A Survey On –Identify Blackhole Attacks on MANET

P.Anusuya 1, R.Chithra Devi 2, S.Dhivya 3

1 (M.Tech-II Year), Department of IT., Dr Sivanchi Aditanar College of Engineering,Tamilnadu.
anusuya0304@gmail.com

2 Assistant Professor, Department of IT., Dr. Sivanchi Aditanar College of Engineering,Tamilnadu.
chetra_rajan2001@yahoo.co.in

3 (M.Tech-II Year), Department of IT., Dr Sivanchi Aditanar College of Engineering,Tamilnadu.
dhivyasundarr@gmail.com

Abstract- A mobile ad hoc network (MANET) is a infrastructure-less network of mobile devices connected without wires. MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. In this paper detecting malicious nodes launching collaborative black hole attacks is a challenge. Implementation of CBDS method implements a reverse tracing technique to achieving the stated goal. This is referred to as the cooperative bait detection scheme (CBDS) that integrates the advantages of both proactive and reactive defence architectures. Also the objective of this paper is to provide a simulation study that illustrates the effects of Black hole attack on network performance.

Keywords: Cooperative bait detection, blackhole attack

I INTRODUCTION
MANET is a collection of mobile, decentralized, and self-organized nodes. This is due to technological advance in laptops and wireless data communication is becoming more popular than ever before. Internet based mobile ad hoc networks (iMANETs) are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. For example, multiple sub–MANETs may be connected in a classic Hub-Spoke VPN to create a geographically distributed MANET. In such type of networks normal ad hoc routing algorithms don't apply directly. The topology of ad hoc networks is dynamic and changes with time as nodes move, join or leave the ad hoc network. This unsteadiness of topology needs a routing protocol to run on each node to create and maintain routes among the nodes. As nodes wish, they should be able to enter and leave the network. Multiple intermediate hops are generally needed to reach other nodes, due to the limited range of the nodes. Each and every node in an ad hoc network must be keen to forward packets for other nodes. This way, every node performs role of both, a host and a router. A malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols.

II BACKGROUND
MANET routing protocols are categorized into three main categories:

- Table driven/ proactive
- Demand driven/ Reactive
- Hybrid

Proactive (table-driven) Routing Protocol - The proactive routing is also called table-driven routing protocol. In this routing protocol, mobile nodes periodically broadcast their routing information to the neighbors. Each node needs to maintain their routing table which not only records the adjacent nodes and reachable nodes but also the number of hops. In other words, all of the nodes have to evaluate their neighborhoods as long as the network topology has changed. Therefore, the disadvantage is that the overhead rises as the network size increases, a significant communication overhead within a larger network topology. However, the advantage is that network status can be immediately reflected if the malicious attacker joins. The most familiar types of the proactive type are destination sequenced distance vector (DSDV) routing protocol and optimized link state routing (OLSR) protocol.

Reactive (on-demand) Routing Protocol - The reactive routing is equipped with another appellation named on-demand routing protocol. Unlike the proactive routing, the reactive routing is simply started when nodes desire to transmit data packets. The strength is that the wasted bandwidth induced from the cyclically broadcast can be reduced. Nevertheless, this might also be the fatal wound when there are any malicious nodes in the network environment. The weakness is that passive routing method leads to some packet loss. Here we briefly describe two prevalent on-demand routing protocols which are ad hoc on-demand distance vector (AODV) and dynamic source routing (DSR) protocol. AODV is constructed based on DSDV routing. In AODV, each node only records the next hop information in its routing table but maintains it for sustaining a routing path from source to destination node. If the destination node can’t be reached from the source node, the route discovery process will be executed immediately. In route discovery phase, the source node broadcasts the route request (RREQ) packet first. Then all intermediate nodes receive the RREQ packets, but parts of them send the route reply (RREP) packet to the source node if the destination node information

© 2015 IJAIR. All Rights Reserved
is occurred in their routing table. On the other hand, the route maintenance process is started when the network topology has changed or the connection has failed. The source node is informed by a route error (RRER) packet first. Then it utilizes the present routing information to decide a new routing path or restart the route discovery process for updating the information in routing table. The design idea of DSR is based on source routing. The source routing means that each data packet contains the routing path from source to destination in their headers. Unlike the AODV which only records the next hop information in the routing table, the mobile nodes in DSR maintain their route cache from source to destination node. In terms of the above discussion, the routing path can be determined by source node because the routing information is recorded in the route cache at each node. However, the performance of DSR decreases with the mobility of network increases, a lower packet delivery ratio within the higher network mobility.

Hybrid Routing Protocol- The hybrid routing protocol combines the advantages of proactive routing and reactive routing to overcome the defects of them. Most of hybrid routing protocols are designed as a hierarchical or layered network framework. In the beginning, proactive routing is employed to completely gather the unfamiliar routing information, then using the reactive routing to maintain the routing information when network topology changes. The familiar hybrid routing protocols are zone routing protocol (ZRP) and temporally-ordered routing algorithm (TORA).

III COOPERATIVE BAIT DETECTION SCHEME

This paper proposed a malicious node detection scheme, named as CBDS, which is able to detect and prevent malicious nodes causing black or grayhole attacks and cooperative attacks. It merges the proactive and reactive define structure, and the source node randomly establishing cooperation with the adjacent node. Using the address of the adjacent node as the destination bait address, it baits malicious nodes to send a RREP reply and detects the malicious nodes by the proposed reverse tracing program and consequently prevents their attacks. We assume that when there is a significant drop in packet delivery ratio, an alarm will be sent by the destination node to the source to trigger the detection mechanism again, which can achieve the capability of maintenance and immediately reactive response. Accordingly, our proposal merges the advantage of proactive detection in the initial stage and the superiority of reactive response that reduce the waste of resource. Consequently, our mechanism doesn’t like the method that just use reactive architecture would suffer black hole attack in initial stage. Although DSR can know the all address of nodes among the route after the source node receives the RREP. Nonetheless, the source node cannot identify exactly which intermediate node has routing information to destination node and reply RREP. This situation make the source node sends packets to the shortest path that the malicious node claim and the network suffer black hole attack that causes packet loss. However, the network that uses DSR cannot know which malicious node cause the loss. In comparison to DSR, the function of Hello message like AODV was added to help the nodes to identify which nodes are their adjacent nodes within one-hop. This function assists in sending the bait address to entice the malicious nodes and utilize the reverse tracing program of CBDS to detect the exact addresses of malicious nodes. In addition, the baiting RREQ packets were created.

IV BLACKHOLE ATTACK

Black hole Attacks are classified into two categories:

Single Black Hole Attack In Single Black hole Attack in which one node acts as attacker. It is also known as Black Hole Attack .It has single malicious nodes.

Collaborating Hole Attack In Collaborative Black Hole Attack more than one nodes act as malicious node. It is also known as Black Hole Attack with multiple malicious nodes According to the original AODV protocol, when first node S wants to communicate with the last node D, the first node S shows the course ask for (RREQ). The neighboring dynamic nodes overhaul their directing table with a section for the source hub S, and check in the event that it is the last hub or has a sufficiently crisp course to the destination hub. If not, the transitional hub redesigns the RREQ (expanding the jump tally) and surges the system with the RREQ to the last hub D until it achieves hub D or some other middle hub which has a sufficiently new course to D, as delineated by illustration in Figure 1. The last hub D or the middle of the road hub with a sufficiently new course to D, starts a course reaction (RREP) in the opposite bearing, as portrayed. Hub S begins sending information parcels to the neighboring hub which reacted in the first place, and losses alternate reactions. This works is fine when the system has no noxious nodes. Specialists have proposed answers for recognize and evacuate a solitary dark gap hub. Be that as it may, the instance of numerous dark opening nodes acting in coordination has not been tended. Case in point, when numerous dark opening nodes are acting in a joint effort with one another, the first dark gap hub B1 altitudes to one of its buddies B2 as the following bounce.The source hub S sends a “Further Request (FReq)” to B2 through an alternate course (S-2-4-B2) other than by means of B1. Hub S inquires as to whether it has a course to hub B1 and a course to last
Since B2 is chipping in with B1, its "Further Reply (FRp)" will be "yes" to both the inquiries. Presently per the arrangement proposed in nodes begins passing the information parcels expecting that the course SB1-B2 is more secure. In any case, in actuality, the bundles are devoured by hub B1 and the security of the system is bargained.

**V CONCLUSION AND FUTUREWORK**

In this paper we have gone through the routing security issues of MANETs, described the black hole attack that can be mounted against a MANET and proposed a feasible solution for CBDS method. The proposed solution can be applied to a) Identify single and multiple black hole nodes cooperating with each other in a MANET; and b) Discover secure paths from source to destination by avoiding multiple black hole nodes acting in cooperation.

The proposals are presented in a chronological order and divided into single black hole and collaborative black hole attack. 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. The black hole problem is still an active research area. This paper will benefit more researchers to realize the current status rapidly.

**REFERENCE**


