ISSN:2229-6093

PERFORMANCE ANALYSIS OF MANET BEFORE AND AFTER BLACK HOLE ATTACK

Ms.Heena Bhalla [1]
Desh Bhagat Institute of Engg. &tech(Moga)[1]
Heena.bhalla11@gmail.com

Abstract

A Mobile ad-hoc network is a temporary network set up by wireless mobile computers (or nodes) moving arbitrary in the places that have no network infrastructure. Due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. One of the prominent attacks is the Black Hole Attack which absorbs all data packets in the network. Since the data packets do not reach the destination node on account of this attack, data loss will occur. In this paper we simulated MANETs with and without Black Hole to study the effects of Black hole attack on network performance. Because of Black Hole Attack the average packet drop increased form 0.25% to 90.69% . The throughput of the network decreased 93.56% due to Black Hole effect.

1. Introduction

Ad hoc network is a wireless network without having any fixed infrastructure. Each mobile node in an ad hoc network moves arbitrarily and acts as both a router and a host. A wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure. The interconnections between nodes are capable of changing on a continual and arbitrary basis. Nodes within each other's radio range communicate directly via wireless links, while those that are far apart use other nodes as relays. Nodes usually share the same physical media; they transmit and acquire signals at the same frequency band. However, due to their inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks.

Black hole attack is one of many possible attacks in MANET. Black hole attack can occur when the malicious node on the path directly attacks the data traffic and intentionally drops, delay or alter the data traffic passing through it. This attack can be easily lessen by setting the promiscuous mode of each node and to see if the next node on the path forward the data traffic as expected. Another type of black hole attack is to attack routing control traffic.

2. SECURITY ATTACKS

There are numerous kinds of attacks in the mobile ad hoc network, almost all of which can be classified as the following two types:

External attacks: In this attack the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services.

Internal attacks: It is an attack in which the opponent wants to gain the normal access to the network and participates the network activities by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviours.

Denial of Service (DoS): It aims to crab the availability of certain node or even the services of the entire ad hoc networks. In the traditional

wired network, the DoS attacks are carried out by flooding some kind of network traffic to the target so as to exhaust the processing power of the target and make the services provided by the target become unavailable.

Impersonation: Impersonation attack is a severe threat to the security of mobile ad hoc network. If there is not such a proper authentication mechanism among the nodes, the opponent can capture some nodes in the network and make them look like benign nodes. In this way, the compromised nodes can join the network as the normal nodes and begin to conduct the malicious behaviors such as propagate fake routing information and gain inappropriate priority to access some confidential information.

Eavesdropping: Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. It aims to obtain some confidential information that should be kept secret during the communication. The information may include the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access.

Sinkhole attack: The attacking node tries to offer a very attractive link e.g. to a gateway. Therefore, a lot of traffic bypasses this node. Besides simple traffic analysis other attacks like selective forwarding or denial of service can be combined with the sinkhole attack.

Wormhole attack: The attacker connects two distant parts of the ad hoc network using an extra communication channel (e.g. a fast LAN connection) as a tunnel. As a result two distant nodes assume they are neighbors and send data using the tunnel. The attacker has the possibility of conducting a traffic analysis or selective forwarding attack.

Sybil attack: The Sybil attack especially aims at distributed system environments. The attacker plays multiple roles. It tries to act as several different identities/nodes rather than one. This allows him to forge the result of a voting used for threshold security methods for more information. The cloud appears to be many different nodes to the outside.

Traffic Analysis: It is a passive attack used to gain information on which nodes communicate with each other and how much data is processed.

2.1 BLACK HOLE ATTACK

In this attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. An attacker listen the requests for routes in a flooding based protocol. When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route. If the malicious reply reaches the initiating node before the reply from the actual node, a fake route gets created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. It can drop the packets between them to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack.

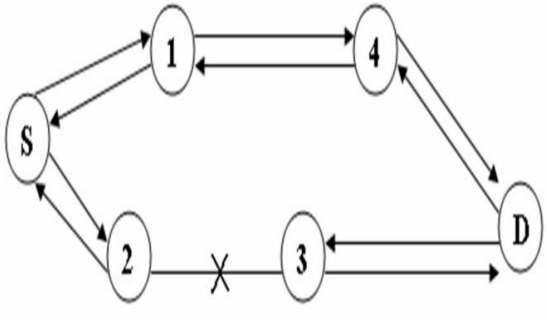

Figure 2.1 Black hole attack

For example, in Figure 2.1, source node S wants to send data packets to destination node D and

initiates the route discovery process. We assume that node 2 is a malicious node and it claims that it has route to the destination whenever it receives route request packets, and immediately sends the response to node S. If the response from the node 2 reaches first to node S then node S thinks that the route discovery is complete, ignores all other reply messages and begins to send data packets to node 2. As a result, all packets through the malicious node is consumed or lost.

3. Proposed work

6 UDP connections are established between nodes (0-7, 1-8, 2-9, 3-10, 4-11, 5-12, 6-13). We used 15 nodes in each scenario where Node 14 did not have a connection to any other node in the network. (Node 0 - Node 6) are the sending nodes and (Node 7 - Node 13) are the receiving nodes. Thus, we could count the sent and received packets between any 2 nodes. UDP agents are attached to the (0-6) nodes and NULL agents are attached to (7-13) nodes.

In all the scenarios, we have a total of 7 connections between 14 nodes and all of these connections are always between the same nodes. But, in each scenario, node (14) exhibits different movements. This helps to get different results with the same nodes.

We attach the CBR (Constant Bit Rate) application that generates constant packets through the UDP connection. Duration of the scenarios is 100 seconds and the CBR connections starts at the 20th second of the scenario and lasts till end. In our scenarios CBR parameters are; Packet Size: 500 bytes, Interval: 0.1sec. Parameters chosen are such that the packet loss due to other reasons except black hole is negligible. CBR connections are created by "for" loop. Nodes in the simulation are also generated by "for" loop statement of the Tcl language. The first loop creates the first 14 nodes that use the configuration.

```
set val(chan)  Channel/WirelessChannel ;
#channel type
set val(prop)  Propagation/TwoRayGround;
#radio-propagation model
set val(ant)   Antenna/OmniAntenna     ;
#Antenna type
set val(ll)    LL                      ;
#Link layer type
set val(ifq)   Queue/DropTail/PriQueue ;
#Interface queue type
set val(ifqlen)50                      ;
#max packet in ifq
set val(netif) Phy/WirelessPhy         ;
#network interface type
set val(mac)   Mac/802_11              ;
#MAC type
set val(rp)    AODV                    ;
# ad-hoc routing protocol
set val(nn)    10                      ;
# number of mobilenodes
set val(x)     500                     ;
set val(y)     500                     ;
```

4. CONCLUSION

In this paper we have implemented black hole attack in AODV MANET and studied its impact

on the performance of MANET. For this purpose we implemented a new AODV routing protocol which behaves as black hole. We simulated scenarios, where each one has 15 nodes that use AODV protocol and also simulated the same scenarios after introducing one Black Hole Node into the network. In each scenario we changed the destination address of the black hole node. Due to the presence of black hole in the network the packet loss increases significantly.

In first case the average packet loss in network with black hole is 90.69 % and that of in normal AODV network is 0.25%. Here only the destination address of the black hole node is changed, as it is evident from the results in appendix D that its impact on the results of different scenarios is negligible. Thus changing the destination position of the black hole node in a small MANET does not have much significance.

6 FUTURE WORK

We simulated the Black Hole Attack in the Ad-hoc Networks and investigated its affects. In our study, we used the AODV routing protocol. But the other routing protocols could be simulated as well. All routing protocols are expected to present different results. Therefore, the best routing protocol for minimizing the Black Hole Attack may be determined. In our thesis, we tried to see the impact of the Black Hole in the network. In future we intend to work towards the detection and solution of the Black Hole attack.We also intend to work on other possible attacks on the network layer of MANET.

7. References

[1] Mohammad AL-Shurman,Seon-Moo Yoo and Seungiin Park," Black Hole Attack in Mobile Ad Hoc Networks" ACMSE'04,April 2-3, 2004.

[2] Payal N. Raj and Prashant B. Swadas,"DPRAODV: A dynamic learning system against black hole attack in AODV based Manet", International Journal of Computer Science Issues (IJCSI), Vol. 2, Issue 3, pp: 54-59, 2009

[3]Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks".

[4] Chang Wu Yu, Tung-Kuang, Wu, Rei Heng, Cheng, and Shun Chao Chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks", PAKDD Workshops, pp. 538–549, 2007.

[5] Chen Hongsong; Ji Zhenzhou; and Hu Mingzeng. A novel security agent scheme for AODV routing protocol based on thread state transition. Asian Journal of Information Technology, 5(1), 54-60, 2006

[6] Tamilselvan, L.; and Sankaranarayanan, V. (2007). Prevention of blackhole attack in MANET. The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications. AusWireless, 21-21.

[7] Dokurer, S.; Ert, Y.M.; and Acar, C.E. (2007). Performance analysis of ad hoc networks under blackhole attacks. SoutheastCon, 2007, Proceedings IEEE, 148 – 153.

[8] Scalable Network Technologies (SNT). QualNet. http://www.qualnet.com/.

[9] Sanjay Ramaswamy; Huirong Fu; Manohar Sreekantaradhya; John Dixon; and Kendall Nygard (2003). Prevention of cooperative blackhole attack in wireless Ad hoc networks. In Proceedings of 2003 International Conference on Wireless Networks, (ICWN'03), Las Vegas, Nevada, USA, pp. 570-575.

[10] C. E. Perkins; E. M. Belding-Royer; and S. R. Das (2003). Ad hoc on demand distance vector (AODV) routing. RFC 3561. The Internet Engineering Task Force, Network Working Group.

[11] Satoshi Kurosawa; Hidehisa Nakayama; Nei Kato; Abbas Jamalipour; and Yoshiaki Nemoto (2007). Detecting blackhole attack on AODV based mobile Ad hoc networks by dynamic learning.