Prevention and Detection of Man in the Middle Attack On AODV Protocol

Kotad Surbhi V.[1] Asst. Prof. Ketan Patel[2]
[1]Student [2]Assistant Professor
[1,2]Department of Computer Engineering
[1,2]Growmore Faculty of Engineering, Himmatnagar

Abstract— In this paper it is discuss about AODV protocol and security attacks and man in the middle attack in detail. AODV Protocol is use to find route and very important protocol for communication in wireless network. So AODV protocol should be Secured and it is a big challenge. There are various attacks that occur on it. Here in this paper it discussed about the detection and preventions of man-in-the-middle attack in detail.

Key words: AODV, Man in the Middle Attack

I. INTRODUCTION

Wireless network is use for communication and use standard network protocols. These networks use microwaves/radio waves as a medium for communication. Mainly network can be categorized into two parts: infrastructure wireless network and infrastructure less wireless networks. In IWN, communication takes place between the nodes through the access point (AP) and well in ILWN does not need any fix infrastructure for communication and also there is no need of AP. These networks are also known as AD HOC networks. [1]

Ad-hoc network is a collection of nodes where all the nodes are dynamically configured without any centralized management. Ad-hoc network is used in many fields like military and police station, as disaster prevention, in robotics, etc. MANET disadvantage is that the various types of security attacks is occurs more as compare to wired network but it has advantage of establishing network at any place and at any time.[2]

II. AODV PROTOCOL

Ad hoc on-demand distance vector routing protocol is designed for ad hoc mobile networks. Ad hoc on-demand distance vector routing protocol uses unicast and as well as multicast routing. This protocol has the both the features of DSR and DSDV algorithm. Therefore it is used more as compare to DSR and DSDV protocols in mobile ad hoc network. In AODV protocol route is establish only when there is a demand and it maintain the route as long as they are needed, due to this advantage AODV Protocol is a better for mobile ad hoc network then other protocols. All the nodes in AODV protocol contain routing tables. The tables contain IP address of both destination and source, hope count and sequence number. Sequence number helps to avoid looping problems. If source node wants to send data to destination node then source broadcast a route request (RREQ) packet to the network. The node will replay with RREP if either the destination node or the intermediate node which is on the way to find the destination node. A node which receives the RREQ will send a reply (RREP) only if it either the destination or if it is a path route to the destination with a corresponding sequence number and only when that number is greater than or equal to the number which contains the RREQ. The AODV algorithm is as shown in figure 1. [3]

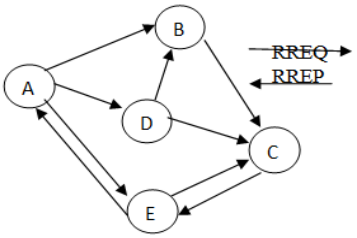

Fig. 1: AODV Algorithm

III. ATTACKS IN WIRELESS AD HOC NETWORKS

Authentication, availability, non-repudiation, confidentiality, privacy and integrity, are the goals for secure Ad hoc network. Classification of attacks occurs in ad hoc routing protocol, according to its security goals. The classification of attacks in wireless Ad hoc network is as shown in figure 2. [4]

IV. MAN IN THE MIDDLE ATTACK

In man in the middle attack the attacker can read and modify the message. When to parties communicate with each other and a third person comes in between and acts as sender/ receiver and communicates with them. The attack appears in many forms. [5] To complete man in the middle attack successfully the attacker has to convince both target nodes that it is source/ destination node. This is done by simply sending false route information. Now when the attacker knows that two nodes are communicating with each other she or he can send both the nodes new faked route message with a high sequence the nodes alter routing tables and starts communication with the attacker. [6]

In black hole attack an active insider can lie about having a new route to the destination and attract all the packets to it. Once it receives the packet it simple discards them without forwarding to the destination. Therefore the first stage of black hole attack can be considered as man in the middle attack. [7]

Fig. 2: Sender A communicate to B

Request sequence number scheme use creditable routing information which is formed and based on the acknowledgements received by the source from the destination. The information of the routing table is centered on the source node of the RREQ and is divided according to the trust value which in turn decides the routing path of the RREQ packets. This ensures that every node has valid information and man in middle and also black-hole attack can be prevented. [8] SLSP is used to prevent DOS attack, Man in the middle attack and it's suitable for authentication of new nodes and it does not suitable for real time traffic. [9]

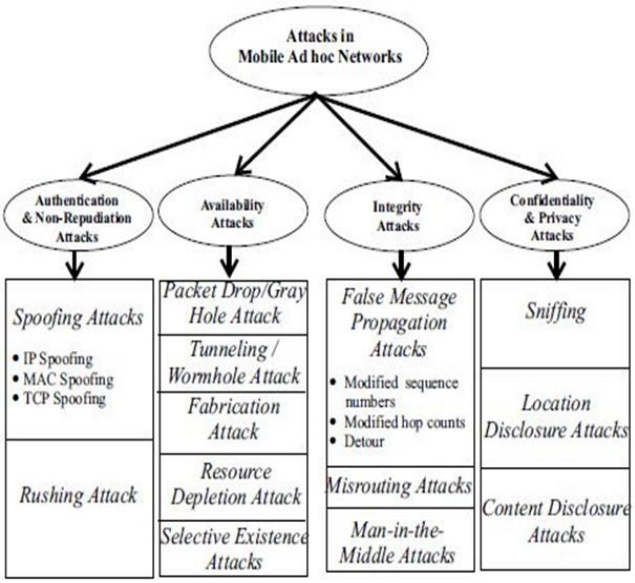

Fig. 3: Attacks in wireless Ad hoc networks

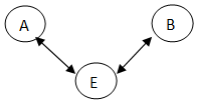

Fig. 4: Node E comes in-between

In path-base method next hop count information of routing table is used to detect the attack. As in scheme does net send out control messages it save the system resources to lower the false positive rate under high network overload, a collision rate reporting system is established in the MAC layer. This adaptive threshold approach decreases the false positive rates. [8] Signature verification is a technique in which the process done to prevent the attacks rather than detecting the attacks. Due to this the spoofing and its related attack like flooding attack and also man in the middle attack are reduced. [5]

V. CONCLUSION

In this paper man in the middle attack detection and prevention possible techniques used in AODV protocol are discussed. It is easy to prevent AODV protocol from man in the middle attack as compare to detection of it. It is difficult to recognize the attacker because here attacker behaves like sender or receiver it-self so to detect it a secure authentication should be provided to the users and also confidentiality should be provided to users. Request sequence number and next hop count are two routing table information by use of it one can recognize the attack. There is more technique use for detection and prevention purposes and not mention here and can be studied.

REFERENCE

[1] Neelam Khemariya, Ajay Khunteta, Krishna Kumar Joshi," A Robust Technique for Secure Routing Against Blackhole Attack in AODV Protocol for MANETs", International Journal of Scientific & Engineering Research, Vol-4, Issue 6, June-2013, ISSN 2229-5518.

[2] Rajul Chowksi, "Effect of Rushing Attack in AODV and its Prevention Technique", International Journal of Computer Applications (0975 – 8887), Volume 83 – No.16, December 2013.

[3] Dimple Saharan, "Detection & Prevention of Wormhole attack on AODV Protocol in Mobile Adhoc Networks (MANETS)", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 9 September 2014 Page No. 7979-7985

[4] Giovanni Vigna, Sumit Gwalani, Kavitha Srinivasan, Elizabeth M. Belding-Royer Richard A. Kemmerer "An Intrusion Detection Tool for AODV-based Ad hoc Wireless Networks", 2004.

[5] B.Dineshbabu, T.Thirunavukarasu, "Prevention of Spoofing Attacks in Wireless Sensor Networks", Vol. 5 (3), 2014

[6] Namrata Marium Chacko, Getzi P. Leelaipushpam, "A reactive protocol for privacy preserving using location based Routing in MANETs", International Journal of Computer Science and Network, Vol- 2, Issue 2, April 2013

[7] Abu Taha Zamani, Javed Ahmad" A Novel Approach to Security in Mobile Ad Hoc Networks(MANETs)", International Journal of Computer Science and Information Technology Research ISSN 2348-120X, Vol. 2, Issue 1, pp: (8-17), Month: January-March 2014

[8] J. Godwin Ponsam1, Dr. R.Srinivasan2, "A Survey on MANET Security Challenges, Attacks and its Countermeasures", IJETTCS, Volume 3, Issue 1, January – February 2014

Book

[9] Kaarina Karppinen, "Security Measurement based on Attack Trees in a Mobile Ad Hoc Network Environment", VTT publications 580, ESPOO 2005

