Black-Hole Attack in MANET: A Study

Minoti Puray, Patel College of Science and Technology, Indore, India
Priyanka Palod, Patel College of Science and Technology, Indore, India

ABSTRACT

Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. It's a real world analogy to the black hole in the universe in which things disappear. The node presents itself in such a way to the node that it can attack other nodes and networks knowing that it has the shortest path. MANETs must have a secure way for transmission and communication which is quite challenging and vital issue.

Study of previous work concludes that works done on security issues in MANET were based on different reactive routing protocol but still there is needs to avoid Black Hole attack in MANETs. This research work proposed detection and mitigation technique to avoid blackhole attack and improve the network performance. Performance of proposed solution is similar with original AODV and tries to maintain privacy of content.

Keywords: MANET, Black Hole, AODV

1. INTRODUCTION

In the traditional network environment, the communication depended on some infrastructures. For example, mobile phones need to connect with base stations; PDAs or laptops have to connect with access points or RJ-45 cable. And these portable equipments loose the connection ability when they leave the radio range of an access point or cable.

Wireless technology is allowing to access information and services electronically from everywhere. Wireless technology has become tremendously popular due to its usage in various new fields of applications in the domain of networking. The wireless communication revolution is bringing fundamental changes to data networking, telecommunication, and is making networking and communications, anytime, anywhere possible.

A mobile ad-hoc network is a self-organizing groundwork less network of mobile devices linked by a network. Each device in MANET is permitted to travel on any route, and will therefore alter its path to other devices frequently. And topology also changes instantly in the network. Each node should forward traffic distinct to its own use, means every node in the network is also acting as a router. Such networks may operate by themselves or may be joined to the larger Internet. It is the autonomous system of mobile hosts. It is shown in figure 1.

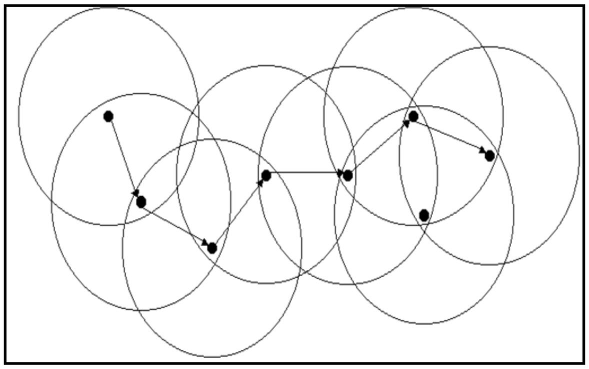

Figure 1: Mobile Ad-hoc Networks

A lot of researches in the last some years are estimated and implemented but the most significant contributions were the trust based security. In a challenge to improve security in MANET lots of researchers worked in a field, some have suggested new techniques and implemented innovative improvements in the protocols and some of them have recommended new protocols.

There are various types of attacks which try to degrade the performance of the network. Flooding attacks occur when a network becomes so heavily traffic loaded with unnecessary packets initiating requests for link that it can no longer process authentic connection requests. Flooding is reason for traffic and congestion in the network and thus incompleteness of legal connection. Once this buffer is full with request packet traffic become uncontrolled no extra connections can be made, and the result is a Denial of Service [2].

In an ad hoc wireless network wherever wired infrastructures don't seem to be likely, energy and information determine conservation are the two key parts presenting analysis challenges. Restricted information determines make a network simply overcrowded by management signals of the routing protocol. Routing scheme developed for wired networks uncommonly acquire into account limitations of this type. as an alternative, they suppose that the network is in general steady and also the overhead for routing messages is slight. Considering these variations between wired and wireless network, it's essential to develop a wireless routing protocol that restricts congestion within the network. The mobile unintended networks have many salient characteristics, like Dynamic topologies, Bandwidth-constrained, variable capability links, Energy-constrain operation, limited physical Security [3]. Owing to these options, mobile unintended networks are notably susceptible to denial of service attacks launched through compromised node.

2. RELATED WORK

Roopak, et. al [1] explore that MANET is the collection of mobile hosts interconnect for communication. Open nature make it vulnerable for various security attacks. Such security attack may leak the confidentiality of content and can disrupt the network. Blackhole attack is such kind of security threat which not only compromises the communication but also degrade the performance. They proposed solution to detect and prevent malicious node in the same. NS-2.34 simulator has been used to simulate the same.

[2] proposed an approach for mitigating the blackhole attack. The node which first receive the RREP packet, initiate the judgment process on replies and forward the packet to source. This judgment is based on opinion of network nodes about replier. After receiving the opinion of neighbour, the node decides whether the replier is malicious node or not. By using the opinion of neighbour node, honesty of nodes is judged. Node must show its honesty in order to transfer the data packets. The drawback of this solution is that there is no guarantee that the opinion of neighbour node is always correct.

[3] Presented an approach to find the black hole nodes in which secure routes are discovered by checking the sequence number. If the difference between the sequence number of source node and intermediate node which sent first RREP is large, then the probability of that node to be malicious is more. The first RREP by any intermediate node usually comes from malicious node. It this approach such node is immediately removed from routing table.

3. AODV ROUTING PROTOCOLS

AODV is a reactive routing protocol designed for ad hoc wireless networks. In AODV routes to connect two nodes are obtained only when it is required i.e. on demand. AODV routing algorithm is specially suited for dynamic self-configured networks like MANET. AODV provides loop free routes along with route management for broken links. Bandwidth requirement of mobile nodes in AODV is comparatively less than other protocols as AODV does not require periodic route advertisements.

There are three types of control messages in AODV which are discussed below.

Route Request Message (RREQ):

Source node that needs to communicate with another node in the network transmits RREQ message. AODV floods RREQ message, using expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.

Route Reply Message (RREP):

A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node.

Route Error Message (RERR):

Every node in the network keeps monitoring the link status to its neighbour's nodes during active routes. When the node detects a link crack in an active route, (RERR) message is generated by the node in order to notify other nodes that the link is down.

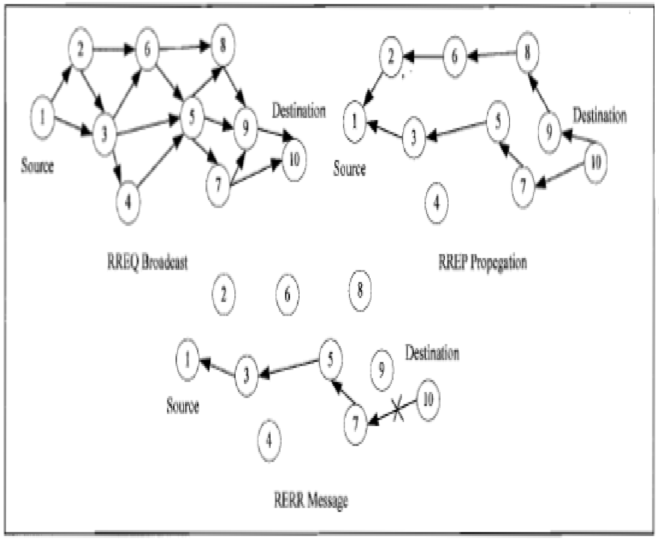

Figure 2: Working Scenario of AODV

4. BLACKHOLE ATTACK

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept.

This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address.

The method how malicious node fits in the data routes varies. Fig. 4.1 shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost.

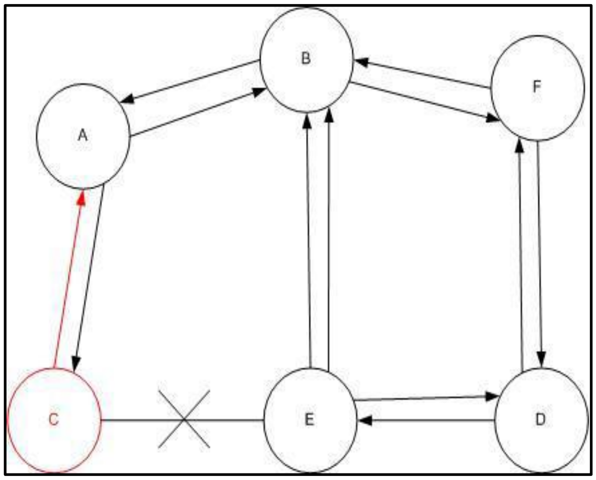

Fig. 3Black-Hole Problem

Black hole attack in AODV

Two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack.

A. Internal Black hole attack

This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element.

B. External Black hole attack

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET.

5. PROBLEM INVESTIGATION

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.

The Black-hole attack may be launched by a single or a pair of collaborating nodes. In commonly found two ended Black-hole, one end overhears the packets and forwards them through the tunnel to the other end, where the packets are replayed to local area. It either drops or selectively forwards the packets, leading to network disruption. Black-hole attack does not require MAC protocol information as well as it is immune to cryptographic technique. This makes it very difficult to detect.

6. SOLUTION DOMAIN

One of the objectives of this thesis work 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 will 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

7. 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 is divided into three categories such as without attack, with attack and preventive network. All the scenarios are evaluated on basis of variable nodes, speed, pause time and area for network. Performance evaluation is based on Throughput, Packet Delivery Ratio, End-to-End Delay and Jitter.

The complete work concludes that proposed solution successfully detect and mitigate the blackhole attack in MANET. It is also observe that proposed algorithm help to improve the network performance during attacking situation.

REFERENCE

1. Monika Roopak, Bvr Reddy, “*Blackhole Attack Implementation In AODV Routing Protocol*”, International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013
2. Mohamed Elboukhari, Mostafa Azizi and Abdelmalek Azizi, “*Impact Analysis of Black Hole Attacks On Mobile Ad Hoc Networks Performance*” , International Journal of Grid Computing & Applications (IJGCA) Vol.6, No.1/2, June 2015
3. Mohamad Y. Alsaadi, Yi Qian, “*Performance Study of a Secure Routing Protocol in Wireless Mobile Ad Hoc Networks*”
4. Virendra Singh Kushwah “*Implementation of NewRouting Protocol for NodeSecurity in a Mobile Ad Hoc Network*” (IJCSIS) International Journal of Computer Science and Information Security,Vol. 8, No. 9, December 2010.
5. Mangesh Ghonge, Prof. S. U. Nimbhorkar, “*Simulation of AODV under Blackhole Attack in MANET*” IJCSIR, Volume 2, Issue 2, February 2012