Black Hole Attacks in MANETs: Preventions by Identification of Thick Node Method

Krishan Kumar
Research Scholar, Masters of Technology,
Computer Science and Engineering
BGIET, Sangrur, Punjab, India

Taranjit Singh Aulakh
Assistant Professor, Computer Science and Engineering,
BGIET, Sangrur, Punjab, India

ABSTRACT
When two or more computer Systems link together with the help of wire or without wire that system is called the network of a computers. A network which is self directed and distributed is known as Mobile Adhoc Network. MANETs consists of mobile nodes that are free to move in and out of the network. Computers, IPod, Mobile Phones constitute to be a Node that participates in the network. Different type of topologies can be formed on the basis of connectivity of the nodes with each other in the network. These nodes can either act as a host or router or it can act as both. These nodes can be deployed in any network and due to their dynamic topology no infrastructure or central management system is required and thus it makes the MANET vulnerable to the security attacks. In these paper two methods i.e. MN-ID broadcasting and thick node identification method were compared and it was found that the thick identification method has got an upper edge on the other method.

Keywords
DoS, MANET, RREP, RREQ, RERR, AODV

1. INTRODUCTION
A network is a system that consists of a group of computers and other hardware related to it connected via communication channel for sharing data and information. There are two types of networks Wired and Wireless Networks. Mobile Ad-Hoc Networks comes under Wireless Networks. MANET is a collection of mobile nodes which does not need any central access point or base station.

The first generation of wireless networks started from 1972. At that time, PRNET was the name given to network system. The ad hoc networks have the history from the DoDi sponsoring PRNET for the armies. The emergence of second generation took place with the enhancement and implementation of ad hoc network as an ally of SURAN program. It has taken the new heights in 1990 with the introduction of notebook computers and the introduction of the mobile of nodes as the brain child at many research platforms. "Ad-hoc networks" was accepted as a term by the IEEE802.11 subcommittee and from then only the versatile regions came under the eye of the researchers and explorers for the implementation of the ad hoc network. Internet Engineering Task Force (IETF), worked hand in gloves with mobile ad-hoc networking groups for the standardization of protocols for routing in ad hoc network.

Mobile Ad-Hoc Networks comes under Wireless Networks. Wireless networks are getting well known because of their convenience. User is no more subject to wires where he/she is, easy to move and appreciate being connected to the network. There are many characteristics of ad-hoc network that make it a hot selling cake. Some of these characteristics have been pen down like it gives the freedom of the mobility to the client while remaining in the network, the client is free from the establishment of the hardware's and it is also easily installable. It is flexible in nature and can be designed as per the requirement of the client. The variability in the number of clients is also accommodated in the ad-hoc network.

Mobile Ad-Hoc Networks are independent and decentralized wireless systems (See Fig. 1). MANETs comprise of mobile nodes that are free to move in and out in the network. Nodes are the devices that are mobile and that participate in the networks such as mobile phone, laptop, personal digital assistance, MP3 player and personal computer. These nodes can act as host/router or both simultaneously. They can structure self-assertive topologies relying upon their connectivity with one another in the system. To configure themselves is a unique ability by the virtue of which the network can be deployed without the infrastructure. IEFT work rigorously for the development of routing protocols for MANET. The development of the routing protocol is the center of attraction in the research zone. Different routing conventions had already been developed for MANET namely AODV OLSR, DSR etc.

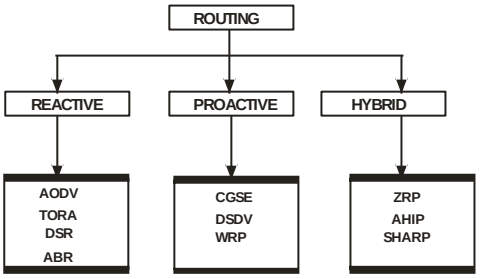

Fig. 1 : MANET Routing in MANETs

2. CLASSIFICATION OF ATTACKS
Understanding of possible form of the attack is the starting point for the development of the secured solution for a secured transmission of information the critical analysis of the security of communication in MANET should be account for. The Vulnerability the cyber-attacks increased by many fold in MANET if there is no central coordination mechanism or it has a shared wireless medium.

The classification of the attack can be done on basis of the origin of attack. It can be classified as internal or external attack. It can also be classified according to the attack behavior which means whether the attack is passive or active. This classification is important as the attacker can attack at any region as classified.

2.1 Internal/ External Attack
External attackers are fundamentally outside the networks who want to get access to the network and once they get access to the network they start sending false packets, denial of service in order to disrupt the performance of the whole

network. The nature of the attack is similar to the wired network attacks. These attacks can be anticipated by executing efforts to establish security such as firewall, which mitigates the access of unauthorized person to the network.

The summary of black hole attack done externally is as below:

a) Detection of active route and the address of destination by malicious node.

b) RREP is send by malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.

c) RREP is being send by Malicious node to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.

d) The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node. The new information received in the route reply will allow the source node to update its routing table.

e) Source node selects new route. Data will be dropped to malicious node on the route on which it is existing.

In the internal attack the attacker who has got the ordinary access to the network or who is present in the network internally or who is participant in some typical exercises of the network can do this attack. As the attacker can access the network so a new malicious node can be introduced either by trading of or by the personation and start acting maliciously. This is better known as internal attack and it is the severe attack as the malicious node is present in your network and that too actively.

2.2 Active/ Passive Attack

When the network is attacked in the active mode its critical information is extracted and destroyed it is done to disrupt the network. These can be internal or external attack. When the active attack has to be used to disrupt the efficiency of the network, at that time it is being used as an internal node in the network. Being dynamically involved in the network it is very easy to nab any internal node and exploit it to introduce bogus packets injection or denial of service. The attacker enjoys a strong position in the network and by the virtue of which the messages can be modified, fabricated and replayed.

Unlike active attacks, disruption of the network operations does not happen in passive attacks. In Passive, attack, the attacker keeps a vigil eye on the network to extract the information of the transmission that is happening currently. The attackers passively wait and watch each and every move of the network and understand the communication of node with each other. Before attacking the network the attacker has an ample information about the network through which he can easily highjack and can make an attack in the network.

2.3 Black Hole Attack

Please the crucial situations like natural disaster, war footing, business conferences, demands both MANET and the secured communication of data between two nodes. To make this demand a reality, many second routing protocols were developed in the recent past. These proposed protocols prevent the attack on the safety properly and avoid hazardous conditions.

Various types of attacks on MANET, like Black hole attack, worm hole attack, denial of service, flooding attack impersonation attack , selfish node misbehaving and many more has made it very challenging and crucial to send the data safely from one node to another. Mobile network security is the need of a day. For this in-depth knowledge of the attacks their behaviors and the damages they may cause must be understood. There are many reasons behind that make MANET prone to these attacks. One of the major reasons is absenteeism of the central point for network management and the communication occurs between the nodes mutually. Vigorously changing topology lack of authentication facility and limited resources add another feather to the cap of attacker.

Black hole attack shatters the communication of the route by forging the routing message. This is not the end, further there is drop the packet a forged nodes and, thus these safety property get threatened.

In Black hole attack the sequence no is forged and forcibly acquiring the route by capturing the hop count of a routing message and make all the data packet drops that passes through it. The malicious node poses itself the destination node by sending the concocted RREP to the source node and start the route discovery.

Black hole exhibits to characteristics (1) the node poses itself as destination and having valid route by capturing the node and the ad hoc routing protocol, though the route is fake but this was done to intercept the packets.

The malicious node fits in the data route by different methods this has been explained in the figure below: The figure is self-explanatory that node 1 is source node and node 4 is the destination node. When the source node flashes RREQ to find the optimized route to the destination node to the intermediate nodes, the intermediate node continuously receive and broadcast RREQ. Everything works in order if the RREP from the normal destination node reaches the source node. As shown the node 3 is an attacker node and act as black hole. Now the node 3 send RREP from itself to the source node before any other intermediate node send the same, making the source node assume that route discovery process has been complete and starts sending the data packets. In the black hole attack the malicious node send RREP to the source node with the hope count of 1 and having large sequence number, in this way the source node will select the malicious node as the destination node as it exhibits minimum hop count after receiving the RREQ from the source node and start sending the data packets to malicious node considering it as the destination node. The Black has got one property that it does not forward any packet and makes all the packets get dropped to itself without the knowledge of source node. The Source node assumes the packets are moving to the destination without having any information that the route has been attacked and the packets are not received by the actual destination node. If these kinds of nodes are multiple in nature and present in a single MANET, makes a situation a crucial, complex and hazards.

Malicious node has one distinct characteristic that it keeps the destination sequence number on the higher side. Since AODV consider the higher value of destination sequence number as the fresh RREP, thus the RREP send the by malicious node is treated as the fresh node. By this way the malicious node

succeed to porch into the route and this is the black hole attack.

2.3.1 Types of Black Hole Attacks

A Black Hole attack is a kind of denial of service attack where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination.

2.3.1.1 Single Black Hole Attack

In single black hole attack only one malicious node poach into the route and attack the MANET (see Fig. 2) by dropping the data packets to its malicious node. The malicious nodes have the routing capability and the attacker take the advantages of the lean routing protocols of MANET . The most vulnerable routing protocol is AODV, which works on the principle that the node having maximum sequence number may be consider as the fresh node that guarantees the loop free route. For the multiple routes, the node which exhibits higher sequence number and having the least hope count is considered as the fresh node with optimized route to the destination.

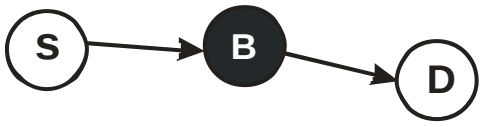

Fig. 2 : Single Black Hole Attack

2.3.1.2 Co-operative Black Hole Attack

When the malicious nodes act in a group and attack the MANET that attack is better known as Co-operative Black Hole. In the Fig. 3 the nodes 2 and 3 act as black holes. The Attack becomes complex when the multiple malicious node work in hands in gloves with each other and disrupt the complete routing of the data. In the cooperative black hole attack the packet forwarding capacity of the system shatter vigorously.one address is needed, center all address text. For two addresses, use two centered tabs, and so on. For three authors, you may have to improvise.

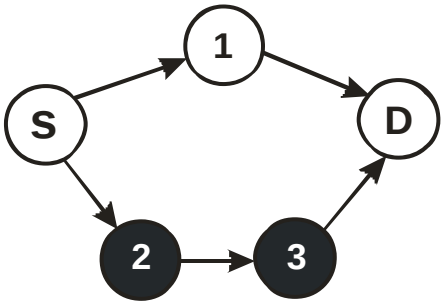

Fig. 3: Cooperative Black Hole Attack

3. SECURITY IN MANETS NORMAL OR BODY TEXT

Please As compare to the wired network securities in MANET is very difficult to be maintained because of its vulnerability. As the Wireless links give path to an Adhoc network making it more prone to the attacks like message replay, Distortion and last but not the least passive eavesdropping to active impersonation. The list of vulnerabilities to which MANET is prone to is as below:

a) Dynamically changing network topology: By the virtue of this Topology malicious node are allowed to connect to the network without having advance detection. The mobile nodes connect and disconnect themselves arbitrarily from the network.

b) Lack of centralized monitoring: Due to absence of centralized monitoring the classical security solutions became imperative. These solutions were based on certification authorities and online server. When some nodes are found to be compromised there is a drastic change in the trust relationship also of the individual nodes.

c) Cooperative algorithms: In MANET mutual trust between the neighboring nodes is necessarily required, which is in complete violation of principal of network security.

d) The authority for certification is absent.

e) The limited physical protection is limited in each node: As network nodes are not kept in lock and key hence there more prone be captured and fall prey to control of an attacker.

f) The connectivity is not continuous.

g) The vulnerability of the links: by breaching the confidentiality injection of fake messages and eavesdropping messages could be done without much effort as there is an easy physical access to the network component.

h) Adversary inside the Network: The compromised nodes which lie within the MANET, can join and leave the network freely are more dangerous than the external attack. These nodes are difficult to detect that the nodes are behaving maliciously. .

4. COMPARISON WITH EXISTED METHOD

Researchers have proposed various techniques to prevent black hole attack in mobile ad-hoc networks. Antony Devassy, K.Jayanthi[10] introduces the use of MN-ID Broadcasting. The main drawback of this technique is that there is a packet drop of app. 300 packets after the simulation of 50 micro seconds while in our proposal approach we identified the thick node and there is almost 0 packet drop at 50 micro seconds of simulation time.

5. PROPOSED APPROACH

The proposed approach contributes highly in avoiding the black hole attacks during path setup between source and destination. The proposed approach is as:

- Deployment of the nodes in network
- Calculate the neighbors and their corresponding distances
- Broadcasting of the RREQ packet from source to the nodes
- Destination nodes send RREP packets to the source
- Calculation of the shortest path from all the paths
- Identification of “One Path Thick Node”
- Comparison of the node IDs with the “One Path Thick Node”
- If the ID matches the packet is accepted and routing is done otherwise the packet is discarded.

6. EXPERIMENTAL RESULTS

The In this section, we describe our simulation environment and the simulation results. The simulation is being implemented in NS-2.35 and the simulation parameters are provided in Table.

Table 1 Simulation Parameters

Number of nodes	50
Initial energy	100 J
Routing protocol	AODV
Tool Used	NS 2.35

The simulation results of throughput versus time and packet delivery ratio versus time are given below. These results are improved by the proposed method.

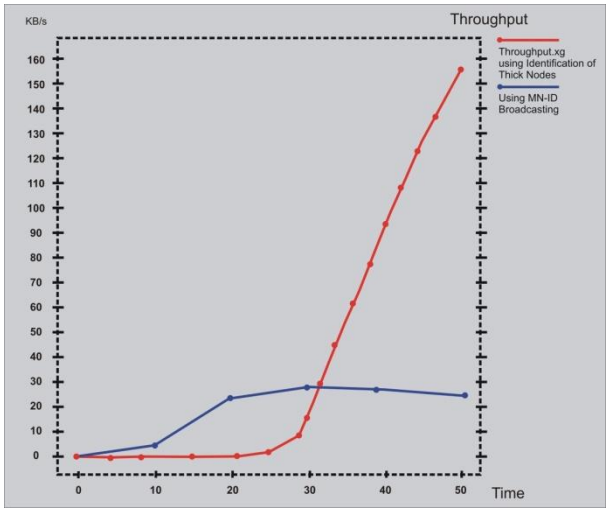

Fig 1 Throughput versus Time

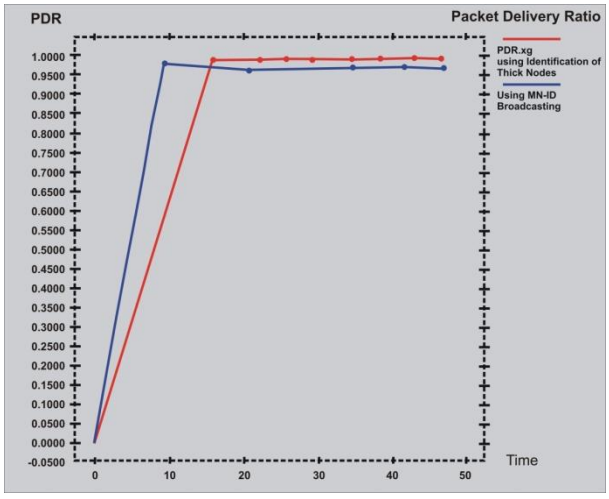

Fig. 2 Packet Delivery Ratio versus Time

7. CONCLUSION AND FUTURE SCOPE

For Black Hole Attack is a main security threat that affects the performance of the AODV routing protocol. This detection is the main matter of concern. Due to the inherent design disadvantages of routing protocol in MANETs, many researchers have conducted diverse techniques to propose different types of prevention mechanisms for black hole problem.

There are still some things we can do for future works. Our proposed solution is likely to reduce the energy consumption and will help to increase the network lifetime. As future work, research work can be extended to develop simulations to analyze the performance of the proposed solution based on the various security parameters like mean delay time, packet overhead, memory usage, mobility, increasing number of malicious node, increasing number of nodes and scope of the black hole nodes and also focusing on resolving the problem of multiple attacks against AODV.

8. ACKNOWLEDGEMENT

I am extremely grateful to my guide for providing invaluable guidance throughout this work. His dynamism, vision, sincerity and motivation have deeply inspired me. The perfection that he brings to each and every piece of work that he does always inspired me to do things right at first time. It was a great privilege and honor to work and study under his guidance. I am extremely grateful for what he has offered me. I am grateful to my parents for their love, prayers, caring and sacrifices for educating and preparing me for my future.

9. REFERENCES

[1] Jaspal Kumar, M. Kulkarni, Daya Gupta), "*Effect of Black Hole Attack on MANET Routing Protocols",* IJCNIS, **5**, (2013), 64-72

[2] Sowmya K.S, Rakesh T. And Deepthi P Hudedagaddi (2012), *"Detection and Prevention of Blackhole Attack in MANET Using ACO"*, International Journal of Computer Science & Network Security, May2012, **Vol. 12** Issue 5, p21-24. 4p

[3] Rajni Tripathi And Shraddha Tripathi , "*Preventive Aspect Of Black Hole Attack In Mobile Ad Hoc Network"*, IJAET, (2012) ISSN: 2231-1963

[4] Tanu Preet Singh Neha Vikrant Das (2012), "*Multicast Routing Protocols in MANETS",***Volume 2**, IJARCSSE(2012)

[5] Shree Om, Mohammad Talib, *"Using Merkle Tree to Mitigate Cooperative Black-hole Attack in Wireless Mesh Networks"*, (IJACSA), **Vol. 2, No. 5,** 2011

[6] Nazmus Saquib1, MD. Sabbir Rahman Sakib1, and Al-sakib khan pathan, *"Performance Analysis of MANET Routing Protocols Using an Elegant Visual Simulation Tool"*

[7] Antony Devassy, K. Jayanthi (2012), "*Prevention of Black Hole Attack in Mobile Ad-hoc Networks using MN-ID Broadcasting*",(IJMER), Vol.2, Issue.3, May-June 2012 pp-1017-1021 ISSN: 2249-6645

[8] Arnab Mitra, Rajib Ghosh, Apurba Chakraborty, Debleena Srivastva (2013), "An Alternative Approach to Detect Presence of Black Hole Nodes in Mobile Ad-Hoc Network Using Artificial Neural Network", **Volume 3,** Issue 3, March 2013 ISSN: 2277 128X IJARCSSE

[9] Saurabh Gupta, Subrat Kar, S Dharmaraja (2011), *"BAAP: Blackhole Attack Avoidance Protocol for Wireless Network",* (ICCCT)-2011

[10] Supriya Tayal, Vinti Gupta (2013), "*A Survey of Attacks on Manet Routing Protocols*", IJIRSET **Vol. 2**, Issue 6, June 2013

[11] DR. A. A. Gurjar, A. A. Dande (2013), "Black Hole Attack in Manet's: A Review Study", (IJIEASR) ISSN: 2319-4413, Volume 2, No. 3, March 2013

[12] Swati Jain, Naveen Hemrajani (2013), "Detection and Mitigation Techniques of Black Hole Attack in MANET: An Overview", (IJSR), India Online ISSN: 2319-7064

[13] MS Monika Y. Dangore, MR Santosh S. Sanbare (2013), "A Survey on Detection of Blackhole Attack using AODV Protocol in MANET", (IJRITCC), ISSN 2321–8169 Volume: 1 Issue: 155–61

[14] Puja Vij, V. K. Banga, Tanu Preet Singh , "Survey on Prevention of Black Hole Nodes in Mobile Ad-hoc Networks", (ICTEEP'2012) July 15-16, 2012 Singapore

[15] Nisha P John, Ashly Thomas (2012), "Prevention and Detection of Black Hole Attack in AODV based Mobile Ad-hoc Network- A Review", IJSRP, **Volume 2**, Issue 9, September 2012 ISSN 2250-3153

[16] Ajay Sharma, Nithesh k. Nandha, Kailash Parik, Prof. K.P. Yadav (2012), "Survey of Secure Routing Protocols for MANETs", IJRREST: **Volume-1**, Issue-2 | September-2012

[17] Rajneesh Narula And Sumeer Khullar (2012), "Security Issues of Routing Protocols in MANETs", IJCT, ISSN: 2277-3061 Volume 3 No. 2, OCT, 2012

[18] Ashwani Garg And Vikas Beniwal (2012), "A Review on Security Issues of Routing Protocols in Mobile Ad-Hoc Networks", Volume 2, Issue 9, September 2012 ISSN: 2277 128X IJARCSSE.

[19] K. Thamizhmaran, R. Santosh Kumar Mahto, V. Sanjesh Kumar Tripathi (2011), "Performance Analysis of Secure Routing Protocols in MANET", IJARCCE **Vol. 1**, Issue 9, November 2012

[20] Priyanka Goyal, Vinti Parmar, Rahul Rishi (2011), "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM, **Vol. 11**, January 2011, ISSN (Online): 2230-7893

[21] Nital Mistry, Devesh C Jinwala, Mukesh Zaveri (2010), "Improving AODV Protocol against Blackhole Attacks",

[22] Harminder S. Bindra, Sunil K. Maakar and A. L. Sangal (2010), "Performance Evaluation of Two Reactive Routing Protocols of MANET using Group Mobility Model" IJCS Issues, **Vol 7**, Iss 3, Pp 38-43 (2010) ISSN(s): 1694-0784, 1694-0814

[23] Nishant Sitapara and Prof. Sandeep B. Vanjale (2010), "Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks", ICETE-2010" on Emerging trends in engineering on 21st Feb 2010

[24] G.Vijaya Kumar, Y.Vasudeva Reddy, Dr.M.Nagendra (2010), "Current Research Work on Routing Protocols for MANET: A Literature Survey", IJCSE **Vol. 02**, No. 03, 2010, 706-713.