# Prevention of Black Hole Attacks in MANETs

Ashutosh Sharma, Lokesh Tharani

**Abstract—** A network is a structure in which more than two (or Two) computer systems are connected together with wires or without wires. Mobile Ad-Hoc networks (MANETs) are independent and decentralized networks. MANETs consists of mobile nodes that are free to move in and out of the network. Any of these nodes can act as a host/router or it can act both at the same time. They can be deployed into the network at any time as they do not need any communications. Many routing protocols have been structured for MANETS, i.e. (Ad Hoc on Demand Distance Vector) AODV, (Dynamic Source Routing) DSR etc. In this paper we have projected a resolution to detect and prevent multiple Black Holes in a network and find a protected way to transfer data from source to destination node.

**Index Terms**— Routing Protocols, mobility, Black Hole, Worm Hole, Active attack, Passive attack, MANET.

## 1 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-functional small sensor nodes that can communicate across short distances. Routing in wireless sensor networks is important, as communication between 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**. Recently wireless networks are getting more and more popular because of its mobility, simplicity and very affordable and cost saving installation.

## 2 ROUTING IN MANETS

Routing is generally the act of moving information from source to destination in a network. Effectiveness of the route is considered in various metric like number of hops, traffic, security etc**.** The main motive of routing protocols is to diminish delay, make best use of network throughput, capitalize on network lifetime and maximize energy efficiency.

MANET routing protocols are characterized into three main categories depending upon the criteria when the source node possesses a route to the destination.

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

### 2.1 Proactive Protocols

Proactive strategy endeavours to maintain consistent and updated routing information for every pair of network nodes by propagating, proactively, route updates at fixed time intervals. These protocols are sometimes referred to as Table-Driven protocols. When a network topology change occurs, respective updates must be propagated throughout the network to notify the change. Some examples of protocols  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).

### 2.2 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. After that 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).

### 2.3 Hybrid Routing Protocols

Hybrid protocols seek to merge the both approaches. Zone Routing Protocol (ZRP) is the example of Hybrid Routing Protocol. ZRP uses proactive mechanism for route establishment within the nodes neighbourhood, and for communication amongst the neighbourhood.

Security is much more complicated 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:

- *Ashutosh Sharma, Research Scholar, Rajasthan Technical University, Kota, India. E-mail: sharmaashu.hcl@gmail.com*
- *Dr. Lokesh Tharani is Associate Professor, Rajasthan Technical University, Kota, India.*

**a)** Dynamically changing network topology:
**b)** Lack of centralized monitoring:
**c)** Cooperative algorithms:.
**d)** The absence of a certification authority.
**e)** The limited physical protection of each of the nodes: The intermittent nature of connectivity
**f)** The vulnerability of the links: Adversary inside the Network:

.

## 4 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.

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 bogus packets, denial of service in order to disrupt the performance of the whole network.

2. Active/Passive Attack

In active attack the attacker disrupts the performance of the network, steal important information and try to destroy the data during the exchange in the network.

Attackers in passive attacks do not disrupt the normal operations of the network.

## 5 PROBLEM DEFINITION

The wireless mobile ad hoc nature of MANETs fetches new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous security attacks. MANET often experience from compromised security because of the its features which are more prone to various threats and attacks.

BLACK HOLE ATTACK:

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.

On demand routing protocol scheme (AODV and DSR) when a node wants to send any packet to another node first it requires path or route towards the destination. The node sends a RREQ to all its neighbouring nodes for getting information about the destination. If any node itself is the destination or has fresh route information then it replies to source node with RREP [14].Route is established between source and destination when RREP reaches at source node. In black hole attack intruder either pretends to be the destination or intruder publicize it as it has the fresh route.

By repeating this process continuously it becomes part of various routes in the network and starts dropping packets instead of processing them or forwarding them. The way of capturing routes may vary in different routing protocols.

## 6 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

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.

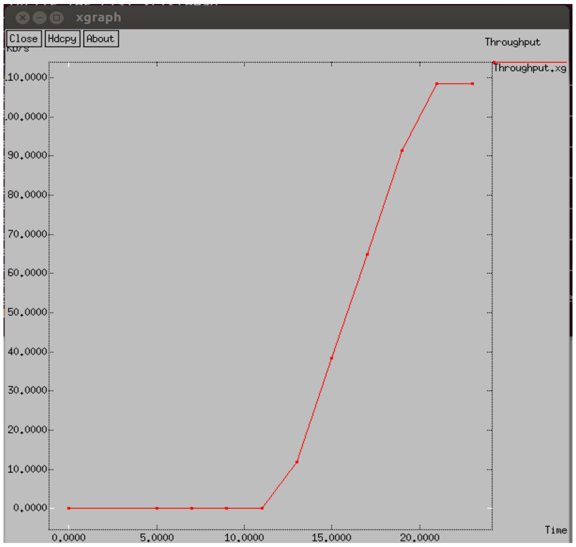

Fig. 1. Throughput versus Time

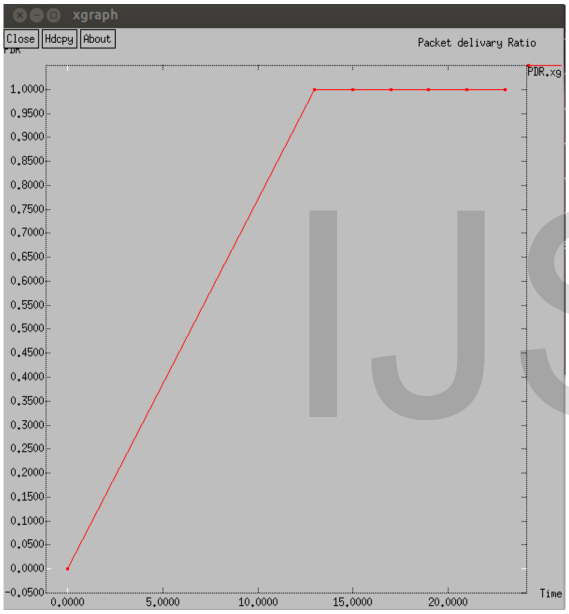

Fig. 2. Packet delivery Ratio versus Time

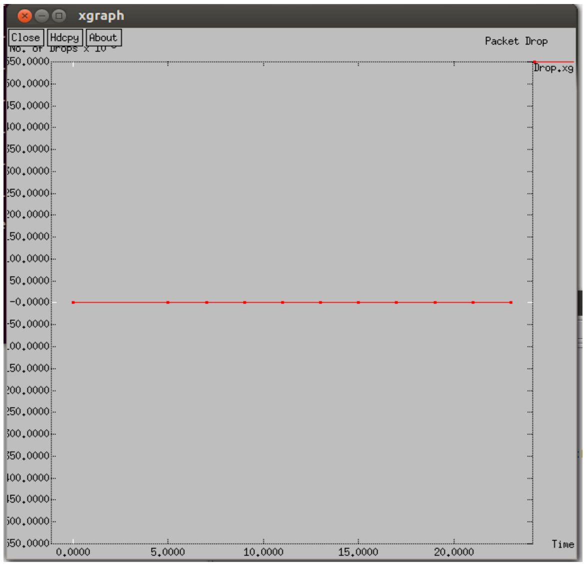

Fig. 3. Packet Drop versus Time

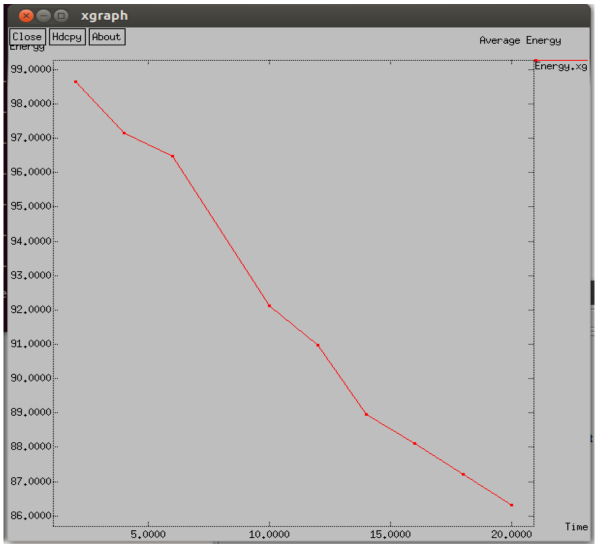

Fig. 4. Average Energy Versus Time

## 7 CONCLUSION AND FUTURE SCOPE

Black Hole Attack is a main security threat that affects the performance of the AODV routing protocol. Its detection is the main matter of concern.

In this paper, schemes and techniques developed to detect and prevent major routing attacks for different protocols are investigated. Since this field has always been in vogue for researchers, various researches are going on to increase purview of scheme. Because of wide use of MANETs around the world, they must be more secured and robust, but on the contrary they are more vulnerable to attacks. This condition gives a huge potential to researchers to develop prevention schemes which cover maximum number of threats and attacks and make nodes energy efficient also.

## 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] Kinagala pavani, Dr. Damodaram Avula,"*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 Shraddha Tripathi, *"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. Bipul Syam Purkayastha, 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, Subrat Kar, S Dharmaraja, "*BAAP: Blackhole Attack Avoidance Protocol for Wireless Network*", International Conference on Computer & Communication Technology (ICCCT)-2011

[8] Nital Mistry, Devesh C Jinwala, Mukesh Zaveri, "*Improving AODV Protocol against Blackhole Attacks*", 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.Vasudeva Reddyr, Dr.M.Nagendra, "*Current Research Work on Routing Protocols for MANET: A Literature Survey*", International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 706-713

[12] Nishant Sitapara, 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] Semih Dokurer, Y.M.Erten, Can Erkin Acar, "*Performance analysis of ad-hoc networks under Black Hole Attacks*", Institute of Electrical and Electronics Engineer (IEEE), 2007.

[14] Getu degu, Tegbar yigzaw, "*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.