Enhancing the Security in Ad-hoc on-Demand Distance Vector

Bhagia Nidhi, Manmohan Sharma

Abstract— MANET is a collection of wireless nodes connected by wireless links without any fixed infrastructure. For communication, a temporary path is established between the nodes. As nodes are mobile, the structure of network changes dynamically. Due to dynamic topology and no centralized monitoring makes it difficult to provide a secure network. So it is vulnerable to attack and one of attack is called black hole attack. In this paper, we will enhance the security. The proposed mechanism will identify the behavior of malicious node in a MANET.

Index Terms— AODV, Black Hole Attack, Malicious Node, MANET.

I. INTRODUCTION

Ad-hoc networks are a new standard of wireless communication for mobile hosts, which we call nodes. MANET is a collection of mobile hosts, devices that are connected by wireless link without any fixed infrastructure. Due to dynamic topology, the nodes or devices in the network can change locations. MANET can have different shapes of network at different locations because of the presence of mobility characteristic in it Ad-hoc devices should be able to detect the presence of other devices. The challenge faced by nodes in a MANET is the security and routing of routing protocols. As mobile ad-hoc networks are characterized by a multi-hop network topology that can change frequently because of mobility, efficient routing protocols are needed to establish communication paths between nodes without causing excessive control. Several forms can occur in ad-hoc wireless communication. One is Peer- to-Peer and other is Remote-to Remote communication. In peer-to-peer communication, communication will occur between them over a period of time until the one of node has moved away. In remote-to-remote, two or more nodes are communicating among themselves and they are migrating in groups. The application areas of the Mobile Ad-hoc network are military communication, home appliances, and emergency services.

Figure 1 Mobile Ad-Hoc Network

Manuscript received on April, 2013.

Bhagia Nidhi, Department of Computer Science, Lovely professional University, India.

Manmohan Sharma, Department of Computer Science, Lovely Professional University, India

A. Routing Protocols

Routing is the process of exchange of information from source place to destination in a network. The aim of the routing protocol is to establish the shortest path between the source and destination with minimum overhead and minimum bandwidth so that packets are transmitted in a timely manner [4]. The major requirements of a routing protocol in ad-hoc networks are the Minimum route acquisition delay, Quick route reconfiguration and loop free routing. Routing Protocols can be categorized into three parts.

- Reactive Protocol
- Proactive Protocol
- Hybrid Protocol

Reactive protocol also known as on-demand protocol. In ad-hoc networks where bandwidth resources are limited and topology changes frequently, on-demand routing protocol to be used. Reactive protocols have two main processes i.e. Route Discovery and Route Maintenance. The routes are discovered on the demand basis so that's why reactive protocols known as on-demand protocol. Examples of reactive protocol are AODV and DSR. Proactive protocol also known as table driven protocol. In this protocol, each node maintains the routing information to every node in the network. The routing information is usually reserved in different tables. These tables are updated regularly if the topology of network is changed. Example of this protocol is DSDV. Hybrid routing protocol is a combination of reactive protocol and proactive protocol. It uses the route discovery mechanism of reactive protocol and the table maintenance mechanism of proactive protocol so as to avoid latency in the network. Hybrid protocol is suitable for large networks.

B. Ad-hoc On-Demand Distance Vector (AODV)

AODV is an on-demand routing protocol. It uses on-demand approach for finding routes and route maintenance. The operation of AODV is loop free by use of sequence numbers which indicate the freshness of the route [2]. When links break, AODV causes the affected set of nodes to be notified to invalidate the route. Route request (RREQ), Route reply (RREP) and Route error (RRER) are three messages types defined by AODV for its working. In route discovery mechanism of AODV, one node wants to send a message to another node; it simply broadcast RREQ to all neighbor nodes. Each neighboring node responds to RREQ by sending a RREP message back to the sender if it knows a path to the destination node otherwise it rebroadcast the RREQ. The advantage of the AODV protocol is that routes are established on demand basis and destination sequence numbers are used to find the latest route to the destination.

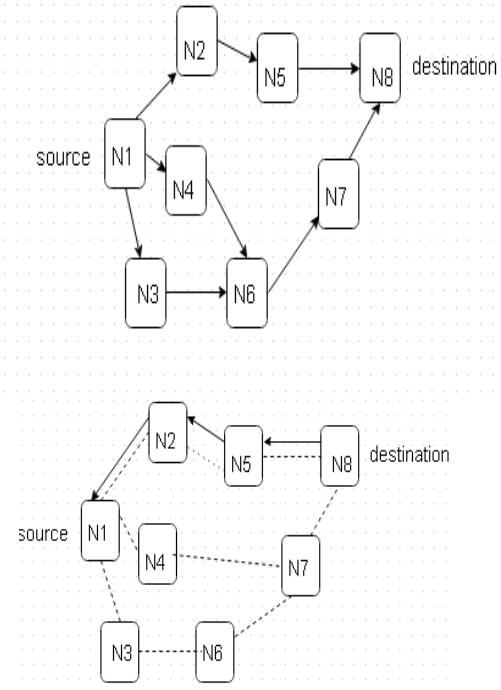

Figure2. Route discovery mechanism

C. Black Hole Attack

There are two types of security attacks in MANET. One is passive attack and another is active attack. In passive attack, the attacker does not interact with the network directly. It monitors the network and snoop the information exchanged in the network. An active attack is an attempt to modify data, gain authentication, or acquire authorization by inserting fake packets into the data stream or modifying packets transition in the network. MANET is more vulnerable to attacks due to the dynamic topology. Black hole attack is a kind of active attack. In black hole attack, the malicious node advertises itself for having the shortest path to the destination node. This attack will affect the whole network performance and the malicious node will provide the shortest route to the destination node.

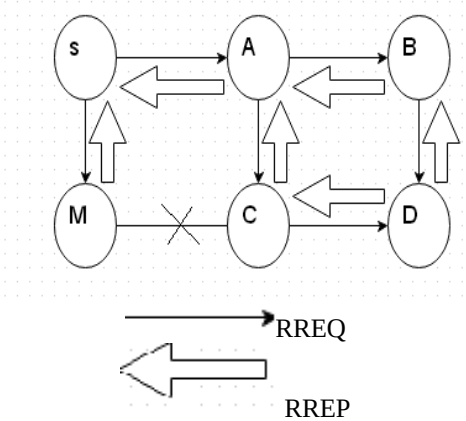

Figure3 black hole attack

In Figure3 Node S is source node, Node D is destination node and Node M is malicious node. The source node sends RREQ to every neighbor node. Upon receiving the RREQ, the malicious node immediately sends RREP to source node with higher sequence number. In this case, the source node assumes that node is having a fresh route towards destination. The source node sends data packets through malicious node and the network suffers from black hole attack.

II. PROBLEM FORMULATION

MANET consists of wireless nodes connected by wireless links without any fixed infrastructure. To maintain a communication, a temporary path is set up between mobile nodes, where each node behaves as a transmitter, a host and a router. As the nodes are mobile the structure of network changes dynamically. Due to dynamic topology and no centralized monitoring makes it hard to provide a secure network. So it is more vulnerable to attacks and one of them is black hole attack. In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node. Our research will enhance the security and routing in AODV by identifying the behavior of malicious node with the help of some parameters like number of packets delivered through it, sequence number generated for these packets, also it will check the status of malicious node and record the status and sequence numbers generated by malicious node for each packet delivery or route request.

III. OBJECTIVES OF OUR RESEARCH

The main aim is to resolve all the problems occurred due to black hole attack. There are so many mechanisms designed for provide the security like watch dog mechanism and enhance route discovery. The objectives of our research are:

- To analyze the behavior of malicious node.
- To implement the security and routing in AODV.

IV. PROPOSED WORK

There are many solutions proposed by different authors to deal with the black hole attack like watch dog mechanism and enhance route discovery for AODV. Our research will focus on enhance the security in Ad-hoc distance vector. We will start with identifying the behavior of malicious node. This research work will focus on providing better security in AODV in MANETs.

A. Delay

The packet delay is the time duration between creations of data packet by source node to the reception of data packet by destination node. It is usually measured in seconds.

B. Throughput

It reflects the completeness and accuracy of the routing protocol. It is the average at which data packets is delivered successfully from one node to another over a communication network. It is usually measured in bits per second. [2]

V. CONCLUSION

Our ongoing research will be base on provide the security in AODV. We tend to provide good solution for detecting the malicious node in AODV. This research is still in process experimentation in running phase to test the developed Scheme on Mobile Ad-hoc Networks.

REFERENCES

1. Kamarularifin Abd. Jalil, Zaid Ahmed, Jamalul-Lail Ab Manan Mitigation of Black Hole Attacks for AODV Routing protocol.

2. Gurpreet Singh, Atinderpal Singh, Anantdeep Kaur "Performance Evaluation of Aodv and Dsr Routing Protocols for VBR Traffic in Mobil Adhoc Networks", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 5, pp.1607-1610, October 2012.
3. Govind Sharma, Manish Gupta "Black Hole Detection in MANET Using AODV Routing Protocol", International Journal of Soft computing and Engineering (IJSCE) ISSN: 2231-2307,January 2012.
4. Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of computer Science, Engineering and Applications (IJCSEA) Vol.2, No.1, February 2012
5. Vivek Sharma, Amit Baghel "Analysis of AODV and DSR in Presence of Wormhole Attack in Mobile Ad-hoc Network", International Journal of Engineering science and technology,vol.2 (11),2010,6657-6662.
6. Subash Chandra Mandhata, Dr. Surya Narayan Patro " A Counter Measure to Black Hole Attack on AODV Based Mobile Ad-hoc Networks", International Journal of Computer and Communication Technology(IJCCT),2011.
7. Marjan Kuchaki Rafsanjani, Zahra Zahed Anvari, Shahla Ghasemi "Methods of Preventing and Detecting Black/Gray Hole Attacks on AODV-based MANET", IJCa, NSC,2011.
8. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method ",International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007
9. Nital Mistry, Devesh C Jinwala, Member, IAENG, Mukesh Zaveri "Improving AODV Protocol against Blackhole Attacks", International MultiConference of Engineers and Computer Scientists, march17-19,2010,hong Kong.
10. Rajeshwar Singh, Dharmendra K Singh**,** Lalan Kumar " Performance Evaluation of DSR and DSDV Routing Protocols for Wireless Ad Hoc Networks", Int. J. Advanced Networking and Applications 732, Pages: 732-737 (2011).
11. Prem Chand, Deepak Kumar "Performance Comparison of Two On-Demands Routing Protocols for Mobile Ad-hoc Networks" , International Journal of Advances in Engineering & Technology, Sept 2011.
12. Madhusudhananagakumar KS, G. Aghila "A Survey on Black Hole Attacks on AODV Protocol in MANET", International Journal of Computer Applications (0975 – 8887) Volume 34– No.7, November 2011.
13. Sirisha Medidi and Peter Cappetto "History-based route selection for reactive ad hoc routing protocols", Pullman 99164-2752, USA.
14. Nilesh P. Bobade, Nitiket N. Mhala " Performance Evaluation of AODV and DSR On-Demand Routing Protocols with varying MANET Size", International Journal of Wireless & Mobile Networks (IJWMN) , February 2012..
15. Yi Xu, Wenge Wang "Detecting and Migrating Dos Attacks in Wireless Networks without affecting the normal behaving nodes", 1-4244-1513, IEEE, 2007 .