Analysis and Implementation of Malicious Node in AODV Routing Protocol

[1] Bhupendra B Patel, [2] Prof Chirag S Thaker, [3] Nidhi R Jani
[1] Department of Master of Engineering, GTU PG School, Ahmadabad, Gujarat
[2] Asst. Prof in Department of Computer Engineering, L D Engg. College, Ahmadabad, Gujarat
[3] Asst. Prof in Department of Master of Engineering, GTU PG School, Ahmadabad, Gujarat

[1] emailtobpatel@gmail.com
[2] chiragthaker@yahoo.com
[3] nidhi.r.jani@gmail.com

ABSTRACT

The Mobile Ad-hoc Network (MANET) is constructed based on wireless medium and it is of self organizing behaviour. MANET is easy to establish and having dynamic topology. The mobile Ad-hoc networks are vulnerable to various networks attacks because MANET operational environment is open and dynamic or live. MANET uses the Routing protocols for data transfer. Two different types of Routing protocols are available: Table Driven and On Demand Routing Protocols. Malicious node is the one type of mobile node but its work is completely different compared to normal Mobile nodes. Malicious nodes have capability to change or remove Routing Information. It also sends or advertises the fake Route Request to attract user’s data. Malicious node disturbs the Network to carry correct flow of operation. It is responsible for attacks on the existing normal mobile nodes and creates receiver collision, limited transmission power, false misbehaviour etc. Malicious or selfish node carries attacks on the networks so it directly effects to the routing Performance. The objective of this work is to check Network performance in malicious environment and provide prevention for the attack. Throughput and Delay are analysed for Denial of Service (DoS) attack and prevention scenarios.

Keywords: MANET, AODV, Selfish Node, DoS Attack, Routing Protocols

1. INTRODUCTION

Mobile Ad-hoc Network is a collection of wireless devices, it means wireless node. The wireless nodes are connecting dynamically and share the information. Basically two types of mobile ad-hoc networks: Infrastructure based and another one is those networks with fixed and wired gateways. In terms of wireless networks bridges for these networks are known as base station [1].

Ad-Hoc Routing is defined by basically two types: first is Proactive and second is Reactive. Reactive Routing protocols are used on time when node wants to send packet or information to the destination [2] unlike the proactive routing protocols. In this type of routing protocols every node should have stored the routing information of its neighbours. Proactive routing protocols discover and maintain a complete set of routes for the lifetime of the network.

A malicious node abuses the collaboration between nodes to interruption operation of the network. It’s also called selfish node. Malicious nodes objective is intentionally interrupt the going on correct operation of the routing protocol, denying network services if possible [3]. Such nodes can use or modify sensitive routing information. Both data packets and control packets, as used by the routing protocol, are vulnerable to attacks.

This paper is organized as follows: Section I presents the introduction about MANET, Routing Protocol and Malicious node. Section II presents the brief AODV Routing Protocol mechanism. Section III introduces the nature of DoS attack. Section IV gives information regarding prevention against the attack. In Section V Proposed Solution for the prevention of DoS attack is explained. Section VI shows Experimental outcomes after applying proposed schema.

2. AODV ROUTING PROTOCOLS

The AODV, Ad-hoc means node move or connected or disconnected with the networks any time, On Demand means when source wants to send data to the destination, Distance means find the distance between source to destination in terms of number hope counts and Vector means list whatever store the node information list.

In AODV, routing protocols are stored routing information on every node which is available on networks [4]. AODV uses the OSPF method/Algorithm. OSPF means Open Shortest Path First; it is based on the Diskjetra's algorithm.
In [5, 6, 7], AODV use some approaches for path or route establishment.

Route Request (RREQ): In Route Request source node transmit/ broadcast the route request message for specific destination neighbours node pass the message to destination Route Reply (RREP): In Route Reply Destination are use the unicast route for reply message to source, neighbour node make next hop entry for destination and forward the reply. If source receives multiple replies that time source node use one with shortest hop count route/path.

SSN (Source Sequence Number) and DSN (Destination Sequence Number): Source node when send the broadcast packet with the sequence number and destination sequence number are define the freshness of the path.

Route Error (RERR): When route error message are generated that time in network link brake between sources to destination. In AODV routing protocols detect the node and if possible do the local repair. When whatever link are break in optimum path means not reached at destination that time neighbor are tell to sent previous request

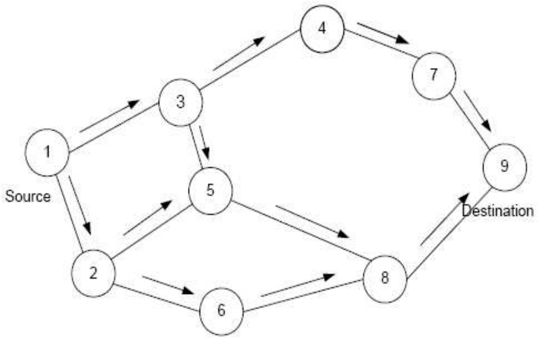

Fig 1. Route Request packets flooding in AODV

In fig 1 is a mobile wireless network. Node 1 (Source) to node 9 (Destination Node) Flood the route request packets with source sequence in the network. Node 1 is send route request to all neighbour and neighbour through Destination.

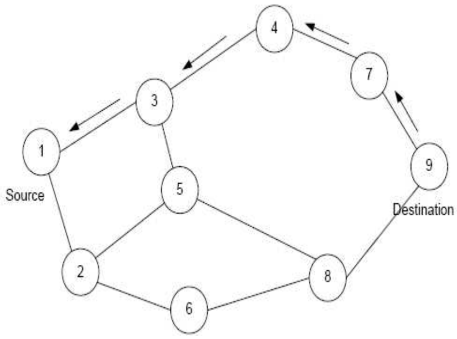

Fig 2. Forwarding of Route Reply packet in AODV

In fig 2 Destination use the unicast path for the route reply. Destination is replying the route request on symmetric link. Destination Sequence number is defines the freshness of the route/path. In network node are the count number hop to the reach at destination and find the minimum number of hope in route that route are select for the data transfer.

In Fig 3 AODV Route maintenance when link are break that time, it broadcasts a route error (RERR) packet to its neighbours, which in rotate propagates the Route Error (RERR) packet towards nodes whose routes may be affected by the disjointed link. Then, the precious source can re-initiate a route discovery operation if the route is still needed. Neighbour is telling to exiting all neighbour this link are break so don't send any packet on that link. In this fig link break between node 7 and node 8 so node 7 tell to node 4 or send RERR this link is break so choose another optimum path means shortest path/route.

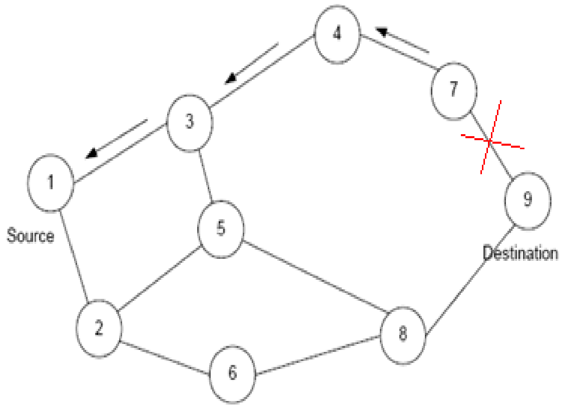

Fig 3. Route maintenance

.

3. DENIAL OF SERVICE ATTACK

This attack aims to attack the accessibility of a node. If the attack is Successful, the services will not be accessible. The attacker normally uses radio signal jamming and the sequence tiredness method [8]. Denial of Service (DoS) is the degradation or avoidance of valid use of network resources. The wireless ad hoc network is mainly Vulnerable to DoS attacks due to its features of open medium environment, frequently changing topology, supportive algorithms, and not have of a comprehensible line up of defence is a growing problem in networks today.

Many of the security techniques developed on a fixed wired network are not applicable to this new mobile environment. How to stop the DoS attacks in a different way and efficiently and keep the very important security ad hoc networks available for its future use is important [9].

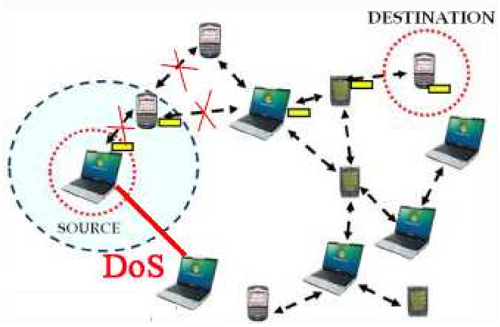

Fig. 4. Denial of Service Attack

In Figure 4, Source node sends the data to destination node via optimum path .But that time one malicious node enter or exiting in the networks it will start the flooding the large number of data packet to source so source node not able to send data original destination . Finally malicious node is the drop the packet and consumes the resources, battery energy.

4. RELETED WORKS

In [5], author defines performance of AODV routing protocol with existing of malicious nodes which has been done using NS2.34 simulator. To measure the performance evaluation, performance metrics like Throughput, Packet Delivery Ratio and End to end delay has been used. In all these scenarios the number of malicious nodes varies from 0 to 5.

In this approach CORE mechanism that enhances watchdog for monitoring and isolating selfish nodes based on a personal, oblique and functional status. The status is calculated based on various types of information on each entity's rate of relationship. Because there is no motivation for a node to maliciously spread negative information about extra nodes, simple denial of service attacks using the collaboration technique itself are prevented [10].

Algorithm proposed in [9], presents Prevention of the DoS/Flooding attack. We summarized the node categorized as friends and strangers based on their relationships with their neighbouring nodes. A trust estimator is used in each node to evaluate the trust level of its neighbouring nodes. The trust level is a function of various parameters like PDR and End-to End Delay. Bytes

5. PROPOSED SOLUTION

The work is mainly focused on to avoid the Denial of Service (DoS) attacks in Mobile Ad-hoc Network. Here first malicious node is detected and then functioning of the malicious node is changed without interrupting middle nodes and destination node by using this Research Schema.

In this Research Schema, malicious node sends continues Route Request. The peak time is added and number of Route request received by neighbour are checked. Here peak time is set at 0.8 and the neighbor receives maximum 7 number of route requests from malicious node then neighbour declares that node as malicious and adds it in malicious list. Other nodes do not give response to malicious node even if it continuously sends request. At one phase malicious node can stop doing malicious things so for that expire time is added. After malicious node expire time exceeded, it can be removed from malicious list.

6. EXPERIMENTAL RESULTS

The performance study is done on Linux Operating System Ubuntu 11.10. Ns –allinone-2.34 configured on that platform.
We suggest the following solution. To prevent DoS attack. The Setup of simulation using parameters defined in Table 1. Here done the different node dynamic scenarios and used CBR traffic and malicious nodes different form 1 to 7.

Table 1 Parameter used in Implementation

Parameters	Values
Number of Nodes	25 ,50 ,75, 100
Area Size	1000*1000
MAC	802.11
Simulation Time	100,200,300,400
Traffic Source	CBR
Packet Size	1000
Bandwidth	10 mb
Data Rate	10mb
Routing Protocol	AODV
Transmission Protocol	UDP
Number Of malicious node	1 to 7

Here we have analysed the performance matrix i.e. Throughput and End-to-End Delay.

In Fig 5 the throughput for various numbers of nodes is analyzed with DoS attack and prevention scenarios. When Number of nodes increases, Throughput will be decreased with Dos Attack and Throughput will be also decreased with Prevention scenario.

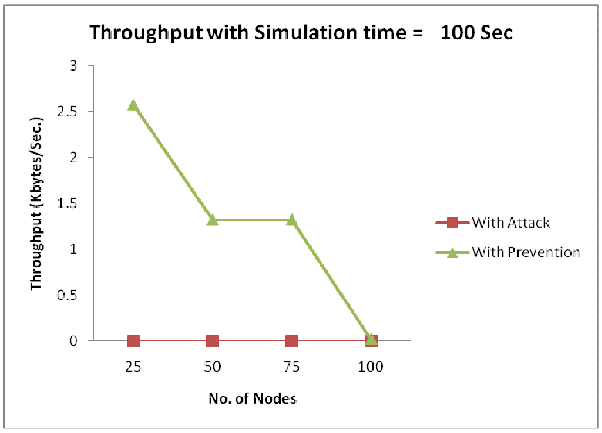

Fig 5 Throughput Vs No Of Nodes

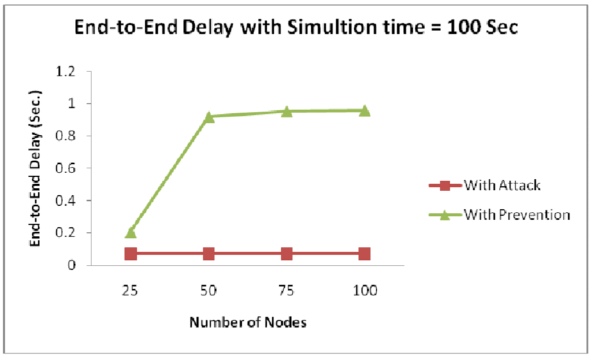

Fig 6 End-to End Delay Vs No Of Nodes

In Fig 6, End-to-End Delay is analyzed for various numbers of nodes with DoS attack and prevention scenarios. End-to-End delay will be increased with increased number of nodes.

7. CONCLUSIONS AND FUTURE WORKS

As malicious node is the main security threat that effect the performance of the AODV routing protocol. This problem has found because mainly required the routing performance in malicious environments. Its detection is the main matter of concern. In general scenario many attacks occur in mobile ad-hoc networks. Therefore this work is focused on mechanism to detect and prevent the DoS attack.

It is analysed that after applying the suggested solution for preventing DoS attack, as the number nodes increases, Throughput will decreased and End-to End delay will also be increased. Work will be focused on securing the network in malicious environment with less delay.

8. ACKNOWLEDGMENTS

I would like to sincerely thank to Prof Chirag S Thaker and my college internal staff, friends for his expert guidance and timely inputs.

9. REFERENCES

[1] Datuk Prof Ir Ishak Ismail & Mohd Hairil Fitri Ja'afar,"Mobile Ad Hoc Network Overview",2007 ASIA-PACIFIC CONFERENCE ON APPLIED ELECTROMAGNETICS PROCEEDINGS

[2] PO-WAH YAU, SHENGLAN HU and CHRIS J.MITCHELL,"Malicious attacks on ad hoc network routing protocols"

[3] S.Gopinath1, Dr.S.Nirmala & N.Sureshkumar, "Misbehavior Detection : A New Approach for MANET",(IJERA) ISSN: 2248-9622 www.ijera.com,Vol. 2, Issue 1,Jan-Feb 2012, pp.993-997

[4] Changling Liu, Jörg Kaiser,"A Survey of Mobile Ad Hoc network Routing Protocols",University of Ulm Tech.Report Series, Nr. 2003-08

[5] Vijay Kumar, Rakesh Sharma, Ashwani Kush, "Effect of Malicious Nodes on AODV in Mobile Ad Hoc Networks", International Journal of Computer Science and Management research Vol 1 Issue 3 October 2012

[6] A.Kush, R.Chauhan,C.Hwang and P.Gupta, "Stable and Energy Efficient Routing for Mobile Adhoc Networks", Proceedings of the Fifth International Conference on Information Technology: New Generations, ISBN:978-0-76953099-4 available at ACM Digital Portal, pp. 1028-1033, 2008.

[7] C. Perkins, E. B. Royer, S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing Internet Draft", RFC 3561, IETF Network Working Group, July 2003.

[8] Akanksha Saini, Harish Kumar, "Effect Of Black Hole Attack On AODV Routing Protocol In MANET",IJCST Vol. 1, Issue 2, December 2010

[9] Ms. Neetu Singh Chouhan, Ms. Shweta Yadav, "Flooding Attacks Prevention in MANET",IJCTEE Volume 1, Issue 3,Nov 13, 2011

[10] Pietro Michiardi and Refik Molva, "CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks"