Investigating the Impact of Selfish Node on AODV Routing Protocol in MANETs in the Context of Simulation Time

P.V.Venkateswara Rao,
Research Scholar,
Dept. of CSE,
JNTUK,
Kakinada-53300,

S. Pallam Shetty,
Professor,
Dept. of CS&SE, AUCE (A),
Andhra University,
Visakhapatnam-530003,

Abstract -- *Mobile Ad hoc networks (MANETs) are a set of wireless mobile nodes which dynamically connect and transfer information. The open and dynamic operational environment of MANETs makes it vulnerable to various attacks. In this paper, an attempt has been made to investigate the impact of selfish node on the performance of AODV routing protocol by varying simulation time through OPNET Modeler version 17.5. Experimental results reveal that by varying simulation time, the performance of routing protocol without selfish node also varies, to obtain the steady state behaviour of a routing protocol the selection of simulation time plays a vital role. The minimum value to obtain the steady state behaviour through results is observed as 1500 sec. The impact of selfish node on performance of the throughput degrades by 40 times of the original AODV throughput. Similarly, the delay is reduced by more than 1000 times. The impact of the simulation time on the performance of the variance in throughput of AODV routing protocol with and without the selfish node is 2532 and 98 and delay in variance is 0.00012 and 0.00000376 sec.*

Keywords**:** *MANETs, Selfish Node, AODV, OPNET Modeler, throughput, delay, Simulation time.*

I. Introduction

MANETs are infrastructure less networks with a collection of multi hop wireless mobile nodes forming a temporary network without the aid of any centralized administration. It establishes a network dynamically among the mobile nodes on the fly. Each mobile node operates not only as a host but also as a router for forwarding packets to intermediate mobile nodes to reach the destination with in the network. They can form arbitrary topologies depending on their connectivity with each other in the network. In spite of having a number of applications and advantages, it has its own limitations i.e., Limited Bandwidth, Dynamic Topology, Routing, High Mobility of nodes, Energy Constraints, Security [1]. This paper concentrates on security issues in MANETs by analysing the impact of selfish node in AODV routing protocol with different simulation times.

The main intention of a Selfish node attack is to preserve its own resources, e.g. battery life or bandwidth. Selfish nodes behave adversely by receiving and forwarding packets of its interest and it may discard packets that are of no interest to conserve energy. Therefore, it may either drop data packets or refuse to retransmit routing packets that are not concerned to it.

Selfish nodes come under active attack, but are non-malicious nodes. They do not perform dangerous adverse activities like alteration of contents, fabrication, Denial of Service (DoS) attacks and spoofing. But they hinder to share the resources and will not cooperate with other nodes in the network to save its battery power [6]. Some of the properties of selfish nodes are, not participating in the process and progress of routing, not sending hello message and reply, dropping data packets and delaying the Route Request (RREQ) packet [7]. Selfish nodes degrade the performance when compared to all the mobile nodes in the network. 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 [8].

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** observed**.** In section VI **Conclusions and future scope of work** is discussed.

II. AODV ROUTING PROTOCOL

Ad hoc On-Demand Distance Vector (AODV) is a reactive routing protocol that creates a path between source and destination only when it is required.

Ad-hoc On-demand Distance Vector (AODV) routing protocol, is a reactive, single-path and hop-by-hop routing protocol. Generally, each routing protocol comprise of two mechanisms i.e. route discovery and route maintenance. The RREQ (route request) and RREP (route reply) are used to discover the path from source to destination and the response from destination, respectively. RREQ is broadcasted by the source node to all its neighbours. The intermediate nodes then forward this RREQ to its one hop neighbours. Along with forwarding the RREQ, an intermediate node maintains the reverse path for that RREQ by using precursor list. In this way route request is disseminated across the network. On reaching this RREQ, the destination node responds with a RREP. Only the first RREQ would be replied by the destination. In this way, each route discovery process can find a single shortest path from source to destination. RREP from the destination is unicast towards the source node with the help of intermediate nodes by the precursor list to use reverse path entry and forwards the RREP towards source node.

It is a distance vector routing type, on demand hop-by-hop routing protocol in which all packets would be forwarded by using route table entry that is maintained at each node. The next hop information is maintained by the intermediate node during the route discovery. A periodic hello packet is sent by each to ensure the node connectivity with its neighbouring nodes. After a number of failed attempts to transmit a packet, a node would undergo local route repair mechanism. In case of failed local route repair, the link failure is delivered to other nodes by a RERR (route error) packet. RERR is sent to all effected nodes to inform link failure so that they should invalidate the routes that contain link failure. A fresh route discovery is initiated to overcome the delayed link failure problem.

Parameter	Value
Network size	1000x1000
No.of Nodes	50
Protocol	AODV
Traffic Model	CBR
Packet Size	1024
Mobility Model	Random Way Point
Transmission Range	50
RouteRequestRetries	0,5
Simulation Time(sec)	500,1000,1500.2000,2500,3

Link failure can be caused due to mobility, congestion and transmission range in our simulation, also due to malicious or selfish node attacks [2, 3, 4,5]

III. METHODOLOGY

Several researchers have been proposed several solutions to support QoS 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.

Properties of the selfish node:

1. Easier to deal with
2. Very common
3. Interested in their own interests.

Configuring the selfish node: Steps

1. Start
2. Read the de-facto values of the AODV routing protocol.
3. Select the node to configure as selfish node.
4. Edit the attributes of the selected node to behave as Selfish node.
5. Stop

IV. SIMULATION AND PARAMETER SETTING

OPNET Modeler 17.5 was chosen as a simulation environment. It is used to run the simulation for the performance evaluation. It provides a comprehensive environment to model and do performance evaluation of the MANETs. It uses the concept of modeling domains to represent its modeling environments, and graphical editors for editing the network.

The AODV routing protocol is analysed in this paper. In the simulation, the attack models are implemented as part of routing process.

The performance of AODV routing protocol with selfish node in MANETs is observed at different Simulation times, Terrain size 1000m X 1000m range, number of nodes set as 50.

Table 1. Simulation Scenario Parameters

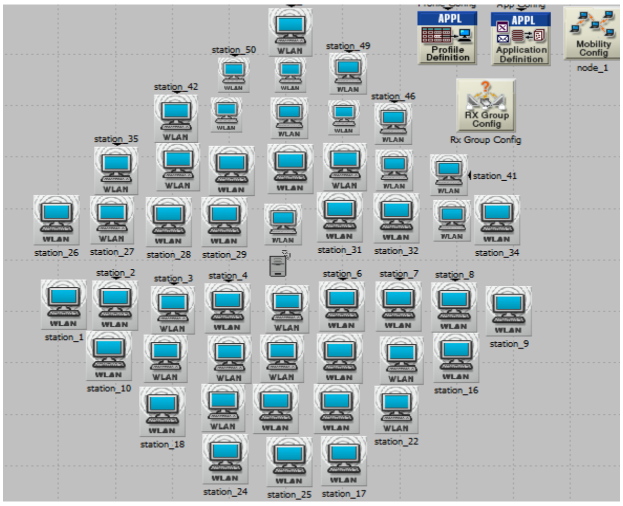

Fig.1 Network topology setup

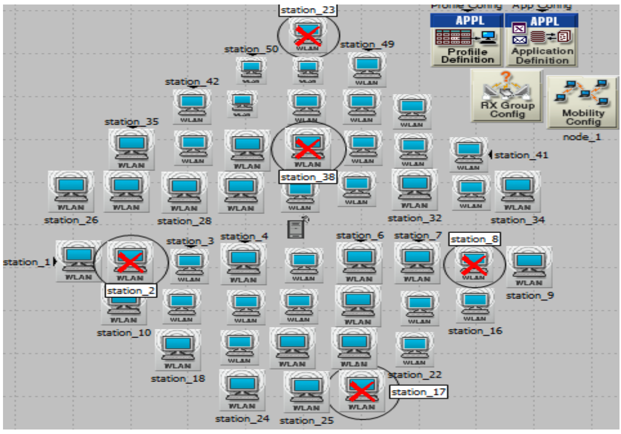

Fig. 2 Network with selfish node

V. RESULTS AND ANALYSIS

Throughput: The rate of successfully transmitted data per second in the network during the simulation. It is calculated according to this formula:

Throughput = Packets Received / Packets Sent

Throughput:

Table 1. Throughput for AODV,AND S AODV

S.No	Simulation Time(Sec)	AODV	Selfish AODV (SAODV)	Impact of selfish node
1	500	10315	263	10052
2	1000	9189	273	8916
3	1500	10582	332	10250
4	2000	12344	361	11983
5	2500	10632	321	10311
6	3000	9812	294	9518

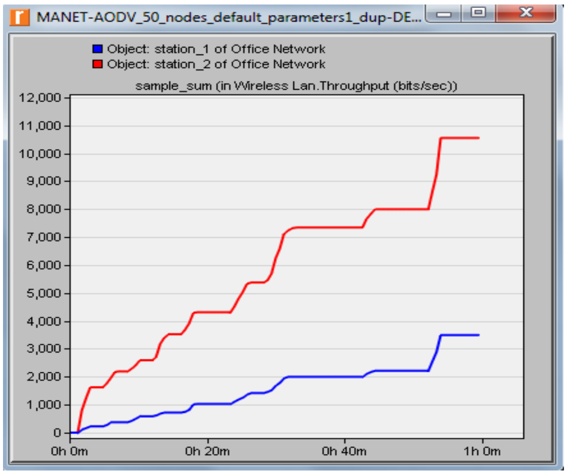

Fig. 3 Throughput with and without selfish node

From the graph, it is observed that in the presence of selfish node, as the simulation time increases throughput degrades.

End to end delay: The time taken for a packet to travel from a source to destination

Table 2 . Delay for AODV and S AODV

S.No	Simulation Time(Sec)	AODV	SAODV	Impact of selfish node
1	500	0.001065	0.0000451	0.0010199
2	1000	0.001154	0.0000481	0.0011059
3	1500	0.0011402	0.00004772	0.00109248
4	2000	0.001181	0.00004873	0.00113227
5	2500	0.001175	0.00004874	0.00112626
6	3000	0.001187	0.00004886	0.00113814

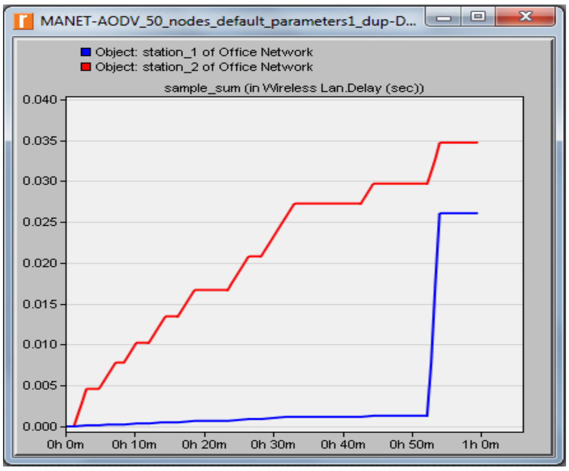

Fig. 4 Delay with and without selfish node

From the graph, it is observed that in the presence of selfish node, as the simulation time increases delay increases.

VI. CONCLUSION AND FUTURE SCOPE OF WORK

The impact of the selfish node on the performance of the AODV routing protocol is that, the throughput degrades by 40 times of the original AODV throughput. Similarly, the impact on delay is reduced by more than 1000 times. The impact of the simulation time on the performance of the variance in throughput of AODV routing protocol with and without the selfish node is 2532 and 98 and delay by variance is 0.00012 and 0.00000376 sec. So, from the experimental results, it is observed that the selfish node influences the performance degradation.

In future, this work may be extended for different mobility models by varying network size, mobility and with different pause times

REFERENCES

[1] AD HOC NETWORKS Technologies and Protocols Edited by PRASANT MOHAPATRA University of California, Davis SRIKANTH V. KRISHNAMURTHY University of California, Riverside – Springer Textbook

[2] C. Perkins, E. Belding-Rover an S. Das, "RFC-3561: Ad Hoc OnDemand Distance Vector (AODV) Routing". Available at: www.ietf.org/ref/ref3561.txt, July 2003.

[3] Abdur Rashid Sangi, Zhiping Liu and Jianwei Liu, "Route Information Poisoning in MANETs: Analysis and Defenses". In Proceedings of 4th IEEE IITA, November 2010, Qinghuangdao, China

[4] Mohammed Saeed Alkatheiri and et. al. 2011 IEEE 978-1-61284-307-0/11 pg. 614-618 .

[5] C Sreedhar, Varun Varma Sangaraju, "A Survey on security issues in routing in MANETS" International Journal of Computer & Organization Trends (IJCOT) ISSN:2249-2593 Volume 3 Issue 9-oct 2013.

[6] Shailender Gupta, C. K. Nagpal and Charu Singla, Impact of Selfish Node Concentration in Manets, International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 2, April

[7] S. Marti, T. J. Giuli, K. Lai, M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. of MobiCom 2000, Boston, August 2000.

[8] Mr. Amir Khusru Akhtar & G. Sahoo Mathematical Model for the Detection of Selfish Nodes in MANETs, International Journal of Computer Science and Informatics (IJCSI) ISSN (PRINT): 2231 –5292, Volume-1, Issue-3

[9] P. Saravanan and S.Chitra, "Selfish Nodes in MANET: Impact on Security and QoS," International Journal of Computer Applications(IJCA) Volume 66– No.1, March 2013.

[10] Dr. S.P Setty and B. Prasad " Comparative Study of Energy Aware QoS for Proactive and Reactive Routing Protocols for Mobile Ad-hoc Networks" International Journal of Computer Applications (0975 – 8887) Volume 31– No.5, October 2011.

[11] Dr. S.P. Setty et. al., "PERFORMANCE EVALUATION OF AODV IN DIFFERENT ENVIRONMENTS", International Journal of Engineering Science and Technology Vol. 2(7), 2010, 2976-2981.

[12] *Venkataramana Attada and S. Pallam Setty " Cross Layer Design Approach to Enhance the Quality of Service in Mobile Ad Hoc Networks" Wireless Pers Commun DOI 10.1007/s11277-015-2609-6 Springer Science+Business Media New York 2015.*