Detection and Prevantion of Black Hole Attack over Manet

Raghvendra Prasad
Fourth Semester M.Tech, LNCT Indore

ABSTRACT

The black hole attack is one of the well-known security threats in wireless mobile ad hoc networks. The intruders utilize the loophole to carry out their malicious behaviors because the route discovery process is necessary and inevitable. Many researchers have conducted different detection techniques to propose different types of detection schemes. In this paper, we survey the existing solutions and discuss the state-of-the-art routing methods. We not only classify these proposals into single black hole attack and collaborative black hole attack but also analyze the categories of these solutions and provide a comparison table. We expect to furnish more researchers with a detailed work in anticipation.

KEYWORDS: *mobile ad hoc networks, routing protocols, single black hole attack, collaborative black hole attack*

I. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of wireless mobile nodes which have the ability to communicate with each other without having fixed network infrastructure or any central base station. Since mobile nodes are not controlled by any other controlling entity, they have unrestricted mobility and connectivity to others. Routing and network management are done cooperatively by each other nodes. Due to limited transmission power, multi hop architecture is needed for one node to communicate with another through network. In this multi hop architecture, each node works as a host and as well as a router that forwards packets for other nodes that may not be within a direct communication range. Each node participates in an ad hoc route discovery protocol which finds out multi hop routes through the mobile network between any two nodes. These infrastructure-less mobile nodes in ad hoc networks dynamically create routes among themselves to form own wireless network on the fly. Thus, mobile ad hoc networks provide an extremely flexible communication method for any place where geographical or terrestrial constraints are present and need network system without any fixed architecture, such as battlefields, and some disaster management situations. Recent research on MANET shows that the MANET has larger security issues than conventional networks [1,2]. Any security solutions for static networks would not be suitable for MANET. Zhou et al. [1] and Lundberg [3] discussed several types of attacks that can easily be performed against a MANET. In the black hole attack, malicious nodes provide false routing information to the source node whose packets they want to intercept. In denial of service attacks, malicious node floods the targeted node so that the network or the node no longer operates correctly. In route table overflow attacks, an attacker tries to create lots of routes to non existence nodes and overflows the routing tables. In impersonation attacks, malicious node may impersonate another node while sending the control packets to create an anomaly update in routing table. In this paper, we will focus on the black hole and cooperative black hole attacks. The main contributions of this work are threefold. First, we implement the simulation of the solutions proposed for the cooperative black hole attacks. Second, we also add some changes to the algorithm to improve the accuracy in preventing black hole attacks. For example, previously the algorithm does not check current intermediate node for black hole if the next hop is not reliable. This proposed algorithm does not give any details about the implementation of the algorithm. In this paper we completely describe the implementation details which we address the several issues which are not considered in [9]. Finally, we compare the performance of the modified solution with other existing solutions in terms of throughput, end-to-end delay,

II. RELATED WORKS

The routing protocols proposed for MANETs can be classified into four broad categories [4]: Flat routing, Hierarchical routing, GPS routing, and Power based routing. Flat routing is the most widely used category. These flat routing protocols can be further classified into two main sub groups [6]: table driven and on-demand routing protocols. The table driven routing protocol is a proactive scheme in which each node maintains consistent and up to date routing information to every other node in the network. Every routing change in the network should be propagated through the network in order to maintain consistent routing information. In the on-demand routing (reactive routing), any node creates route only when it needs to send some data to the destination. The source node initiates route discovery process when necessary. There are three main routing protocols proposed for MANETs [4]: Ad hoc on demand Distance Vector (AODV) [5] routing, Dynamic Source Routing [DSR] [6], and Destination Sequence Distance Vector routing (DSDV) [7]. AODV and DSR belong to on-demand routing protocols and DSDV is a table-driven routing protocol. In this paper, we focus on AODV. However, the proposed solution is also applicable to other on-demand protocols, such as DSR. The AODV protocol is vulnerable to the well-known black hole attack. A black hole is a node that always responds positively with a RREP message to every RREQ, even through it International Journal of Software Engineering and Its Applications Vol. 2, No. 3, July, 2008 41 does not really have a valid route to the destination node. Since a black hole node does not have to check its routing table, it is the first to respond to the RREQ in most cases. Then the source routes data through the black hole node, which will drop all the data packets it received rather than forwarding them to the destination. In this way the malicious node can easily misroute lot of network traffic to itself and could cause an attack to the network with very little effort on it. These black hole nodes may work as a group. That means more than one black hole nodes work cooperatively to mislead other nodes.

This type of attack is called cooperative black hole attack. Researchers have proposed solutions to identify and eliminate black hole nodes . Deng et al. proposed a solution for individual black holes. But they have not considered the cooperative black hole attacks. According to their solution, information about the next hop to destination should be included in the RREP packet when any intermediate node replies for RREQ. Then the source node sends a further request (FREQ) to next hop of replied node and asks about the replied node and route to the destination. By using this method we can identify trustworthiness of the replied node only if the next hop is trusted. However, this solution can not prevent cooperative black hole attacks on MANETs. For example, if the next hop also cooperates with the replied node, the reply for the FREQ will be simply “yes” for both questions. Then the source will trust on next hop and send data through the replied node which is a black hole node. Ramaswamy et al. proposed a solution to defending against the cooperative black hole attacks. no simulations or performance evaluations have been done. Ramaswamy et al. studied multiple black hole attacks on mobile ad hoc networks. However, they only considered multiple black holes, in which there is no collaboration between these black hole nodes. In this paper, we evaluate the performance of the proposed scheme in defending against the collaborative black hole attack. Yin et al. proposed a solution to defending against black hole attacks in wireless sensor networks. The scenario that they considered in sensor networks is quite different than MANETs. They consider the static sensor network with manually deployed cluster heads. They did not consider the mobility of nodes. Also they have one sink node and all sensors send all the data to the sink. Each node needs to find out the route only to the sink. Since this scenario is not compatible with MANET, we are not going to discuss it further. In this paper we simulate the algorithm proposed with several changes to improve the accuracy of preventing cooperative black hole attacks and to improve the efficiency of the process. We also simulate AODV

Blackhole attack: In this attack a malicious node may advertise a good path to a destination during routing process. The intention of the node may be to hinder the path finding process or interpret the packet being sent to destination. Alternatively black-hole scenario may be defined as the one in which the cannel properties tend to be asymmetric i.e. the signal strength in both direction may not be same. In this case a node which receives the data packet but does not forward it is termed as black hole. In either case the normal operation of the MANET is disrupted.

Wormhole attack: In this attack , an attacker receives packets at one location and tunnels them at another location where these packets are resent into the network. In the absence of proper security mechanisms, most of the existing routing protocols may fail to find the valid routes.

Byzantine attack: Here compromised intermediate nodes carries out attack such as loops, routing packets on non optimal paths and selectively dropping packets.

Information disclosure: A compromised network node may leak the important or confidential information such as network topology, geographical information of nodes and optimal routes to the nodes etc.

Resource consumption attack: An attacker node acting as intermediate node may initiate unnecessary request for routes, frequent generation of beacon packets or forwarding stale routes to nodes. This result in over consumption of nodes limited resources and keeps the node unnecessary occupied.
In this paper we analyze the impact of the presence of the black-hole nodes on the MANET performance. We have found that as the percentage of black hole nodes increases, the network performance degrades.

AD-HOC ROUTING PROTOCOLS AND BLACK HOLE ATTACK : An ad-hoc routing protocol[8] is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network. Being one of the category of ad-hoc routing protocols, on-demand protocols such as AODV [4] (Ad-hoc On demand Distance Vector) and DSR (Dynamic Source Routing) establish routes between nodes only when they are required to route data packets. AODV is one of the most common ad-hoc routing protocols used for mobile ad-hoc networks. As its name indicates AODV is an on-demand routing protocol that discovers a route only when there is a demand from mobile nodes in the network. In an ad-hoc network that uses AODV[4][6] as a routing protocol, a mobile node that wishes to communicate with other node first broadcasts an RREQ (Route Request) message to find a fresh route to a desired destination node. This process is called route discovery Every neighboring node that receives RREQ broadcast first saves the path the RREQ was transmitted along to its routing table. It subsequently checks its routing table to see if it has a fresh enough route to the destination node provided in the RREQ message. The freshness of a route is indicated by a destination sequence number that is attached to it. If a node finds a fresh enough route, it unicast an RREP (Route Reply) message back along the saved path to the source node or it re-broadcasts the RREQ message otherwise. Route discovery is a vulnerability of on-demand ad-hoc routing protocols, especially AODV, which an adversary can exploit to perform a black hole attack on mobile ad-hoc networks. A malicious node in the network receiving an RREQ message replies to source nodes by sending a fake RREP message that contains desirable parameters to be chosen for packet delivery to destination nodes. After promising (by sending a fake RREP to confirm it has a path to a destination node) to source nodes that it will forward data, a malicious node starts to drop all the network traffic it receives from source nodes. This deliberate dropping of packets by a malicious node is what we call a black hole attack.

III. CONCLUSION

In this paper, we studied the problem of cooperative black hole attacks in MANET routing. Due to the inherent design disadvantages of routing protocol in MANETs, many researchers have conducted diverse techniques to propose different types of prevention mechanisms for black hole problem. The proposals are presented in a chronological order and divided into single black hole and collaborative black hole attack. According to this work, we observe that both of proactive routing and reactive routing have specialized skills. The proactive detection method has the better packet delivery ratio and correct detection probability, but suffered from the higher routing overhead due to the periodically broadcast packets. The reactive detection method eliminates the routing overhead problem from the event-driven way, but suffered from some packet loss in the beginning of routing procedure. Therefore, we recommend that a hybrid detection method which combined the advantages of proactive routing with reactive routing is the tendency to future research direction. However, we also discover that the attacker's misbehavior action is the key factor. The attackers are able to avoid the detection mechanism, no matter what kinds of routing detection used. Accordingly, some key encryption methods or hash-based methods are exploited to solve this problem. The black hole problem is still an active research area. This paper will benefit more researchers to realize the current status rapidly.

REFERENCES

[1] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Computer Communications Review, pp. 234-244, October 1994.
[2] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network," IEEE Communications Magzine, vol. 40, no. 10, October 2002.
[3] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA
[4] Jian Yin, Sanjay Madria, "A Hierarchical Secure Routing Protocol against Black Hole", IEEE SUTC 2006 Taiwan, 5-7 June 2006.
[5] Xiaoyan Hong, Kaixin Xu, and Mario Gerla, "Scalable Routing Protocols for Mobile Ad hoc Networks," IEEE Network Vol. 16(4) pp11-21, July/August 2002.
[6] Elizabeth M. Royer and Chai-Keong Toh, "A Review of Current routing Protocols for Ad Hoc Mobile Wireless Networks," IEEE Personal Communications, pp 46-55, April 1999.

[7] Sanjay Ramaswamy, Huirong Fu, and Kendall E. Nygard, "Simulation Study of Multiple Black Holes Attack on Mobile Ad Hoc Networks," International Conference on Wireless Networks (ICWN' 05), Las Vegas, Nevada, Jun. 2005.

[8] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, ―Security in mobile ad hoc networks: Challenges and solutions‖ (2004). IEEE Wireless Communications. 11 (1), pp. 38-47.

[9] Hao Yang,Haiyun Luo, Fan Ye, Songwu Lu, Lixia Zhang,"Security in mobile ad hoc networks: challenges and solutions",Wireless Communications, IEEE Feb 2004.

[10] Hongmei Deng, Wei Li, D.P.Agrawal,"Routing security in wireless ad hoc networks",Communications Magazine, IEEE Oct 2002.

[11] B.Kannhavong, H.Nakayama, Y.Nemoto, N.Kato, A.Jamalipour,"A survey of routing attacks in mobile ad hoc networks",Wireless Communications, IEEE October 2007.