Detection of Malicious Node in MANET under AODV Protocol over CBR
Er. Shalini Chopra¹ Er. Ishan Singal²

¹Assistant Professor ²M.Tech Student
1,2Department of Computer & Science Engineering
1,2Global Research Institute of Management and Technology, Radaur

Abstract— An Ad Hoc network is a collection of mobile nodes which dynamically forms a temporary network without the use of any existing network infrastructure or centralized administration. In mobile Ad Hoc network, each mobile node acts as a host as well as a router. These nodes communicate to each other by Hop – to – Hop communication. AODV is a prominent on-demand reactive routing protocol for mobile Ad Hoc networks. But in existing AODV, there is no security provision against a well-known malicious attack. This type of attack is called cooperative “Black Hole” attack. This paper includes the behavior of the Black Hole node studied by considering different scenarios. Performance of the Black Hole AODV protocol has been analyzed by varying the number of mobile nodes and black hole nodes. These black hole nodes participate in the network actively and degrade the performance of network eventually. This method first detects a “Black Hole” attack and then gives a new route by passing this node. In this thesis, an attempt has been made to compare the performance of original AODV and modified AODV in the presence of multiple black hole nodes on the basis of throughput and packet delivery ratio.

Key words: MANET, Black hole, attack, security, protocol

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 its dynamic nature MANET has larger security issues than conventional networks. It Stands for "Mobile Ad Hoc Network." A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission.

A MANET protocol should function effectively over a wide range of networking context—from small, collaborative, ad hoc groups to larger mobile, multihop networks. The preceding discussion of characteristics and evaluation metrics somewhat differentiate MANETs from traditional, hardwired, multihop networks. The wireless networking environment is one of scarcity rather than abundance, wherein bandwidth is relatively limited, and energy may be as well.

A black hole is a malicious node that falsely replies for any Route Requests (RREQ) without having active route to specified destination and drops all the receiving packets. If these malicious nodes work together as a group then the damage will be very serious. This type of attack is called cooperative black hole attack. A gray hole attack is a variation of the black hole attack, where the malicious node is not initially malicious, it turns malicious sometime later.

II. PROBLEM FORMULATION
The major problem in the manet is malicious nodes. When data is transmitted among nodes it may reach to the destination node with response time less than the threshold value. Such types of nodes are known as black hole nodes. A black hole is a malicious node that falsely replies for any Route Requests (RREQ) without having active route to specified destination and drops all the receiving packets. If these malicious nodes work together as a group then the damage will be very serious.

This type of attack is called cooperative black hole attack. A gray hole attack is a variation of the black hole attack, where the malicious node is not initially malicious, it turns malicious sometime later. The problem is to detect and remove the above two types of malicious nodes.

We approach this problem by selecting some nodes which are trustworthy and powerful in terms of battery power and range. These nodes which are referred to as Back Bone Nodes (BBN) will form a Back Bone network and has special functions unlike normal nodes. For the co-ordination between the Back Bone Nodes (BBN) and the Normal Nodes, it is assumed that the network is divided into several grids. It is assumed that the nodes, when initially enters the network is capable of finding their respective grid locations. It is also assumed that the numbers of normal nodes are more than the number of black/gray nodes at any point of time.

Allocation of IP address-The IP address configuration in case of MANETs can broadly be classified into-

- Stateless approach
- Statefull approach

A. Stateless Approach:
In the stateless approach an unconfigured host must obtain its own IP address by self assignment. This stateless approach adopts random address assignment and is followed by duplicate address detection mechanism to achieve address uniqueness. Stateless approaches do not keep any allocation table.

B. Statefull Approach:
In the statefull approach an unconfigured host asks its neighbouring MANET to work as proxies to obtain an ip address. We have devised a new type of state-full approach viz. Core Maintenance of the Allocation Table.

Based upon the Literature survey, following are the objectives for thesis work:
To avoid the malicious nodes those are known as Black/Gray nodes in MANET.

To build a network that only consists of trusted nodes and act as a backbone for the proposed architecture designed for MANET.

Selection of nodes that can become a part of backbone of trusted nodes and should also must be energy efficient to support the set of trusted nodes that are used to lay foundation for building backbone nodes.

Introduction of concept of restricted IP’s (RIP) along with the construction of backbone of trusted nodes.

The main objective of our proposed algorithm involves, initially a backbone network of trusted nodes is established over the ad hoc network. The source node periodically requests one of the backbone nodes for a restricted(unused) IP address. Whenever the node wants to make a transmission, it not only sends a RREQ in search of path to destination node but also in search of the restricted IP simultaneously. As the Black/Gray holes send RREP for any RREQ, it replies with RREP for the Restricted IP (RIP) also. If any of the route responds positively with a RREP to any of the restricted IP then the source node initiates the detection procedure for these malicious nodes.

The main objective of our proposed algorithm involves, initially a backbone network of trusted nodes is established over the ad hoc network. The source node periodically requests one of the backbone nodes for a restricted(unused) IP address. Whenever the node wants to make a transmission, it not only sends a RREQ in search of path to destination node but also in search of the restricted IP simultaneously. As the Black/Gray holes send RREP for any RREQ, it replies with RREP for the Restricted IP (RIP) also. If any of the route responds positively with a RREP to any of the restricted IP then the source node initiates the detection procedure for these malicious nodes.

III. RESULTS & ANALYSIS

Figure 1, displays the total packet received and total packet loss with both AODV with black hole and with AODV without black hole effect i.e named as modified AODV in our approach. The total packet received without black hole in AODV(modified approach) is 420,000 where as the packet received in the AODV with introduction to black holes are 90,000. The modified approach consists of 140,000 packet loss where as the packet loss in AODV with black holes is 280,000 that is too less. above figure 2 displays the end-to-end delay with respect to time with both AODV with black hole is 290,000 and with AODV without black hole effect(modified one) is 140,000. The end-to-end delay in AODV with black holes is much more as compared to modified one the AODV without black holes.

IV. CONCLUSION

Two most important security problems in MANET are black hole and gray holes attacks. Black hole starts in route discovery phase and gray hole as an attack which drops packets in transmitting step. It is more difficult to detect a gray hole than black hole, because the attacker works as normal node then starts dropping of data. The main focus of the proposed study is to detect black and gray holes attacks and to investigate their advantages and disadvantages and at the end. The main objective of the study is to achieve protection against both attacks in one detection system and decrease the number of errors. It is highlighted that the Black Hole effect on the AODV protocol and on packet loss is much lower as compared to the effect on delay. The main matter of concern is the detection of malicious node as it is the main security threat that affects the performance of the AODV routing protocol. Improvement for overcoming the effect of Black Hole should orient towards controlling the delay. This proposal is guided towards lessening the effect of Black Hole for future researchers and to find the feasible solution to detect two types of malicious nodes (Black/Gray Hole) in the ad hoc network. The proposed solution can be applied to identify and remove any number of Black Hole or Gray Hole Nodes in a MANET and discover a secure path from source to destination by avoiding the above two types of malicious nodes.

REFERENCES


Detection of Malicious Node in MANET under AODV Protocol over CBR


[31] Mansoor Mohsin and Ravi Prakash, “IP Address Assignment in a mobile ad hoc network”, The University of Texas at Dallas Richardson, Mario Gerla Computer Science Department at UCLA, Los Angeles, CA 90095.