SURVEY ON BLACK HOLE ATTACK IN MOBILE AD_HOC NETWORK

Rakshitha H C¹, Sowndarya R², Bhat Geetalaxmi Jayram³
¹,²,³Information science and engineering, NIE

Abstract---There are two types attacks in the mobile ad-hoc networks. Black hole attack and Grey hole attack. Node receives packets sent from source and drops the packets instead of forward the packets it is called block hole attack. Node initially act as good after some time act as malicious node drops the packets it is called grey hole attack. Detect the malicious node node in the networks. finding the secure path from source to destination by Avoiding block hole attack and grey hole attack. Our project is detect these attacks using bait detection scheme. To detect these attacks there are many methods already there but our project is more useful than others.

Keywords---DSR, Selective repeat, UDP, TCP, Packet delivery ratio.

I. INTRODUCTION

Now a day’s mobile ad-hoc networks are wildly used. In military application also use the mobile ad hoc network. So secure the mobile ad hoc network is very important. Because hackers hac the confidential data, to secure the mobile ad-hoc network to detect the malicious node there are many different techniques are available. Here we studied the different papers on attacks in the mobile ad-hoc networks. these papers are related our project. there are two types of attack accurs namely BLACK HOLE attack and GRAY HOLE attack. A black hole attack is a malicious node that replies with a false statement about the routing information for the route request. It falsely states the destination address to the source node. After receiving packets through this route, this malicious node drops all the packets which are passing through this false route. If these malicious node combine together and drop all the nodes the problem become very serious. This type of attack is known as cooperative black hole attack. In Gray hole attack the malicious node initially sends a correct routing information to the source node and forward the packet without fail, after some time it will going to drop the packets. This type of attack is known as gray hole attack. We are going to introduce a solution for identifying the correct route or identifying malicious node and avoid these attacks on a Network. There by we can make a secured connection between the source and the destination.

II. PREVENTION OF COOPERATIVE BLACK HOLE ATTACK IN WIRELESS AD-HOC NETWORK [7]

I.1 Abstract:
The main problem in mannet is the security attack. Mobile ad hoc networks widely used in military and civilian application. The black hole attack and grey hole attacks these are two types attack. In this paper identifies the multiple black hole attack and discover a safe route by avoiding black hole. there are three protocols are currently available they are destination sequenced distance vector routing(DSDV), distance vector routing (DSR), AODV, in DSDV maintains a routing table. This routing table update periodically. problem is the networks grow as O(n²), the DSR protocol is the on demand routing protocol this has cache memory there will be memory overhead and it does not support multicast. This paper use the AODV protocol. It is a source initiated on demand routing protocol. All nodes has routing table it has next hop information from source to destination. this table entry has the list of possible nodes it can reach. In this paper using AODV protocol to identify multiple black hole attack and safe route. here using data routing information table. This table
contains binary values. Based on this find the secure route from host to destination. Advantage identifies multiple black hole in the group. Discover the safe route. Disadvantages are every node must have DRI table. The DRI table has to update frequently. There is no solution for gray hole attack, and it is only the theoretical approach.

III. AVOIDING BLACK HOLE AND COOPERATIVE BLACK HOLE ATTACKS IN WIRELESS AD HOC NETWORK[1]

2.1 Abstract: MANET (Mobile AD HOC Network) is a infrastructureless network connected to a mobile device without wire. Now a days this is widely used when source node want to transfer a data to destination, it count the number of intermediate node and forward the data to intermediate node this intermediate node in turn transfer and finally it will reach the destination, but some intermediate node act as a malicious node this is because mobile ad-hoc network is a infrastructureless networks any malicious node can easily attack network and can act as a malicious node in that network. this malicious node instead of transferring data to destination it will drop the data. This attack is called BLACK HOLE ATTACK, so to provide best security for data transfer before forwarding data we have to check the intermediate node which are all malicious node. This proposed system provides best mechanism to avoid black hole attack and for secure data transmission.

IV. DYNAMIC SOURCE ROUTING IN AD HOC WIRELESS NETWORK [2]

3.1 Abstract: An ad hoc network is a infrastructure-less network, in which there are mobile hosts and the movement of the hosts are unpredictable. In such a situation it is necessary that one host should help the other host in the network such that the packet sent by the source host reaches the desired destination. This paper presents “Dynamic Source Routing” protocol for routing. This protocol is adapted in the situation where the hosts are moving at a faster rate(i.e frequently) else it is a less over head or no overhead, if the hosts are moving at a slower rate(i.e less frequently). On the basis of the results from a packet-level simulation of mobile hosts operating in the network, the protocol performs well over a variety of environmental conditions such as host density and movement rates. Even when the host movement is at very high rate, the overhead of the protocol is quite low, falling to just 1% of total data packets transmitted for moderate movement rates in a network of 24 mobile hosts. In all cases, the difference in length between the routes used and the optimal route lengths is negligible, and in most cases, route lengths are on average within a factor of 1.01 of optimal.

V. CBDS: A COOPERATIVE BAIT DETECTION SCHEME TO PREVENT MALICIOUS NODE FORM MANET BASED ON HYBRID DEFENSE ARCHITECTURE [4]

4.1 Abstract: Due to the large usage of mobile devices, the need of Mobile Ad hoc network (MANET) has increased rapidly, which in turn needs technology to be improved rapidly too. Since MANET is infrastructure-less network, it can be established anywhere, whenever it is needed. Since MANET is infrastructure-less, its security is a threat in establishing it. So a great importance should be given to its security for a safe transmission of packets in network. The most commonly used protocols for routing such as DSR, AODV and so many, are not adopting any method of detection or responding to the malicious node in MANET. On the basis of the Dynamic Source Routing (DSR), and the various types of attacks by malicious node, this paper has formally introduced a mechanism to detect black and gray hole attacks and also co-operative black hole attack. And the mechanism is called Cooperative Bait Detection Scheme (CBDS). This mechanism will make use of both proactive and reactive defense protocol and sometimes support the stochastic neighbor node. At the initial stage, it will make use of the proactive defense protocol to detect the black hole attack in network. In this protocol the source node will make use of the address of one of its adjacent node as “bait destination address” to detect the malicious node. For this, the malicious node will reply with false RREP (Route
Reply) and thus it will be detected by making use of proposed reverse tracing Mechanism, thus we can avoid their attacks.

4.2 Related work:
Many research have been done to detect malicious node. But most of this method detect only single node or it take much time to detect. this methods even require specific environment. in this paper wear talking about recent papers which uses both proactive and reactive schema. proactive schema in this method it simply checks the network regardless of malicious node either present or what. But overhead simple waste of time and resource. but it avoid the attack in a beginning stage only. Reactive schema it only checks the network whenever destination talks about packet drop ratio .over head here is it try to resolve once malicious node exits in path and start the attack. Marti et al. presents a method in which contain Watchdog and Path rater for detecting black hole. Watchdog uses neighbor node to detect malicious node. Path rater initially find the defeat value of each node , then it keep track of each node . Value will change according to transmitted behavior. when time passes if value below threshold value treated as malicious node. t. we use the concept of Backbone network, some group of nodes are called as backbone nodes which are powerful in battery and range. Backbone network is formed with these nodes which are permitted to allocate Restricted IP addresses (RIP) to newly arrived nodes. now author thinks that environment is in backbone network. If source want to transmit a data it ask nearest BBN and RIP. If destination receive packet from BBN only then it is safe . If it even receive from RIP means black hole is in this route.

VI. PREVENTING COOPERATIVE BLOCK HOLE ATTACK IN MOBILE AD-HOC NETWORK: SIMULATION IMPLEMENTATION AND EVALUATION [8]

5.1 Abstract:
Mobile ad-hoc network is a moving network hence the attackers can easily hack the data. to give the security to the data here the they studied the previous algorithms and simulate the their work change the some features to algorithm and add the extra feature to the algorithm to give better output, then compares with other existing algorithms based on performance. Cooperative block nodes are identified and isolated to secure route from route to destination via simulation, here compare the pocket loss percentage, throughput of proposed system with existing system. in the proposed system less pocket losses, high throughput. they are using modified AODV protocol with data routing information table. this table has entry of binary values is the packet is sent and receive from neighbor nodes. based on this entry while sending packets which is trust node for that node, forward to that node.

5.2 Related work:
The routing protocols in MANETs are classified as four categories 1.Flat routing, 2.Hierarchical routing, 3.GPS routing, 4. Power based routing. Flat routing widely used. The flat routing protocol is further classified into two main sub categories. 1. table driven protocol 2. 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.

VI. ROUTING SECURITY IN WIRELESS AD HOC NETWORKS[12]
6.1 Abstract:
A mobile ad hoc network contains a wireless mobile nodes that are going to be communicate with each other without the use of network. MANET has practical applications. For providing security in a network, routing plays an important role. In this paper we are going to study the routing security of MANET and study in detail one type of attack called "Black hole & quote; attack. Black hole attack is a malicious node, it false reply for route request. It falsely states the routing information and destination address to the source node. It drop all the packets which are passing through this incorrect route. If the group of malicious node combine together the problem become very serious. This type of attack is known as Black hole attack. We are also introduce a solution for ad hoc black hole attack on-demand distance vector routing protocol.

VIII. Advantages and disadvantages

Advantages
1. Avoids multiple black hole attack and cooperative block hole attack.
2. The malicious nodes are identified dynamically.
3. Dynamic routing information table(DRI) is used.
4. Modifies existing algorithm to improve the efficiency.

Disadvantages
1. Avoids either the black hole attack or grey hole attack not both.
2. DRI table avoids only the black hole attack.
3. Either proactive methods or reactive methods not both.

By combining these advantages to overcome the disadvantages of these methods used in a cooperative bait detection scheme to detect malicious node in manet

IX. CONCLUSION

All these methods are on black hole attack. These methods try to avoid the black hole attack and finding the secure route from source to destination by avoiding the black hole attack and grey hole attack. Using different routing protocols. Few methods on proactive defence method, few of them on reactive defense method. Our project use both method using dynamic source routing protocol.

REFERENCES