Volume 5, Issue 7, July 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Modified AODV Routing Protocol to Detect the Black Hole Attack in MANET

M.Sc.Ali Abdulrahman Mahmood, Dr. Taha Mohammed Hasan, M.Sc.Dhiyab Salman Ibrahim
University of Diyala, College of Sciences, Diyala,
Iraq

Abstract-- An ad hoc network is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure. Designing a foolproof security protocol for ad hoc network is a challenging task due to its unique characteristics such as, lack of central authority, frequent topology changes, rapid node mobility, shared radio channel and limited availability of resources. There are a lot of routing protocol for Ad-hoc network such as OLSR,AODV and ZRP; AODV (Ad Hoc On-Demand Distance Vector) is one of such protocols that helps to create and maintain routes in spite of the dynamic network topology. This protocol is vulnerable to a number of security threats that come from internal malicious nodes which have authorization credentials to participate in the network. Malicious nodes deliberately drop data packets and disrupt the correct operation of the routing protocol. This paper propose a security technique to detect and isolate the malicious node in the AODV routing protocol that cause black hole attack.

Keywords—Ad hoc Network, AODV, Black hole attack, MANET, Security, Malicious Node

I. INTRODUCTION

A Mobile Ad-hoc Network (MANET), as the name suggests, is a self-configuring network of wireless and hence mobile devices that constitute a network capable of dynamically changing topology [1]. The network nodes in a MANET, not only act as the ordinary network nodes but also as the routers for other peer devices. The routers move freely and organize themselves randomly and the network topology may change rapidly and spontaneously also there is no centralized gateway device to monitor the traffic within network. Since the medium is open for all nodes, both legitimate and malicious nodes can access it [2]. Moreover, there is no clear separation between normal and unusual activities in a mobile environment false routing information can come from a compromised node or a legitimate node that has outdated information.

The black hole or sequence number attack is one of the most common attacks made against the reactive routing protocol in MANETs. The black hole attack involves malicious node(s) fabricating the sequence number, hence pretending to have the shortest and freshest route to the destination. The aim of this paper is to investigate black hole & detection methods within the scope of ad hoc on demand distance vector (AODV) routing protocol.

The rest of this paper is organized as follows. In Section II we briefly describe the different types of routing protocols with its descriptions and detail note on AODV routing protocol. Section III provides an overview of the Black Hole attack. Section IV describes about the previous work done on black hole attack. Section V gives the detail information about our proposed solution. We conclude with plan for future work in Section VI.

II. ROUTING PROTOCOLS

The primary goal of routing protocols in ad-hoc network is to establish optimal path (min hops) between source and destination with minimum overhead and minimum bandwidth consumption so that packets are delivered in a timely manner [3]. Routing in mobile ad hoc networks is a biggest challenge such as end-to-end delay, packet delivery ratio, overhead, node mobility, energy efficiency, etc. As fig 1 shows the categorization of these routing protocols [4].

1. **Table driven or Proactive routing protocols:** This protocols are exchanging topological information among the nodes. Each node broadcast routes of routing table periodically to its neighbors. The main advantage of this protocol is short response time and find a good route from source to destination because of its up-to-date information of each node. Some protocols are OLSR and DSDV.
2. **On-demand or Reactive routing protocols:** This protocols are establish a route when required at destination only. They do not store all paths. A node does not broadcast the routing table periodically but it improves the network bandwidth. Some protocols are AODV and DSR.
3. **Hybrid routing protocols:** They combines the proactive and reactive protocols, which will gives a better solution when compared to a particular routing protocols. Each node proactively maintain a routing table for nodes and reactively finds a route to its destination. Some protocols are ZRP and ZHL.

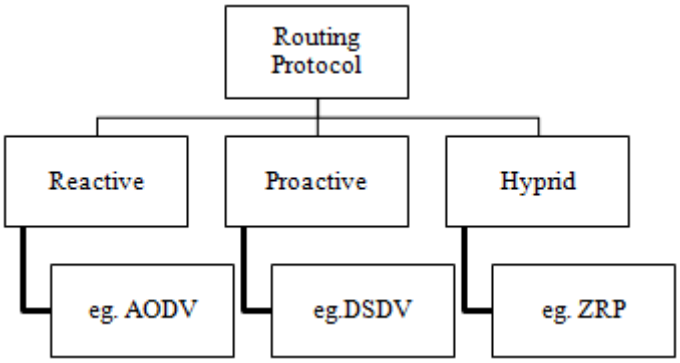

Fig 1. Hierarchy of Routing Protocols

III. AN OVERVIEW OF AODV ROUTING PROTOCOL

Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol uses a reactive approach to find a path to the destination in an ad-hoc network. To find the path to the destination all mobile nodes work in cooperation using the routing control messages. AODV Routing Protocol offers quick adaptation to dynamic network, conditions, low processing and memory overhead, low network bandwidth utilization with small size control messages [5]. The most distinguishing feature of AODV compared to the other routing protocols is that it uses a destination sequence number for each route entry. The destination sequence number is generated by the destination when a connection is requested from it. Using the destination sequence number ensures loop freedom. AODV makes sure the route to the destination does not contain a loop and is the shortest path [1] [6].

Route Requests (RREQs), Route Replay (RREPs), Route Errors (RERRs) are control messages used for establishing a path to the destination, sent using UDP/IP protocols. Header information of these control messages are explained in [7] [8]. In general, the nodes participating in the communication can be classified as source node, an intermediate node and a destination node. With each role, the behavior of a node actually varies. When a source node wants to connect to a destination node, first it checks in the existing route table, as to whether a fresh route to that destination is available or not. If a fresh enough route is available, it uses the same. Otherwise the node initiates a Route Discovery by broadcasting a RREQ control message to all of its neighbors. This RREQ message will further be forwarded (again broadcasted) by the intermediate nodes to their neighbours. This process will continue until the destination node or an intermediate node having a fresh route to the destination. At this stage eventually, a RREP control message is generated. Thus, a source node after sending a RREQ waits for RREPs to be received. Fig. 2 depicts the flow of control messages.

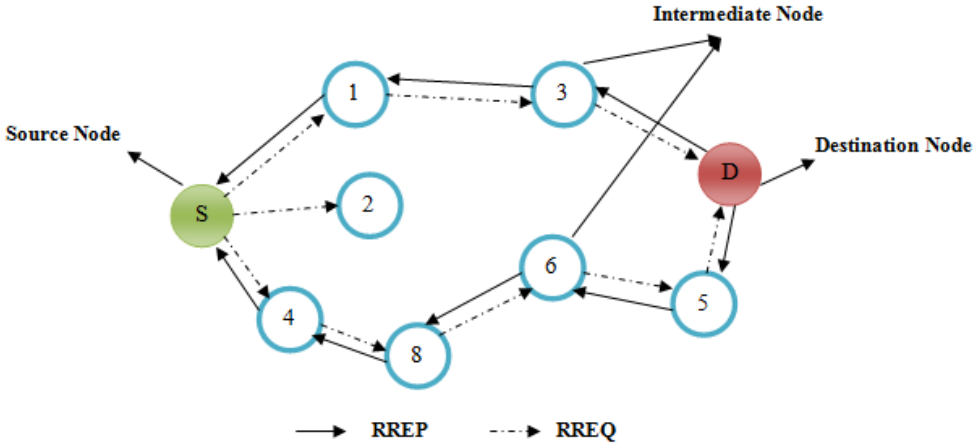

Fig. 2 Flow of Control Messages

IV. BLACK HOLE ATTACK

Routing protocols are exposed to a variety of attacks. Black hole attack is one such attack and a kind of Denial Of Service (DoS) in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept [7]. The black hole attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. In the traditional AODV protocol the route from the source to destination is selected on the basis of hop counts and sequence number. The route which has minimum number of hop counts and highest sequence number will be selected as the best route. The sequence numbers tells us the freshness of the route. During the Route Discovery process, the source node sends RREQ packets to the intermediate nodes to find fresh path to the intended destination. Malicious nodes respond immediately to the source node as these nodes do not refer the routing table. The source node assumes that the route discovery process is complete, ignores other RREP messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to the reply packet. The attacker now drops the received messages instead of relaying them as the protocol requires [9].

As an example, consider the following fig 3, when the source node broadcast the RREQ message, the black hole node will immediately reply RREQ through an RREP message. This RREP have an extremely large sequence number. Apart from this RREP, other normal nodes also receive the RREQ and destination node will select the route with minimal hop count and return the RREP. But as per AODV, largest sequence number and minimal hop count will be selected by source node. So, source node will select the black hole node for sending the data. Eavesdropping or direct dropping of received data packet is done by black hole node. Black hole node does not check its routing table and will respond to RREQ message before any other node check its routing table and respond to RREQ message.

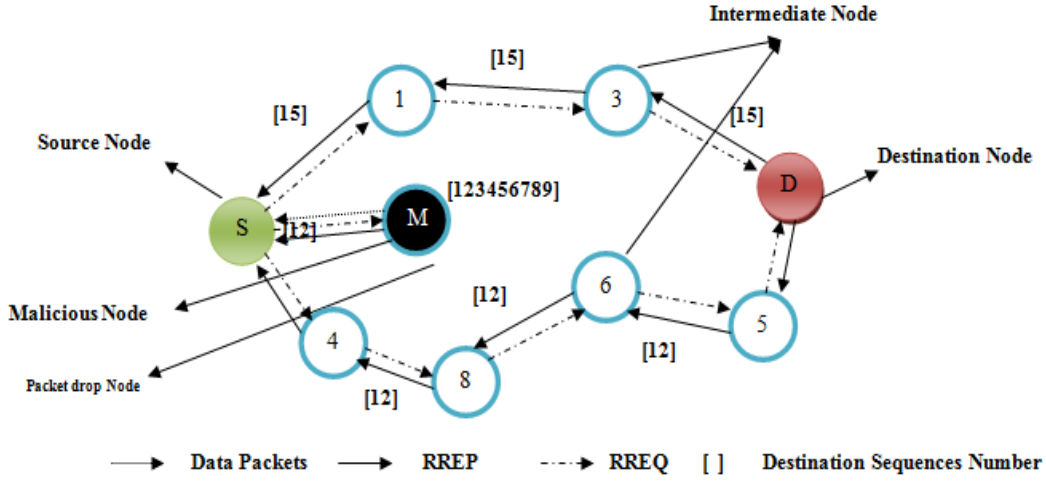

Fig. 3 Black hole attack

V. RELATED WORK ON BLACK HOLE ATTACK

There are many existing solution for detecting and mitigating the malicious node in the network. In [10] proposed a method for identifying multiple black hole nodes. They are first to propose solution for cooperative black hole attack. They slightly modified AODV protocol by introducing data routing information table (DRI) and cross checking. Every entry of the node is maintained by the table. They rely on the reliable nodes to transfer the packets.

In [11] proposed a solution with the enhancement of the AODV protocol which avoids multiple black holes in the group. A technique is give to identify multiple black holes cooperating with each other and discover the safe route by avoiding the attacks. It was assumed in the solution that nodes are already authenticated and therefore can participate in the communication. It uses Fidelity Table where every node that is participating is given a fidelity level that will provide reliability to that node. Any node having 0 value is considered as malicious node and is eliminated.

In [12] proposed the solution which discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes. This solution adds on some changes in the solution proposed by the S.Ramaswamy [13] to improve the accuracy. This algorithm uses a methodology to identify multiple black hole nodes working collaboratively as a group to initiate cooperative black hole attacks. This protocol is a slightly modified version of AODV protocol by introducing Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP). Most of the papers have addressed the black hole problem on the protocol such as AODV.

In [14], an approach is proposed for mitigating the black hole attack. By using the opinion of neighbor node, honesty of nodes is judged. Node must show its honesty in order to transfer the data packets. The node which first receive the RREP packet, initiate the judgment process on replies and forward the packet to source. This judgment is based on opinion of network nodes about replier. After receiving the opinion of neighbor, the node decides whether the replier is malicious node or not. The drawback of this solution is that there is no guarantee that the opinion of neighbor node is always correct.

In [3], to find the black hole nodes, secure routes are discovered by checking the sequence number. If the difference between the sequence number of source node or intermediate (who sent first RREP) is large, then the probability of that node to be malicious is more. The first RREP by any intermediate node is usually comes from malicious node. It is recommended that such node should be immediately removed from routing table.

In [15], the authors describe a protocol in which the source node verifies the authenticity of a node that initiates RREP by finding more than one route to the destination. When source node receives RREPs, if routes to destination shared hops, source node can recognize a safe route to destination.

In [16] presents a trust based security framework to identify malicious nodes in ad hoc on-demand distance vector (AODV) protocol. In this framework each node calculates trust level of its neighboring nodes for route selection. Trust calculation process involves opinions of other nodes about the node whose trust level is to be determined. If a neighboring node has a trust level lower than a predefined threshold value, it is identified as malicious and it is not considered for route selection. The proposed security framework does not use any key distribution process and no changes are made in control packets of AODV. Simulation results show that the proposed framework improves performance of AODV by identifying and removing malicious nodes.

VI. PROPOSED CONCEPT

In proactive and reactive routing protocol, there must be good co-operation among the nodes so that the data can be routed successfully from source to destination. If nodes have good co-operation between them then there will be no packets dropping or modification in the content. If there is no co-operation between the nodes, then there are high possibilities that an attacker take the advantage of situation and perform the malicious function. AODV routing protocol provides such situation when source node want to send the message to destination node which is not directly in contact with the source node then a route discovery process is initiated by broadcasting the RREQ message in the network. Now malicious node will take the advantage of this RREQ message and immediately send the RREP message to source node of having the route to the destination node without checking its routing table. This RREP message has the large sequence number and minimal hop count. When source node starts transmitting the data, the malicious node will drop the packet rather than forwarding it to the destination node.

Therefore, to prevent such attack from destroy the network functions. The solution that we propose here is basically only modifies the working of the source node without altering intermediate and destination nodes, here two things are added.

1. A new Trust-Table to store all the Request Reply with node ID and the trust value for each node in the network to the data structures in the default AODV Protocol.
2. Timer to compute the amount of time that the node should wait to receive the Route Replay form another nodes

The trust value for each node compute throughout monitor the packets sent and acknowledgments received and adjusts the trust values of nodes accordingly [17]. Whenever a node transmits a packet, it starts a timer, places its receiver in promiscuous mode, and maintains copies of recently forwarded packets to compare them with the packet transmissions overheard by the neighboring nodes [18]. As soon as it hears its neighboring node forwarding the packet, the sender node deletes the buffered packet, cancels the timer, and confirms that the neighboring node has behaved well so the number of forwarded packets is increased. Similarly, if the neighboring node does not transmit the packet within a certain timeout period; packet acknowledgement time out, its corresponding number of dropped packets is increased accordingly. By this continuous monitoring, the nodes trust values are adjusted based on the experiences that the node has with its neighbor nodes. When a node receives data packets or acknowledgements from its neighbor node, the trust value for this neighbor node will be increased. Neighbor node that is encountered for the first time will have an initial trust value assigned. A high trust value is initially assigned for unknown nodes. If a route contains known nodes, the trust values of these neighbor nodes are used to assign the initial trust value. If a requested acknowledgement was not received, the trust value for this neighbor node is decreased. A node is identified as malicious when the number of packet dropped exceeds the predefined threshold value during a fixed trust update interval. When threshold is reached, the trust value of a neighbor node is calculated. The algorithm describe as follow:

Algorithm:

DSN – Destination Sequence Number, NID – Node ID, T – Trust Value, SSN – Sources Sequence Number

Step 1: (Initialization Process)

Start the timer after sending the RREQ to the nodes in the network.

Step 2: (Storing Process)

Store all the Route Replies DSN and NID in Trust-Table until the time exceeds

Step 3: (Identify and black list the Malicious Node)

Sort the content of Trust-Table according to the DSN and retrieve the first entry from table then If DSN is much greater than SSN and the trust value is below the trust value then Remove the entry from Trust-Table and add the node to the black list and send the acknowledgment to the rest of nodes in the network.

Step 4: (Node Selection Process)

Sort the contents of Trust-Table entries according to the DSN. Repeat the **step3** until find the node with the highest DSN and has the accepted trust value among table entries.

Step 6: (Continue default process)

Call ReceiveReply method of default AODV Protocol.

The above algorithm starts from the initialization process, first set the waiting time for the source node to receive the RREQ coming from other nodes. Then in storing process, store all the RREP Destination Sequence Number (DSN) and its Node Id in Trust-Table until the computed time exceeds. Then sort the content of table according to the DSN and retrieve the first entry from Trust-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, and the trust value below the threshold value this node will be mark as the malicious node, and immediately remove it from the Trust-Table and send the acknowledgment to the rest of nodes in the network. This is how malicious node is identified and removed. Final process is selecting the next node id that have the higher destination sequence number, is obtained by sorting the Trust-Table according to the DSN-RR column, whose packet is sent to ReceiveReply method in order to continue the default operations of AODV protocol.

Table 1: Content of RR-table with malicious node

RR-No.	DSN-RR	TRUST VALU	NID
1	**122**	**0**	**N3**
2	**14**	**2**	**N5**
3	**12**	**3**	**N6**

Table 2: Content of RR-table without malicious node and sorted according to DNS.

RR-No.	DSN-RR	TRUST VALU	NID
1	150	2	N6
2	14	2	N5
3	12	3	N3

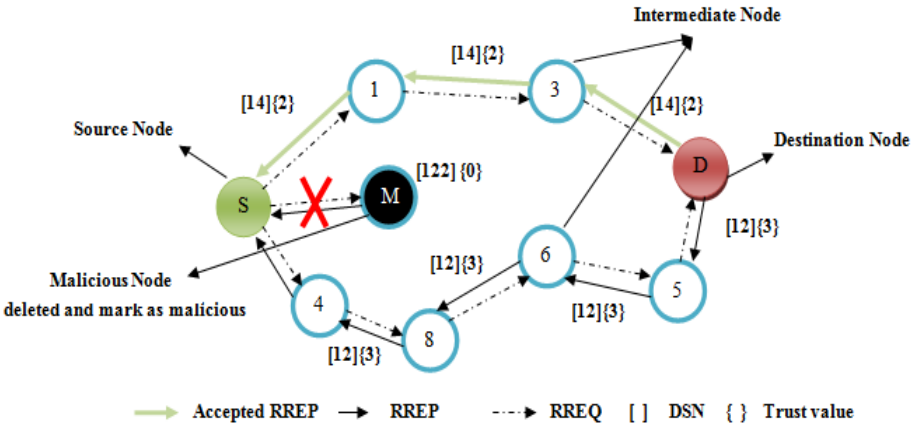

Fig. 4 Isolating the Malicious Node depending on the DSN and Trust Value

VII. CONCLUSION

This paper shows various works related to black hole attack for detecting and preventing in AODV routing protocol. A malicious node can reduce the ratio of end to end delivery. We propose an efficient and simple approach for defending the AODV protocol against Black Hole attacks that can be implemented on the AODV protocol. The Proposed method can be used to find the secured routes and prevent the black hole nodes in the MANET.

This proposed method can be used to find out the secure routes and preventing the black hole nodes in the MANET by indentifying the nodes with their sequence number; and maintain the trust value for each node. The trust value for each node compute throughout monitor the packets sent and acknowledgments received and adjusts the trust values of nodes accordingly. In addition, the proposed solution may be used to maintain the identity of the malicious node, so that in future, it can discard any control messages coming from that node. Now since malicious node is identified, the routing table and the control messages from the malicious node, too, are not forwarded in the network.

As future work, we aims to develop simulations to analyze the performance of the proposed solution based on the various security parameters like packet delivery ratio (PDR), mean delay time, packet overhead, memory usage, mobility, increasing number of malicious node, increasing number of nodes and scope of the black hole nodes and also focusing on resolving the problem of multiple attacks against AODV.

REFERENCES

[1] C. Hongsong, J. Zhenzhou, H. Mingzeng, F. Zhongchuan, and J. Ruixiang, "Design and performance evaluation of a multi-agent-based dynamic lifetime security scheme for AODV routing protocol," *J. Netw. Comput. Appl.*, vol. 30, no. 1, pp. 145–166, Jan. 2007.

[2] E. M. Belding-Royer and C. E. Perkins, "Evolution and future directions of the ad hoc on-demand distance-vector routing protocol," *Ad Hoc Networks*, vol. 1, no. 1, pp. 125–150, Jul. 2003.

[3] L. Himral, V. Vig, and N. Chand, "Preventing AODV Routing Protocol from Black Hole Attack," *Int. J. Eng. Sci. Technol.*, vol. Vol. 3, no. No. 5.

[4] J. Kumar, M. Kulkarni, and D. Gupta, "Effect of Black Hole Attack on MANET Routing Protocols," *Comput. Netw. Inf. Secur.*, vol. 5, no. April, pp. 64–72, 2013.

[5] P. Ning and K. Sun, "How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols," *Ad Hoc Networks*, vol. 3, no. 6, pp. 795–819, Nov. 2005.

[6] S. Liu, Y. Yang, and W. Wang, "Research of AODV Routing Protocol for Ad Hoc Networks1," *AASRI Procedia*, vol. 5, pp. 21–31, 2013.

[7] C. Perkins, "(RFC) request for Comments-3561, Category: Experimental, Network, Working Group." .

[8] L. Pengwei and X. Zhenqiang, "Security enhancement of AODV against internal attacks," *Inf. Sci. ...*, pp. 584–586, Dec. 2010.

[9] J. von Mulert, I. Welch, and W. K. G. Seah, "Security threats and solutions in MANETs: A case study using AODV and SAODV," *J. Netw. Comput. Appl.*, vol. 35, no. 4, pp. 1249–1259, Jul. 2012.

[10] S. Ramaswamy, H. Fu, M. S. J. Dixon, Nygard, and Kendall, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks," in *International Conference on Wireless Networks (ICWN 03), Las Vegas, Nevada, USA*, 2003.

[11] Tamilselvan, L. Sankaranarayanan, and V, "Prevention of Blackhole Attack in MANET," *J. Networks*, vol. Vol.3, no. No.5.

[12] H. Weerasinghe and H. Fu, "Preventing Cooperative Black Hole Attacks in Mobile Adhoc Networks: Simulation implementation And Evaluation," *IJSEA*, vol. Vol2, no. No.3.

[13] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks," in *International Conference on Wireless Networks (ICWN 03)Las Vegas, Nevada, USA*, 2003.

[14] Medadian, M., Mebadi, A., Shahri, and E, "Combat with Black Hole attack in AODV routing protocol," in *Communications (MICC), 2009 IEEE 9th Malaysia International Conference on*, 2009, pp. 530–535.

[15] M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks," in *Proceedings of the ACM 42nd Southeast Conference (ACMSE'04)*, pp. 96–97.

[16] I. Raza and H. S.A., "A Trust based Security Framework for Pure AODV Network," in *International Conference on Information and Emerging Technologies (ICIET)*, 2007, pp. 1 – 6.

[17] A. M. Pushpa, "Trust Based Secure Routing in AODV Routing Protocol," *IEEE*, 2009.

[18] R. Di Pietro, S. Guarino, N. V. Verde, and J. Domingo-Ferrer, "Security in wireless ad-hoc networks – A survey," *Comput. Commun.*, vol. 51, pp. 1–20, Sep. 2014.

