Volume 3, Issue II, Feb 2015
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

A VERNAL APPROACH FOR THE DETECTION OF DOS ATTACKS IN MOBILE AD HOC NETWORKS

Swati Gossain[1], Jagbir Singh Gill[2]

swatigossain@gmail.com[1]
cgccoe.cse.jagbir@gmail.com[2]

ABSTRACT: *In the MANET, different types of attacks are possible. These attacks are categorized as: active attacks and passive attacks. The most common attack in MANET is black hole attack. In the wireless networks, radio communication is the medium of choice. A wireless network is any type of network that uses wireless data connections for connecting nodes. It enables people to access and communicate to other devices without any need of wires. MANET is a collection of various mobile nodes. . The black hole attack is a most common attack and it comes under the category of denial of services attacks. Here in this paper we are going to purpose a novel approach to detect and prevent black hole attack in MANET. Our schema is based on modification of AODV with fake RREQ packets and DRI tables and cross verification.*

KEY WORDS: *AODV, MANET, Black hole attack, Network, Ant colony optimization.*

1. INTRODUCTION

A wireless network is any type of network that uses wireless data connections for connecting computers/ nodes. It enables people to access and communicate to other devices without any need of wires. [1] Wireless network allows the people to browse the internet from any location. Wireless network is defined in many types.

- **Ad hoc network**

An ad hoc network is a network composed only of nodes. It does not require any access point. The communication is takes place in between nodes only. Hence the messages are exchanged and relayed between the nodes. The ad hoc network has the capability of making communications between two nodes. If the distance between two nodes is large, then packets that are exchanged between these nodes are forwarded by intermediate nodes. In the ad hoc network shown in Figure 1, node A can communicate with node D via nodes B and C, and vice versa. A sensor network is a special kind of ad-hoc network. It composed of devices equipped with sensors to monitor temperature, sound, or any other environmental condition. These devices are usually deployed in large number and have limited resources in terms of battery energy.

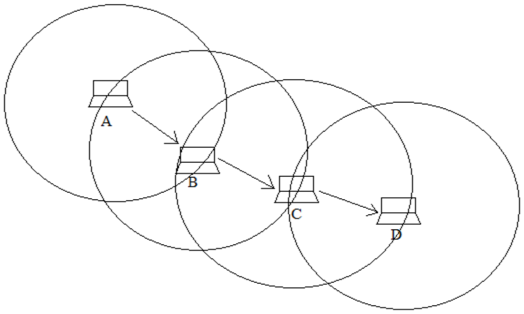

Fig 1: Ad-hoc networks

- **Mobile ad-hoc Network**

Mobile ad hoc network is a collection of mobile nodes. It is a type of infrastructure less network. [2] In the infrastructure less network, no centralized access point is required. The access point contains the base stations.

Types of Attacks:

- **Passive Attack**

In case of passive attacks, confidentiality breaks. As the attacker snoops the data exchanged in network without altering it. Snooping is an unauthorized access to other person data. In this case, attacker only watch the data and it does not modifies it, hence it become very difficult to find the passive attacks.

- **Active Attacks**

In case of active attacks, data integrity is break. As the attacker modified the data and sends to the user.

2. RELATED WORK

Detection and Mitigation Techniques of Black Hole Attack in MANET: An Overview, (2013): in this paper, [6] author discuss about various detection techniques of black hole attack in MANET. Mobile ad hoc network is a collection of the mobile nodes. It does not require any centralized access point. MANET is self-configurable network. Here the nodes are free to move in any direction. Mobile ad hoc networks can be established where the nodes have connectivity with other nodes and can join and leave the network at any point of time. Routing of the data in the MANETs are done on the basis of the node discovery. In the MANET, each node work as a relay agent to route the data traffic. As MANET is dynamic in nature so it is accessible to all the users. The user may be a legitimate user or the malicious user. In this paper, author describes the features, application, and vulnerabilities of mobile ad hoc network.

Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method, (2007): In this paper, author discuss about black hole attack detection in mobile ad hoc networks. Mobile ad-hoc network is a collection of host nodes. It does not require any centralized access point called base station. MANET is vulnerable to various kinds of attacks. Black hole attack is one of many possible attacks in MANET. In this attack, a malicious node sends a forged Route Reply packet to a source node that initiates the route discovery in order to pretend to be a destination node. By comparing the destination sequence number contained in RREP packets when a source node received multiple RREP, it judges the greatest one as the most recent routing information and selects the route contained in that RREP packet. In this paper, author analyzes the black hole attack. In this paper, author propose an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals [5].

A Mechanism for Detection of Black Hole Attack in Mobile Ad Hoc Networks,(2012): In this paper, author discuss a mechanism to detect black hole attack in MANET. A mobile ad hoc network is a collection of several nodes. These nodes are communicates with each other by forming a multi hop radio network [4]. It maintains many connections in a decentralized manner. Security remains a major challenge for these networks due to their features of open medium, dynamically changing topologies, reliance on cooperative algorithms, absence of centralized monitoring points, and lack of clear lines of defense. MANETs are vulnerable to various types of attacks. These include passive eavesdropping, active interfering, impersonation, and denial of service. One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols. In this paper, author proposed a new solution that is an enhancement of the basic AODV routing protocol. It helps to avoid and detect black holes. In this a malicious node falsely advertises good paths to a destination node during the route discovery process.

Securing and Preventing AODV Routing Protocol from Black Hole Attack using Counter Algorithm,(2012): in this paper, author discuss the [9]methods to secure and prevent AODV routing protocol from black hole attack. For this purpose author uses the counter algorithms. Wireless network is an emerging technology, it allows the users to access information. MANET is a collection of nodes. Each node can connect by wireless communication links, without any fixed station such as base station. In this paper, author analyzed the security system with proposed and modified AODV algorithm. The Proposed method can be used to find the secured routes and prevent the black hole nodes in the MANET by identifying the node with their sequence number. This method is check whether there is large difference between the sequence numbers of source node or intermediate node, if the sequence number is greater, than it is check from which node send back to the RR table. In this paper author proposed a counter algorithm for identifying the malicious node in AODV protocol suffering from black hole attack.

Detection and prevention of Routing Attacks in MANET using AODV, (2012): in this paper, [7] author discuss about the detection and prevention of routing attacks in MANET. Mobile ad hoc network is a type of wireless network. Wireless networks allow hosts to travel without the constraints of wired connections. Hosts and routers in a wireless network can move around. A MANET uses multi hop peer to peer routing as an alternative of fixed network infrastructure to provide network connectivity. There are no permanent routers, because each node acts as router and frontwards traffic from other nodes. In this paper, author a new method based on AODV behavioral metrics detect and prevent MANET attacks. In this paper, author proposed a routing based method to detect DoS attack like flooding, black hole. Author’s main concern is about AODV. AODV is a well-known and popular reactive type protocol used in MANET. In this paper, author discuss about different types of attack that have been launch during routine procedure like a Flooding, Black Hole and Gray Hole. In this paper, author proposed a solution detection and prevention of these attacks.

A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks, (2011): in this paper, [8] author discuss a new protocol for the detection of black hole attack in Mobile ad hoc network. A mobile ad hoc network is a collection of infrastructure less nodes. Security is more challenging in ad-hoc networks, because it is dynamic in nature. Due to this, the nodes are free to move. In this paper, author discuss about security problems in MANET, called black hole problem. This attack occurs when a malicious node referred as black hole joins the network. In this paper, author used the AODV protocol to build a new protocol. It includes the following functionalities: source node waits for a reliable route, each node has a table in which it adds the addresses of the reliable nodes, RREP is overloaded with an extra field to indicate the reliability of the replying node. Security is the main issues for networks. It becomes more challenging in ad hoc networks due to the lack of central access point to monitor node behaviour and to manage node membership.

3. BLACK HOLE ATTACK

Black hole attack is one of the denial-of-service attack in ad-hoc networks. As we know RREQ, RREP, RRER are three types of packets that are used for route fining. In case when black hole node present in network when source node broadcast RREQ packets for route to destination, the black hole node fake reply with RREP packets. It shows that it's having shortest path to destination but in actual it's replying with fake RREP packets. After getting all replies from all possible paths when source node do hope count then it will found that the black hole node is having shortest path and it will selects this path to send data. But the black hole did not forward packets it will receive packets and drop them.

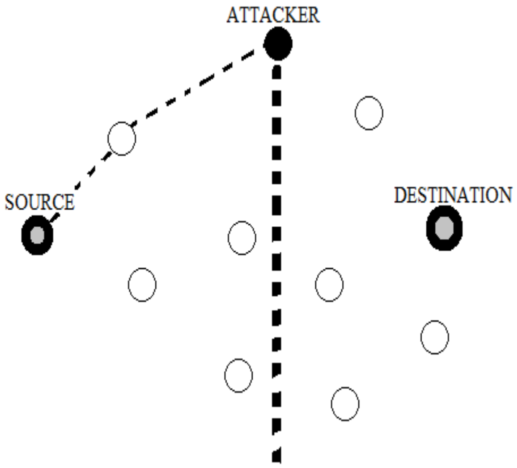

Fig 2: Black hole attack

4. PURPOSED SCHEMA

Here to detect black hole attack in MANET a novel method is proposed. It contain fake RREQ messages and DRI values. According to this method during path selection process before broadcasting actual RREQ packets it will flood fake RREQ packets in network. Now as per black hole node nature the malicious node will give respond of fake RREP message means for non-existing node. In this mechanism, before discovering the actual route for data transmission in AODV, it will send some rough data and cross verify from destination, if destination node is not receiving data then it will isolate the very first neighbour node of destination, then it will transmit fake RREQ packets and the only malicious node will reply with RREQ all other nodes will reply with RRER packets. So from this scenario it will detect the rest malicious nodes and will isolate them.

Also integrate the concept of DRI (data routing tables) for path selection. After detecting black hole node when it will select path it also consider DRI tables for path selection. As we know that in promiscuous mode we can check DRI tables of node. Promiscuous mode is a mode which is caused to generate and receive all traffic through node. DRI table is which contain dynamic routing information. It contains all values of THROUGH and FROM. If the node is normal and passing all traffic through it then the value of it's FROM table is 1 and if it's malicious then the THROUGH table contain value 0. So to check whether the node is malicious or not we will use DRI tables. So in our scenario before communication source node broadcast promiscuous mode activation message to all nodes and requests and requests them to show there DRI tables after that we will see all possible paths from source to destination and also checks the values of DRI tables of nodes that are on the paths.

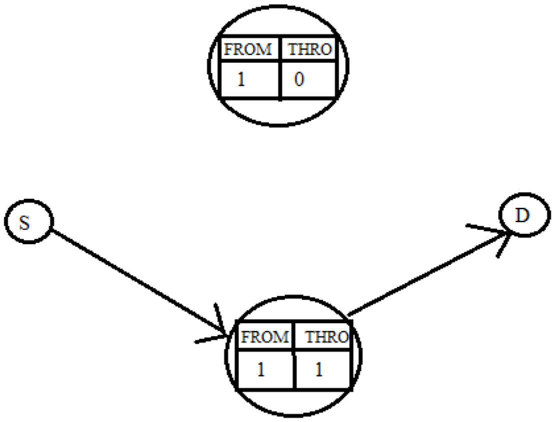

Fig 3: DRI based path selection

After that will choose the path in which all nodes are having FROM and THROUGH values 1-1. The nodes are having value 0 will be isolated for communication and the path which is chosen on the bases on this scenario will be the safe path for communication.

- Initialize network with n number of wireless nodes.
- Select source node from network.
- Source node broadcast fake RREQ packets for non existing node.
- Black hole node will reply with RREP packets.
- Find nodes from network from where source node get RREP packets.
- Consider these nodes as black hole nodes.
- Select path on the basis of DRI tables.
- If the DRI value is [1-1] then consider node as reliable node and use it for path for data transmission.

5. RESULTS AND DISCUSSIONS

The simulation is done by using network simulator (NS-2.34). Here the attack and purposed schema is implemented by taking 50 wireless nodes and the results are plotted in terms of throughput and delay measurement. The comparison between both scenarios is shown in graphs. To perform simulation following parameters to be taken:

Table 1: Simulation parameters

Network	Wireless
Antenna	Omni directional
Routing Protocol	AODV
Queue	Drop tail (50)
Number of Nodes	50

Delay: Here the delay between both scenarios is shown. In this graph red line shows delay curve for old scenario and green line show delay curve for purposed scenario. In old case because of black hole attack it drops packets in between path and destination is disabling to receive any packet so the delay curve is rising with packet loss but in new case because of prevention of black hole attack destination node can properly receive packets, so here it is less delay.

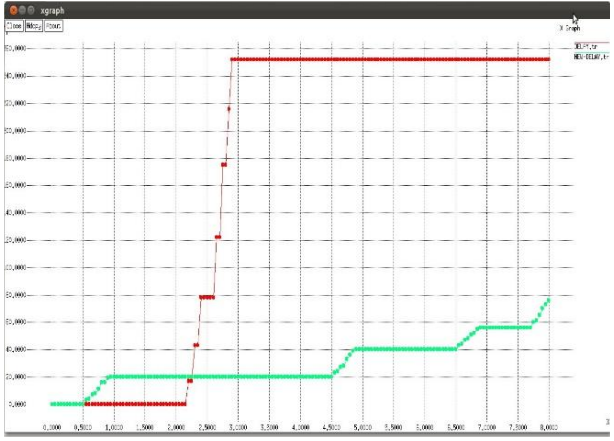

Fig 4: Delay Graph

PDR: In this graph PDR comparison between both scenarios is shown. Here red curve shows PDR for old case and green curve shows PDR for new case. Because of packet loss in old case PDR is very loss and because of prevention of attack in new case throughput is high.

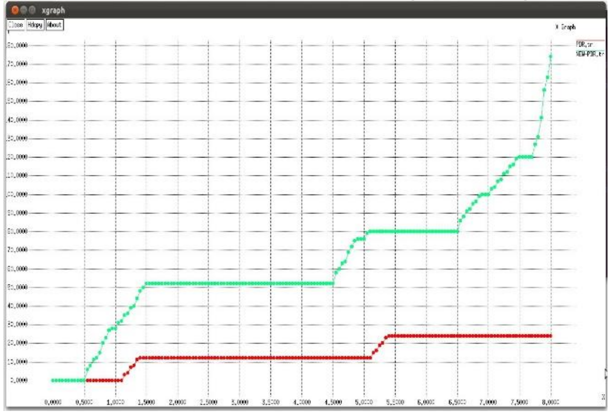

Figure 5: PDR graph

6. CONCLUSION AND FUTURE WORK

Using the approach of Fake RREQ packets and data routing tables we can easily detect the black hole node and can enhance the performance of network. As we know that MANET is infrastructure less network and it's a type of self-configured network, as we are working in cooperative black hole nodes where both nodes belongs to black hole nature if in case the cooperation is in between black hole and grey hole node is there then the process of DRI will be failed so in future we can work upon it, so here we can use learning process of neural network to overcome from that kind of situation.

REFERENCES

[1]. http://computernetworkingnotes.com/wireless-networking-on-cisco-router/types-of-wireless-networks.html

[2]. http://mobileeadhocnetwork.blogspot.in/2012/02/types-of-manet.html

[3]. Marco Dorigo, Thomas Stutzle, the Ant Colony Optimization Metaheuristic: Algorithms, Applications, and Advances.

[4]. S. L. Dhende, Prof. Mrs. D. M. Bhalerao, A Mechanism for Detection of Black Hole Attack in Mobile Ad Hoc Networks, International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 6, August – 2012

[5]. 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, International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007

[6]. Swati Jain, Naveen Hemrajani, Detection and Mitigation Techniques of Black HoleAttack in MANET, International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064

[7]. Jasleen Arora, Paramjeet Singh and Shaveta Rani. Article: Detecting and Preventing Attacks in MANET. *International Journal of Computer Applications* 81(5):14-18, November 2013. Published by Foundation of Computer Science, New York, USA.

[8]. Yaser khamayseh, Abdulraheem Bader, Wail Mardini, and Muneer BaniYasein, A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks, International Journal of Communication Networks and Information Security (IJCNIS), Vol. 3, No. 1, April 2011

[9]. Dr. S. Tamilarasan, Securing and Preventing AODV Routing Protocol from Black Hole Attack using Counter Algorithm, International Journal of Engineering Research & Technology, Vol.1 - Issue 5 (July - 2012).