attack in AODV protocol for MANET", International Journal of Computer Applications,vol. 50, pp. 1-4, 2012.

[6] B.Patel and J.Baria. "Black hole Attack inMobile Ad Hoc Networks – Issuesand Solutions", International Journal of Engineering Research & Technology (IJERT), vol.1,pp. 1- 6, 2012.

[7]F.Y.Alem and H.Z. Xaun, "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection", Vol.2,2010.

[8]N. Mistry, D.C Jinwal and M.Zaveri, "Improving AODV Protocol against Blackhole Attacks" Proceedings of the international Multi Conference of Engineers and Computer Scientists, Vol.2, 2010.

[9]P.Sahu,S.K .Bisoy andS.Sahoo "Detecting and isolatingmalicious node in AODV routing algorithm",Internationaljournal of computer applications (0975-8887),vol. 66, pp. 8-10, 2013.

[10]S. Jain, S.Patel and A. Verma, "Behaviour of AODV MANET reactive routing protocol in presence of black hole active attack using network simulator",International Journal of Advanced Computer Technology (IJACT), Vol.2