ISSN:0975-9646

Investigating the Impact of Malicious Node on the Performance of AODV Routing Protocol in MANETs

P.V.Venkateswara Rao[*1], S. Pallam Shetty[*2],

[1]*Research Scholar,* [2]*Professor,*
[1]*Dept. of CS&SE, AUCE (A),* [2]*Dept. of CSE,*
[1]*JNTUK,* [2]*Andhra University,*
[1]*Kakinada-533003,* [2]*Visakhapatnam-530003,*

Abstract – Ad hoc network is a collection of wireless nodes forming a temporary network without the use of any network infrastructure. In MANETs, malicious node can deny a valid route to a particular node. Malicious node intentionally drops the data or control packets whatever they receive and also advertises correct path to destination and drops packets. It can intentionally send unnecessary route error messages and nullifies the presence of the nodes. In AODV routing protocol, in the route discovery process malicious node can add fake information or may drop some data packets. In this paper, an attempt has been made to investigate the impact of the malicious node on the performance of a prominent on demand routing protocol i.e., AODV. The performance is analysed in terms of throughput, and delay. From the experimental results, it is observed that the impact of malicious node on the performance is minimum at higher simulation time and maximum at lower simulation time. Further it is observed that there is no impact of malicious node on the performance of the AODV routing protocol at 2000sec Simulation time.

Keywords: ***MANETs, Malicious Node, AODV, OPNET modeler, throughput, delay, Simulation time.***

I. INTRODUCTION

An ad-hoc network is a collection of wireless mobile nodes that forms a temporary network without any centralized administration. In such an environment, it may be necessary for one node to enlist other hosts in forwarding a packet to its destination due to the limited transmission range of wireless network interfaces. Each mobile node operates not only as a host but also as a router forwarding packets for other mobile nodes in the network that may not be within the direct transmission range of each other. Each node participates in an ad-hoc routing protocol that allows it to discover multi-hop paths through the network to any other node. This idea of mobile ad-hoc network is also called infrastructure less networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly.

There has been a tremendous growth in the use of wireless communication in the past few decades. Mobile Ad hoc Network (MANET) is one of the most important one among various wireless communication mechanisms. In MANET [1], each node in a network performs as both a transmitter and a receiver. They rely on each other to store and forward packets. Its unique infrastructure less network and self-configuring capability makes it ideal for many mission critical applications, including military use and remote exploration. However, these characteristics also make MANET vulnerable to passive and active attacks [4], [5], [8], [9] due to its open medium, changing topology and lack of centralized monitoring. To address the new security challenges, Intrusion Detection System (IDS) is required to detect the malicious attackers [3] before they can accomplish any significant damages to the network.

If malicious nodes are present in a MANET, they may attempt to reduce network connectivity (and thereby undermine the network's security) by pretending to be cooperative but in effect dropping any data they are meant to pass on. These actions may result in defragmented networks, isolated nodes, and drastically reduced network performance. We aim to evaluate the added effect of the presence of malicious nodes on ad hoc network performance.

Performance can be evaluated by some of the Quality of Service (QoS) parameters such as throughput, cumulative sum of number of received packets and end to end delay

This paper is organized as follows: In Section II, **AODV routing protocol** is discussed. Section III includes **Methodology** followed. In Section IV **Simulation and Parameter setting** is provided**.** In Section V incorporates **Results and Analysis.** In section VI **Conclusions and Future Scope of Work** is discussed.

II. AODV ROUTING PROTOCOL

Ad hoc On-Demand Distance Vector (AODV) routing protocol is a reactive routing protocol [2], [7] that creates a path between source and to destination only when required. Routes are not established until any node sends route discovery message that the node want to communicate or transmit data with other node in the network. Routing information is stored in source node and destination node, intermediate nodes dealing with data transmission. This Approach reduces the memory overhead, minimize of the network resources, and runs well in high mobility scenario. The communication between nodes involves main three procedures known as path discovery, Path establishment and path maintenance. Three types of control messages are used to run the algorithm, i.e. Route Request (RREQ), Route Reply (RREP) and Route Error (RERR).

Route Request and Route Reply

- Route Request (RREQ) includes the last known sequence number for the destination
- An intermediate node may also send a Route Reply (RREP) provided that it knows a more recent path than the one previously known to sender, Intermediate nodes that forward the RREP, also record the next hop to destination
- A routing table entry maintaining a reverse path is purged after a timeout interval
- A routing table entry maintaining a forward path is purged if *not used* for a *active_route_timeout* interval

Link Failure and Route Error

- A neighbor of node X is considered active for a routing table entry if the neighbor sent a packet within *active_route_timeout* interval which was forwarded using that entry
- Neighboring nodes periodically exchange hello message
- When the next hop link in a routing table entry breaks, all active neighbors are informed
- Link failures are propagated by means of Route Error (RERR) messages, which also update destination sequence numbers

Route Maintenance:

The two endpoints of a failed link are transmitted to the source in a route error packet. Upon a receiving a RERR packet a node invalidates all the routes going through that link. If the route is invalidated and it is needed, a new route must be discovered. Extensive use of caching.Transmitting packets or sending back replies make me learn routes.A node that knows a route to a given destination(has a route source in cache)can immediately answer a RREQ.Security is a very dangerous point in mobile communication. AODV defines no special security mechanisms. So an impersonation attack can easily be done.

III. METHODOLOGY

Several researchers have been proposed several solutions to support QoS [6] in the dynamic MANET environment but they are not taking care about the provisioning of security requirements in hand held devices where the resources are scare. To evaluate the designs proposed in this paper, to choose the most suitable evaluation methodology. Three evaluation methodologies were identified

1. Simulation,
2. Experimental and
3. Mathematical

Simulation was chosen, as experimental methodology was not practicable and mathematical methodology is highly restrictive. The research method was to evaluate, collection of the results, and the results were analysed and compared with those from the work, conclusions were drawn from evaluations of the identified.

IV. SIMULATION AND PARAMETER SETTING

We use OPNET as a simulator. OPNET adapts three hierarchical modelling mechanisms including network domain, node domain and process domain. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.

Table 1. Simulation Scenario Parameters

Parameter	Value
Simulator	OPNET
Routing Protocol	AODV, MAODV
No.of Nodes	50
Area Size	1000*1000
Traffic Model	CBR
Packet Size	1024
Mobility Model	Random Way Point
Transmission Range	50
Route Request Retries	0 , 5
Simulation Time	500,1000 ,1500,2000, 2500,3000 sec

In our simulation, 50 mobile nodes move in a 1000 meter x 1000 meter square region for 60 seconds simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 50 meters. In our simulation, the speed is varied from 15 m/s to 55m/s. The simulated traffic is Constant Bit Rate (CBR).Our simulation settings and parameters are summarized in table 1.

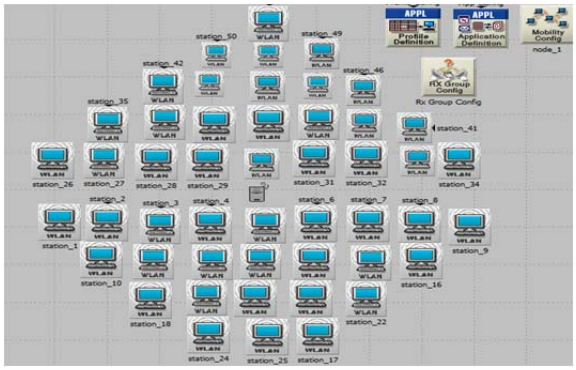

Figure 1 Simulation Scenario without Malicious Nodes for Execution

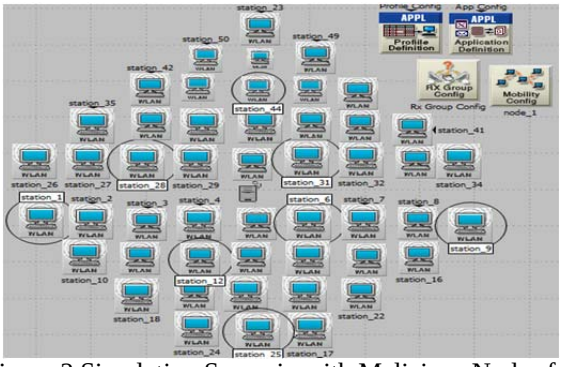

Figure 2 Simulation Scenario with Malicious Nodes for Execution

V. RESULTS AND ANALYSIS

Our simulation model was carried out using the OPNET Modeler 17.5. It is a useful research tool for achieving good simulation results. Each cycle of the simulation runs for 20 minutes. The simulated network consists of 50 randomly allocated nodes in a space of 1000*1000 square-meters. All scenarios are run under identical mobility and traffic conditions.

Impact of malicious node is discussed. Experiment results show that performance of AODV decreases when malicious nodes are present. In order to compare the performance of AODV – four scenarios are created.

Case 1: In AODV, in the absence of malicious node by varying the simulation time from 500 seconds to 3000 seconds the minimum throughput is 9159 bits/sec, the maximum throughput is 12467 bits/sec and the variance in throughput is 3308 bits/sec.

Case 2: In MAODV, in the presence of malicious node by varying the simulation time from 500 seconds to 3000 seconds the minimum throughput is 8681 bits/sec, the maximum throughput is 12246 bits/sec and the variance in throughput is 3565 bits/sec.

Case 3: In AODV, in the presence of malicious node by varying the simulation time from 500 seconds to 3000 seconds the minimum delay is 0.001092 sec, the maximum delay is 0.001192 sec and the variance in throughput is 0.0001sec.

Case 4: In MAODV, in the presence of malicious node by varying the simulation time from 500 seconds to 3000 seconds the minimum delay is 0.001012 sec, the maximum delay is 0.001152 sec and the variance in throughput is 0.00014 sec.

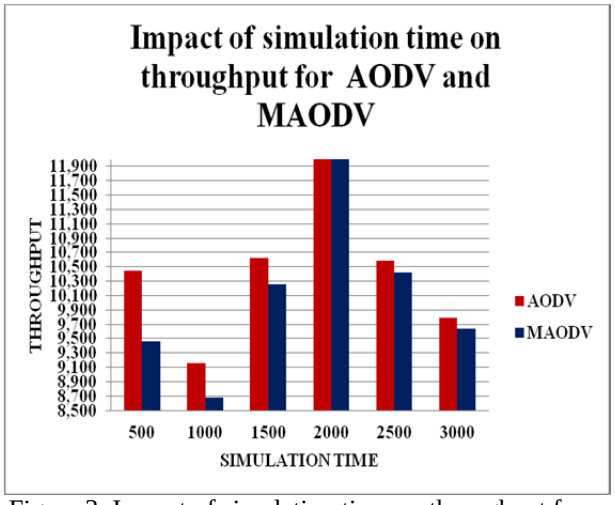

Figure 3: Impact of simulation time on throughput for AODV and MAODV

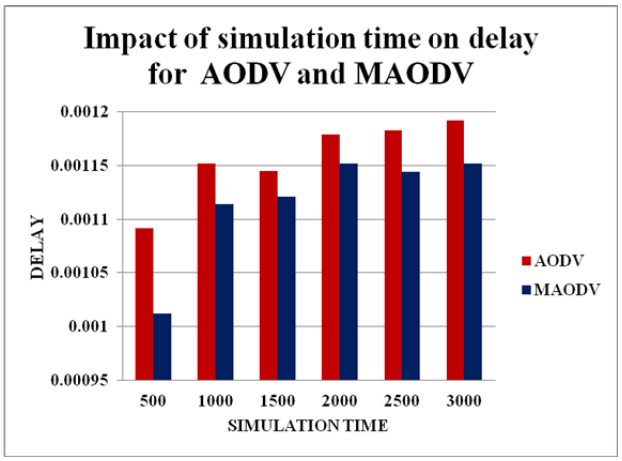

Figure 4: Impact of simulation time on delay for AODV and MAODV

VI. CONCLUSION AND FUTURE SCOPE OF WORK

It is observed that the impact of malicious node on the performance is minimum at higher simulation time and maximum at lower simulation time. Further it is observed that there is no impact of malicious node on the performance of the AODV routing protocol at 2000sec Simulation time In the future scope of work, we would extend different types of attacks on different routing protocols in MANETs.

REFERENCES

[1] I. Chlamtac, M. Conti, and J.-N. Liu, “Mobile ad hoc networking: imperatives and challenges,” Elsevier Ad Hoc Networks Journal, vol. 1, pp. 13–64, 2003.

[2] Hongbo Zhou "A Survey on routing protocols in manets”: Technical report: MSU-CSE-03-08 mar 28,2003

[3] P.V.VenkateswaraRao, S. Pallam Shetty, Investigating the impact of Black hole attack on AODV Routing protocol in manets under responsive and non-responsive traffic . International Journal of computer Applications(0975-8887) Vol 120.,NO 22 JUNE 2015

[4] Khairul Azmi Abu Bakar and James Irvine “Contribution Time-based Selfish Nodes Detection Scheme” ISBN:978-1-902560-24-3 © 2010 PGNet.

[5] Dipali Koshti, Supriya Kamoji “Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks”, (IJSCE) ISSN: 2231-2307, Volume-1, Issue-4, September 2011

[6] Venkataramana Attada, and S. Pallam Setty, “Cross Layer Design Approach to Enhance the Quality of Service in Mobile Ad Hoc Networks” Wireless Personal Communications, DOI 10.1007/s11277-015-2609-6, May 2015, Springer.

[7] Sunil Taneja and Ashwani Kush, “A Survey of Routing Protocols in Mobile Ad Hoc Networks”, International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010 ISSN: 2010-0248.

[8] P.V.VenkateswaraRao, S. Pallam Shetty, Investigating the impact of Selfish node on AODV Routing protocol in manets in the context of Simulation time. International Journal of computer & organization trends. Vol .21, No 1 JUNE 2015.

[9] Amandeep Kaur1 , Hardeep Singh2,” A Study of Secure Routing protocols”, International Journal of Application or Innovation in Engineering & Management (IJAIEM) ISSN 2319 – 4847 Volume 2, Issue 2, February 2013.