Black Hole Attack Detection And Mitigation Technique In Manet

Abstract—

MANET stands for Mobile ADHOC Network also called a wireless ADHOC network or ADHOC wireless network that usually has a routable networking environment on top of a Link Layer ad hoc network. Because MANETS are mobile, they use wireless connections to connect to various networks. Each node in MANET is free to move independently in any direction and the topology is changing dynamically. MANET is popular for various types of security attacks for its dynamic topology, lack of centralized monitoring. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission. MANET are more prone to attacks due to limited physical security. The black-hole attack is considered one of the most common attacks that decrease the performance and credibility of the network therefore, malicious node drops all incoming packet. Here, we discuss about the advance BFO Algorithm to detect and mitigate the black Hole Attack in MANET, an algorithm which mitigates the Blackhole attack in AODV routing.

Keywords— MANET, ADHOC, BFO, Wi-Fi connection, AODV, Topology.

I. Introduction

Manet (Mobile ad-hoc network) is a composed of a collection of mobile nodes which create a temporary network without any central nodes and it does not usual network support devices. It is infrastructure less which access multi hops without any central node. MANET's are unconstrained and dynamic in nature so any hub can join or leave the system at some random time. Because of this, they are generally utilized in military and salvage territories where correspondence among fighters in front line and in zones where new brief system is required on the grounds that the system may be crumpled because of some fiasco [3]. Blackhole attack means vindictive hub assimilates every one of the bundles in it like a hole which sucks in all things, hence it is named as black hole attack. Manet’s work through pair to pair connectivity between intermediate hops. In these networks, all hop is capable of moving any direction with any speed. This feature makes creates an unpredictable topology for the network. This type of open boundary feature makes the network highly challengeable regarding safety issues. If nodes are facing any sort of security attack, malicious nodes can access data packets. Security attacks are Jamming attack, Gray hole attack and wormhole attack which are against routing protocols. Black hole attack is one of the most crucial attacks against routing protocols. In black hole attack, affected nodes create fault reply packet for request packet and selected as the best path from source to destination. While malicious nodes receive the data packets it will drop the packets. AODV (ad-hoc on-demand distance vector) is mostly used routing protocols for manet. AODV uses a sequence number for finding the fresh path from source to destination. In our work, we will detect black holes nodes in AODV based network by considering the total number of affected nodes. There are two types of black hole one is single black hole another is a cooperative black hole. In a single black hole there is only one single affected node on the other hand in cooperative there are multiple nodes affected. It is very hard to detect cooperative

malicious nodes because they have some internal mechanism which makes it very hard to track and detect. Malicious nodes send data packet between them by using the sniffing approach. We considered two situations true positive and false positive. Nodes that are affected can be considered as false positive. Detecting false-positive nodes are the major challenge in cooperative black holes. In order to detect the malicious nodes, we proposed a new approach to detect and elements malicious nodes in a path. In our method when source nodes want to send the data packet to the destination, it's usage and routing protocols. After that, it checks previous hop and next-hop of the route reply generator to make the path secure. The source node can detect malicious nodes and eliminate them by using a data routing protocols [1][5][6].

II. Literature Review

In this paper, we will be discussing about some algorithm for Black Hole Attack Detection and Mitigation in manet. Ad Hoc On-Demand Vector (AODV) is a routing protocol for MANET [2]. It is an adaptation of DSDV protocol [2]. AODV is a reactive routing protocol. They proposed two algorithms for mitigating the black hole attack is

1.ANB-AODV and 2.AFB-AODV [1].

Bacterial foraging optimization algorithm (BFO) has been commonly recognized for global optimization. BFO is inspired by the social foraging behavior of Escherichia coli. It has good proficiency in solving real-world optimization problems arising in several application domains. Therefore, it is very famous among researchers. In this paper [3] [4] BFO has been proposed to optimize multiple base stations at the same time in order to increase the percentage of packet delivery even in the presence of black hole attack. The percentage of detection could be increased.

Jain, S., and Khuteta, D. proposed [6] proposed a simple method to successfully detect and mitigate black hole attack in the mobile ad-hoc network. it used a vulnerability of the blackhole node itself to overcome this issue. Blackhole node generally responds to every RREQ(route request) and discard the packets when the packet has been sent to the falsified blackhole node.

In the Paper by Tripathi, A., and Mohapatra, A. proposed [7] simple but effective method of detecting and mitigating blackhole attack simply by using hop count. This method matches the hop count of the confirmation packet and hop count from the routing table.

Here, we have discussed about BFO algorithm the advantages of this algorithm and also an algorithm that mitigates the Blackhole attack in AODV routing. Additionally, we tried to find the limitation of this paper.

III. Research Questions

1. What is AODV?
2. What is the difference between ANB-AODV and AFB-AODV?
3. WHY USE BFOA IN MANETs?
4. How Many Types of Black Hole Attacks?
5. How to detect and overcome the black hole attack
6. Without using so much computational power and complex algorithms?

7. How to detect and mitigate the Black Hole attack by using hop count?
8. what is the disadvantage of finding blackhole node by RREP packets sequence number?

IV. Review Methodology

Ad Hoc On-Demand Vector (AODV) is a routing protocol, which is a reactive type routing protocol in MANET. [2].

ANB means anti near black hole. AFB means anti far black hole. The main difference of ANB and AFB is, Black hole is placed near from the sender in ANB and far from the sender in AFB. [1].

The Bacterial Foraging Optimization Algorithm is new comer among various bio-energized computations and has a spot with the field of Bacteria Optimization Algorithms and Swarm Optimization, in addition, all the more extensively to the fields of Computational Intelligence also, Metaheuristics. It is related to other Swarm Intelligence figuring, for instance, Ant Colony Optimization and Particle Swarm Optimization. It has been used in many research districts like concealing pictures quantization, face affirmation, structuring plan issues. On exploring these issues' answer by BFOA, results got are better than other bio impelled and normal approaches. It is computationally feasible and faster and deals with hard numerical issues. There have been various enlargements of the approach that try to hybridize the estimation with other Computational Intelligence counts likewise, Metaheuristics, for instance, Genetic Algorithm, Particle Swarm Streamlining and Tabu Search, etc . So stirred from other issue's answer we are using BFOA in MANETs on AODV show in this paper and explore the results obtained. [3].

A Black Hole attack is a kind of repudiation of organization strike where a harmful center point can pull in all groups by wrongly stating a new course to the objective and a short time later hold them without sending them to the objective. [4].

1. Single Black Hole Attack
2. Co-operative Black Hole Attack

Jain, S. and Khuteta, D. proposed [6] Base Node method to detect and mitigate black hole node without solving any complex algorithms. It is done by just sending RREQ (route request) of any node which does not exist in the network. Only the Black hole node will respond with RREP (route reply) to such kind of RREQ (route request) and thus black hole node will be detected.

In the Paper written by Tripathi, A., and Mohapatra, A. proposed [7] when Source will send a packet to the destination, the destination will send a packet saying how many hop count the data packet had. Then source will match its existing routing table and count how many hop count supposed to have by that packet. when calculated hop count and real hop count equal to same then rest of the packets will be sent to the destination. If hop count doesn't match, then the middle node is black hole node.

Black Hole node or malicious node's common behavior is they respond with the high sequence number in the route reply packet [7]. But there is no specification or proper definition of high sequence number from route reply packet [7]. And thus, detecting black hole node by high

sequence number will be less effective. moreover, if hacker modifies black hole node to show less sequence number then detecting black hole node by RREP sequence number will completely fail.

In ANB-AODV figure [1.A], when the sender broadcast RREQ packet then the malicious node reply first which is near to the sender, but in ANB sender will not send the data instantly, figure [1.B] it will wait for second reply from the actual node which is nearest to the destination then it will send the packet. In AFB, when the sender broadcast RREQ packet. The sender node will get the reply from the actual node which is nearest to the destination figure [2.A] after that it will get the reply from the malicious node which is far away from the sender figure [2.B]. Sender will send the data to the first node. The impact of blackhole attack will be decreased by using this two algorithms. [1] [2].

In BFO algorithm, main aim is for delivery of packets from the supply node to a minimum of one base station within the presence of region.The below figure shows the system design within which the node transfers packets to its nearest base station, whose position is given by the BFO rule. part assailant node drops all the packets returning to that. the base station when being placed within the correct position it detects the part and sends its report. We tend to optimize the position of 4 base stations every which way within the network at constant time. once very little iteration the bottom stations are placed at the foremost fittest position among all. The fitness price is calculated by the density of nodes round the base station. Once the base stations are placed consistent with their fitness price the supply node sends packets, the packet is transferred to the closest base station. If a part or a black hole region is gift in between the supply node and therefore the base station, we will modification the position of the base station itself and move to a brand new location supported their fitness price. in order that the packets are delivered to a minimum of one base station in presence of part attack. [3] [4]. In previous section a discussion about the previous methodology to prevent black hole attack is presented. In these section we discussed our methodology in detailed. In our method each node contains a data routing information table. Since manet uses dynamic topology so neighbor nodes can change in order to time. In DRI table node column determine the neighbor by using id. On the other hand, other two columns are used to determine if node communicate with other node or not. From column means node receive data packet from any specific node or not. On the other hand, through means if nodes sent any to a particular destination or not. If the value of from and through column is 1 so the node is safe. To implement our approach, we can follow three steps.

1. Find out the freshest path
2. Checking path
3. Eliminating malicious node.

1. Find out freshest path: the goal for this stage is to find the best path using AODV protocols. For sending data from source to destination at first it has to be broadcast PREQ, in that case malicious node generates a PREQ with large sequence number. In our method each PREQ generator put it’s previous hop and next hop nodes. It also generate DRI entries for of them and send it back to the source node. Malicious node also select it’s cooperative previous hop nodes and next hop nodes. While malicious nodes are first and last host of the path it will select random nodes as previous and next hopes. Cooperative nodes can communicate each other and other nodes and DRI tables from and through value is 1. When source receive the Preq packets it’s select the largest path by selecting large number of sequence number.

2. checking path: our aim is to generate a secure path. In this approach source node at first check it’s next hop and looking for two parameters 1.it’s own id and DRI table information for previous node and source also check if there are any intermediate nodes or not. If through value is 1 from column value is zero there will be a malicious nodes. Then source nodes marks it as a malicious node and looking for new path. If next hope nodes is trustable the path between source and destination is safe and the from and through column value in DRI table is 1.

3. Eliminating malicious node: at this stage we elements the attacked nodes. If source detect any malicious path It can generates a packet and put detected id’s. Then broadcast this packet through the network. [5]

Jain, S. and Khuteta, D. proposed [6] proposed that their Will be a base Node which will be responsible for figuring out the Blackhole Node. Base Node Will generate a packet with the destination network of a node which does not exist in the network.

Blackhole node is configured to respond to every RREQ(route request) with RREP(rout reply) without acknowledging the destination address.

A normal node will check the routing table for RREQ(route request) and respond RREP(route reply) only if the destination node is available to the network. For the falsified address of the destination network, the normal node will not respond with RREP(route reply). And thus, the Black Hole node will get detected to the base node by providing route reply to the false destination address. When the Base Node successfully detects any blackhole node, it will broadcast the blackhole node address to all other nodes of the network.

That Blackhole node will be isolated and rejected by every node of the network.

Advantage of this proposed method by Jain, S. and Khuteta, D. [6] is it can detect single as well as multiple numbers of blackhole node without using much computational power. Other algorithmic and cryptographic methods for mitigating blackhole node are computation hungry and thus it could drain the battery life of any MANET device (e.g. walkie-talkie) dramatically.

The disadvantage of the proposed method by Jain, S., and Khuteta, D. [6] is what if any node pretends to be a base node and broadcast all other healthy node as blackhole node , then full mobile ad-hoc network will get isolated from each other and it will become impossible to communicate with each other .

In the Paper by Tripathi, A., and Mohapatra, A. proposed [7] hop count to detect blackhole attack. for mitigating blackhole attack, it broadcast blackhole node information to others. And thus, the blackhole node gets isolated.

Proposed algorithm for detecting and mitigating blackhole node by In the Paper by Tripathi, A., and Mohapatra, A. proposed [7] is source Broadcast RREQ (route request) && source receives RREP (route reply)

- if (replying node == malicious node && chance given>1)
- chance given ++
- Drop RREP

- Else
- Send 1st Data Packet towards Destination and
- Destination will send Confirmation packet on receiving 1st Data Packet
- if ((Confirmation packet arrives before Threadshold time) &&(Value in source node
- matches the value of the Last hop count in
- Confirmation packet))
- Send all Data packet
- else Add node that sends route reply to Malicious node table.
- Broadcast black packet where chance=1
- if (chance After a Wait time, Broadcast White Packet by telling that the node is again available for
- communication

Here,

Black Packet Contains

1. Source Node Address
2. Malicious Node Address
3. Request ID

White Packet Contains same information as Black packet. Confirmation packet contains

1. Source and destination node address
2. last hop count

- the black packet indicates node to be isolated (blacklisted)
- the white packet indicates node to be given one more chance
- the confirmation packet used to count 'last hop count' value

The proposed method by Tripathi, A., and Mohapatra [7] is energy efficient and can work very well, but the disadvantage is, if a device gets damaged and can't pass packet then it will be permanently blocked in-network even if repaired.

V. Conclusion

In this research paper, we have discussed about the mitigation technique using AODV routing protocol. ANB-AODV and AFB-AODV is the algorithms to reduce the impact of blackhole attack in MANET. In BFO algorithm optimize multiple base stations used to increase the percentage of packet delivery. Effective in reducing the power consumption, increase packet delivery.

Here it is also discussed that how to mitigate blackhole attack using hop count and by asking RREQ for a node which doesn’t even exist. Moreover, a new method for detecting and mitigating blackhole attack using byzantine general problem[8] has been proposed .

VI. Future Research

In future, any can chip away at improving dark opening assault discovery strategy and

increment the level of location.