Volume 3, Issue 3, March 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Black hole attack in Manet

Puneet Kansal[*]
Assistant Professor
Department of Computrer Sc.&Engg
PIET Kurukshetra Universty

Nishant Prabhat
Assisatnt Professor
Department of Computrer Sc.&Engg
PIET Kurukshetra Universty

Amit Rathee
Assisatnt Professor
Department of Computrer Sc.&Eng
PIET Kurukshetra Universty

Abstract— The black hole attack in wireless Ad Hoc traffic between victim node and the malicious node then network is major issue that needs efficient solutions. In black hole attack more than one node can be malicious. Most of the time black hole attack occurs in large Ad Hoc networks. The black hole attacks in wireless Ad Hoc network creates misunderstanding in network by introducing error in routing information that leads the node to select wrong path hence data lose occur. Ad Hoc network by introducing automatic error correction in routing information that leads the node to select correct path thus secure transmission will take place between source and destination. The black hole attack is major problem for the wireless network and needs better solutions. In black hole attack the victim node sends the request for shortest path that leads its data towards destination.

Keywords— AODV, Ad-hoc network, Black Hole Attack, malicious node, Security

I. INTRODUCTION

An ad hoc network is a collection of nodes that do not need to rely on a predefined infrastructure to keep the network connected. Ad hoc networks can be formed, merged together or partitioned into separate networks on the fly, without necessarily relying on a fixed infrastructure to manage the operation. Nodes of ad hoc networks are often mobile, which also implicates that they apply wireless communication to maintain the connectivity, in which case the networks are called as mobile ad hoc networks [2]

The most important feature of the Ad hoc is that its network topology changes with the movement of the nodes, therefore, the communicating mode has a certain difference between it and the general network, and each node in Ad hoc network has the functions of host and router. In recent years Ad Hoc network technology is a very active research field; however, most research has focused on the key technologies of multi-hop routing. Although a great many routing protocol were raised, but which rarely considered the security issue of Ad Hoc network. This paper analyzes the routing protocol security of the Ad Hoc network, introduces the working principle of the AODV protocol and optimizes the reconstruction process of the AODV routing in detail, and emphatically analyzes the potential safety hazard of the AODV protocol and presents a black hole solution.

1.2AODV ROUTING PROTOCOL

AODV (Ad Hoc on Demand Distance Vector Routing) [2] is an important Ad Hoc Network on-demand routing protocol, it generates routing only when the source nodes need. AODV routing protocol receives widespread concern for its most performance indexes such as network overhead and the algorithm complexity are superior to others, which is also considered as one of the most practical prospects for the Ad Hoc network routing protocol, it has been standardized by the IETF nowadays. When a node (the source node) needs to communicate with another (the destination node) of the network while there is no legitimate routing information to the destination in the source node routing table, the source node will launch the process of finding routing. The steps for finding and establishing routing as shown in Figure 1:

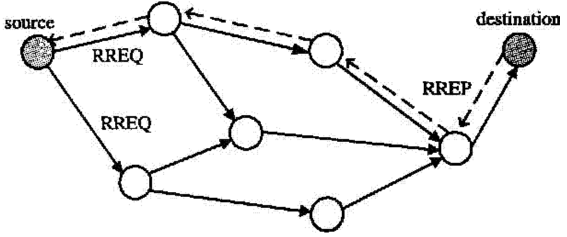

Figure 1. AODV routing request

(1)Source node broadcasts a routing requirement (RREQ) to its neighbor nodes. RREQ includes the following six items: <source-addr, source-sequence-#, broadcast-id, dest-addr, dest-sequence-#, hop-cnt>, among which the source-addr and broadcast-id can identify a sole RREQ packet.

(2) After receiving RREQ package, the intermediate nodes automatically create a reverse routing pointing to the upper hop node which transmits RREQ package to it. At the same time, investigating its routing table in the purpose of detecting whether there is routing to the destination node and whether the routing is new enough, if so, transmitting the response package (RREP) to source node from the reverse routing, and

if not, then broadcasting out after adding one to hop-cnt. If the node receives RREQ packets marked the same source-addr and broadcast-id and then discarding it directly, that is, only deal with the first arrival of RREQ process which avoids the circular of routing. RREQ packet broadcasts along this way,
finally arrives at the destination node.
(3) After receiving RREQ, the destination nodes will also select the first RREQ to establish the reverse routing, at the same time, sending the response packet RREP (unicast) to the source node from reverse routing. RREP includes the following five pieces of information: <Source-addr, dest-addr, dest-sequence-#, hop-cnt, lifetime>.
(4) Each intermediate node received RREP will set up an indicator pointing to the neighborhood node of RREP (at the same time this node owns indicator pointing to its up and downstream neighborhood node) and record the latest series of destination nodes. And then sending the RREP to the direction of the destination node through the last established reverse routing. The other nodes that received RREQ establish reverse routing will delete the reverse routing indicators automatically in a certain period of time (that is the survival time of reverse routing) because of not receiving RREP.
(5) After RREP eventually reach the destination node, then the destination node can transmit data through the just-established.

2. Related Work

Maha Abdelhaq1, Sami Serhan, Raed Alsaqour3 and Rosilah Hassan et al [1] Mobile Ad hoc Network (MANET) is a group of wireless nodes that are distributed without relying on any standing network infrastructure. MANET routing protocols were designed to accommodate the properties of a self organized
environment without protection against any inside or outside network attacks. a Local Intrusion Detection (LID) security routing mechanism to detect Black Hole Attack (BHA) over Ad hoc On Demand Distance Vector (AODV) MANET routing protocol. In LID security routing mechanism, the intrusion detection is performed locally using the previous node of the attacker node instead of performing the intrusion detection via the source node as in Source Intrusion Detection (SID) security routing mechanism. By performing LID security routing mechanism, the security mechanism overhead would bedecreased. Simulation results using the GloMoSim simulator show that the improvement ratio of the throughput gained by LID security routing mechanism and overall improvement reduction in the end-to-end delay and routing overhead.
Nidhi Purohit, Richa Sinha and Khushbu Maurya)et al [2] Wireless networks are gaining popularity to its peak today, as the user's wants wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). The attacks studied in this paper are against the routing protocols inMobile ad hoc network. We have used AODV for simulating this attacks using NS3. Black hole attack is one of the security threat in which the traffic is redirected to such a node that drops all the packets or the node actually does not exist in the network. Black holes refer to places in the network where incoming traffic is silently discarded or dropped. Jellyfish (JF) attack is a type of selective black hole attack. When JF node gets hold of forwarding packet it starts delaying/dropping data packets for certain amount of time before forwarding normally. Since packet loss is common in mobile wireless networks, the attacker can exploit this fact by hiding its malicious intents using compliant packet losses that appear to be caused by environmental reasons .
Alekha Kumar Mishra, Bibhu Dutta Sahoo et al [3] Mobile ad hoc networks are vulnerable to various security threats because of its dynamic topology and self configurable nature. SAODV (secured Ad hoc On Demand Vector routing) is one of the popular existing secured mechanism which takes help of digital signature and hash chain techniques to secured AODV packets. Since, digital signature technique consumes heavy computational time, the degradation of SAODV performance can be a major issue. In a recent work called A-SAODV(Adaptive SAODV), an adaptive mechanism that tunes the behaviour of SAODV t improve its performance. In this paper we have proposed an extension to Adaptive-SAODV of the secure AODV protocol extension, which includes further filtering strategies aimed at improvingits performance. Moreover, we analyze how our proposed algorithm can help to further improve the performance of adaptive SAODV.
King Sun Chan1 and Mohammad Rafiqul Alam et al [5] There are many forms of Byzantine attacks, including byzantine black hole attack, Byzantine flood rushing attack, and byzantine wormhole attack. Among all these attacks, Byzantine wormhole attack is considered one of the most complicated and severe attack in mobile ad hoc networks (MANET). In Byzantine wormhole attack, a compromised attacker actively participates in all network functions, and at the same time records packets at one location, tunnels them to another location, and then retransmits them there into the network. Most of the existing solutions targeting Byzantine wormhole attack rely on encryption and authentication which tries to detect packet dropping or modification. propose to detect some abnormal topological features introduced by Byzantine wormhole tunnel to detect Byzantine wormhole attack. Our scheme is easy to implement. The simulation results also show that our scheme can achieve both high Byzantine wormhole detection rate and detection accuracy.

3. Black Hole Attack

A packet drop attack or black hole attack is a type of denial-of-service attack accomplished by dropping packets. Black holes refer to places in the network where incoming traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its intended recipients [8,9]. Black Hole attacks effects the packet delivery and to reduce the routing information available to the other nodes causes: (i) It down grade the communication, (ii) Effects of making the destination node reachable.

In this method the AODV protocol is used and NS2 simulator is used. The detection scheme used neighborhood-based method to detect the black hole attack and then present a routing recovery protocol to build the true

path to the destination. Based on the neighbor set information, a method is designed to deal with the black hole attack, which consists of two parts: detection and response. In detection procedure,
two major steps are:
Step 1- Collect neighbor set information.
Step 2- Determine whether there exists a black hole attack.

Table 3.1 Black Hole Attack

Caused by RREQ	Caused by RREP
Set the originator IP address in RREQ to the originating nodes IP address.	Set the originator IP address in RREQ to the originating nodes IP address.
Set the destination IP address in RREQ to the originating nodes IP address.	Set the destination IP address in RREQ to the originating nodes IP address.
Set the destination IP address of IP Header to broadcast address	Set the destination IP address of IP Header to IP address of node that RREQ has been received
Set the source IP address of IP header to its own IP address	Set the source IP address of IP header to its own IP address

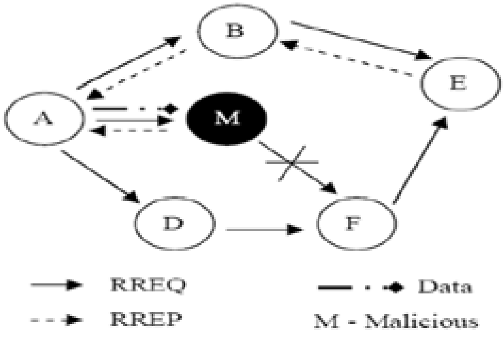

Figure 3.1 Black hole attacks in AODV

REFERENCES

1]Maha Abdelhaq1, Sami Serhan2, Raed Alsaqour3 and Rosilah Hassan"A Local Intrusion Detection Routing Security over MANET Network" 2011 International Conference on Electrical Engineering and Informatics 17-19 July 2011, Bandung, Indonesia.

[2] Nidhi Purohit, Richa Sinha and Khushbu Maurya" Simulation study of Black hole and Jellyfish attack on MANETusing NS3" INSTITUTE OF TECHNOLOGY, NIRMA UNIVERSITY, AHMEDABAD – 382 481, 08-10 DECEMBER, 2011.

[3] Alekha Kumar Mishra, 2Bibhu Dutta Sahoo" A MODIFIED ADAPTIVE-SAODV PROTOTYPE FOR PERFORMANCE ENHANCEMENT IN MANET" INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS IN ENGINEERING TECHNOLOGY AND SCIENCES (IJ-CA-ETS)

[4] King Sun Chan1 and Mohammad Rafiqul Alam" TCBWD: Topological Comparison-based Byzantine Wormhole Detection for MANET"2011 IEEE International Conference on Wireless and Mobile Computing.

[5] Adrian Perrig" SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks" Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02) 0-7695-1647-5/02 $17.00 © 2002 IEEE.

6] Kimaya Sanzgiri_ Bridget Dahilly Brian Neil Leviney Clay Shieldsz Elizabeth M. Belding-Royer "A Secure Routing Protocol for Ad Hoc Networks "Proceedings of the 10 th IEEE International Conference on Network Protocols (ICNP'02) 1092-1648/02 $17.00 © 2002 IEEE.

[7] Suman Sarkar "Hybrid Wireless-Optical Broadband-Access Network (WOBAN): A Review of Relevant Challenges" JOURNAL OF LIGHTWAVE TECHNOLOGY, VOL. 25, NO. 11, NOVEMBER 2007.

8] H. Weerasinghe and H. Fu, "Preventing cooperative black hole attacks in mobile ad-hoc networks: simulation, implementation and evaluation," International Journal of Software Engineering and Its Applications, Vol. 2, No. 3 (2008) pp. 39-54.

[9] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless adhoc network," IEEE Communications Magazine, vol. 40, no. 10 (2002) pp. 70-75.

[10] P. Raj and P. Swadas, "A dynamic learning system against black hole attack in AODV based MANET," IJCSI International Journal of Computer Science, Vol. 2, (2009) pp. 54-59.

[11] S. Sharma and R. Gupta, "Simulation study of blackhole attack in the mobile ad-hoc networks," Journal of Engineering Science and Technology, Vol. 4 , No. 2 (2009) pp. 243-250.