VOL. 10, NO. 12, JULY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

SECURING AODV PROTOCOL FROM SELFISH NODE ATTACK

Mani Bharathi, Ranjith Sairam, S. Sundar and C. M. Vidhyapathy
School of Electronics Engineering, VIT University, Vellore, Tamilnadu, India
E-Mail: manibharathi22@gmail.com

ABSTRACT

Mobile ad-hoc networks are self-configuring wireless networks without any specific infrastructure. MANETs are highly subjected to several attacks due to continuously changing network topology, lack of central monitoring and lack of efficient defense mechanism. Selfish nodes in MANETs are the defective nodes which drop the packets that are not intended to them. A malicious selfish node is introduced in the network to analyze the selfish node attack and a prevention algorithm for selfish node attack is also suggested. For the analysis, the routing protocol used in this paper is AODV. Network parameters meters like throughput, end to end delay and load are evaluated and compared. Simulation tool used in this paper is Riverbed Modeler.

Keywords: MANET, AODV, selfish node, riverbed modeler.

1. INTRODUCTION

A mobile ad-hoc network is a wireless network that configures by itself and doesn't have an infrastructure. MANETs usually have a routable networking environment. MANETs are a group of mobile nodes which can communicate with other nodes in the network [1]. There are several routing protocols in MANET. The purpose of protocol in MANET is to show the shortest and most efficient route for packet forwarding between the nodes. If the protocols are not efficient the overall performance of the network is degraded [1]. MANET routing protocols can be characterized into tree types. They are,

- **Proactive (table driven):** These protocols maintain a routing table which contains lists of destinations and their respective routes. The contents of the routing table are updated for every hop between the nodes. These protocols are slow and needs to store all the routing information [2]. These are more prone to failures.

Example: [3] OLSR - Optimized Link State Routing protocol

- **Reactive (on demand):** These protocols find a route on demand by continuously sending Route request packets RREQ to the nodes in the network [2].These have high latency time in route finding

Example: [4] AODV, [5] DSR

- **Hybrid:** These protocols combine the advantages of reactive and proactive routing protocols. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding [2].

Example: [6] Zone routing protocol (ZRP)

In MANETs, the presences of intermediate nodes are vital to forward packets to distance receivers. If the intermediate node is a selfish node, then it not only drains the resources but also discard the packets during communication.

Many researchers have proposed many protocols for MANETs, but AODV and DSR are more popular among the other protocols. According to [7], [8] these protocols are based on the principle of trust your neighbour's relationship; these are easy victim of selfish node and malicious node problems.

In [9], it is stated that the main advantage of AODV Protocol is that routes are established on demand and destination sequence numbers are used to find the latest route to destination and connection setup delay is less. Hence in this paper we have chosen AODV for our analysis.

This paper is organised as follows: In Section II, the AODV protocol and the concept of Selfish Node is explained. Section III describes about the Algorithm and the Simulation is presented in the Section IV. Finally, Section V concludes the major findings.

2. AODV PROTOCOL

Ad-Hoc on Demand Distance Vector (AODV) falls in the category of reactive routing protocol. AODV create path to the destination node only when it is required. The Routes are established only when certain nodes initiates route discovery process as on will to communicate or transmit data with each other [10]. Only source node, destination node and intermediate node stores the routing information along with the route that is established and deals with packet transmission. This

scenario has many advantages such as it reduces the memory overhead, minimizes the use of network resources and performs well in high mobility situations [10]. For the purpose of running algorithm AODV uses three types of control messages abbreviated as RREQ (route request), RREP (route reply) and RERR(route error) messages as shown in Figure-1.

2.1 AODV route discovery

To establish the communication between source node and destination node, the source node issues the route discovery process. For this purpose RREQ broadcasts through source node to all its neighbors [11]. The intermediate nodes check the received RREQ. If it is destined to the intermediate node, it replies with RREP. If it is not the case, the RREQ will be forwarded to the other neighbor nodes. The broadcast identifier and the previous node number from which the request came will be stored by each node before forwarding the packet [11].

The intermediate nodes will use the timers to delete entry when there is no reply for the request. If there is a reply, intermediate node will store the broadcast identifier and the previous nodes from which the reply came [11]. To detect if the node has received the route request message previous broadcast identifier and source ID is used. This will prevent the redundant request receive in same node.

In case of link failure, this can be due to the node mobility; the routing table will be invalidated by the node. This link failure will make all destinations unreachable. Then a route error message which lists all of these lost destinations will be generated. Source node will get RERR sent upstream towards it by the node. After the source receives RERR, the route discovery process will be re-initiated if it still requires the route.

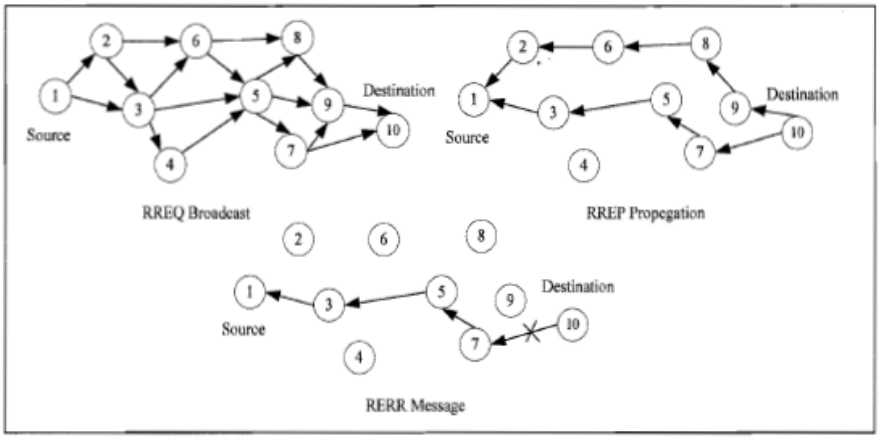

Figure-1. AODV Route Discovery.

2.2. Selfish node attack

Selfish node aims to save its very own resources and consumes very less power. This type of malicious node discards all the packets that it receives except those which are destined to it. It drops control packets, that is considers the nodes would not be included in the routing. Selfish nodes probably reduce the performance of a MANET [12]. This Simulation shows that the percentage of malicious nodes can reduce the number of packets that are successfully delivered in the network. However, selfish node reduces the performance of network by reducing Throughput, load and Delay. As the number of selfish nodes been increased, the sender node will have less option on which route the data packets should be sent. In this paper we overcome the selfish node attack with the help of enabling and disabling the selfish nodes.

3. PROPOSED ALGORITHM

The proposed algorithm approach is detailed in three sections as given below,

A. Implementation of AODV protocol

In the first scenario, we are going to establish a communication using AODV protocol considering 50 nodes. Once the communication is initialized, RREQ messages are sent from Source node requesting for a route to the destination. The remaining nodes of the network sent RREP messages in reply to RREQ messages showing that they have a route to the destination. After the RREP messages are received at the source node Source node sends the data packets. This process is carried out using AODV protocol. Here software we used was RIVERBED Modeler. That 50 nodes we use here was WLAN work stations, which are maintained by WLAN server with the help of Application configuration, Profile configuration

and Rx group configuration. The implementation of AODV in RIVERBED Modeler is shown in Figure-2.

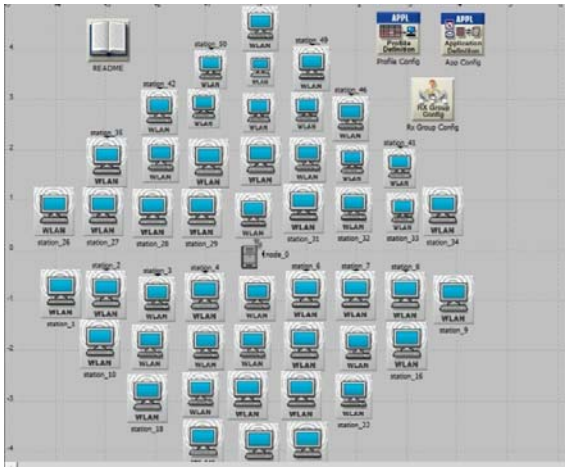

Figure-2. Implementation of AODV protocol in riverbed modeler.

B. Simulation of selfish attack

Now we are going to introduce a malicious node into the network. In order to implement the black hole attack we have to make some modifications. We can easily add the Black Hole behavior to any node. We configure any node as selfish by disabling it in Edit attributes.

Once the data packets reach the malicious node, it will drop the packets leading to communication failure in the network. Then the throughput, delay and the load of the nodes get reduced.

C. Prevention from selfish node attack

In Previous Scenario we are enabling the attributes of one or many nodes to make them act as selfish nodes in the MANET. In that scenario the throughput will be low and the delay will be high due to the selfish nodes which not only affects itself but also it affects the neighboring nodes.

To prevent this selfish node behavior we are enabling back the nodes that we disabled in the previous scenario so that those selfish nodes will now behave as normal nodes and thus the MANET is being protected from selfish node attacks. Now in this Scenario we are enabling the parameters of the disabled nodes so that we are getting a better throughput and low delay than the previous scenario.

The above scenarios are implemented in the Riverbed Modeler as per the following steps,

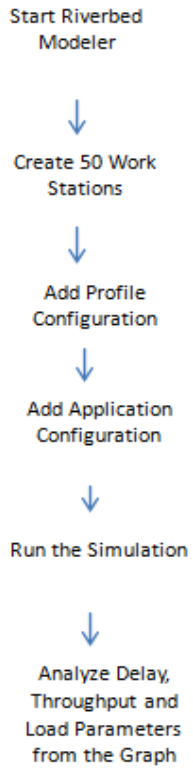

Figure-3. Algorithm for Securing AODV Protocol from Selfish node attacks.

4. SIMULATION RESULTS

All the three above mentioned scenarios are simulated in Riverbed Modeler. Throughput, delay and load are calculated and graphs are shown in Figure-4 to Figure-6.

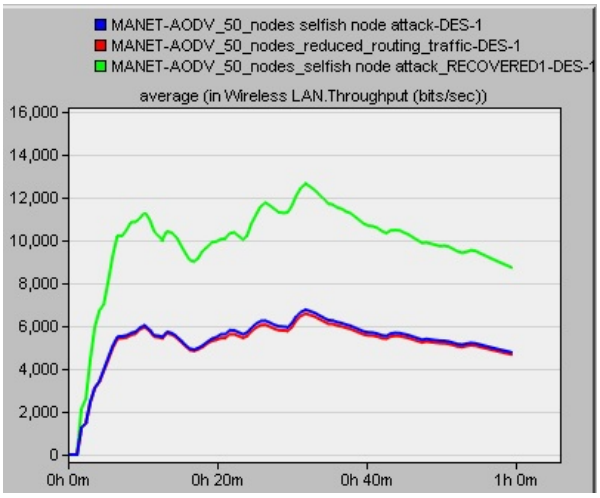

Figure-4. Comparison of throughput.

When Selfish Nodes are introduced in the network it affects the performance of the neighboring nodes thereby decreasing the overall throughput as seen in the Figure-4.1.

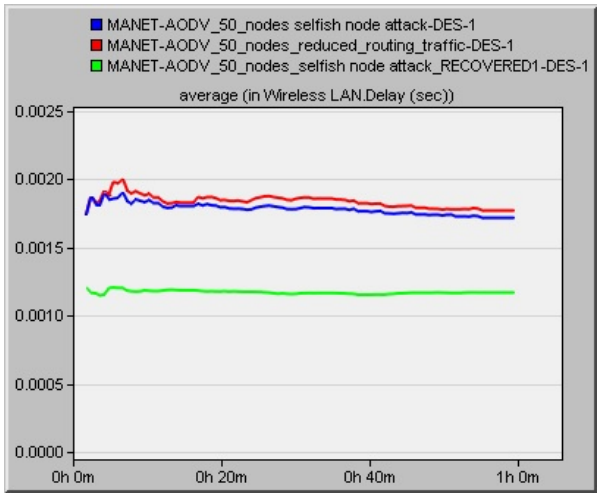

Figure-5. Comparison of delay.

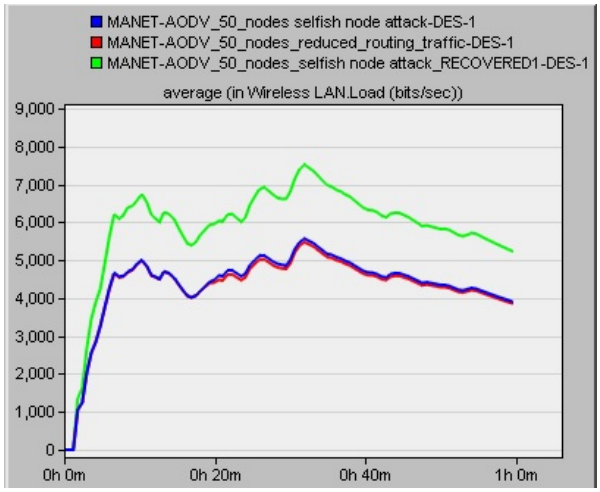

Figure-6. Comparison of load.

In Figures 4 to Figure-6, it is shown that, the performance of nodes in the network with and without the presence of Selfish Node Attacks and also the nodes recovered after Selfish Node Attacks. It is observed that, the overall throughput is increased and the delay is decreased when the nodes are secured from the Selfish Node Attack.

5. CONCLUSIONS

In this paper, the effect of selfish node attack on AODV is analyzed. For this analysis, there are 50 nodes are chosen and among these, there are 5 nodes are chosen as selfish nodes. The simulation is carried out in Riverbed Modeler and various performance parameters are studied. It is observed that, initially there is very less data loss in the AODV network. If a selfish Node is enabled/introduced in the network then the data loss is increased. When the selfish nodes are eliminated, the data loss is decreased and the throughput is increased. This study proves that the AODV protocol is not having guard against selfish nodes and it is suggested that AODV performs better if it is used with minimum intermediate nodes.

REFERENCES

[1] Md. Amir Khusru Akhtar1 and G. Sahoo. Mathematical Model for the Detection of Selfish Nodes in MANETs. International Journal of Computer Science and Informatics (IJCSI) ISSN (PRINT): 1(3) 2231-5292.

[2] Hicham AMRAOUI, Ahmed HABBANI, Abdelmajid HAJAMI. 2014. Effect of selfish behavior on OLSR and AODV Routing Protocols in MANETs. Computer & Information Technology (GSCIT). pp. 1-6.

[3] T.H. Clausen, G. Hansen, L. Christensen and G. Behrmann. 2001. The Optimized Link State Routing Protocol, Evaluation through Experiments and Simulation. Proceedings of IEEE Symposium on Wireless Personal Mobile Communications.

[4] C.E.Perkins and E. M. Royer. 1999. Ad-hoc on-demand distance vector routing. In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications. pp. 90-100.

[5] D.B. Johnson and D.A. Maltz. 1996. Dynamic Source Routing in Ad Hoc Wireless Networks. Mobile Computing, Kluwer Academic Publishers. 353: 153-181.

[6] Z.J. Haas. 1997. The Routing Algorithm for the Reconfigurable Wireless Networks. Proceedings of ICUPC. 2: 562-566.

[7] Yaser khamayseh, Ruba Al-Salah, Muneer Bani Yassein. 2012. Malicious Nodes Detection in MANETs: Behavioral Analysis Approach. Journal Of Networks. 7(1).

[8] Kravets R., Naldurg P. and Yi, S. 2001. Security-aware Ad Hoc Routing for Wireless Networks, In The ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC01), Long Beach, CA.

[9] Hu Y., Johnson D. and Maltz D. 2003. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR).

[10] C. Siva Ram Murthy, B.S. Manoj. Ad-Hoc Wireless Networks Architectures and Protocols.

[11] Hicham Araoui, Ahmed Habbani, Abdel majid Hajami. Effect of selfish behaviour on OLSR and AODV Routing Protocols in MANETs.

[12] J. Vijithanand, K. Sreerama Murthy. A Survey on Finding Selfish Nodes in Mobile Ad Hoc Networks Department of Information Technology Sreenidhi Institute of science and Technology Hyderabad-India.