International Journal of Electronics and Electical Engineering

Volume 2 | Issue 2 Article 4

October 2013

DETECTION AND REMOVAL OF BLACK HOLE IN MOBILE AD-HOC NETWORK (MANET)

SHRADDHA RAUT
Electronics & Telecommunication Department, Priyadarshini College of Engineering, Nagpur, India,
shradha.raut22@gmail.com

SD CHEDE
Electronics & Telecommunication Department, Priyadarshini College of Engineering, Nagpur, India,
santoshchede@rediffmail.com

Follow this and additional works at: https://www.interscience.in/ijeee

 Part of the Power and Energy Commons

Recommended Citation

RAUT, SHRADDHA and CHEDE, SD (2013) "DETECTION AND REMOVAL OF BLACK HOLE IN MOBILE AD-HOC NETWORK (MANET)," *International Journal of Electronics and Electical Engineering*: Vol. 2 : Iss. 2 , Article 4.
Available at: https://www.interscience.in/ijeee/vol2/iss2/4

This Article is brought to you for free and open access by Interscience Research Network. It has been accepted for inclusion in International Journal of Electronics and Electical Engineering by an authorized editor of Interscience Research Network. For more information, please contact sritampatnaik@gmail.com.

DETECTION AND REMOVAL OF BLACK HOLE IN MOBILE AD-HOC NETWORK (MANET)

[1]SHRADDHA RAUT & [2]SD CHEDE

[1,2]Electronics & Telecommunication Department, Priyadarshini College of Engineering, Nagpur, India
Email:shradha.raut22@gmail.com; santoshchede@rediffmail.com

Abstract: This paper gives information about the detection technique of black hole in the MANET. An ad hoc network is a collection of mobile nodes that dynamically form a temporary network. It operates without the central administration. Hence it becomes more susptable to the attacker .Mostly used on- demand routing protocols used in Ad-Hoc networks is AODV (Ad-Hoc On demand DistanceVector) protocol. The security of the AODV protocol is compromised by a particular of attack called "Black Hole" attack. In this attack, a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. To reduce the probability, it is proposed to wait and check the replies from all the neighboring nodes to find a safe route.

Keywords: *Black hole, ad-hoc network, AODV protocol malicisious node*

1. INTRODUCTION

A mobile ad hoc network (MANET), is a self-configuring infrastructure less network of mobile devices connected by wireless links. *ad hoc* is Latin and means "for this purpose". As the importance of computers in our daily life increases it also sets new demands for connectivity. Wired solutions have been around for a long time but there is increasing demand on working wireless solutions for connecting to the Internet, reading and sending E-mail messages, changing information in a meeting and so on. There are solutions to these needs, one being wireless local area network that is based on IEEE 802.11 standard. However, there is increasing need for connectivity in situations where there is no base station (i.e. backbone connection) available (for example two or more PDAs need to be connected). This is where ad hoc networks step in. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. MANETs are often defined as follows: A "mobile ad hoc network" (MANET) is an autonomous system of mobile routers (and associated hosts) connected by wireless links - the union of which forms an arbitrary graph. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. The characteristics of these networks are follows:

- Communication via wireless means.
- Nodes can perform the roles of both hosts and routers.
- No centralized controller and infrastructure.
- Dynamic network topology. Frequent routing updates.
- Autonomous, no infrastructure needed.
- Can be set up anywhere.

Some of the applications of MANETs are

- Military or police exercises.
- Disaster relief operations.
- Mine site operations.
- Urgent Business meetings
- Robot data acquisition

Security attack type that occurred mainly in the MANET is Black hole . Black hole problem in MANETS is a serious security problem to be solved. In this problem, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. In flooding based protocol, if the malicious reply reaches the requesting node before the reply from the actual node, a forged route has been created. This malicious node then can choose whether to drop the node then can choose whether to drop the packets to perform a denial-of-service attack or to use its place on the route as the first step in a man-in-the-middle attack.

2. DETECTION OF BLACK HOLE

Black hole is nothing but the malicisious node. This node accepts the data from source but does not forward it to the destination. This node used for hacking purpose. There are two detection techniques are involved in the detection of black hole:

1. Depending upon how many times that path is used for transmission.
2. By updating the routing table and comparing unique sequence number at each time.

    a. 1st Method

In this method, the sender node needs to verify the authenticity of the node that initiates the RREP packet by utilizing the network redundancy. Since any packet can be arrived to the destination through many redundant paths, the idea of this solution is to wait for the RREP packet to arrive from more than two nodes. During this time the sender node will buffer its packets until a safe route is identified. Once a safe route has identified, these buffered packets will be transmitted. When a RREP arrives to the source, it will extract the full paths to the destinations and wait for another RREP. Two or more of these nodes must have some shared hops (in ad hoc networks, the redundant paths in most of the time have some shared hops or nodes). From these shared hops the source node can recognize the safe route to the destination. If no shared nodes appear to be in these redundant routes, the sender will wait for another RREP until a route with shared nodes identified or routing timer expired. This helps for find secure type of communication between the source and destination. But the major disadvantage of the this method is its time consuming. Because here secure intermediate node is find out on the basis how many times that node is used for the data transfer. Now if that node is busy when source wants to transmit data then source have to wait for it. It might be possible that another node which is available for transmissions not black hole. This increase unnecessary delay for transmission of data.

b. 2nd method

Every packet in MANETs has a unique sequence number. This number is an increasing value, i.e., the next packet must have higher value that the current packet sequence number. The node in regular routing protocols keeps the last packet sequence number that it has received and uses it to check if the received packet was received before from the same originating source or not. Packet-sequence-numbers for the last packet received from every node. These tables are updated when any packet arrived or transmitted. The sender broadcasts the RREQ packet to its neighbors. Once this RREQ reach the destination, it will initiate a RREP to the source, and this RREP will contain the last packet-sequence-numbers received from this source. When an intermediate node has a route to the destination and receives this RREQ, it will reply to the sender with a RREP contains the last packet-sequence-numbers received from the source by this intermediate node. This method provides secure type of data transmission and fast transmission of data as compared to the previous method .

3. RELATED WORK

In our project of detection and removal of black hole in MANET, here we considering 23 nodes with 1 malicious node. We are comparing the routing table for 3 times with each node's unique sequence number. Because each node has its unique sequence number which is not change but the node which malicious used to send fake sequence number to the source. So it will easily identified in this way. Following figures shows the detection of black hole

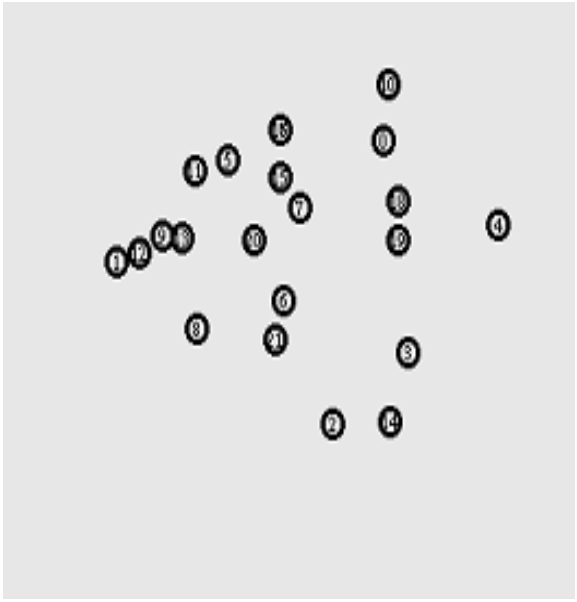

Fig 1.Node formation

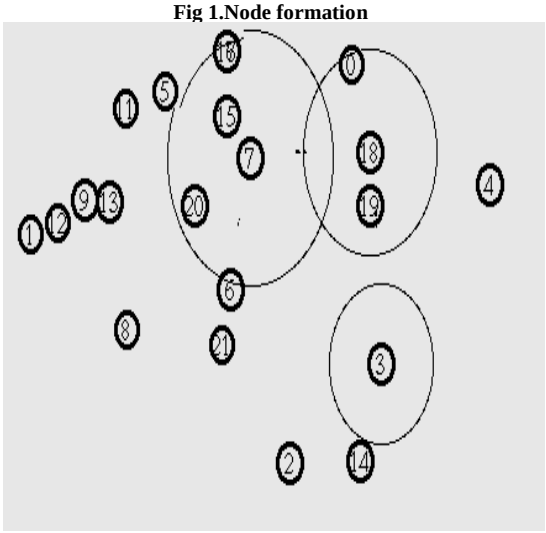

Fig.2.sending request

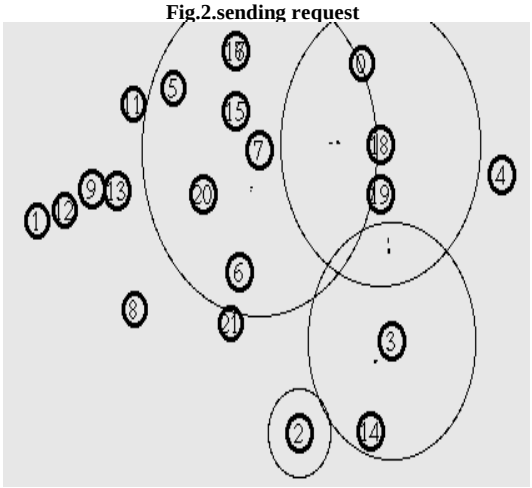

Fig.3.reply on request

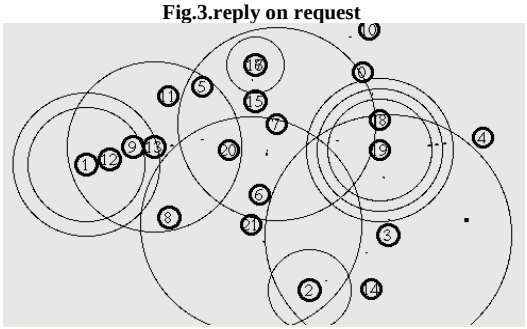

Fig.4.finding shortest path

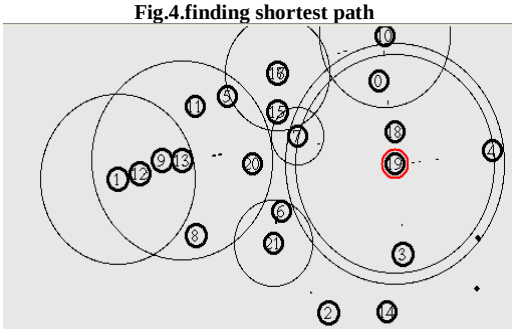

Fig.5. detection black hole

4. FUTURE SCOPE

We are designing algorithm for removing the black node from MANET. After this we are trying to implement for more malicious node in MANET. This possible that new algorithm can be designed for the detection and removal of black hole. Also new protocol can be designed for the detection and removal of black hole.

REFERENCES

[1] Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park," Black Hole Attack in Mobile Ad Hoc Networks"

[2] Vishnu K, Amos J Paul," Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks"

[3] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto," Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method"

◈◈◈