A Review of Black Hole Attack in MANET
Gurpreet Singh1Simarjeet Kaur2
1M.Tech 2Assistant Professor
1,2Department of Computer Science Engineering
1,2SGGSWU, FGS

Abstract— Black hole attack is a serious security problem to be solved for successful delivery of packets in mobile ad-hoc network. In this attack, a malicious node uses routing protocol to advertise itself as having the shortest path to the node whose packets it wants to seize. In flooding based protocol, if the malicious node reply reaches the requesting node before the reply from the actual node, a forged route is created. This paper deals with the presentation of Black hole attack in MANET. Various previous techniques have been discussed in these papers that were used to prevent black hole attack. MANETs are susceptible to various attacks, so attack has to be mitigated in initial setup. Keywords: Routing, Ad-hoc, Black Hole, Security, AODV

I. INTRODUCTION

Wireless network is the network of movable computer nodes or stations that are not physically wired. The main gain of this is communicating with rest of the world while being mobile. The drawback is their limited bandwidth, memory, processing capability and open medium (1). Two basic system models are fixed backbone wireless system and Wireless Mobile Ad hoc Network (MANET): An ad hoc network is a collection of nodes that do not rely on a predefined infrastructure to keep the network coupled So the performance of Ad-hoc networks is dependent on the trust and co-operation between nodes. Nodes help each other in passing on information about the topology of the network and share the responsibility of managing the network. Hence in addition to act as hosts, each mobile node does the function of routing and relaying messages for other mobile nodes (1). Most essential networking operations include steering and network management (2). Routing protocols can be separated into proactive, reactive and mix protocols, depending on the routing topology. Proactive protocols are typically table-driven. Instances of this type include DSDV, WRP. Reactive or source-initiated on-demand protocols, in contrary they do not periodically update the routing information. It is propagated to the nodes only when necessary. Example of this type include DSR, AODV and ABR. Hybrid protocols make use of both reactive and proactive approaches. Exemplar of this type includes TORA, ZRP. Safety is a major concern in all forms of communication networks, but ad hoc networks face the greatest challenge due to their inherent nature. As a result, there exist a swerve of attacks that can be performed on an Ad hoc network. (1)(4). But these protocols does not work well so this paper contains the introductory part to swarm optimization algorithms. This paper presents the concept of black hole assault in MANET in addition to black hole prevention methods.

A. Black hole attack

The black hole attack is individual type of association layer attack in Mobile ad-hoc Network. In this attack, a fake node presents itself that has direct path to reach destination (3). So it collects the complete packet from source and drops it. The Black hole attack is off two types.

1) Single Black Hole attack

In Single Black hole attack, only one node act as a false node that collects the entire packet from source and drops the packet (4). The single Black hole attack is shown in Fig.1.1. The source node S wants to talk with destination D. Initially, it sends RREQ to the neighbor node. If it has valid route to reach destination then it sends the packet through the path. If it does not have a route then it forwards the RREQ to the neighbor’s node until reach destination. The node F act as a false node that sends RREP with maximum sequence number before any other node respond, even if any transitional node sends RREP to the source. The Source node S rejects the reply and it assumes that the F node has direct path to reach Destination and it sends the packet from end to end on that path. So, the node F collects all the packets coming from founded node which creates black hole problem.

![Fig. 1.1: Single Black Hole Attack](image)

2) Co-operative Black hole attack

In Co-operative Black Hole assault, additional than one node combined uniformly and act as Fake nodes is called as supportive Black hole attack (4). This will degrade the network performance. The accommodating Black Hole attack is shown in Fig.1.2.

![Fig. 1.2: Co-Operative Black Hole Attack](image)

II. LITERATURE SURVEY

Hu et al (2006) introduced the wormhole attack, a brutal attack in ad hoc networks that is mainly difficult to protect against. The wormhole attack is likely even if the attacker has no cooperation with any hosts and even if all communication provides authenticity and confidentiality. In the wormhole attack, an attacker records packet at one location in the network, passageway them to another position, and retransmits them there into the network. The wormhole attack can form a grave threat in wireless networks, particularly against many ad hoc network routing
protocols and location-based wireless security systems. They present a universal apparatus, called packet leashes, for detecting and, thus defensive against wormhole attacks, they also argue topology-based wormhole invention, and show that it is impracticable for these approach to notice some wormhole topologies.(5)

Azer et al (2009) discussed trouble of mainly severe security attacks that affect the ad hoc networks routing protocol, it is called the wormhole attack. Wormhole attack is a two stage process launch by one or several nasty nodes. In the first phase, these nasty nodes, called wormhole nodes, try to entice rightful nodes to send data to other nodes via them. In the second phase, wormhole nodes develop the data in diversity of ways. It will bring in the wormhole attack modes and classes, and point to its clash and threat on ad hoc networks. They also observe the wormhole attack modes from an attacker’s viewpoint and suggest new improvement to this type of attacks.(6)

Tandan and Saurabh (2011) An Ad hoc network is the complex with no fixed communications. There is no middle manager so any node can come and move in and exterior of the network in a dynamic way. This makes it more active and difficult which makes it more vulnerable to attacks. A few effects of malicious nodes are rejection of service, Routing table flood, Impersonation, power consumption, Information exposé etc. A black hole attack node attracts all sachets by incorrectly claiming a fresh route to the destination node and absorbs them without forward them to destination. In this paper apparatus based on PDR is proposed to detect the black hole attack in MANET with AODV procedure. A foreword of black hole in MANET with QUALNET 5.0 is done, after apply the detection technique result reflect the performance degradation.(7)

Nath and Chaki (2012) Black hole attack is single variety of direction-finding troubling attacks and can bring great damage to all clusters of a MANET. Security residues a major challenge for these network due to their facial appearance of open medium, energetically changing topologies, and infrastructure-less property. As a consequence, a well-organized algorithm to notice black hole attack is significant. This paper suggests and evaluates strategies to detecting black hole attacks and build dependable and protected inter cluster routing in wireless ad hoc network. (8)

Trupti et al (2012) MANET consists of mobile hosts prepared with wireless devices. If two wireless hosts are out of their conduction ranges in the ad hoc networks, other mobile phone hosts situated between them can ahead their message, which efficiently builds associated networks among the mobile hosts in the deployed area. One main defy in design of these networks is their susceptible nature to security attack. These attacks can be deploying by insider or alien attacker. A little bit, the node from network can be attacker. This happen because of mobility of nodes and altering network topology. There are dissimilar kind of attacks obtainable in writing and can be implementing on MANET. One of these attacks is Grey Hole attack that has risky effect on Mobile Ad-Hoc Network. This paper discussed the effect of Grey Hole attack on Dynamic Source Routing protocol in Mobile Ad-Hoc Network.(9)

A Review of Black Hole Attack in MANET

III. TECHNIQUES USED

A. ACO (Ant Colony Optimization)

Detection and Prevention Technique: The basic principle of an ant routing algorithm is that ants drop on the ground a hormone, the pheromone, while they travel looking for foodstuff. Ants can also stink pheromone and tend to follow with higher probability those paths characterized by strong pheromone concentrations (12). The pheromone trails let the ants to find their way to the food source (or back to the nest). The same pheromone trails can be used by other ants to find the location of the food sources discovered by the in nest mates. It was confirmed experimentally that this pheromone-trail-following behavior gives raise to the appearance of the shortest path. An ant routing algorithm can be briefly described in the subsequent way in Fig. 3.1

Fig. 3.1: Basic Principle of Ant Routing Paradigm.

B. BFO (Bacterial Foraging Optimization)

The technique BFOA (bacterial foraging optimization algorithm) is new comer to the biological techniques (11). The process, in which a bacterium moves by taking small steps while probing for nutrients, is called chemo taxis and main idea of BFOA is mimicking chemo tactic movement of virtual bacteria in the problem search space, individual bacterium communicate to other by sending signals. It is a global optimization algorithm for various optimization problems. This technique is also inspired by the social foraging behavior like ant colony and particle swarm optimization. It attracts the researchers due to its efficiency in solving real world optimization problems and gives better results than traditional methods of problems solving real world optimization troubles and gives better results than conventional methods of problems solving.

This algorithm consists of three phase to detect and prevent from BLACKHOLE attack in MANET.

1) Phase 1: Network Construction phase
- Create network.
- Select source and the destination node.
- The transmission will start from source to destination by multi hop.

2) Phase 2: Detection of attack
- The black hole attack is detected in the network by the chemotactic movement of data in the network.
- The node that is not transmitting the data forward is the black hole node.

3) Phase 3: Recovery
- In the elimination mode of BFOA, eliminate the black hole node.
- In the dispersion and reproduction phase, a node is generated that is the substitute of black hole node.
- Analyze the P.D.R, throughput and the routing overhead.

C. PSO (Particle swarm optimization)

Multidimensional Optimization Technique: Particle swarm optimization (PSO) is a popular multidimensional
optimization technique (13). Ease of implementation high quality of solutions, computational efficiency and speed of convergence are strengths of PSO. PSO has been an accepted method used to solve optimization problems in WSNs due to its simplicity, high class of solution, fast convergence and insignificant computational burden. An iterative nature of PSO can exclude its use for high speed real time applications, mainly if optimization needs to be carried out regularly. PSO require large amount of memory, which may limit its completion to resource rich base stations.

D. ABC (Artificial Bee Colony)

The ABC algorithm is a swarm based algorithm based on the foraging behavior of honey bee colonies. It is a very easy, strong and population based stochastic optimization algorithm. The presentation of the ABC algorithm is compared with those of other well-known modern heuristic algorithms such as, Differential Evolution (DE), Particle Swarm Optimization (PSO) on constrained and unconstrained problems (13).

IV. CONCLUSION

Black hole attack in wireless network can be prohibited using different protocols and optimization algorithms so that data can be securely transferred from source to destination. Black hole attack is a huge hazard to the security of mobile ad hoc networks. Various techniques have been discussed and each has its own significance.

REFERENCE


