# Securing Mobile Ad Hoc Networks Against Packet Dropping Attack

**Sushant R. Bahadure**

Roll. 213CS2158

*under the guidance of*

**Prof. Pabitra Mohan Khilar**


**Department of Computer Science and Engineering**

**National Institute of Technology Rourkela**

**Rourkela – 769 008, India**

# Securing Mobile ad Hoc Networks against Packet Dropping Attack

*Dissertation submitted in*

*June 2015*

*to the department of*

***Computer Science and Engineering***

*of*

***National Institute of Technology Rourkela***

*in partial fulfillment of the requirements*

*for the degree of*

***Master of Technology***

*by*

***Sushant R. Bahadure***

*(Roll. 213CS2158)*

*under the supervision of*

***Prof. Pabitra Mohan Khilar***


**Department of Computer Science and Engineering**

**National Institute of Technology Rourkela**

**Rourkela – 769 008, India**

Computer Science and Engineering
**National Institute of Technology Rourkela**
Rourkela-769 008, India. www.nitrkl.ac.in

**Dr. Pabitra Mohan Khilar**
Professor

June 1, 2015

# Certificate

This is to certify that the work in the thesis entitled *Securing Packet Dropping Attack in Mobile ad Hoc Networks* by *Sushant R. Bahadure*, bearing roll number 213CS2158, is a record of an original research work carried out by him under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of *Master of Technology* in *Computer Science and Engineering Department*. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

***Pabitra Mohan Khilar***

# Acknowledgment

First of all, I would like to express my deep sense of respect and gratitude towards my supervisor Prof. Pabitra Mohan Khilar, who has been the guiding force behind this work. I want to thank him for introducing me to the field of Mobile Ad Hoc Network and giving me the opportunity to work under him. His undivided faith in this topic and ability to bring out the best of analytical and practical skills in people has been invaluable in tough periods. Without his invaluable advice and assistance it would not have been possible for me to complete this thesis. I am greatly indebted to him for his constant encouragement and invaluable advice in every aspect of my academic life. I consider it my good fortune to have got an opportunity to work with such a wonderful person.

I thank our H.O.D. Prof. S. K. Rath for their constant support in my thesis work. They have been great sources of inspiration to me and I thank them from the bottom of my heart.

I would also like to thank all faculty members, PhD scholars, my seniors and juniors and all colleagues to provide me their regular suggestions and encouragements during the whole work.

At last but not the least I am in debt to my family to support me regularly during my hard times.

I wish to thank all faculty members and secretarial staff of the CSE Department for their sympathetic cooperation.

***Sushant R. Bahadure***

# Abstract

Need of infrastructure less, self operating, self configuring, communication networks have resulted in the formation of mobile ad hoc networks (MANET). MANET has proved very useful over traditional networks in disastrous conditions. In MANET all mobile devices work cooperatively for route discovery and data transmission. Due to its broadcast nature of transmission, and cooperative model of working, routing the traffic is a tedious task in MANET. Routing protocols are constantly targeted by attackers to cause damage to network. Routing protocols in MANET needs to be robust against various security threats. Ad hoc on-demand distance vector routing (AODV) protocol is widely used and studied in the area of mobile ad hoc networks.

In this work, we present a secure AODV protocol to mitigate Black Hole Attack. In black hole attack a node maliciously diverts the data to route through it, and then drops the data packets, which results in lower packet delivery ratio. For this we have introduced a decision module in routing algorithm, which scans the RREP messages coming from a node before forwarding them towards the sender. Decision module has been build to exploit the black hole attack model. We check for the freshness and the path length mentioned in the reply message. Depending upon these values we decide whether to forward this reply or not. Thus eliminating the false replies. We simulated this proposed scheme to measure its effectiveness using *NS-3*. The results shows that our proposed algorithm shows better performance in terms of higher packet delivery ratio.



***Keywords*:** MANET, Routing Protocol, Security, Black Hole Attack

# Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

**Mobile ad hoc Network**

**Motivation**

**Research Objectives**

# Chapter 1

# Introduction

## 1.1 Introduction

Wireless communication has many pros over the wired networks. Mobile Ad-hoc Network (MANET) has gained lot of popularity over wired networks due to their unique characteristics. The word ad hoc has Latin roots and means on the fly. MANET is a particular network for a particular application. MANET requires no fixed infrastructure for its working. Network devices (nodes) are mobile and communicate over a wireless medium. Also, there is no central controlling authority that manages the network. The participating nodes do network management and routing of data. The participating nodes of the network have limited resources. This difference from the wired network, MANET faces various challenges such as battery constraints, dynamic topology, and bandwidth constraints [1].

Mobile ad hoc network faces various security challenges due to its nature. A lot of vulnerabilities arise due to no central authority and wireless medium of transmission. Route establishment and data transmission are two important functions of routing algorithm in MANET. These two phases need to be secured from attackers. The routing protocol must be so robust that it can withstand various attacks. Hence, reliable communication implies secure routing algorithm.

In this research work, we consider securing route management phase of the routing protocol to mitigate a particular type of attack called as Black Hole Attack [2]. In this attack a malicious node forces to route the data traffic through it by not following the actual algorithm and then drops the data packets without forwarding them to the destination node. Thisattackwill result in denial of service to the destination node. Before transmitting the data, we make sure that data packets wont be routed via a malicious node. Our proposed algorithm has a better packet delivery ratio when under attack than the original routing algorithm.

## 1.2 Motivation

Security and privacy are very vital aspects of any communication. MANET has many advantages over the wired network that makes it highly useful in many fields where wired network cannot be operated. The network performance is degraded if a malicious node is present in the network. A malicious node can exploit the vulnerabilities in the MANET in number of ways. Routing protocol in MANET is another important part that plays very crucial role in data delivery. A node can misbehave and violate the routing rules causing damage to data transmission.

Tampering with routing protocol can lead to many malicious behaviors, such as modifying routes, dropping a packet, forging of routing control messages. Thats why intruder targets the routing protocols to attack MANET. By attacking routing protocol, alone MANET can be attacked in many ways; such as Hello Flooding Attack, wormhole attack, Location-Disclosure, Rushing Attacks, Invisible Node, and Routing Table Attack. Black Hole attack is another attack that disrupts networks data traffic flow. So a mobile ad hoc network needs a secure routing protocol to have reliable data flow from source to destination.

## 1.3 Research Objectives

The objectives that we framed to work in the area of mobile ad hoc networks are as follows:

1. To design secure routing protocol that will identify the black hole node during the path setup phase, and hence avoid that path for transmission of data.

2. To analyze the performance of the proposed algorithm using the NS-3 simulator and compare it with the existing algorithm.

## 1.4 Our Contribution

In this work, we launched a black hole attack, on the mobile ad hoc network and evaluated its effect on the performance of the network. We modeled the new approach to avoid the packet dropping scenario in the MANET. This new approach considers 'hop count' as also a metric to identify the forged reply messages.

## 1.5 Thesis Organization

In this chapter, we have discussed the motivation for the need for secure routing protocol that can safeguard against the packet dropping attack in MANET. Objectives of our research are outlined in a nutshell. The organization of the rest of the thesis and a brief overview of the chapters in this thesis are given below.

**Chapter 2:** We have briefly described the basic theory about the MANET such as security issues, routing protocols, and also the works done so far in the area of packet dropping attack. **Chapter 3:** in this chapter we have described our proposed routing protocol to mitigate the packet dropping behavior in the MANET. **Chapter 4:** in this chapter we have described the evaluation of proposed algorithm using the NS-3 simulator. **Chapter 5:** We have concluded our work in this chapter.

# Chapter 2

# Background

**MANET Applications**

**MANET Challenges**

**Security Issues**

**Related Work**

# Chapter 2

# Background

## 2.1 Introduction

People must be able to communicate if even they are mobile. With the advancement in communication technology devices have become smaller yet more powerful and cheaper. Thus, users can exchange information with their devices while traveling through the large area. To maintain such communications over a large area, there is a need for some fixed infrastructure like access points, transceivers. Mobile devices connect this infrastructure to retain their connection while roaming. These supports are associated with the cost of installments, cost of maintenance. Also, they must withstand the rough weather, power constraints. Due to some geographic challenges, such mobile communication support is not available everywhere. Also because of high cost, low usage rate, poor performance or other commercial reasons access points cant be set up in some locations. Such cases may arise during conferences; in situations such as natural calamities, military operations carried out in remote and inaccessible areas. Ad hoc network enables users to communicate without taking support of fixed infrastructure. Here we briefly explain the mobile ad hoc networks.

Chapter Organization: Sub-section 2.2 describes the brief about Mobile Ad Hoc Network, its applications, characteristics, complexity and design of MANET,

Section 2.3 describes the different routing protocols that exist in MANET, Section 2.4 describes the security issues that arise in the MANET. This section also describes the security of routing protocols. Section 2.5 describes the related work that is been done in the secure routing protocol area specifically about mitigating the black hole attack. 2.6 describe the summary of the chapter.

## 2.2 Applications & Challenges

A typical mobile ad hoc network comprises of mobile communicating devices that can roam in and out of network at any time. They transmit and receive messages over the wireless medium, and require no fixed access point or infrastructure. Also, there is no central authority to monitor and control the network. The topology of the network can change rapidly in unpredictable manner because, the nodes can move in a random fashion in a random direction at any time. A MANET can work on own, or it can be connected to fix wired network. The nodes in the ad hoc network handle network management and packet forwarding, i.e. the nodes also work as routers. There is no special authority to facilitate the communication between nodes, but instead nodes work in a cooperative manner to communicate with each other. If nodes fall within each others range, then they communicate directly using wireless links. If nodes are far from each other, then source relays packet through intermediate nodes to destination. Here intermediate nodes act as routers.Hence, each node in the network is a Host (sends and receives data) and a Router (forwards the packets meant for other nodes.). Hence, such networks sometimes call as multi-hop wireless ad hoc networks.

A mobile ad hoc network is shown in Figure 2.1. This network consists of heterogeneous devices ranging from phones to laptops, personal digital assistant, computing devices and so on. A neighboring node is the one that falls within the transmission range of the sending node. Device A can directly communicate to machine B and E whereas it routes packets through C and B to communicate with

node D.

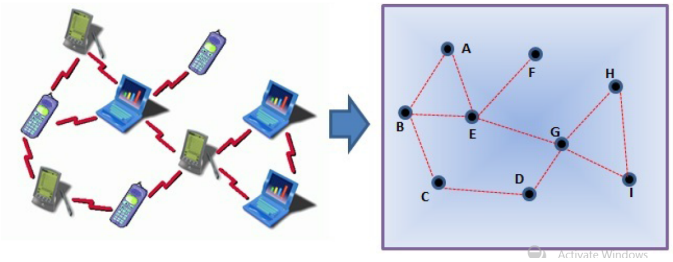


Figure 2.1: Mobile Ad hoc Network

### 2.2.1 MANET Applications

MANET is useful in many situations and hence has found many applications [3] [4]. We name some applications bellow.

- Military Applications
  - Battlefields
  - Communications in Hilly area.
- Emergency Applications
  - Search missions
  - Rescue and Relief Operations
  - Natural Calamities
  - Medical camps during disaster management
- Academics
  - Virtual Classrooms
  - Meetings or conferences
  - Campus Settings

- Personal
  - Conferences/ Meetings
  - Home/ office wireless networking
- Commercial Applications
  - Visitors network
  - Stadiums, Malls, Trade Fairs
  - Electronic Payments
  - Mobile Offices
  - Road guidance
  - Inter vehicle networks
- Sensor Networks
- Coverage Extension

### 2.2.2 Challenges

The features such as no infrastructure need, no central regulatory authority, on the go setup has imposed few challenges compared to the wired network. Some problems arise due to the wireless nature of communication while some new issues arose due to the ad hoc nature. Mobility of nodes imposes new challenges to routing algorithms. Also, limited resources add up more challenges to the mobile ad hoc networks. Few characteristics and notable challenges are as follows [5] [6]

- **Challenges due to Wireless Medium:** Broadcast nature of transmission imposes limitations on communication. Nodes have limited transmission ranges. Also over shared medium bandwidth for communication is limited. A lot of packets are lost in transmission. Link capacities vary over places. The absence of fixed boundaries in wireless medium imposes some more challenges.

- **Limited Resources:** mobile nodes are smaller in size and lighter in weight and thus are supplied with limited battery supplies. Lesser battery backup can prevent nodes from doing computation intensive tasks. An attacker may target to disconnect the batteries of nodes thus partitioning the network. If mobile hosts have limited computational power, than computational intensive cryptographic solutions might become difficult to implement.
- **Mobility Challenges:** Mobile hosts are free to move anywhere in the network with varying speeds. Thus, network topology changes arbitrarily and frequently. This leads to network partitions, packet loss, link failures.

## 2.3 Routing Protocols

Routing Protocols in Ad hoc networks handle communication between nodes. They maintain information that helps nodes to find routes to required destinations. Routing algorithms set up the path, and also routes the packets on that path from source to destination. It also takes into account the error in communication that might arise. Hence, the effectiveness of communication depends upon the efficiency of the routing algorithm. Various routing algorithms are available in theory. According to the mode of operation, these protocols are classified in two broad categories [7].

1. Proactive Routing Protocols
2. Reactive Routing Protocols

Proactive Routing Protocol: A Routing Table data structure is maintained at every node. All existing paths to remaining destination nodes are kept in that table. The table is updated with latest information. Any change in the network topology is reflected in the routing table in no time. Hence, a node has route information to every other node in all instance of time. Examples are

Reactive Routing Protocol: In contrast to proactive routing protocols, here the path is setup from source to destination, only when it is needed. The path is maintained till the data is transmitted. Either source node asks to terminate the path, or the path information is deleted after a time limit expires. Examples are

Ad hoc on-demand distance vector routing protocol: This is a reactive routing protocol. When a source node needs to send information to a far destination node, and it does not have the path information it broadcasts Route Request (RREQ) message to its neighbors. An intermediate node having fresh enough path to destination replies with a Route Reply (RREP) message on the reverse path to the source node. If the intermediate node does not have the route information, it rebroadcast the RREQ message to its neighbors. When the destination node receives such request, it send a unicast reply message back to the source node. Forward path and reverse path are setups while transmitting these control messages, and this route is then used for data transmission [8]. The freshness of path is maintained by assigning sequence number to each node. Internet draft explains the working, message types, header formats in detail.

## 2.4 Security Issues

Due to the lack of central authority and resource constraints MANET is much more vulnerable to various attacks. They can be classified by the location of the attacker or by the mode of operation. They can be classified as internal attack or external attack, depending on the attacker's location. Also, attacks can be grouped as Active or Passive, depending upon the damage it causes to the network. [9]

### 2.4.1 Passive Attack

When an intruder launches the passive attack, the network continues to operate normally as there is no alteration being made to the network traffic. The attacker silently listens to the network traffic, without tampering it. The security service

of confidentiality is violated here. As there are no visible changes in the network traffic, this kind of attacks is very difficult to detect. Brief information about various passive attacks is as follows.

- **Traffic Analysis:** An intruder captures and analyze the network traffic to know the destination information, source information.
- **Eavesdropping:** The primary objective to launch this attack is to gain some secret information that can be later used to launch another attack. The information stolen can be passwords, private keys, locations of the nodes, etc.

### 2.4.2 Active Attack

This type of attack disrupts the normal behavior of the network. The attacker listens to the traffic as well as does the modification to it. An attacker may destroy the packets or alter some information in it. brief information about active attacks is as follows.

- **Network Jamming:** It is a type of denial of service attack. The attacker tries to block the legitimate communication. It does so by not allowing source node to send out data packets. An attacker can also prevent a receiver from receiving the traffic from the network.
- **Fabrication:** A malicious node creates its forged packets and sends it out to the network. In such attack, the malicious node does not modify or interrupt the original packets in the network. The forged packets consume the bandwidth and other network resources.
- **Black Hole Attack:** This attack has two stages. Firstly, the malicious node advertises false route information and thus forces to route the data traffic to pass through it. And then this malicious node drops the received data packets without forwarding them to the destination node.

- **Byzantine:** In this attack a single malicious node or a set of nodes perform malicious activities to degrade the network performance. These activities may be selective packet dropping, routing packets via a non-optimal route, creating routing loops. This attack is a combination of various malicious activities performed together.

- **Wormhole Attack:** An attacking node capture and stores the packets in one place in the network and transmits them to another location in the network. The attack causes more damage when control packets are tunneled. The wormhole refers to this tunnel between the malicious nodes.

- **Repudiation:** The attacking node denies the responsibility of participation in part or entire communication.

- **Denial of Service attack:** An attacker floods the network with garbage traffic in gigantic amount, which causes unnecessary resource consumption. This traffic consumes network bandwidth and thus stopping the legitimate traffic to flow into the network. The actual users can not avail the services of the network.

- **Sybil attack:** In this attack, a malicious node impersonates to be fake nodes thus giving an impression that there are several malicious nodes in the network.

- **Neighbor Attack:** Attacker modifies the packet content so that the receiving node assumes that the attacker is also a neighbor node. This causes disruption in the route. The attacker does so by replacing its ID with the existing identifier in the packet and then it forwards this packet to next node. Thus, two nodes mark each other as neighbors.

- **Modification Attack:** attacker modifies the routing packets and forward them into the network; thus packet's integrity is at risk.

- **Jellyfish Attack:** This attack is similar to packet dropping attack. The attacking node put itself into the path by forging the routing control packets. And then before forwarding the packets the attacker delays the forwarding for some time, thus increasing the total delay.

- **Gray Hole Attack:** This attack is a slight variant of black hole attack. The first part of the attack is same as black hole attack. Instead of dropping all the data packets the node selectively drops the packets, thus making it harder to detect.

### 2.4.3 Attacks on Routing Protocols

Any network needs its communication to be secure and safe. Maintaining the same security and safety while communication in MANET is a challenging task. To communicate securely, route discovery mechanism must also be protected from attackers along with the data. By tampering with the routing algorithm, an attacker can launch many attacks on the network. There can be many attacks found in the literature on the routing protocols, some of them are as follows.

- **Sleep Deprivation:** The methodology for this attack is to keep other nodes busy with the routing activity to drain their battery power. An attacker frequently sends route requests for some destination node to all its neighbors. The neighboring nodes keep on replying to those messages and thus losing their resources.

- **Flooding Attack:** in this attack, attacker node floods the network with false requests messages, hello messages to clog the network bandwidth, resulting in DoS attack.

- **Routing Table Flooding:** The attacker node frequently keep sending route information to its neighbors, thus forcing them to continually update their routing tables.

- **Black Hole & Wormhole Attack :** As explained previously, these two attacks are the result of the vulnerability of the routing protocols. A malicious node exploits the routing protocol mechanism to launch these attacks.

In this research work, we will be focusing more on the packet dropping attack i.e. Black Hole attack. We further assume that routing protocol used in the network is AODV.

## 2.5 Related Work

Routing protocols in MANET are a little bit complicated than the traditional one. The complexity arises due to dynamic nature of topology, mobility of the nodes and lack of central authority. Also, a routing protocol should withstand again some security threats to avail the secure communication. The mobility of nodes may cause more link failures.

Many researchers have designed routing protocols to mitigate the packet dropping scenario in the ad hoc networks. Kishor Jyoti Sarma et. al. [10] have presented a survey of various black hole attack detection techniques.

Abderrahmane Baadache et. al. [2] have suggested an approach that uses acknowledgments to authenticate and to correctly forward packets on the path. In this method, each packet receiving node sends a reply to the sender node to mark the successful reception of the message. The communication is authenticated using hash values. This approach is very computation intensive. Each node on the path has to recompute the hash value and check. Also, there is communication overhead due to lack being sent by each node on the route.

Anuj Rai et. al. [7] have proposed a novel way of detecting a black hole node in the network by using Trap RREQ messages. The method involves sending a trap route request message, before sending an actual route request. Sender's of all the reply messages are blacklisted as malicious nodes. This approach introduces a significant amount of delay, and it doesn't address the co-operative black hole attack.

Nabarun Chatterjee [11] et. al. suggested a method involving encryption to avoid black hole node during the path setup phase. Sender node sends some plain text to the destination node with the route request message, and the destination node sends the encrypted text with the reply message. This method allows only destination node to respond to route request; thus this method is not scalable.

S.Sankara et. al. [12] have used the hash-based technique to avoid black hole attack. Each node has a unique Id that it uses while sending back the reply. The response message is hashed, and the hash value is saved in the message to ensure that reply reached tamper free to the source node. Source node collects all the response messages for a period, and the then correct route is identified.

Anand Aware et. al. [13] proposed to discard the first reply to reach sender node, and find the second optimal reply message to carry out the data transmission. This method fails if the network size is large.

Debarati Roy Choudhury et. al. [14] have given an approach that prevents any alteration of the normal behavior of the AODV protocol. The source node maintains two tables, one to store the received replies and other to save the malicious node's information.

Satoshi Kurosawa et. al. [15] has given another approach to avoid black hole attack. In this approach, a threshold value of the valid sequence number is calculated using feature vector. The mean value for the feature vector is calculated at each fixed time interval

## 2.6 Summary

We have discussed mobile ad hoc networks briefly in this chapter. We have also seen various security issues pertaining the MANET. Various techniques have been proposed to mitigate the black hole attack in the mobile ad hoc networks. We have discussed some of them in this chapter. In the next chapter, we describe our approach to secure against the black hole attack.

# Chapter 3

# Secure Routing Protocol

**Attack Model**

**Proposed Model**

**Analysis**

**Summary**

# Chapter 3

# Secure Routing Protocol

## 3.1 Introduction

Secure communication in any network is the an essential thing. The routing protocol needs to be strong enough to sustain various attacks. One such attack is Blackhole attack. This attack reduces the packet delivery ratio of the network. Here we describe the proposed mechanism to safeguard the network against the packet dropping attack. Our approach is to identify the forged RREP messages sent by the malicious node during the path setup phase. By identifying these fake replies, we avoid the path formation through the malicious node, and hence data is not sent to the attacking node. Thus, we avoid the packet dropping scenario at the first place. We first explain the attack model in detail, then the assumptions and the network model. Then we describe the working of our proposed scheme.

## 3.2 Attack Model

This section explains how the black hole attack or packet dropping attack is carried out. For a simpler explanation, we assume that the network is running AODV routing protocol. A malicious node performs the attack by just not following the actual protocol. We first explain the path discovery mechanism in AODV protocol,

and then how a malicious node exploits this protocol to launch the attack.

### 3.2.1 Path Discovery, Control Messages.

When a source node wants to send some data to a destination node, it checks whether it has an existing route to the destination. When source node does not have a route, it starts the path discovery mechanism within the routing protocol.Source node broadcasts the RREQ message to all its neighbours asking for the path to a specified destination node. Every request is unique and is identified by request ID


Figure 3.1: Source Node

and sequence number pair. Sequence number depicts the freshness of the information contained in the message. Also, request message holds the addresses of the originator and destination node. When the RREQ is received, a reverse path is created towards the sender of the message.

The request is transmitted hop by hop throughout the network of intermediate nodes. An intermediate node may or may not have the path information to the destination node. Hence if the intermediate node has the fresh path information, then that node generates a Route Reply (RREP) message and sends that reply to the next hop on the reverse path. It also sends a gratuitous reply to the destination node on the path that it already has. If there is no information about the destination node in the routing table of intermediate node, then it simply rebroadcasts the RREQ message to its neighbours and then waits for the reply to arrive.

When the destination node receives the route request, it creates its reply message and sends it back to the source node. The reply message contains its fresh sequence

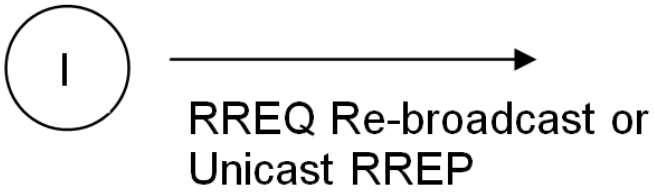


Figure 3.2: Intermediate Node

number, and the hop count is set to zero. This reply message is sent to the reverse path hop by hop. Each intermediate node on the reverse path increment the hop count by one and then forwards it to the next hop.

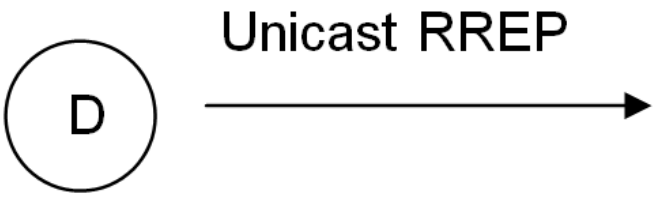


Figure 3.3: Destination Node

### 3.2.2 Malicious Nodes Behaviour

The malicious node doesnt follow the actual protocol. When it receives the legitimate RREQ message requesting the route to a destination, it just drops the request message without forwarding it. Then it generates a false reply message and sends it back to the node on the previous hop. This false response conveys that the path, the malicious node has the route to the destination. The path information is very fresh, and the path is shortest from the malicious node. Malicious node put a very high sequence number in the destination sequence number field and put the hop count as one. The high sequence number means that the path information will be fresh than information in any other reply messages, and also the path is the shortest. The


Figure 3.4: Malicious Node

source nodes send data on the shortest and most recent path; hence it routes the data packets to pass through the malicious node. The malicious node upon receiving the data packets just drops the packets without forwarding them. Thus, it affects the packet delivery ratio.

## 3.3 Proposed Routing Protocol

### 3.3.1 Assumptions & Network Model

The network consists of devices, which are of similar type and can communicate over a wireless medium. We term each device as a network node. All the nodes will be identified using a unique ID. Each node in the network is free to leave the network at any time also; new nodes can join the network. Any node can malfunction at any point of time. Each node can be mobile at any time. The node can decide to move or halt at any location freely. There is no time constraint on the timing of movement or being stationary. Nodes communicate peer-to-peer over the wireless medium. The communication channel is multi-hop, error-prone and shared. In our network model server, node will be the receiver and the client node will send the data to the server node.

We assume that nodes operate in non-promiscuous mode. This will save the energy consumption and extra computational overhead. We also assume that any node having the path information can send the reply message to the source node. This will reduce the end to end delay up to some extent. The client node is assumed to have known the address of the server node. We assume that source and destination

node is different from the malicious node. If there is more than one malicious node in the network, then we assume that both are unaware of each others presence in the network. Each malicious node would assume that all other nodes are sane. The malicious node can target any other node at any time. We also assume that the malicious node will behave maliciously throughout the lifetime of the network.

### 3.3.2 Routing Protocol

The success of packet dropping attack depends on, whether the data traffic is routed through the malicious node or not. The data traffic will be routed through a node if the source node finds that the path to the node is shortest and fresh. We propose to modify the existing ADOV protocol to identify the forged reply messages sent by the malicious node.

Each node in the network upon receiving a reply would check for two elements in the reply message. The destination sequence number, and hop count value. The malicious node will set these values very high and very low respectively. Each node in the network follows the steps mentioned in the algorithm 1.

```
function RECEIVE REPLY(packet,sender);
    max_seq = get_seq();
    if ((dst_seq_no > max_seq&&hop < 2))
    {
     DropRREP;
     DeleteSender;
    }
    else
    {
     IncrementHopvalue;
     ForwardReply(nextHop);
    }
end function
```

**Algorithm 1:** Receive Reply

We have also taken the hop count value into account to identify a malicious node. Most of the approaches doesn't take this value into consideration. Thus, each node in the network acts as a guard to protect from the malicious node.

**function** GET_SEQ();
$S \leftarrow get\_start\_time()$;
$seq \leftarrow 0$;
**while** $(S \leq (start\_time + current\_time))$
**{**
$Seq \leftarrow Seq + 1$;
$S \leftarrow S + NetTraversalTime$;
**}**
**return** $Seq$;
**end function**

**Algorithm 2:** Sequence Number Generation

## 3.4 Analysis

Consider a MANET of ten similar nodes enclosed in a small area as shown in Figure 3.5. We assign a sender node, a receiver node and a malicious node. The attack to happen, the malicious node must place itself in the path between sender and receiver. The path doesn't exist between these two nodes. Sender node will initiate route discovery mechanism, by broadcasting the route request. As soon as the malicious node receives the route request, it replies with a fake reply consisting of the high value of sequence number and a short path length. Now as per original AODV protocol, the reply will be routed back to the sender node through the intermediate nodes as it is.

Our modification to the original protocol is as per Algorithm 1. The immediate receiving node checks the content of the route reply message. As routing control message does not hold any sensitive information, these messages can be checked for their content by any node. The immediate receiving node calculates the threshold sequence number at the time of reception of message using Algorithm 2. The values

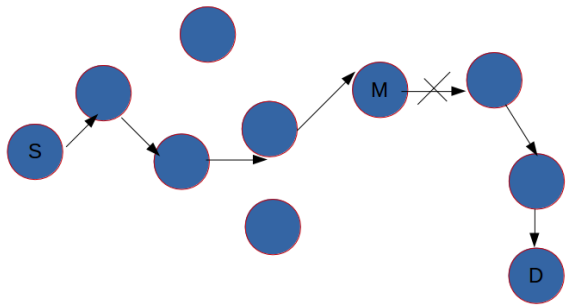


Figure 3.5: Example Scenario - 1

for the Node Traversal Time and Net Diameter are taken from the internet draft of AODV protocol.

$NTT = 2 * NodeTraversalTime * NetDiameter$

This algorithm returns upper value of sequence number that can be reached at a given instance of time since the start of data communication. If the sequence number in the reply message falls below this value, then a legitimate node could have sent the reply. Thus a response with sequence number value greater than the calculated value, must be from a malicious node.

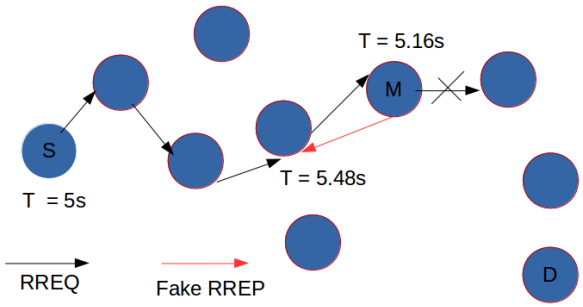


Figure 3.6: Example Scenario - 2

Let us assume that, the sender has data to send and it starts sending data

at $T = 5s$. As per the internet draft, the Node Traversal Time is 40 ms and Net Diameter 35 hops. Hence, the Net Traversal Time is calculated to be 2.8 sec. The figure 3.6 shows the time line of events. The intermediate node when receives the reply message from malicious attacker, it processes the packet using modified procedure. The result of procedure 2 is as per the Table 3.1.

Table 3.1: Sequence Number Generation

| S | SeqNo |
|---|---|
| 5 | 0 |
| 7.8 | 1 |
| 10.6 | **2** |

If the value of destination sequence number acquired from reply packet from the attacker is higher than 2 it will be marked as malicious and hence will be dropped by the receiving node. Thus, eliminating the inclusion of malicious node in the path.

## 3.5 Summary

In this chapter, we described, how a malicious node launches the packet dropping attack on the network, by exploiting the route discovery mechanism of AODV protocol. Our approach to avoid this attack is simple. In the next chapter, we delineate the simulation environment and the output that we've accquired using the NS-3.

# Chapter 4

# Evaluation of Proposed Protocol

**Network Parameters**

**Results**

**Summary**

# Chapter 4

# Evaluation of Proposed protocol

## 4.1 Introduction

In this chapter, we have compared the performance of the our proposed model with the existing AODV protocol using the simulator. The NS-3 simulator is used for simulations. Experiments were carried, to test the packet delivery ratio achieved with the proposed scheme. The details of the simulation and the results are as follows.

## 4.2 Network Parameters

All the simulations were carried using N-3.20 on Linux machine. The following aspects were decided randomly, before the start of simulation:

- Initial Position of each node
- Sender Node and receiver Node
- Connection Duration
- Beginning time of each connection

For each protocol, following metrics were calculated and compared.

- Average Packet Delivery Ratio: it is the ratio of number of packets received to the number of packets transmitted.
- End to end delay.: it is the average value of delay of all the packets received.

To have transmission range near 250m, environment variable values were fixed as follows.

Table 4.1: Environmental Parameters

| **Parameter** | **Value** |
|---|---|
| Energy Detection Threshold | -61.8 dBm |
| Clear Channel Assessment Threshhold | -64.8 dBm |
| Transmission Gain | 0 dBm |
| Reception Gain | 0 dBm |

Some other simulation parameters were set as follows. The data traffic was generated using Constant Bit Rate traffic generator.

Table 4.2: Simulation Parameters

| **Parameter** | **Value** |
|---|---|
| Area | 600 m x 600 m |
| Number of Nodes | 25 |
| Packet Size | 1024 B |
| Simulation Time | 350 s |
| Transmission Rate | 200 kbps |
| Transmission Range | 250 m |
| Mobility Model | Random Way-point |

Parameter values for AODV protocol are summarized in following Table. The values are set as specified in the AODV Request for Comment document.

Table 4.3: AODV Protocol Parameters

| **Parameter** | **Value** |
|---|---|
| Enable Hello | Enable |
| Hello Interval | 3 s |
| Destination Only | False |
| Net Traversal Time | 2.799 s |
| Route Rate Request Rate Limit | 10 messages/s |
| Route Request Retry | 5 |
| Active Route Timeout | 100 s |
| Path Discovery Time | 5.599 s |
| Max Queue Time | 30 s |
| Max Queue Length | 255 |
| Allowed Hello loss | 20 |

## 4.3 Simulation Results

We have analyzed the network performance with original AODV protocol and the enhanced protocol. The results obtained are as follows.

Figure 4.1 shows the packet delivery ratio for increasing network size. Our proposed algorithm tends to achieve higher packet delivery ratio when under attack.

Figure 4.2 shows the end to end delay values of the algorithms against the number of nodes. We have also measured the end to end delay value as the network grows as shown in figure 4.3. We compared our proposed approach with the existing approach mentioned in [11], and the simulation result shows that our approach gives lover delay value when under attack as the network size increases.

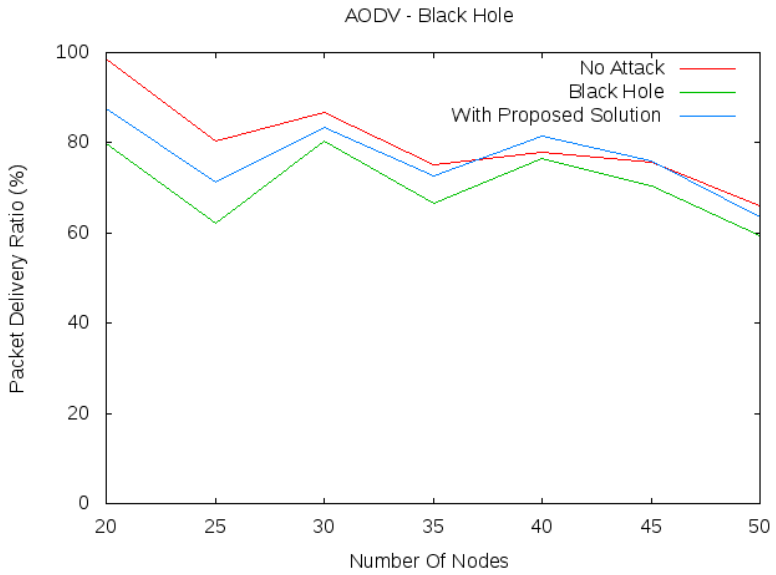


Figure 4.1: Packet Delivery Ratio

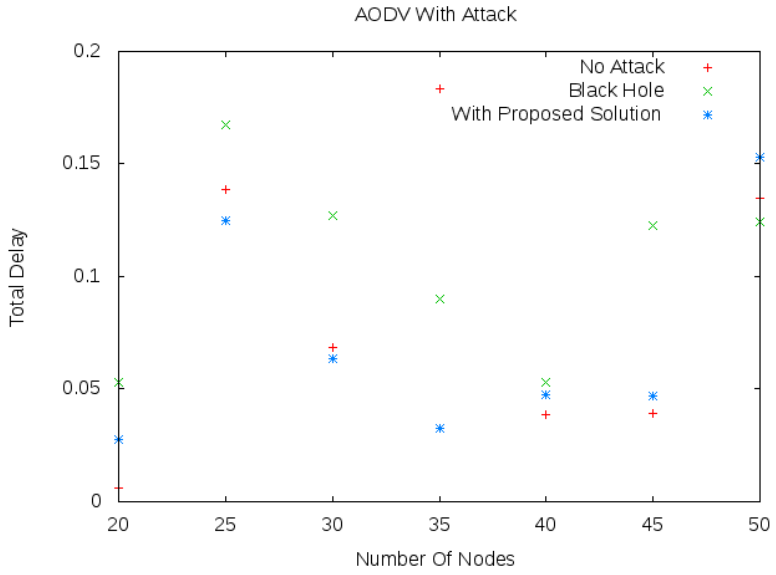


Figure 4.2: Total Delay

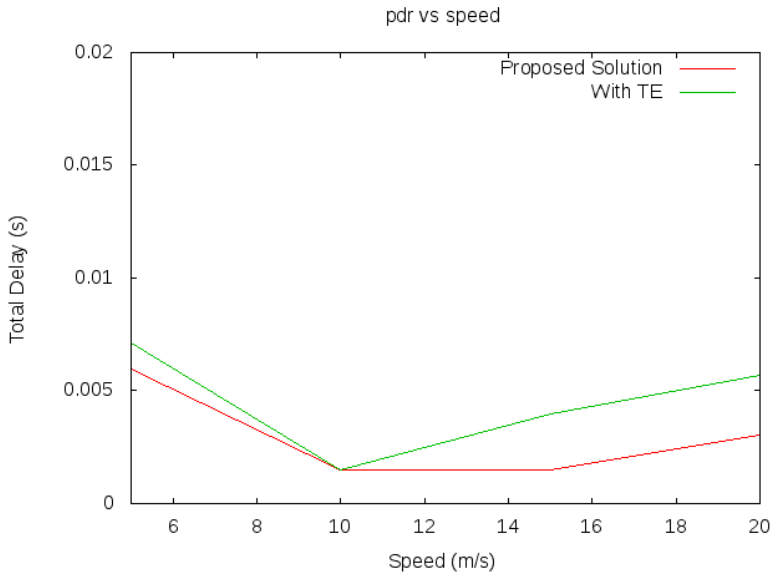


Figure 4.3: Total Delay

## 4.4 Summary

In this chapter, we have evaluated our proposed approach, using the NS-3 simulator. We have also evaluated our Enhanced AODV and our protocol shows better performance than [11] approach in terms of end to end delay.

# Chapter 5

# Conclusion

# Chapter 5

# Conclusion

## 5.1 Conclusion

Packet dropping attack reduces the network performance. Our secured AODV protocol is capable of mitigating the packet dropping attack in MANET. Our approach doesn't need any extra massive computational support to withstand this attack. Hence, more packet delivery ratio is achieved. This approach identifies and avoids black hole node in the path discovery phase and hence path chosen by the source node will be secured for data transmission. This approach also has a high point that it does not depend upon the relationship between the nodes. Thus, even if a trusted node turn into a malicious node then also our approach can stop the attack from happening. The simulation is carried out in NS-3. Thus, we evaluated that our algorithm shows better routing performance than an existing approach in terms of end to end delay.

### Scope For Further Research

Security in MANET is a very vast area of research, we have just touched the surface of this field. In our algorithm, we have managed to mitigate only packet dropping attack. This algorithm can be further expanded to mitigate more other attacks.

# References


[1] Mourad Elhadef, Azzedine Boukerche, and Hisham Elkadiki. Diagnosing mobile ad-hoc networks: two distributed comparison-based self-diagnosis protocols. In *Proceedings of the 4th ACM international workshop on Mobility management and wireless access*, pages 18–27. ACM, 2006.

[2] Abderrahmane Baadache and Ali Belmehdi. Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks. *Computer Networks*, 73:173–184, 2014.

[3] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, and Piet Demeester. An overview of mobile ad hoc networks: Applications and challenges. *Journal-Communications Network*, 3(3):60–66, 2004.

[4] Humayun Bakht et al. Survey of routing protocols for mobile ad-hoc network. *International Journal of Information and Communication Technology Research*, 1(6), 2011.

[5] Samba Sesay, Zongkai Yang, and Jianhua He. A survey on mobile ad hoc wireless network. *Information Technology Journal*, 3(2):168–175, 2004.

[6] Imrich Chlamtac, Marco Conti, and Jennifer J-N Liu. Mobile ad hoc networking: imperatives and challenges. *Ad hoc networks*, 1(1):13–64, 2003.

[7] Anuj Rai, Rajeev Patel, RK Kapoor, and DS Karaulia. Enhancement in security of aodv protocol against black-hole attack in manet. In *Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies*, page 91. ACM, 2014.

[8] Charles E Perkins and Elizabeth M Royer. Ad-hoc on-demand distance vector routing. In *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on*, pages 90–100. IEEE, 1999.

[9] Sudhir Agrawal, Sanjeev Jain, and Sanjeev Sharma. A survey of routing attacks and security measures in mobile ad-hoc networks. *arXiv preprint arXiv:1105.5623*, 2011.

[10] Kishor Jyoti Sarma, Rupam Sharma, and Rajdeep Das. A survey of black hole attack detection in manet. In *Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on*, pages 202–205. IEEE, 2014.

[11] Nabarun Chatterjee and Jyotsna Kumar Mandal. Detection of blackhole behaviour using triangular encryption in ns2. *Procedia Technology*, 10:524–529, 2013.

[12] S Sankara Narayanan and S Radhakrishnan. Secure aodv to combat black hole attack in manet. In *Recent Trends in Information Technology (ICRTIT), 2013 International Conference on*, pages 447–452. IEEE, 2013.

[13] Anand A Aware and Kiran Bhandari. Prevention of black hole attack on aodv in manet using hash function. In *Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2014 3rd International Conference on*, pages 1–6. IEEE, 2014.

[14] Debarati Roy Choudhury, Leena Ragha, and Nilesh Marathe. Implementing and improving the performance of aodv by receive reply method and securing it from black hole attack. *Procedia Computer Science*, 45:564–570, 2015.

[15] 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. *IJ Network Security*, 5(3):338–346, 2007.