Volume 3, Issue 6, June 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Detection of Black Hole Attack in MANET under AODV Routing Protocol

Vipan Chand Sharma*
Software Engineer, Drinity Softwares
India

Atul Gupta
CSE Deptt, GLBIMR Greater Noida
India

Vivek Dimri
IT Deptt, Sharda University
India

Abstract*— An Ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. In Mobile Ad-hoc Networks (MANET), each mobile node acts as a host as well as a router. These nodes communicate to each other by hop-to-hop communication. The dynamic topology of MANET allows nodes to join and leave the network at any point of time. Wireless MANET is particularly vulnerable due to its fundamental characteristics such as open medium, dynamic topology, distributed cooperation and constrained capability. So security in MANET is a complex issue. There are a lot of routing protocol for Ad-hoc network like Ad-hoc On Demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR), Destination Sequence Distance Vector Routing (DSDV) and Temporally Ordered Routing Algorithm.AODV is an on-demand reactive routing protocol for mobile ad hoc networks. But in existing AODV, there is no security provision against a well-known "Black Hole" attack. Black Hole nodes are those malicious nodes that agree to forward packet to destination but do not forward packet intentionally. These Black Hole nodes participate in the network actively and degrade the performance of network. In this paper we proposed a solution for identifying the malicious node in AODV protocol suffering from Black Hole attack.

***Keywords*— MANET, AODV, Black Hole Attack, RREQ, RREP, RERR.**

I. Introduction

Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. 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. The network nodes in a MANET, not only act as the ordinary network nodes but also as the routers for other peer devices [1]. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, and personal computer that are participating in the network and are mobile. The dynamic topology, lack of a fixed infrastructure and the wireless nature make MANETs susceptible to the security attacks. Due to the unique characteristics of MANET, developing an Intrusion Detection System (IDS) in this network is very challenging task. 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. Moreover, there is no clear separation between normal and unusual activities in a mobile environment. Since nodes can move arbitrarily, false routing information can come from a compromised node or a legitimate node that has outdated information. 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. Section VI shows the methodology used for evaluation. We conclude with plan for future work in Section VII.

II. Routing Protocol

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. A MANET protocol should function effectively over a wide range of networking context from small ad-hoc group to larger mobile Multihop networks. Fig. 1 shows the categorization of these routing protocols.

Routing protocols in MANETs are classified into **proactive, reactive and hybrid protocols**, depending on the routing topology. Proactive protocols are typically table-driven. Examples of this type include Destination Sequence Distance Vector (DSDV). Reactive or source-initiated on- demand protocols, in contrary, do not periodically update the routing information. It is propagated to the nodes only when necessary. Example of this type includes Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV). Hybrid protocols make use of both reactive and proactive approaches. Example of this type includes Zone Routing Protocol (ZRP).

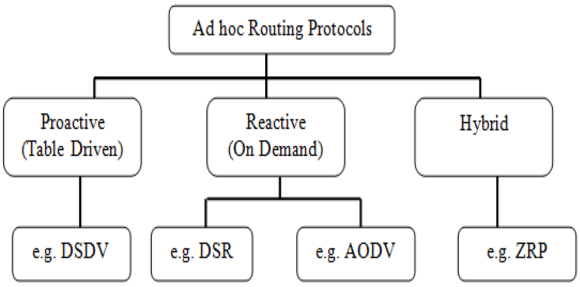

Fig. 1 Hierarchy of Routing Protocols

A. Proactive Routing Protocol

These protocols are also called as Table Driven protocols since they maintain the routing information even before it is needed [2]. Each and every node in the network maintains routing information to every other node in the network. Routes information is generally kept in the routing tables and is periodically updated as the network topology changes. There exist some differences between the protocols that come under this category depending on the routing information being updated in each routing table. Furthermore, these routing protocols maintain different number of tables. The proactive protocols are not suitable for larger networks, as they need to maintain node entries for each and every node in the routing table of every node. This causes more overhead in the routing table leading to consumption of more bandwidth.

B. Reactive Routing Protocol

These protocols are also called On Demand routing protocols since they don't maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet [3]. The route discovery usually occurs by flooding the route request packets throughout the network. Reactive search procedures can also add a significant amount of control traffic to the network due to query flooding. Because of these weaknesses, reactive routing is less suitable for real-time traffic or in scenarios with a high volume of traffic between a large numbers of nodes.

C. Hybrid Routing Protocol

This type of protocols combines the advantages of proactive and of reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The basic idea is that each node has a pre-defined *zone* centered at itself in terms of number of hops. For nodes within the zone, it uses proactive routing protocols to maintain routing information. For those nodes outside of its zone, it does not maintain routing information in a permanent base. Instead, on-demand routing strategy is adopted when inter-zone connections are required.

D. 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. 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.

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 [4]. In general, the nodes participating in the communication can be classified as source node, an intermediate node or a destination node. With each role, the behaviour 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 neighbours. 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.

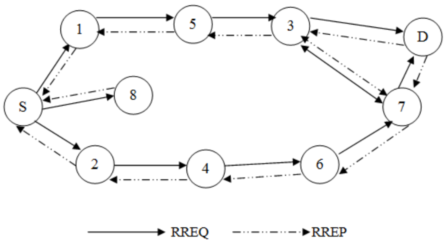

Fig. 2 Flow of Control Messages

III. BLACK HOLE ATTACK

A Black hole attack is one of the active DoS attacks possible in MANETs. In this attack, a malicious node sends a false RREP packet to a source node that initiated the route discovery, in order to pose itself as a destination node or an immediate neighbour to the actual destination node. When a source node broadcasts the RREQ message for any destination, the black hole node immediately responds with an RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the black hole and discards the other RREP packets coming from other nodes. The source then starts to send out its data packets to the black hole trusting that these packets will reach the destination. A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. As a result, therefore, the source and the destination nodes became unable to communicate with each other [5].

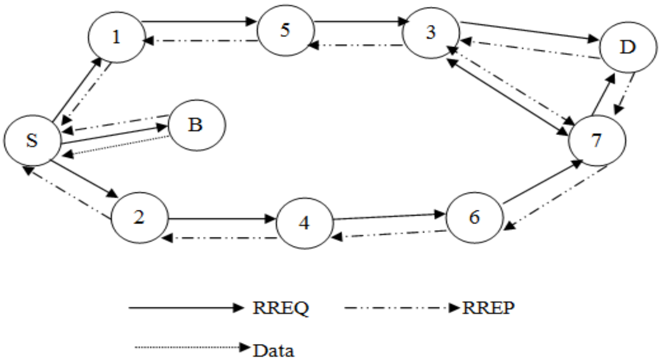

Fig. 3 Protocol Packet Exchanges

As shown in Fig. 3, we assume that Node B is the malicious node. When Node S broadcasts the RREQ message for Node D, Node B immediately responds to Node S with an RREP message that includes the highest sequence number of Node D, as if it is coming from Node D. Node S assumes that Node D is behind Node B with 1 hop and discards the newly received RREP packet come from Node 2. Afterwards Node S starts to send out its data packet to the node B trusting that these packets will reach Node D but Node B will drop all data packets. In a Black Hole Attack, after a while, the sending node understands that there is a link error because the receiving node does not send TCP ACK packets. If it sends out new TCP data packets and discovers a new route for the destination, the malicious node still manages to deceive the sending node. If the sending node sends out UDP data packets the problem is not detected because the UDP data connections do not wait for the ACK packets.

IV. RELATED WORK

There indeed have been numerous attempts published in the literature that aim at countering the Black attacks. We survey them in the following. In [6], the authors discuss a protocol that requires the intermediate nodes to send RREP message along with the next hop information. When the source node gets this information, it sends a RREQ to the next hop to verify that the target node (i.e. the node that just sent back the RREP packet) indeed has a route to the intermediate node and to the destination. When the next hop receives a FurtherRequest, it sends a FurtherReply which includes the check result to the source node. Based on information in FurtherReply, the source node judges the validity of the route. In this protocol, the RREP control packet is modified to contain the information about next hop. After receiving RREP, the source node will again send RREQ to the node specified as next hop in the received RREP. Obviously, this increases the routing overhead and end-to-end delay. In addition, the intermediate node needs to send RREP message twice for a single route request. Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park [7] proposed two different approaches to solve the Black hole attack. The first solution the sender node needs to verify the authenticity of the node that initiates the RREP packet by utilizing the redundancy of the network. The idea of this solution is to find more than one route for the destination. The SN unicast the ping packet using different routes. The IN or destination node or malicious node will ping requests. The SN checks the acknowledgment and processes them to check which one is safe or having malicious node. In the meantime the SN buffered its packet until it found the safe route. When the route is identified the buffered packets will be transmitted to it. The drawback of the solution is the time delay. The second solution is to store the last sent packet sequence number and the last received packet sequence number in the table. It is updated when any packet is arrived or transmitted. When node receives reply from another node it checks the last sent and received sequence number. If there is any mismatch then an ALARM indicates the existence of a Black hole node. This method is faster and more reliable and has no overhead. Sanjay Ramaswamy, et al [8] 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. Latha Tamilselvan, Dr. V Sankaranarayanan[9] 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.

Hesiri Weerasinghe [10] 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 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.

V. Proposed Approach

The solution that we are proposing here only modifies the working of the source node without altering intermediate and destination nodes by using a method called Prior_RceiveReply. In this method we add the two things, a new routing table RR-Table (Request Reply), a timer WT (Waiting Time) to the data structures in the AODV Protocol.

Algorithm:

DSN – Destination Sequence Number, NID – Node ID, and MN-ID – Malicious Node ID.

Step 1: (Initialization Process)

Retrieve the current time and add this current time with waiting time. Waiting time is the half of the RREP wait time.

Step 2: (Storing Process)

Store all the Route Replies DSN and NID in RR-Table. Repeat the above process until time exceeds.

Step 3: (Identifying and Removing Malicious Node)

Retrieve the first entry from the RR-Table

If DSN is much greater than SSN then the discard entry from the RR-Table and store its NID in MN-ID

Step 4: (Node Selection Process)

Sort the contents of RR-Table entries according to the DSN. Select the NID having highest DSN among RR-table entries

Step 5: (Continue default process)

Call ReceiveReply method of default AODV Protocol

The above algorithms first set the waiting time for the source node to receive the RREQ coming from other nodes and then add the current time with waiting time. In the storing process, it stores all the RREQ Destination Sequence Number (DSN) and its Node Id in the RR_Table until the time expires. Generally the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table.

Then it compares the first destination sequence number with the source node sequence number, if there exist more difference between them, and then the node is malicious node. So remove that entry from the RR-Table. This is how the malicious node is identified and removed from the RR-Table. The final step is to choose the next id node that having the higher DSN, is obtained by sorting the RR-Table according to the Destination Sequence Number column and this packet is sent to the ReceiveReply method to continue the default operation of AODV protocol.

The control messages from the malicious nodes are not forwarded into the network. In order to maintain the freshness, the RR-Table is flushed once a route is chosen from it. The operation of the proposed algorithm is same as the original AODV, once the malicious node has been detected.

The main benefits for modifying AODV protocol is

a) The malicious node is identified at the initial stage itself and immediately removed so that it cannot take part in further process.

b) With no delay the malicious node are easily identified. Generally the malicious node having the highest DSN and its RREP is first to arrive.

c) No modification is made in the default operation of AODV.

d) Better performance produced in little modification.

e) Less memory overhead.

VI. Methodology For Evaluation

A. Simulation Environment

For the simulations, we use NS-2 (v-2.34) network simulator. NS-2 provides faithful implementations of the different network protocols. The implementation of the protocol has been done using C++ language in the backend and tcl language in the frontend on the Ubuntu Linux 10.04 operating system. At the physical and data link layer, we used the IEEE 802.11 algorithm. The channel used is Wireless Channel with Two Ray Ground radio propagation model. At the network layer, we use AODV as the routing algorithm. Finally, UDP is used at the transport layer. All the data packets are CBR (continuous bit rate) packets. The size of the packet is 512 bytes. The packets transmission rate is 1 Mbps. The connection pattern is generated using *cbrgen* and the mobility model is generated using *setdest* utility. *Setdest* generates random positions of the nodes in the network with specified mobility and pause time. The terrain area is 750m X 750m with 20 nodes with chosen maximum speed 20 m/s. The duration of time is 500sec.

B. Metrics used for Simulation

To analyze the performance of our solution, various contexts are created by varying the number of nodes and node mobility. In these simulations we used the following evaluation metrics:

1. **Packet delivery ratio (PDR):**
   The percentage of data packets delivered to destination with respect to the number of packets sent. This metric shows the reliability of data packet delivery.

2. **Packet Loss:**
   This metric informs us about the amount of control packets fails to reach its destination in a timely manner.

Performance comparison is made on the basis of above two metrics between existing AODV and proposed AODV.

1. **Packet Delivery Ratio (PDR):** PDR is the ratio of the number of data packets received by the destination to the number of data packets sent by the source. In the Fig. 4 it is clear that PDR of AODV is heavily affected by the malicious nodes where as the PDR of Proposed AODV is immune to it.

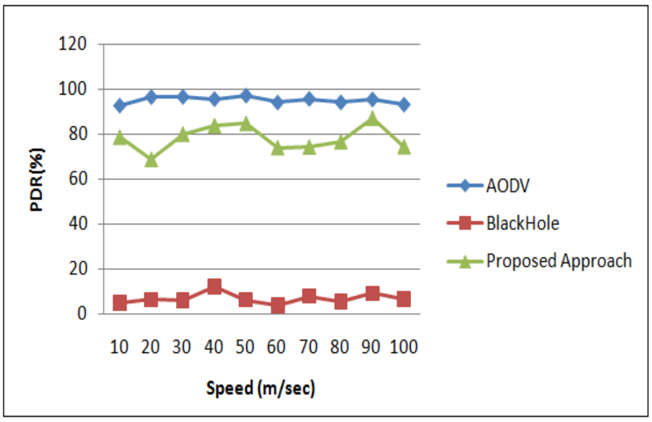

Fig. 4 Showing PDR (Packet Delivery Ratio)

2. **Packet Loss**
   This graph shown in Fig. 5 shows the packet loss for the each UDP connection in the simulation. We use total 9 UDP connections in the simulation. The graph concludes that there is very less packet lost percentile in the proposed AODV as compared to the AODV.

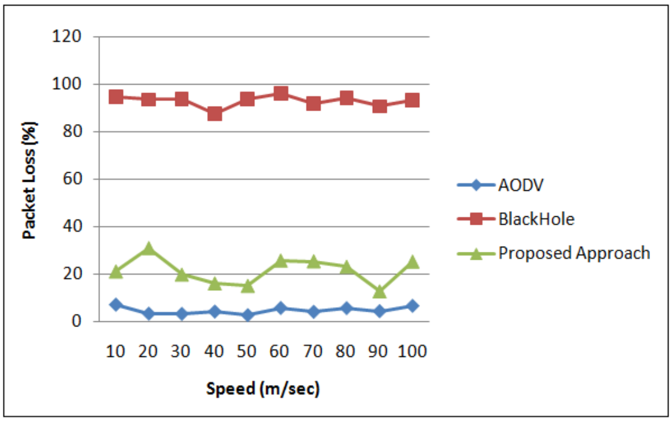

Fig. 5 Showing Packet Loss

VII. Conclusions

We propose an efficient and simple approach for defending the AODV protocol against Black Hole attacks. Thisproposed 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; check is made for whether there is large difference between the sequence number of source node or intermediate node who has sent back RREP or not? Generally the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely that node is the malicious node, immediately remove that entry from the RR-Table. In addition, the proposed solution may be used to maintain the identity of the malicious node as MN-Id, 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 analyse the performance of the proposed solution based on the various security parameters like mean delay time, packet overhead, memory usage, 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] Ebrahim Mohamad, Louis Dargin. “Routing Protocols Security.” In: Ad Hoc Networks”. A Thesis at Oakland University School of Computer Science and Engineering.

[2] Charles E. Perkins. Ad Hoc Networking. Addision Wesley, 2001.

[3] Tseng Y.C., Shen C.C, and Chen W.T. Mobile ip and ad hoc networks: An integration and implementation experience. Technical report, Deptartment. of Computer Sci. and Inf. Eng., Nat. Chiao Tung Univ., Hsinchu,, Taiwan, 2003.

[4] C. Perkins. "(RFC) request for Comments-3561", Category: Experimental, Network, Working Group, July 2003.

[5] Satoshi Kurosawal, Hidehisa, Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto. "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method." In: International Journal of Network Security, Vol. 5, No.3, pp.338–346, Nov. 2007.

[6] H. Deng, W. Li, and D. P. Agrawal. "Routing Security in Adhoc Networks." In: IEEE Communications Magazine, Vol. 40, No. 10, pp. 70-75, Oct. 2002.

[7] Mohammad Al-Shurman and Seong-Moo Yoon and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks" Publisher ACM press, pp 96-97, April 2004

[8] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", 2003 International Conference on Wireless Networks (ICWN 03), Las Vegas, Nevada, USA.

[9] Tamilselvan, L. Sankaranarayanan, V. "Prevention of Blackhole Attack in MANET", Journal Of Networks, Vol.3, No.5, May2008.

[10] Hesiri Weerasinghe and Huirong Fu, Member of IEEE, Preventing Cooperative Black Hole Attacks in Mobile Adhoc Networks: Simulation implementation And Evaluation, IJSEA, Vol2, No.3, July 2008.