ISSN:0975-9646

Simulation of Misbehaving Nodes in AODV Routing

Shweta Rohilla

Department of Computer Science & Engineering
ABES Engineering College, Ghaziabad, India

Pankaj Sharma

Department of Information Technology
ABES Engineering College, Ghaziabad, India

***Abstract*— Ad hoc On Demand Vector (AODV) is a reactive routing protocol in Mobile Ad hoc Network (MANET). As we know this protocol has been used entirely, but there are still some security issue in it so it becomes susceptible to various attacks such as black hole, which excessively affects the performance of the mobile ad hoc network. Thus in this paper, an attempt has been made to uncover the blackhole node and retain the network against them. The proposed algorithm not only work against the blackhole but also against nodes which are greedy or selfish in the network. Simulations have been carried out using NS2. Simulation results show that the proposed algorithm is better in defending against such malicious nodes.**

***Keywords*— AODV Protocol, MANET, Greedy Nodes, Black Hole Attack.**

I. INTRODUCTION

A mobile ad hoc network is a collection of mobile nodes with no infrastructure. It is self-organizing system of mobile nodes that communicate with each other. Each node in a MANET is free to move independently in any direction in the network. MANET has received spectacular consideration because of their self-configuration and self-maintenance [1]. Various mobile ad hoc network protocols has been surveyed which are based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

Figure 1. Wireless Mobile Ad-hoc Network

In MANET, nodes are limited size and battery imposes limitation on the power capacity as well as transmission range. So, design of network protocols in ad hoc networks becomes demanding due to limited processing power and storage. The main aim of any protocol is to maximize performance with minimum resource usage. The performance depends upon hop count, delay loss rate, throughput [2]. The nature of MANET is an influential so it changes dynamically, so it is defenceless for ample amount of attack. The Characteristics of MANET acts as both threat and convenience in carrying out the security goals.

II. AD HOC ON-DEMAND DISTANCE VECTOR ROUTING PROTOCOL

A routing protocol determines how mobile nodes will communicate with each other, propagating of information that enables them to select routes between any two nodes of the network. Route will be preferred the choice by routing algorithms. In this paper we focus on Ad hoc On-demand Distance Vector (AODV) protocol which is one of the reactive ad hoc routing protocols in MANET. As it is a Reactive (On-demand) protocols. It works as follows:

- Discover routes when needed
- Source-initiated route discovery

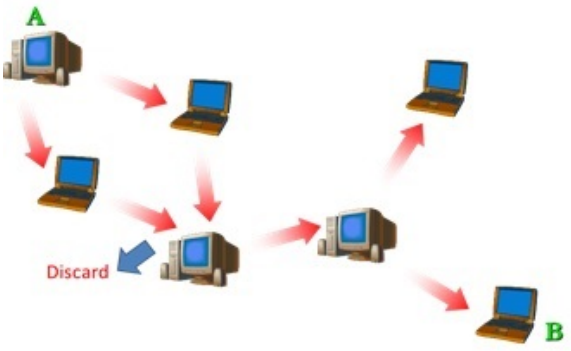

Figure 2. AODV Protocol – Route Request (RREQ)

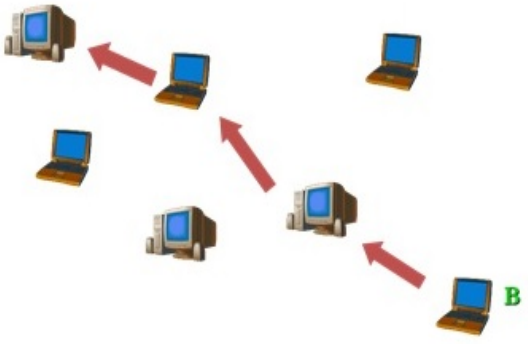

Figure 3. AODV Protocol – Route Reply (RREP)

The AODV protocol uses different types of messages to discover and maintain routes to destination. In this the process is to discover the route to the destination node. It finds a route to that node it broadcasts a Route Request message (RREQ) to all its neighbors and they transmit the packet to their neighbors and so on until they reach to the destination or any intermediate node which has a 'fresh' route to the destination. When the route becomes invalid or lost, AODV will again issue a request. Each node maintains two counters: the sequence number and the broadcast ID which is incremented when a broadcast is started in the node. The copies of the same RREQ received later which are coming from the other neighbors are deleted.[4] The intermediate nodes or destination nodes send RREP (route reply packets), if they have a fresh route to the destination with a sequence number greater or equal to the sequence number of the RREQ.

III. Malicious Nodes and Their Effects

MANET is sensitive to many 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 [5]. A node which receives the data packet but does not forward it is termed as Black hole and a node may behave selfishly by agreeing to forward the packets and then failing to do so due to Overloaded, Selfish, Malicious or Broken. Selfish or Misbehaving nodes attempt to benefit from other nodes, but refuse to share its own resources. The behavior of such nodes are termes as selfishness or misbehavior. In Blackhole attack, all network traffics are redirected to a specific node which does not exist at all. Because traffics disappear into the special node as the matter disappears into Blackhole in universe [6]. The motive of the malicious nodes could be to delay the path finding process or to inhibit all the data packets being sent to the destination node. The misbehaving node can use the network when it needs to use it and after using the network it turn back to its silent mode. In the silent mode the selfish node is not visible to the network.

RREQ and RREP traversal of messages are shown in fig.4. S is considered as source node and D is considered as Destination node. Therefore, node S propagates RREQ to its neighboring nodes and nodes are responding as RREP. Destination Sequence Number [15] is a 32-bit integer and is used to conclude the freshness of route. The larger the sequence number, the fresher is the route. A route to node D, they will again send the RREQ message. A request message is broadcasted and is received by node M (which is a malicious node in the network). Thus, malicious node will generate a false RREP message and send it to node C with a very high destination sequence number, that will forwarded to source node. Now we have high sequence number, and this route is considered as a fresh route. Hence node S would now start sending packets to node C and it will send the same packets to the node M. Since the node S has a RREP message with that route, therefore it will instantly ignore genuine RREP control messages.

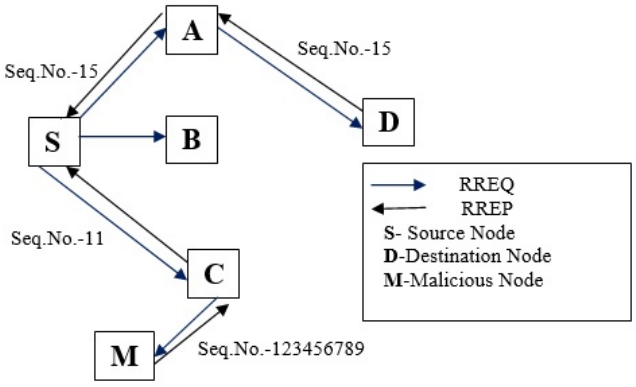

Figure 4. Black hole Attack in AODV

IV. Problem and Proposed Algorithm

Misbehaviour node is one that admits to perform route forwarding packets but then frantically drops all data packets that are routed through it. It arises for several reasons. When a node is faulty, its inconsistent behavior can deviate from the protocol and thus produce non intentional misbehavior. Intentional misbehavior aims at providing an advantage for the misbehaving node. An advantage for a malicious node arises when misbehavior enables it to mount an attack.

Without appropriate countermeasures, the effects of misbehavior have been shown to dramatically decrease network performance. Depending on the proportion of misbehaving nodes and their specific strategies, network throughput can be severely degraded, packet loss increases, nodes can be denied service, and the network can be partitioned. These detrimental effects of misbehavior can endanger the functioning of the entire network.

The problem we want to solve is that how we can keep an existing network functional system working by neglecting the presence of misbehaving nodes when other nodes do not route and forward correctly.

A. Proposed Solution

In the proposed solution we define two type of nodes, type 0 for the non-malicious node and type 1 for malicious node and we define two threshold value for the comparison of the node i.e. the node is malicious or non-malicious.

1) Evolution of Threshold value th1 and th2:

Threshold 1 th1 = gp/10
Threshold 2 th2 = th1/(gp-th1)
gp →Total Generating Packets or Total Data Packets Send

In the algorithm if the node type is 1 than number of drop packets checked by the threshold th1, if drop packets are greater than th1 and ratio of dropped packet to the forwarded packet is infinity or large value i.e. if number of forward packet is zero than it confirms the node is black hole node. And if ratio of dropped packet to the forwarded packet is greater than threshold th2, it simply imply that the node is misbehaving.

V. Simulation Scenario

The simulation scenario and parameters used for performing the detailed analysis of misbehaving nodes in MANET AODV routing protocols are as follows. We have used NS-2 simulator for our assessment. In our simulation model, nodes are placed randomly within a 2000m x 2000m physical terrain area. We choose a square area in order to allow nodes to move more freely with equal node density. The physical characteristics of each mobile node such as transmitted power, received power of the destination antenna, antenna gain, and radio frequency were chosen to approximate value. We have chosen IEEE 802.11 as MAC protocol, IP as network protocol and UDP as transport protocol. CBR (constant bit rate) is used to generate the traffic source with packet size of 512 bytes and traffic flow of 12 pkts/sec.

The following details describes how the performance parameters have been evaluated to simulate the routing protocols.

A. *Following files have been used for simulation:*

1) *Input to Simulator:*
   - Scenario File – Movement of nodes.
   - Traffic pattern file.
   - Simulation TCL file
2) *Output File from Simulator:*
   - Trace file
   - Network Animator file
3) *Output from Trace Analyzer Program:*
   - Text file containing output

B. *Generation of Traffic Pattern File:*

Ns cbrgen.tcl [-type cbr|tcp] [-nn nodes] [-seed seed] [-mc connections] [-rate rate]> [file name]

C. *Generation of Scenario File:*

./bm -f<scenario_file_name> <mobility model> -n <num_of_nodes> -d<duration> -x <maxx> -y <maxy> -h<highest_mobility_speed> -l<lowest_mobility_speed> -p <pause_time> -s<seed>

D. *Trace Analyzer Program:*

We develop a program in JAVA language for analysing the trace file generated after simulating the TCL network script using the NS-2.34. The trace analyser program reads the trace file and produce the output in the form of text file containing packet delivery ratio, routing load, mac load, and delay.

VI. Result

RFC 2501 describes a number of quantitative metrics that can be used for evaluating the performance of a routing protocol for mobile wireless ad hoc networks. In this paper we use two quantitative metrics. The throughput is the most important for the best-effort traffic and the normalized MAC load is a measure of the effective utilization of the wireless medium for data traffic.

A. *Throughput:*

In communication networks, such as Ethernet or packet radio, throughput or network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

B. *Normalized MAC Load:*

The normalized MAC Load is defined as the fraction of all control packets (routing control packets, Clear-To-Send (CTS), Request-To-Send (RTS), Address Resolution Protocol (ARP) request and replies and MAC ACKs) over the total number of successfully received data packets. This is the metric for evaluating the effective utilization of the wireless medium for data traffic. We count al the send events with agent type MAC and packet type RTS, CTS, ARP and ACK and add to this number the sum of all control routing packets. To calculate the normalized MAC load, we divide the sum of all control packets (MAC and routing control packets) by the number of received packets.

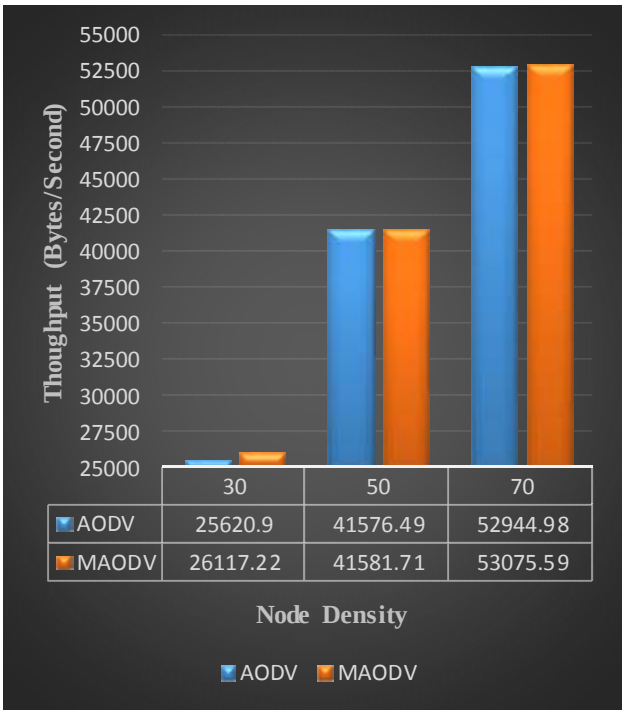

Fig. 4 Throughput vs Node Density for pause time p = 10 sec.

Figure 4 and 5 shows the throughput for the 30, 50, 70 number of nodes with the pause time of 10 sec and 25 sec respectively. Figure 4 shows the simulation under the original AODV protocol while figure 5 shows the simulation under the modified AODV protocol with the same parameter. Both the protocols are simulate under the presence of the black hole node and some misbehaving node. Here throughput is calculated in bytes per second.

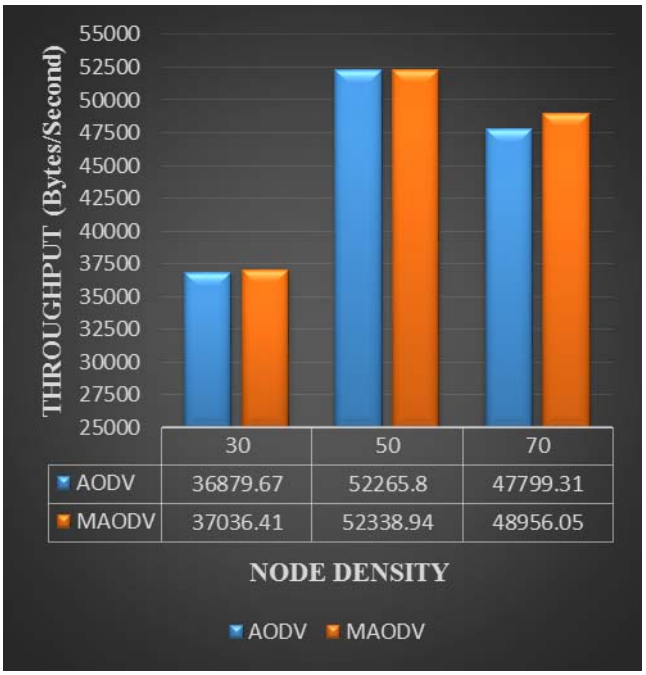

Fig. 5 Throughput vs Node Density for pause time p = 25 sec.

Figure 6 shows the normalized routing load for the 30, 50, 70 number of nodes for the pause time of 10 under the original AODV protocol and modified AODV protocol.

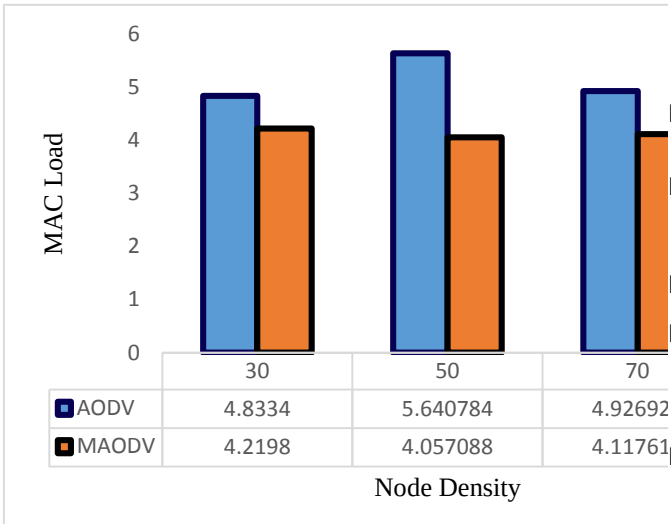

Fig. 6 Normalized MAC Load vs Node Density

The simulation shows that the throughput is higher for the modified AODV as compare to the original AODV under the different circumstances and normalized routing load is lower for the modified AODV protocol because the modified AODV successfully detects the presence of the black hole and misbehaving nodes.

VII. CONCLUSIONS

In this paper, the issue of misbehaviour of node and its effect on the AODV routing protocol has been discussed. A method to overcome this problem have been proposed. The route discovery process in the AODV is vulnerable to black hole attack and therefore, it is crucial to have an efficient security method built into the AODV protocol in order to reduce the effect of such attacks.

Thus it can be concluded that the approach presented in this paper successfully detects the presence of the black hole nodes and also the misbehaving nodes, which didn't send the data packet to the black hole node and ensures that the flawless and reliable route has been found out with the greater throughput and less normalized MAC load.

REFERENCES

[1] Sowmya K.S, Rakesh T. and Deepthi P Hudedagaddi, "Detection and Prevention of Blackhole Attack in MANET Using ACO" *International Journal of Computer Science and Network Security*, VOL.12 No.5, May 2012.

[2] S.J Lee., M. Gerla. and C.K. Toh, "A Simulation study of Table driven and On demand Routing Protocols for mobile Ad hoc Networks"

[3] Kamarularifin Abd. Jalil, Zaid Ahmad and Jamalul-Lail Ab Manan, "Mitigation of Black Hole Attacks for AODV Routing Protocol" *International Journal on New Computer Architectures and Their Applications (IJNCAA)* 1(2): 336-343 The Society of Digital Information and Wireless Communications, 2011 (ISSN: 2220-9085)

[4] Shilpi Jain, Alankar Shastri, Brijesh Kumar Chaurasia "Analysis and Feasibility of Reactive Routing Protocols with Malicious Nodes in MANETs"

[5] K. Lakshmi, S.Manju Priya, A.Jeevarathinam, K.Rama, and K. Thilagam "Modified AODV Protocol against Blackhole Attacks in MANET" *International Journal of Engineering and Technology* Vol.2 (6), 2010, 444-449

[6] Sheenu Sharma, Roopam Gupta "Simulation Of Blackhole Attack in the Mobile Ad Hoc Networks"

[7] Nital Mistry, Devesh C Jinwala, *Member, IAENG*, Mukesh Zaveri, "Effect of Black Hole Attack on MANET Routing Protocols" Proceedings of the international MultiConference of Engineers and Computer Scientists 2010 Vol II. IMECS 2010, March 17-19, 2010, Hong Kong

[8] Jaspal Kumar, M. Kulkarni, Daya Gupta, "Effect of Black Hole Attack on MANET Routing Protocols" *I. J. Computer Network and Information Security*, 2013, 5, 64-72 Published Online April 2013 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2013.05.08