Volume 3, Issue IV, April 2015
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

*WINGS TO YOUR THOUGHTS.....*

# CO-OPERATIVE BLACK-HOLE DETECTION SCHEME TO ENHANCE THE PERFORMANCE OF MANET

[1]Harmandeep Kaur, [2]Ramanjit Singh
[1]20harmangrewal@gmail.com,[2]raman.lcet@gmail.com

***ABSTRACT:*** *Due to its dynamic topology, resource constraints, no centralized infrastructure and limited security, it is vulnerable to various attacks and black hole attack is one of them. Mobile Ad hoc Networks is an infrastructure less network which is self-configuring and it consists of independent mobile devices that can communicate via wireless medium. Each mobile device can move freely in any direction, and changes their links to other devices frequently. Security is an essential part of ad hoc networks. Due to its dynamic topology, resource constraints, no centralized infrastructure and limited security, it is vulnerable to various attacks and black hole attack is one of them. In black hole attack, the malicious node advertises itself as having the shortest path to the destination and falsely replies to the route requests, and drops all receiving packets.*
***KEY WORDS:*** *AODV, MANET, Black hole attack, Network, DRI.*

## 1. INTRODUCTION

MANET is widely used in military purposes, sensor networks, rescue operations, personal area networks etc. Today wireless networks have been gaining popularity, as the user wants wireless connectivity irrespective of their geographic position. The devices in wireless network can communicate with each other directly or via some centralized infrastructure. With centralized infrastructure, we need a central controller like base station to provide [1] communication and authentication. But in ad hoc networks, there is direct communication between devices without any central controller which leads to security threats.

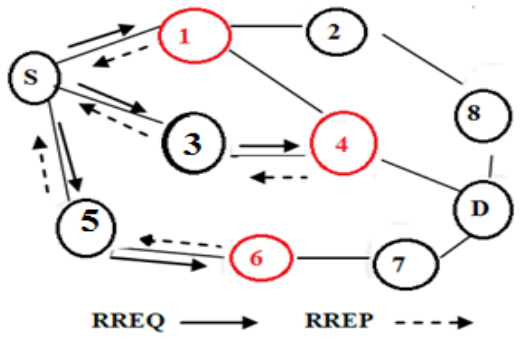


**Fig 1:** Black Hole Nodes in MANET

In AODV, the sequence number is used to determine the freshness of routing information contained in the message from the originating node. If the source node receives more than one RREP packets, it will select the route with highest destination sequence number or minimum hop count. In case black hole attack, the malicious node forges the RREP packet by having the highest destination sequence number to advertise itself as a shortest path towards the destination. Then, the source node believes the malicious node and starts sending the data packets towards that node and malicious node will start dropping the data packets. It may happen that more than one malicious node exists in the network at different places. [2]

The nodes in ad hoc networks act as a host as well as router to forward the data packets. As the topology of MANET changes frequently, it is vulnerable to various security threats. The routing protocols are exploited by the attackers with the aim to intercept the data packets. In MANET, we have three types of protocols i.e. Proactive, Reactive and Hybrid protocols. Proactive protocols (DSDV, OLSR) are table-driven protocols in which the nodes maintain and update the routing tables periodically even when there is no communication. But in reactive protocols (AODV, DSR) or On-Demand Protocols, the routes are discovered on the demand of the source node. Proactive protocols have low latency rate in discovering the route but high routing overhead. This is because the nodes periodically exchange control messages and routing table information in order to keep up-to-date routes to any active node in the network. [3] The reactive protocols have the low routing overhead at the expense of delay to discover the route when desired by the source. Due to periodically exchange of routing information, the proactive protocols are less prone to security attacks like black hole, Sybil attack etc, as compare to reactive protocols. Mostly, the researchers have more focused on securing the AODV and DSR from different types of attacks and black hole attack is one of them. A lot of schemes have been proposed on detecting and preventing the black hole attack but these schemes have some pros and cons too. In AODV, the RREQ (Route Request) packet is sent by the source to discover the route. If the intermediate node has the fresh enough route towards the destination, it can reply the RREP packet back to the source. Otherwise, broadcast the RREQ packet to other nodes in the network.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

*WINGS TO YOUR THOUGHTS.....*

## 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 proposes 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

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

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 behavior 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.

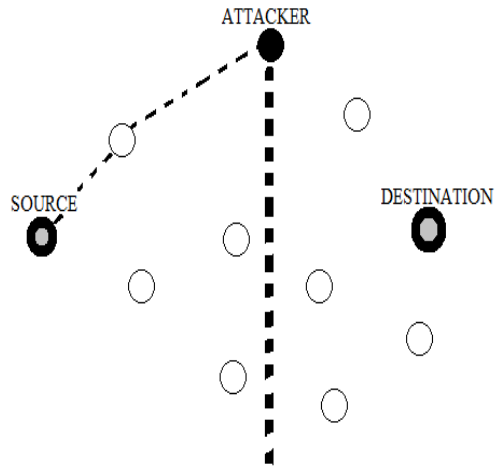


**Fig 2:** Black hole attack

## 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.

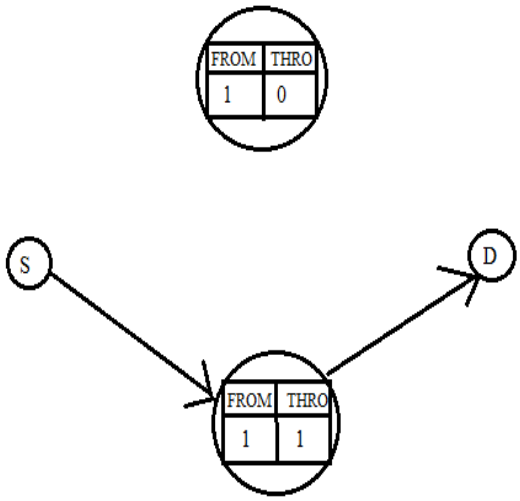


**Fig 3:** DRI based path selection

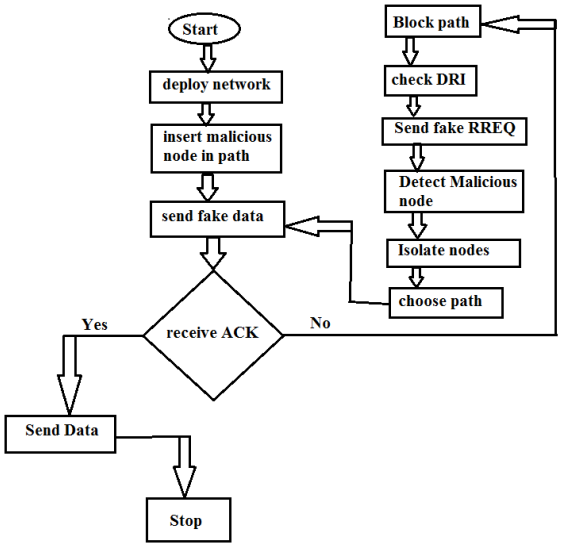


**Fig 4:** Proposed work

**Detection Steps**

- Choose any one node as a SOURCE NODE and one DESTINATION NODE and consider that the network contain multiple black hole nodes.
- Source node will broadcast RREQ packets with original destination address.
- Destination node will reply with RREP packets towards source node. And black hole nodes will also do fake reply.
- During hop count source node will select black hole node's path. Because black hole node did fake reply that it contain destination node's path. So here to

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

*WINGS TO YOUR THOUGHTS.....*

enhance security and to detect black hole node we will set timer on source node. This timer will work on the basis of acknowledgement (ACK) of original destination. So for checking malicious nodes in path initially source node will send some empty data packets and will request to original destination for ACK through longer path.

- if source node does not get any ACK till timer expire then it knows that there is some malicious node in the path. So it will stop sending empty packets and will temporary block this path. On the other hand if it will get ACK then it means data is successfully receiving at destination and it will start sending original data.
- Here the path which was selected is given below.
  S → B1 → B2 → D
  It means B2 node is having path till destination node. It means Destination node also have path till B2 node. So we will check DRI table of destination node. But when we will check DRI of destination node it does not contain any entry for B2 it means B2 node is telling lie, means it's malicious. So we will send ALERT message to its neighbor nodes and make it isolate.
- Now B2 node is isolated and to now source node will broadcast fake RREQ packets with Fake destination address (for non-existing node). Here all normal nodes will reply with RRER packets and the only black hole node will reply with RREP packets.
- As source node knows that the destination is not exist and if it got any RREP packet then it come to know that black hole node is replying only. So it will again send ALERT message and isolate it.
- Now all the nodes are isolated and network is clear to send data. So it will broadcast RREQ packets for original destination as in Step 2 and will choose shortest path and start transmitting data.

## 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.

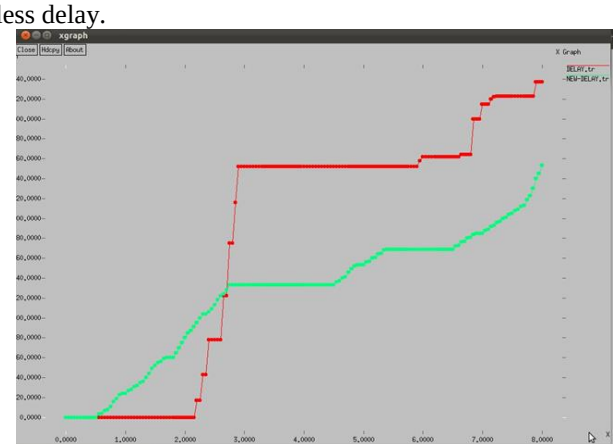

**Fig 5:** Delay Graph

**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 less and because of prevention of attack in new case throughput is high.

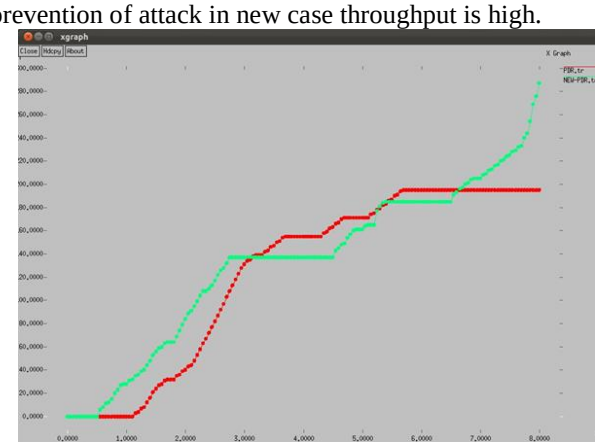

**Fig 6:** PDR graph

## 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.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

*WINGS TO YOUR THOUGHTS.....*

## 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).**