Black-Hole Attack in Mobile Ad-hoc Networks: A Review

Mr. Ankush Jain , Mr. Sandeep Gupta
Dept. of Electronics & communication, SD Bansal College of Technology, Indore

Abstract - A blackhole attack is one of severe security threat which not only impress nearest neighbor node to get better position but redirect traffic from self. It attracts neighbor nodes to drop packets with majority. Here, malicious node present itself in such a way that neighbor node should directly send packet through malicious node. The complete work observes AODV is vulnerable routing protocol for various security threats and may be compromise for blackhole attack. This research paper proposed detection and mitigation technique to avoid blackhole attack and improve the network performance. The complete work is simulated and evaluated on Qualnet simulator. Proposed solution is evaluated on basis of variable mobile node, pause time speed and area. Improved Throughput and Packet delivery ratio has been observed in proposed solution in compare with blackhole attack. Performance of proposed solution is similar with original AODV and tries to maintain privacy of content.

Keywords - MANET, Black-Hole, Security, Attacks.

1. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of mobile nodes or mobile devices which may be easily relocate and replace easily. Wireless medium is recommended to interconnect mobile nodes with radio frequency without using fixed infrastructure. Due to temporary network and decentralized control, every node is capable to work as router and discover route from source to destination. Thus, cooperation of nodes is suggested to forward packets and establish communication.

In mobile ad-hoc networks, nodes may be in stationary condition or may move with variable speed. Here, source and destination may not be directly connected with each other and require intermediate node to forward packet to ultimate destination. For example A is source node and D is destination which is slightly far away from source. Node B and C are in the intermediate position and placed between A and D. Here, A will forward packet to B with destination address of D. B will work as router and forward packet to C subsequently to D using respective routing table. Figure shows the block representation of mobile ad-hoc network.

Due to mobility factor, every node may join and move the ad-hoc network frequently. It gives an immense insecure environment where attacker node may join, attack and leave the node with rapid action. Thus there is strong requirement to enhance security level of ad-hoc network to ensure a flexible and handy vibrant network topology. Some of the MANET applications include emergency disaster relief, military operations over a battlefield, medical sensor network.

2. RELATED WORK

A number of techniqueshave been proposed on securing routing protocols against various attacks. A survey of these techniques is given in this section.

Manita et. al. [1] proposed a nature inspired technique to detect and mitigate blackhole attack. Proposed technique uses real world cases and develop solution model for computational problem. The Proposed Ant Colony Optimization technique is inspired from behavior and living style of real ant. It observes their living style and approach to find the shortest path between living area to food source. Proposed technique attempt to solve the blackhole attack problem and help to prevent it.

Rashmi, et. al. [2] address that a blackhole attack is an attack where malicious node broadcast falsely packets and impress genuine node for shortest fresh route. Here, malicious node may propagate falsely update or generate fake reply to attract packets. This research paper gives cluster based detection technique to detect malicious node. They simulate the complete solution in NS-2.35 and observe results on basis of detection rate throughput and packet delivery ratio.

R. Kaur, et. al. [3] explores the possibilities of cooperative blacklist attack and also investigates prevention technique to overcome the same. Here, single blackhole attack deploys with single malicious node but corporate blackhole attack deploy in group format. Due to different deployment strategy, corporate blackhole attack can't be resolve with traditional prevention techniques. Proposed solution

compares the registered signature with retrieved signature of intermediate node and observes the authenticity of route.

R. Prasad et al. [4] proposed a method to provide security for routing packets where the malicious node acts as a blackhole and drops packets. In this method, the collaboration of a group of nodes is used to make accurate decisions. In the proposed model validity of intermediate node, which forward RREQ or RREP packets in each hop is checked. Validating received RREPs allows the source to select trusted path to its destination. This technique increases overhead as the node that is forwarding RREQ or RREP packets need to acknowledge the intermediate node.

A. Sharma et al. [5] attempts to secure the AODV protocol, so that it can withstand the blackhole attack by adding an IDS_node to AODV protocol. IDS checks which node updates the routing table and sends higher sequence number to the sender node, if find out so IDS sends the message to the sender node for elimination of that particular path and search new route according to IDS instruction. IDS module provides only trust communication between sender and destination. After prevention trace analysis is done to detect blackhole node. The IDS module protect through the blackhole attack only if blackhole node is in the range of IDS. Using this technique, packet drop ratio is decreased by desirable amount.

3. BLACK-HOLE ATTACK

Mobile ad-hoc network faces various security threats aims to disrupt the performance of network. Such security threats may be passive or active depend on nature of security attack. Blackhole attack is one of severe security threat which applies on neighbor nodes. This section explains the details and basic brief of blackhole attack.

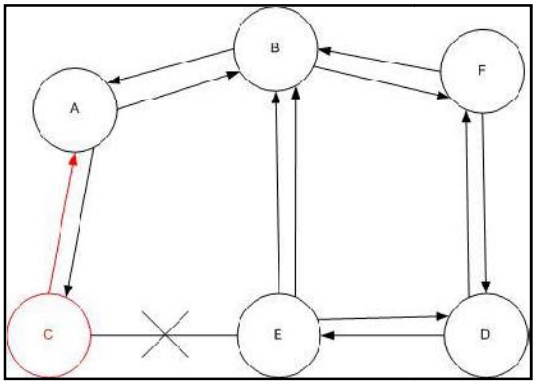

Fig. 2 Blackhole Problem

In blackhole attack, a malicious node uses its routing power capability to advertise itself as shortest neighbor node or every nearest mobile node to register itself for having shortest path towards destination. Afterwards, hostile nodes advertise for fresh route from source to destination, blackhole node captures this advertisement and frequently reply to add it as shortest path. When source node starts forwarding packet to destination, it goes from malicious node because of corrupt routing table. Hence all data packet will be redirected form malicious node and can be easily dropped.

Figure 2 shows how blackhole attack problem arise and drop packet respectively. Here, Node A send packet to node D and start route discovery. In any case if node C is malicious node it will claim for shortest route towards D and redirect all incoming through C. Now its depend on Node C whether to drop packet or not. But in any case Data packet will lose the privacy of information.

Black hole attack in AODV

The complete study observes that Blackhole attack may be deploying through two ways; which may be listed as follows;

1. Internal Blackhole Attack

2. External Blackhole Attack.

Internal Black hole attack

This type of attack applies through trusted node of networks. An Internal malicious attack attempts to compromise the most trusted node. It also tries to get benefit of reputation of trusted node. As soon as security system attempt to detect malicious node, it completed its task and affect the network performance. Internal attack is more severe then external attack because of difficulty to detect the internal behavior of mobile node.

External Black hole attack

This kind of attack is applies from external side of network. Here, malicious node attempt to compromise the mobile node by creating shortest path or disrupting network performance by flooding unwanted packets.

External black hole attack can be summarized in following points

a) Malicious node attempt to discover active route into destination path.
b) Attacker node compromises the RREP and spoofed the information.

c) Attacker node forward packet to all the nearest available nods. Which can be directly connected?
d) When neighbour node receives RREP they register attacker node as neighbour node and update routing table.
e) When source node forward packet to destination it redirect to malicious node an dropped as per attacker policy.

4. PROBLEM DEFINITION

The AODV routing protocol is a popular reactive routing protocol in wireless networks, but AODV routing protocol designed for better performance of the network not for security of node, secure protocols are generally designed to have features such as authentication, integrity, confidentiality and non-repudiation. For security purpose AODV have vulnerabilities and it is easily manipulate by malicious node to destroy its network routing.

Previously the works done on security issues i.e. attack (Black-Hole attack) involved in MANET were based on proactive routing protocol. Black-Hole attack is studied under the AODV routing protocol and its effects are elaborated by stating how this attack disrupt the performance of MANET. Very little attention has been given to the fact to study the impact of Black-Hole attack in MANET using both Reactive and Proactive protocols and to compare the vulnerability of both these protocols against the attack. There is a need to address both these types of protocols as well as the impacts of the attacks on the MANETs for detecting and preventing security threat based on AODV routing protocol.

In short, major concern with AODV is:-

- Insecure Routing
- Packet Dropping
- Security
- Uphold Confidentiality.

5. SOLUTION DOMAIN

One of the objectives of this research paper is to mitigate the effects of blackhole attack on the performance of on demand reactive routing protocol, AODV. Blackhole attack adversely affects the performance of AODV routing protocol. An adaptive technique is presented in this thesis work which is based on the on demand AODV routing protocol. The basic idea behind the proposed technique is based on Blackhole Detection System.

In the proposed work, every AODV node executes a BDS mechanism, i.e. each node in the network has a BDS agent in-built in the form of module with AODV routing protocol. BDS module estimates the suspicious of each node to recognize the high capability node into network. When a suspicious value for a neighboring node exceeds a threshold, then that node is isolated from the network as other nodes do not forward packets through the suspected malicious node.

6. CONCLUSION

This research work carried out the detailed study and analysis of AODV routing protocols and security issues and attacks in MANET theoretically and through simulation. The complete work concludes that proposed solution will successfully detect and mitigate the blackhole attack in MANET.

REFERENCES

[1] Manita, Vinay Nassa, Kapil Chawla, "*Improving AODV Protocol by Nature Inspired Technique against Blackhole and Grayhole Attacks in MANETs*", in Journal of International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 8, Aug.-14.

[2] Rashmi, Ameeta Seehra, "*Detection and Prevention of Black-hole Attack in MANETs*", in Journal of International Journal of Computer Science Trends and Technology(IJCST), Vol. 2, Issue 4, Aug.-14.

[3] Ravinder Kaur, Jyoti Kalra, "*Detection and Prevention of Blackhole Attack with Digital Signature*", in Journal of International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 8, Aug.-14.

[4] Raghvendra Prasad, Kuntal Barua, "*Implementation, Detection and Prevention of Blackhole Attack for MANET using NS-2* ", in Journal of International Journal of Science and Research, Vol. 3, Issue 3, March.-14.

[5] Ravinder Kaur, Jyoti Kalra, "*A review of Blackhole Attack in MANETs*", in Journal of International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 8, Aug.-14.