Prevention of Black Hole attacks in MANETs Using Identification of Thick Node

Mukesh Goyal[1], P.S.Bhullar[2], Mamta Goyal[3]

1. *Lecturer ECE BHSBIET, Lehragaga,PSBET&IT, Punjab, Chandigarh, India*
2. *Assistant Professor ECE GTBKIET, Chappianwali , Malout, India*
3. *Assistant Professor Applied Sci., MIMIT, Malout, India*

goel_mukesh2000@yahoo.com, p.bhullar@rediffmail.com, goel_mamta2000@yahoo.com

***Abstract*—Anetwork is a system in which two or more than two computer systems are linked together with wires or without wires. Mobile Ad-Hoc networks (MANETs) are autonomous and decentralized networks. MANETs consists of mobile nodes that are free to move in and out of the network. Nodes may be mobile phones, laptops, PCs, Printers, mp3 players, iPods etc. that participate in the network. Any of these nodes can act as a host/router or it can act both at the same time. They can form different topologies depending on their connectivity with each other in the network. These nodes can configure themselves since they have self-configuration ability. They can be deployed into the network at any time as they do not need any infrastructure. Some of the routing protocols have been developed for MANETS, i.e. (Ad Hoc on Demand Distance Vector) AODV, (Dynamic Source Routing) DSR etc. Due to their dynamic topology, no infrastructure and no central management system MANETs are vulnerable to various security attacks. In this paper we have proposed a solution to detect and prevent multiple Black Holes in a network and find a secure way to transfer data from source to destination node.**

***Keywords*— Routing Protocols, mobility, MANET-Mobile Adhoc Networks, AODV-Adhoc On demand Distance Vector, Dynamic Source Routing, Destination Sequence Distance Vector.**

I. INTRODUCTION

In recent years, there have been significant advances in the technology used to build Micro-Electro-Mechanical Systems (MEMS), digital electronics, and wireless communications.This has enabled the development of low-cost, low-power, multi-functionalsmall sensor nodes that can communicate across short distances. There has been a lot of research into routing in wireless sensor networks. Routing in wireless sensor networks is important, as communicationbetween nodes is central to most

applications that use them. 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. Wired Networks are those networks which are connected through the wired connection. The wire is used asmedium of communication for transmitting data from one point of the network to other point of the network. A wireless network is a network in which computer devices communicates with each other without any wire. Computers are connected with each other through the wireless medium. When a computer device wants to communicate with another device, the destination device must lie within the radio range of each other. Systems in the wireless network transmit and receive data using electromagnetic waves. Now days wireless networks are getting more popular because of its simplicity, mobility, and very affordable and cost saving installation.

Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems,In this system mobile nodes that are free in moving in and out in the network. Nodes are thedevices or systems i.e. mobile phone, laptop, personal digital assistance, personal computer and MP3 player d that are participating in the network and are mobile. These nodes can act as router /host or both at the same time. These nodes/hosts/routers can form arbitrary topologies depending on their connectivity with each other in the network. This type of nodes has the ability to configure themselves and because of their self- configuration ability, they can be deployed on priority basis without the need of any

infrastructure. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for developing IP routing protocols. This routing protocols is one of the challenging and interesting research areas. Most of the routing protocols have been developed for MANETS, i.e. OLSR,AODV, DSR etc.

II. ROUTING IN MANETs

Routing is generally the act of moving information from source to destination in a network. Efficiency of the route is measured in various metric like number of hops, security ,traffic etc. The main goal of routing protocols is to maximize network throughput, minimize delay, maximize network lifetime and maximize energy efficiency.In routing, two basic activities are involved: determining optimal routing path and packet transfer through an internetwork.

MANET, routing protocols are categorized into three main categories depending upon the criteria when the source node possesses a route to the destination, as shown in figure 1.

- Table driven/ Proactive
- Demand driven / Reactive
- Hybrid

A. Proactive Protocols:

Proactive strategy attempt to maintain consistent and updated routing information for every pair of network nodes by proactively, propagating, route updates at fixed time intervals. This routing information is usually maintained in tables, these protocols are sometimes referred to as Table-Driven protocols. When a network topology change occurs, updates must be propagated throughout the network to notify the change. Some protocols that are considered as table- driven are: Destination sequenced Distance vector routing (DSDV), Wireless routing protocol (WRP), Fish eye State Routing protocol (FSR), Optimised Link State Routing protocol (OLSR), Cluster Gateway switch routing protocol (CGSR), Topology Dissemination Based on Reverse path forwarding (TBRPF).

B. Reactive Protocols:

Reactive routing protocols for mobile ad hoc networks are referred as "on demand" routing protocols. In a reactive routing protocol, it creates routes only when these routes are needed. When the source node requires a route to a destination, it take initiates a route discovery process within the network. When process is completed once a route is found or all possible route permutations have been examined. After this there is a route maintenance procedure to keep up the valid routes and to remove the invalid routes. Different types of On- Demand protocols are: Ad hoc On Demand Distance Vector (AODV), Dynamic Source routing protocol (DSR), temporally ordered routing algorithm (TORA), Associativity Based routing (ABR).

C. Hybrid Routing Protocols

Hybrid protocols seek to combine the proactive and reactive approaches. The network is differentiating into zones, and use different protocols in two different zones i.e. one of the protocol is used within zone, and the another protocol is used between them. Zone Routing Protocol (ZRP) is the example of Hybrid Routing Protocol. Zone Routing Protocol uses proactive mechanism for route establishment within the nodes neighbourhood, and for communication amongst the nearest nodes, it takes the advantage of reactive protocols and local neighbourhoods are known as zones, and this protocol is named as zone routing protocol. Every zone can have different size and each node may be within multiple overlapping zones. The zone size is given by P (radius of length), where P is number of hops to the perimeter of the zone.

III. SECURITY IN MANETS

Security is much more difficult to maintain in MANETs due to their vulnerability, than wired networks. The use of wireless links render an ad hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and distortion. The MANET vulnerabilities include:

a) Dynamically changing network topology: Mobile nodes join and leave the network arbitrarily, resulting to dynamic change of network topology. This allows a malicious node to join the network without prior detection.

b) Lack of centralized monitoring: There is absence of any centralized infrastructure that prohibits any monitoring mechanism in the network. This makes the classical security solutions based on certification authorities and on-line servers inapplicable. Even the trust relationships among individual nodes also changes, especially when some of the nodes are found to be compromised. Hence, security mechanisms need to be on the dynamic and not static.

c) Cooperative algorithms: MANET routing algorithms require mutual trust between

neighbouring nodes, which violates the principles of network security.

d) The absence of a certification authority.

e) The limited physical protection of each of the nodes: network nodes usually do not reside in physically protected places, such as locked rooms. Hence, they can more easily be captured and fall under the control of an attacker.

f) The intermittent nature of connectivity

g) The vulnerability of the links: messages can be eavesdropped and fake messages can be injected into the network without the difficulty of having physical access to the network components. Eavesdropping might give an attacker access to secret information thus violating confidentiality.

h) Adversary inside the Network: The mobile nodes within the MANET can freely join and leavethe network. All the nodes within network may also behave maliciously. This is hard to detect that the behaviour of the node is malicious. This attack is more dangerous than the external attack. These type of nodes are called compromised nodes.

IV. ATTACKS IN MANETS

Security is the cry of the day. In order to provide secure communication and transmission, it is utmost important to understand different types of attacks and their effects on the MANETs. Black hole attack,Wormhole attack, , impersonation attack ,Sybil attack, , routing table overflow attack,flooding attack, Denial of Service (DoS), selfish node misbehaving, are kind of attacks that a MANET can suffer from. A MANET is open to these kinds of attacks because communication is based between the nodes on the behalf of mutual trust and there is no central point for network management, , vigorously changing topology,no authorization facility and limited resources.

Understanding possible form of attacks is always the first step towards developing good security solutionsfor secure transmission of informationin MANET is important. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber-attacks than wired network there are a number of attacks that affect MANET.

The attacks can be categorized on the basis of the source of the attacks i.e. External or Internal, and on the behaviour of the attack that's Passive or Active attack. This type of classification is important because the attacker can exploit the network either as internal and external or as well as active or passive attack against the network.

1. Internal/ External Attack

External attackers are mainly outside the networks who want to get access to the network and once they get access to the network they start sending fake packets, DOS in order to disrupt the performance of the whole network. This attack is similar, like the attacks that are made against wired network. This type of attacks can be prevented by implementing security measures such as firewall, where the unauthorizedaccess of person to the network can be mitigated.

While in internal attack as its name implies, it is exists in the network internally.But Here, the attacker wants to have normal access to the network as well as participate in the normal activities of the network. Attacker gain access in the network as new node either by compromising a current node in the network or by malicious impersonation and start its malicious behaviour. This type of attacks is called an internal attack because here node itself belongs to the network internally. Internal attacksare more severe to attack because here malicious node present inside the network actively.

2. Active/Passive Attack

In active attack the attacker disrupts the performance of the network,steal crucial information and try to destroy the data during the exchange in the network. Active attacks can be an internal or an external attack. These active attacks are meant to destroy the performance of network in such case the active attack act as internal node in the network. It being an active part of the network it is easy for the node to exploit and hijack any internal node to use it to introduce bogus packets injection or denial of service. These types of attacks bring the attacker in strong position where attacker can modify, replays and fabricate.

the battlefield, and business conferences, there is a need for guaranteed safety of data transfer between two communicating nodes. Thus, secure routing protocols have been recently proposed.

Secure routing protocols are mostly designed to prevent hazards to safety properties, such as:

(i) Identity authentication and non-reputation;
(ii) Availability of resources;
(iii) Integrity; (iv) confidentiality and privacy.

The wireless mobile ad hoc nature ofMANETs brings new security challenges to the network design.As these wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile and ad hoc networks are intrinsically exposed to numerous security attacks.Security in MANET is the most important concern for the basic functionality of network. Availability of network confidentiality, services and integrity of the data can be achieved by assuring that security issues have been met. These MANET often suffer from security attacks because of the its features like changing its topology dynamically, open medium, lack of central monitoring and management, no clear defence and cooperative algorithm mechanism. These factors have changed the battle field situation for the MANET against the security threats.

BLACK HOLE ATTACK:

A Black Hole attack scrambles the route by forging a routing message, and then further either drop the packets or eavesdrops, posing a possible bugs to safety properties. A Black Hole attack forges the sequence number and hop count of a routing message to forcibly acquire the route, and then eavesdrop or drop all the data packets that pass. A malicious node impersonates a destination node by sending a spoofed RREP to a source node that initiated a route discovery.

A Black Hole node has two properties: (1) the node exploits the ad hoc routing protocol and advertises itself as having a valid route to a destination, even though the route is spurious, with the intention of intercepting packets, and (2) the node consumes the intercepted packets.

Source node broadcasts route request packet (RREQ) to find a route to destination node; with the normal intermediate nodes receiving and continuously broadcasting the RREQ, except the Black Hole node. Everything works well if the RREP from a normal node reaches the source node first. The attacker node sends a route reply packet (RREP) to the source node. But a route reply from attacker node reaches to source node before any other intermediate node. This makes the source node to conclude that the route discovery process is complete, ignoring all other RREPs and beginning to send data packets. The Black Hole node would directly send a route reply (RREP) to the source node S, with an extremely large sequence number. The malicious node always sends RREP as soon as it receives RREQ without performing standard AODV operations, while keeping the Destination Sequence number very high. Since AODV considers RREP having higher value of destination sequence number to be fresh, the RREP sent by the malicious node is treated fresh. Thus, malicious nodes succeed in injecting Black Hole attacks.

5. COMPARISON WITH EXISTED METHOD Researchers have proposed various techniques to prevent black hole attack in mobile ad-hoc networks. Antony Devassy, K.Jayanthi[2] 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.

V. 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 ofthe RREQ packet from source to the nodes
- Destination nodes sendRREP 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.

VI. EXPERIMENTAL RESULTS

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 1.

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.

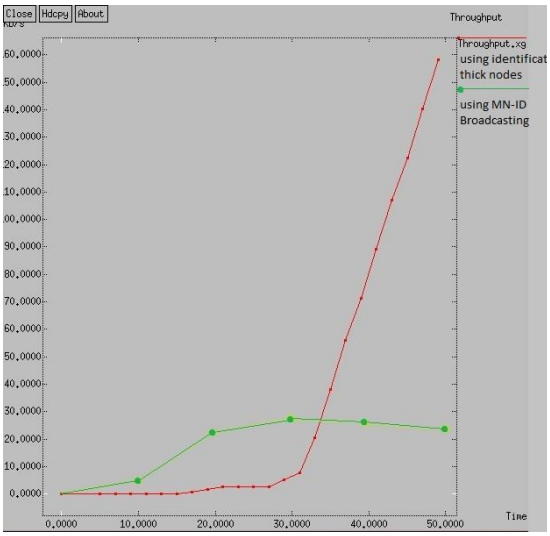

Fig 1 THROUGHPUT VERSUS TIME

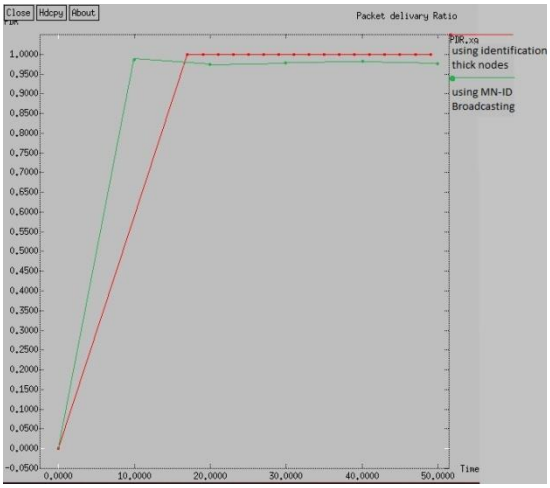

Fig. 2 PACKET DELIVERY RATIO VERSUS TIME

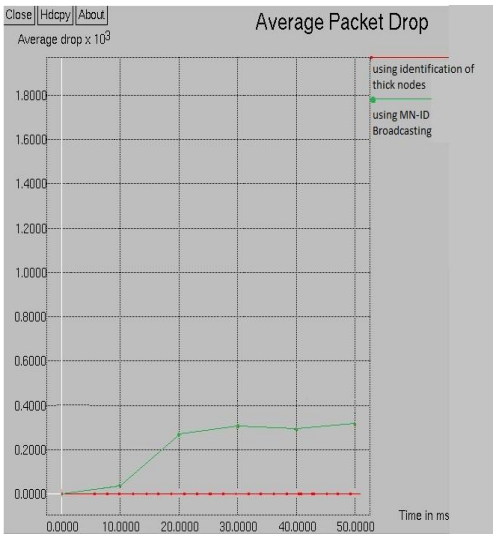

Fig. 3 PACKET DROP VERSUS TIME

CONCLUSION AND FUTURE SCOPE

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.

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 honour 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.

REFERENCES

[1] Swati Jain, Naveen Hemrajani, "*Detection and Mitigation Techniques of Black Hole Attack in MANET: An Overview*", International Journal of Science and Research, 2(5), 70 - 73. (2013)

[2] Antony Devassy1, K. Jayanthi, *"Prevention of Black Hole attacks in Mobile Ad-hoc Networks using MN-ID Broadcasting*", International Journal of Modern Engineering Research (IJMER) www.ijmer.com Vol.2, Issue.3, May-June 2012 pp-1017-1021 ISSN: 2249-6645

[3] Kinagalapavani, Dr. DamodaramAvula,"*Injection of attacks in MANET*", IOSR Journal of Computer Engineering (IOSRJCE), Vol 4, Issue 3, Sep-Oct. 2012.

[4] Sowmya K.S, Rakesh T. and Deepthi P Hudedagaddi, "*Detection and Prevention of Blackhole Attack in MANET Using ACO",* International Journal of Computer Science and Network Security, VOL.12 No.5, May 2012

[5] Rajni Tripathi1 and ShraddhaTripathi, "*Preventive Aspect Of Black Hole Attack In Mobile Ad Hoc Network*", International Journal of Advances in Engineering & Technology, July 2012.ISSN: 2231-1963

[6] Rajib Das, Dr. BipulSyamPurkayastha, Dr. Prodipto Das, "*Security Measures for Black Hole Attack in MANET: An Approach*",International Journal of Engineering Science and Technology (IJEST), vol.3 No.4 Apr 2011.

[7] Saurabh Gupta, SubratKar, S Dharmaraja, "*BAAP: Blackhole Attack Avoidance Protocol forWireless Network*", International Conference on Computer & Communication Technology (ICCCT)-2011

[8] Nital Mistry, Devesh C Jinwala, MukeshZaveri, "*Improving AODV Protocol against BlackholeAttacks*", International MultiConference of Engineers And Computer Scientists 2010, Vol 2,

[9] N. Shanti, Lganesan and K. Ramar, "*Study of Different Attacks On Multicast Hoc Network*", International Journal of Engineering Science and Technology Vol. 2, 2010.

[10] Pradip M. Jawandhiya, Mangesh M. Ghonge, Dr. M.S.Ali, Prof. J.S.Deshpande, "*A survey of Mobile Ad-Hoc Network Attacks"*, Interational journal of Engineering Science and Technology, vol 2, 2010.

[11] G.Vijaya Kumar, Y.VasudevaReddyr, Dr.M.Nagendra, "*Current Research Work on Routing Protocols for MANET: A Literature Survey*", International Journal on Computer Science and EngineeringVol. 02, No. 03, 2010, 706-713

[12] NishantSitapara, Prof. Sandeep B. Vanjale, "*Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks*", International Conference" ICETE-201O" on Emerging trends in engineering on 21st Feb 2010

[13] SemihDokurer, Y.M.Erten, Can ErkinAcar, "*Performance analysis of ad-hoc networks under Black Hole Attacks*", Institute of Electrical and Electronics Engineer (IEEE), 2007.

[14] Getudegu, Tegbaryigzaw, "*Research Methodology*", The Ethopia ministry of Health and The Ethopia Ministry of Education, 2006.

[15] William Stallings, "*Cryptography and Network Security Principles and Practices*", Fourth Edition, Prentice Hall ISBN-10: 0-13-187316-4, November 16, 2005.

