Agent based AODV Protocol to Detect and Remove Black Hole Attacks

Roopal Lakhwani
ME (Software Systems)
Shri Ram Institute of Technology
Jabalpur, India

Sakshi Suhane
Assistant Professor
Shri Ram Institute of Technology
Jabalpur, India

Anand Motwani
Assistant Professor
NRI Institute of Research & Technology
Bhopal, India

ABSTRACT

A mobile ad hoc network (MANET) is a collection of mobile nodes and is autonomous having communication through the insecure wireless links. Security is very important issue for this type of networks because the nodes in the network dynamically add and join the network. This nature of nodes makes them vulnerable to malicious attacks. One of the widely adopted network routing protocols for Mobile Ad hoc Network (MANET) is AODV (Ad hoc on demand Distance Vector) protocol. Black hole attack is one such attack in which a malicious node makes use of susceptibility of Route Request (RREQ) packets of routing protocol to advertise itself with a fake Route Reply (RREP) message as having the shortest path to the destination node. Black hole attack has serious impact on routing and delivery ratio of packets. Most of the conventional methods to detect and avoid such attacks are likely to be suffered from high rate of errors in detection. To detect the black hole it is proposed to check the replies from all neighboring nodes to find the safe route but all such approaches suffered from high processing delay. In this paper we proposed a new approach called Agent based method to detect and eliminate black hole attack. Agent based method will not only efficiently detect the black holes but completely overcome the problem by eliminating the black hole from participating in MANET thus improving the security of the AODV. In simulation using NS - 2.33, the Agent based AODV has shown outstanding results as compared to AODV in presence of black holes. Results obtained from simulation have shown that Agent based method does not introduce high overhead for the duration of secure time (no attacks) and provide better performance during attack time (presence of Black hole) in the network.

General Terms

Black Hole Detection and Prevention

Keywords

Mobile Ad Hoc networks (MANET), AODV, malicious node, Black hole attack, RREQ, RREP.

1. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of wireless mobile nodes which have the ability to communicate with each other without having any centralized administration or fixed network infrastructure. In such networks, the routing protocols should be able to deal with dynamically changing node topology and handle information exchange among nodes. The major open issues of such networks are limited bandwidth, memory, reliable data delivery, processing capabilities and so these are more prone to malicious attacks. Common security attacks include replay attack, denial of Service (DoS), modification, masquerading, routing table overflow, impersonation, energy consumption, and so on [7]. One such attack is the Black Hole attack. In the Black Hole attack, a malicious node makes a false reply that it has the shortest route to the destination node and sender node starts to send data packets through this node. The black hole absorbs all data packets in itself, similar to a hole which sucks in everything in. Due to this, all packets in the network are dropped.

In the rest of the paper, next section briefly introduces the AODV routing protocol and discusses the effects of black hole attack on network performance. Section 3 gives the details about the black hole attack that we used in the implementation. Section 4 presents the proposed "Agent based AODV", a novel method to detect and eliminate black hole attack and modification to the AODV. Section 5 describes the simulation environment, simulation metrics, simulation results and analysis. Finally, the paper is concluded with conclusion and future work in Section 6.

2. PRELIMINARY STUDY ON AODV

The Ad hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multi hop routing between participating mobile nodes wishing to establish and maintain an ad hoc network [8]. AODV allows mobile nodes to exchange routing messages to obtain the routes quickly for new destinations and does not require nodes to maintain routes to destinations that are not in active communication. It makes sure that these routes do not contain loops and it also tries to find the shortest route possible. AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner [8]. In case of link breakages AODV notifies the affected nodes to invalidate the routes in routing table.

2.1 Route Discovery Process

In this, source node S will broadcast RREQ message to its neighbours in order to find the best possible path to destination node. Upon receiving RREQ message, the received node either:

a) reply to the source node with a RREP message if receiving node is the destination node or an intermediate node with a 'fresh enough' route information to the destination, or

b) update its routing table entry which may be used in the reverse path and rebroadcasting of RREQ message until destination node or intermediate node with 'fresh enough route' is reached .

On receiving RREQ message from intermediate node, destination node will reply with RREP message to source node by forwarding the message to intermediate node. In turn, node A will forward the message to source node. Once source node receives RREP message, it will process the message by calling AODV recvReply () function. This function will update the route entry for destination if either one of this condition is met.

a) The destination sequence number in routing table is less than destination sequence in RREP message or
b) The destination sequence number in routing table is equal with destination sequence number in RREQ message but with hop count is less than the one in routing table.

2.2 Types of Control packets

The Following control packets are used: Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV and these message types are received via UDP. HELLO messages are used for detecting and monitoring links to neighbours. When there is danger of unidirectional links preventing the completion of a route discovery cycle the Route Reply Acknowledgment (RREP-ACK) message format is used.

2.3. Sequence Number

A monotonically increasing number maintained by each node that initiates an AODV route discovery message to be processed and possibly retransmitted by other nodes in the adhoc network. The use of a destination sequence number for each route entry is one of the distinguished features of AODV. In [8] it is discussed that destination sequence number is created by the destination to be included along with any route information it sends to requesting nodes. It is also discussed in [8] that the destination sequence numbers ensures loop freedom and is simple to program.

3. BLACK HOLE ATTACK AND ITS EFFECTS ON NETWORK PERFORMANCE

3.1 Black Hole Attack

This attack is initiated by a type of malicious node that would participate in route discovery mechanism and try to become part of an active route [2]. A black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the data packets that need to be forwarded to destinations. These nodes would drop all the data packets received that they need to forward during whole simulation.

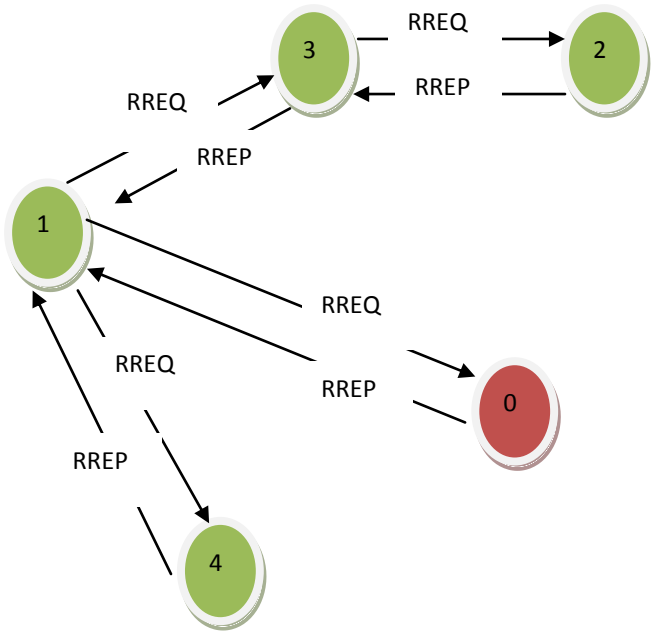

Figure 1 Normal operation of AODV

An example is shown as Figure 1, node 1 is the source node and node 2 represents the destination node. Node 0 is a malicious node who replies the RREQ packet sent from source node, and makes a false response that it has the shortest route to the destination node. Therefore node 1 wrongly judges the route discovery process with completion, and starts to send data packets through node 0. As what mentioned above, a malicious node probably drops or absorbs the packets. A source node updates its routing table for the new route to the particular destination node and discards any RREP message from other neighboring nodes even from an actual destination node. This malicious node can be regarded as a black hole problem in MANETs.

3.2 Effects of Black Hole Attack on Network Performance

After becoming part of an active route, the black hole attack nodes were constantly dropping data packets. So during black hole attack, the worst delivery ratio was reported. Generally, PDR is diminishing severely as a result of black hole attack [1] – [6], Generally, most methods discussed in [1, 3, 4, 6], and in many others there involved some overhead on intermediate and source node in terms of processing. So, to get better performance our proposed algorithm has the following objectives:

- Maximize packet delivery ratio.
- Minimize routing overhead.
- Maintain optimal end to end delay.
- Minimize packet drop.
- Efficient processing as no memory overhead.

4. PROPOSED ALGORITHM

Figure 2: Agent based AODV algorithm

AGENT BASED AODV

NODE INTIALIZATION BEGIN

AGENT IS SET UP to detect and eliminate black holes

//On receiving RREP, AGENT do the following task

recvReply(Packet P) {

IF (node itself is destination and the FLAG is set)

{

Normal operation carried out, as destination itself generated RREP

}

// If malicious node pretend as destination node

ELSE IF (node itself is the destination and the FLAG is not set)

{

Detection of malicious node is done by AGENT at source node

Simply discard the RREP as it may be generated by malicious node.

Eliminate such nodes from route

}

// If malicious node claims to have shortest route

ELSE IF (node is the intermediate hop AND having route AND FLAG is set)

{

Detection of malicious node is done by AGENT

Simply discard the RREP as it may be generated by a normal node and intermediate node may send / forward it maliciously.

Eliminate such nodes from route

}

ELSE IF (node is the intermediate hop AND having route AND FLAG is set)

{

Agent checks for malicious behavior and if not detected then

Simply forwards the RREP towards source node.

Normal operation carried

}

Agent is a basically process running at mobile node.

AODV is designed for use in networks where the nodes can all trust each other, either by use of preconfigured keys, or because it is known that there are no malicious intruder nodes [8]. Based on the facts discussed in Section 2 and 3, a protocol which is the enhancement of AODV is proposed. The "Agent based AODV" is designed to achieve the objectives mentioned in Section 3. The proposed solution will employ minimum modification to existing AODV algorithm.

Two new modifications are proposed to improve the existing AODV

1) *sendReply()* function to accommodate flag in RREP packet,

2) Agent to detect malicious nodes in *recvReply()* function.

This modified algorithm will help in identifying the malicious nodes and also prevent them to participate in the network.

The algorithm used to detect black holes is explained in Fig. 2.

5. SIMULATION SYUDY

5.1 Simulation Setup

A simulation model was developed using network simulator NS-2 [10] (version 2.33) on Red Hat Enterprise Linux (RHEL) – 5. In our simulation environment, Two Ray Ground radio propagation model for Wireless Channel along with the IEEE 802.11 standard is used at the physical and data link layer. At the network layer AODV is used as the routing protocol. Two AODV conditions are considered 1) normal AODV with black hole attack and 2) "Agent based AODV" with black hole attack. UDP is used at the transport layer protocol and for data packet transmission at application layer, CBR (constant bit rate) packets is used. The size of the packet is 512 bytes and transmission rate is set at 2 Mbps. In the simulation model, the topological area is fixed to 500m x 600m for all simulations .The number of nodes taken for simulation is 10 in three different mobility scenarios. The mobility model is generated having the node movement varied from 1 to 20 m/s. The simulation parameters are summarized in Table 1.

TABLE 1: SIMULATION PARAMETERS

Parameter	Value
Simulator	NS-2 version 2.34
Simulation Time	120s
Number of nodes	10
Number of Mobility Scenarios	3
Channel type	Wireless

Radio-propagation model	Two Ray Ground
Antenna type	Omni antenna
Transmit range	250m
MAC type	802.11
Routing protocol	AODV
Transport layer protocol	UDP
Traffic model	CBR
CBR packet size	512 bytes
Packet rate	10 packets/sec
Number of connections	2
Pause time/Mobility	10
Speed	1 to 20m/s
Average speed	5.20 m/s
Topology	500x600
No. of malicious node	2

5.2 Simulation Metrics

Four important metrics were used to evaluate the result of the experiments and the details are as follows:

Packet Delivery Ratio (PDR): The ratio of total packets that were received at destination nodes, to the total packets that were sent by the source nodes in a predefined simulation time.

Network Routing Load (NRL) [5]: The percentage of total routing packets and total data packet ratio transmitted in the network.

Average End-to-End Delay (Delay): The average delay time (milliseconds) spent to deliver each data packet between sender and recipient. It includes all delays caused during route discovery, buffering, processing at intermediate nodes and retransmission delays at the MAC layer, etc.

Number of Packet Dropped: Total number of MANET packets dropped out of total number of generated packets.

5.3 Simulation Results and Analysis

Fig. 3, Fig. 4, and Fig. 5 compare between the packet delivery ratios, network routing load and average end to end delay in both 1) normal AODV with black hole attack and 2) "Agent based AODV" with black hole attack. By implementing Agent based method in AODV, the result shows marked improvement during attack time.

Fig. 3 shows that the PDR in normal AODV during attack time has dropped nearly upto 48%. By implementing Agent based method in AODV, the result shows marked improvement where the PDR increases up to 99% (during attack time). Furthermore, while considering individual scenario this rise varies from 20% to 100%.

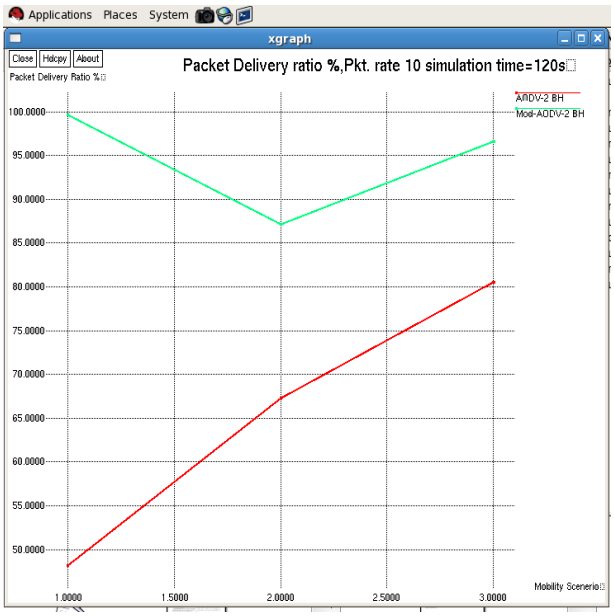

Figure. 3: Packet delivery ratio, in the mobility scenarios

Fig. 4 shows significant change in NRL which means that there is less overhead during attack time.

Fig. 4 shows that the NRL in normal AODV during attack time goes nearly upto 0.06. By implementing Agent based method in AODV, the result shows marked improvement where the NRL decreases upto 0.01(during attack time). Furthermore, average improvement is of 0.03, i.e. 100%.

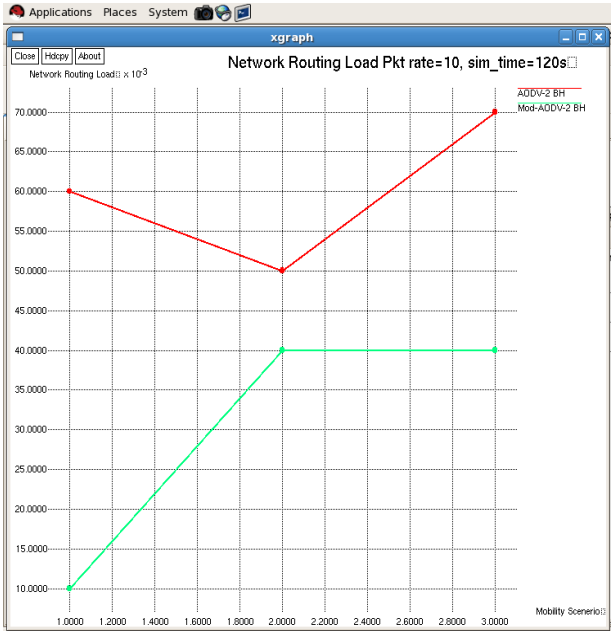

Figure.4: Network routing load, in the mobility scenarios

Fig. 5 shows the marginal rise in average end-to-end delay in few scenarios in Agent based AODV during attack time. But

it can be seen that the average improvement in end to end delay in both conditions is about 10%.

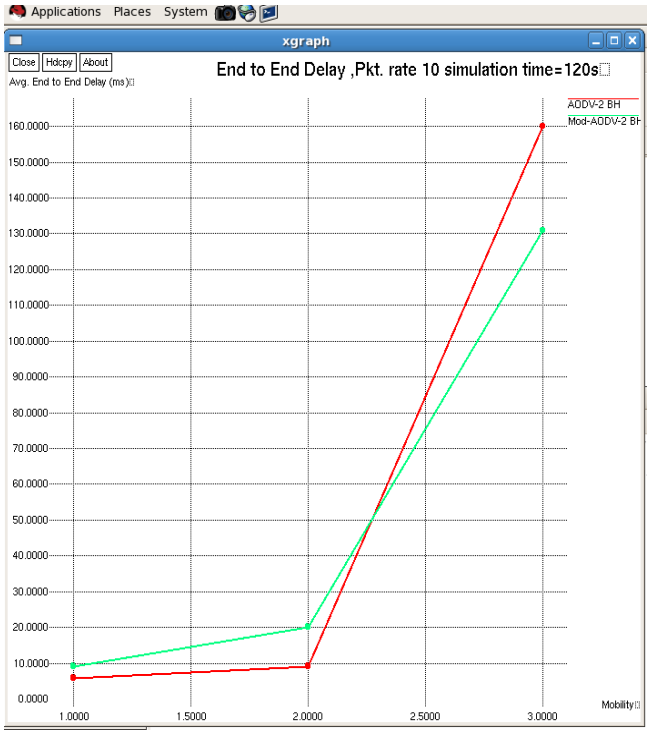

Figure. 5: Average end to end delay, in the mobility scenarios

6. CONCLUSION AND FUTURE WORK

In this paper we have studied the routing security issues of MANETs, described the black hole attack that can be mounted against a MANET and proposed a feasible solution for it in the AODV protocol. The results have shown that proposed algorithm will not only help in identifying the malicious nodes but suitably preventing them to participate in the network. Also, the algorithm is evaluated against various performance metrics. With appropriate implementation and simulation using NS-2.33, our analysis shows significant improvement in Packet Delivery Ratio (PDR) of AODV in presence of Black hole attacks, with marginal rise in average end-to-end delay in few scenarios. The number of data packets dropped is drastically reduced with our proposed solution.

As a piece of future work, the proposed solution can be applied to 1.) Identify Collaborative black hole attacks [9] in a MANET; and 2.) Discover secure paths from source to destination by avoiding Collaborative black hole nodes. More enhanced intrusion detection mechanism will be performed that could perfectly detect Collaborative attacks if applied on the MANET. And then, the new enhanced security mechanism will be evaluated using the same performance metrics and other network parameters such as network size and node's transmission range. As future work, we intend to develop simulations to analyze the performance of the proposed solution.

7. REFERENCES

[1] Htoo Maung Nyo, Piboonlit Viriyaphol "Detecting and Eliminating Black Hole in AODV Routing" 978-1-4244-6252-0/11/2011 IEEE

[2] Mohammed Saeed Alkatheiri, Jianwei Liu and Abdur Rashid Sangi, "AODV Routing Protocol Under Several Routing Attacks in MANETs" 978-1-61284-307-0/11/2011 IEEE

[3] Kitisak Osathanunkul and Ning Zhang, "A Countermeasure to Black Hole Attacks in Mobile Ad hoc Networks" 2011 International Conference on Networking, Sensing and Control Delft, the Netherlands, 11-13 April 2011

[4] Mohammad Taqi Soleimani, Abdorasoul Ghasemi, "Secure AODV against Maliciously Packet Dropping", IEEE

[5] Kamarularifin Abd Jalil & Zaid Ahmad, Jamalul-Lail Ab Manan, "Securing Routing Table Update in AODV Routing Protocol" 2011 IEEE Conference on Open Systems (ICOS2011), September 25 - 28, 2011, Langkawi, Malaysia

[6] Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Rosilah Hassan, "A Local Intrusion Detection Routing Security over MANET Network" 2011 International Conference on Electrical Engineering and Informatics 17-19 July 2011, Bandung, Indonesia.

[7] H. Deng, W. Li, and D. P. Agrawal. Routing security wireless ad hoc networks. IEEE Communications Magazine, 2(1), 2002.

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

[9] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks" Tseng et al. Human-centric Computing and Information Sciences 2011, 1:4 http://www.hcis-ournal.com/content/1/1/4

[10] Network Simulator 2. http://isi.edu/nsnam/ns/.