"A NOVEL TECHNIQUE TO DETECT & PREVENT BLACK & GRAY HOLE ATTACKS IN MANET USING TVRI APPROACH"

A Dissertation Proposal
Submitted By

Manan Arora

(10800360)

To
Department of Computer Science & Engineering

In partial fulfilment of the Requirement for the
Award of Degree of
Master of Technology in Information Technology

Under the guidance of

SAMI ANAND
Assistant Professor, LPU

(APRIL 2015)

PAC FORM

LOVELY PROFESSIONAL UNIVERSITY

Transforming Education Transforming India

School of: Computer Science and Engineering

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student	: Manan Arora	Registration No	: 10800360
Batch	: 2008	Roll No	: RK2308B1
Session	: 2014-2015	Parent Section	: K2308

Details of Supervisor:

Name	: Sami Anand	Designation	: Assistant Professor
UID	: 16840	Qualification	: M.Tech
		Research Exp.	: 2.5 years

Specialization Area: Network and Security (pick from list of provided specialization areas by DAA)

Proposed Topics:-

1. Improving power efficiency and prevention in mobile Ad-hoc network.
2. Mobile Ad-hoc networks protocols.
3. Networks and Security.

Sami Anand

Signature of supervisor

PAC Remarks: Topic "1" is approved.

13/9/2014

APPROVAL OF PAC CHAIRMAN

Signature: 10/9/14

Date:

*Supervision should finally encircle one topic out of three proposed topics and put up for an approval before Project Approval Committee (PAC).
*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.
*One copy to be submitted to supervisor.

ABSTRACT

Wireless network technically, refers to the category of network in which communication is carried out without using wires. In modern era wireless network has great importance because the communication is taking place with the use of radio waves. Thus, the use of ad-hoc network starts yielding a great importance in variety of applications. The certain research work is carried out in this particular field. Mobile Adhoc Network is a constructed from various mobile nodes that can move anywhere and anytime without any need of fixed infrastructure. MANET can be made on fly due to lack of fixed infrastructure. MANET is vulnerable to various types of attacks due to dynamic changing topologies and wireless medium. Security of the MANET becomes one of the challenging task. Black and Gray hole attacks are the two main types of attacks that are possible in MANET. Black hole node not forward any data packets to the neighbor node instead it drops all the data packets and on the other hand the Gray hole node forwards selective data packets and drops all other data packets. Black and Gray hole attacks are bit hard to detect due to lack of centralized access.This study concentrates to enhance the security of MANET by detecting and preventing the black & gray hole attacks. The proposed solution is based on some threshold values, DRI tables and cross verifying technique which will prevent and detect the gray and black hole attack in MANET. Network Simulator 2 (NS2) is used for the simulation process.

CERTIFICATE

This is to certify that **Manan Arora**has completed M.Tech Dissertation Proposal titled "**A NOVEL TECHNIQUE TO DETECT& PREVENT BLACK & GRAY HOLE ATTACKS IN MANET USING TVRI APPROACH**" under my guidance and supervision. To the best of my knowledge, the present work is the result of his original investigation and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma.

The dissertation proposal is fit for the submission and the partial fulfillment of the conditions for the award of M.Tech Computer Science & Engineering.

Date: Name: **Mr. Sami Anand**

Signature of Advisor: UID:**16840**

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my advisor **Mr. Sami Anand** for the continuous support of my thesis study, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my M.Tech study.

DECLARATION

I hereby declare that the dissertation proposal entitled **"A NOVEL TECHNIQUE TO DETECH & PREVENT BLACK & GRAY HOLE ATTACKS IN MANET USING TVRI APPROACH"** submitted for the M.Tech Degree is entirely my original work and all ideas and references have been duly acknowledged .It does not contain any work for the award of any other degree or diploma.

Date: 01-May-2015

Investigator

MANAN ARORA

Reg.No. 10800360

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

The group of computers or mobile devices that are linked connected together through a medium is known as Networking. The devices can be linked through a wired or wireless medium. Networking is used to exchange information like data transmission. The two type of network used in the data transmission are wired and wireless. Wired network is that which used wires for communicate with each other's and wireless network is that which communicate without the use of wires through a medium.

1.1 WIRELESS NETWORK

The network that do not require any type of wire to communicate is commonly known as wireless network. Wireless Network uses radio waves for the communication between the devices. Now a day's wireless network become one of the common need because it provides you the facility to communicate without using wires using radio waves. Wireless Network commonly known as Wi-Fi. The standard defined by IEEE for wireless network is 802.11. Wireless Network defines some protocols that are responsible for providing the communication service between the devices.

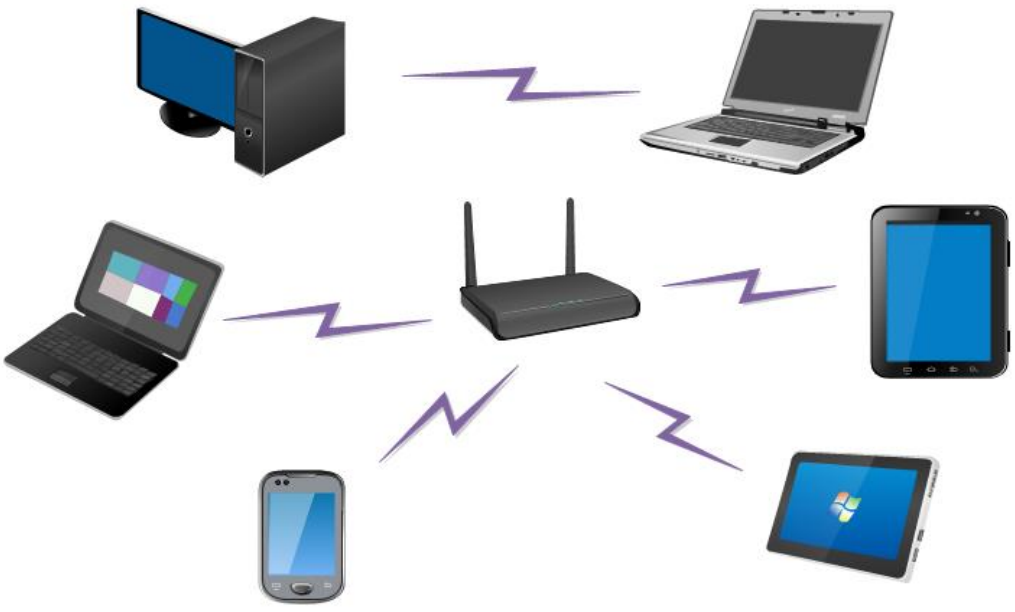

Figure 1: Wireless Networks

Wireless Network is based on some operating modes named as follows:

- Infrastructure Mode
- Infrastructureless Mode or Adhoc Mode

Infrastructure mode is one that uses a pre constructed infrastructure for the communication between the devices. Infrastructure mode uses a centralized control and access point for providing the access.

Infrastructure less or Adhoc Modeis that which do not need any pre constructed infrastructure for the communication. In Adhoc mode every device act as router and forwards the data to the next device.

1.1.1 Types of wireless network:

Wireless Network nowadays become one of the major part of networking. The use of wired network become history, now wireless networks are provided as much speed as wired network. Wireless network is mainly divided into two parts:-

- **Infrastructure Based Network:**

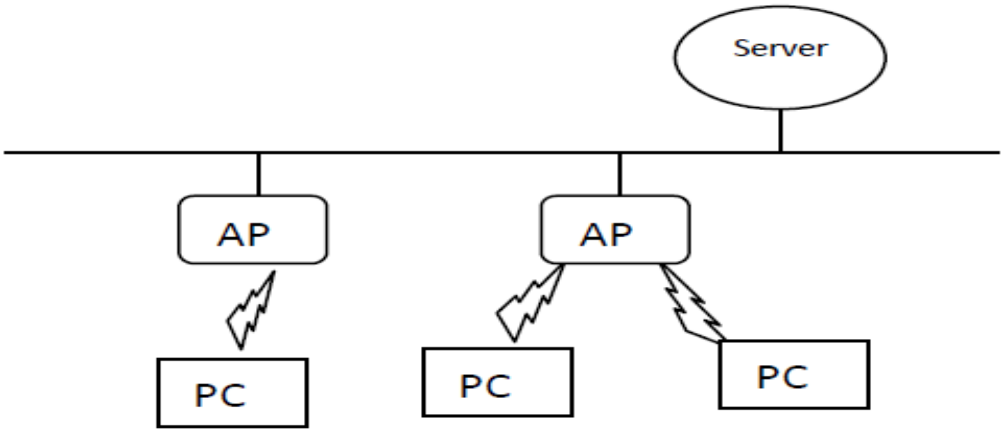

Figure 2: Infrastructure Based Network

Infrastructure Based Network is depend on a pre-constructed infrastructure. Infrastructure Based Network need an access point to communicate with one another. Infrastructure mode network are set up either by communicate indirectly through a central place or through an access points directly to one another. The first is called infrastructure modes. At this stage some access points are defined which provides the small network.

Infrastructure modes are advantage of the high power of an access point to cover wide region. In this case access points are directly connected with the server with the wireless network. Also, these access points are further connected to the different systems with the wireless link.

- **Infrastructure less Network:**

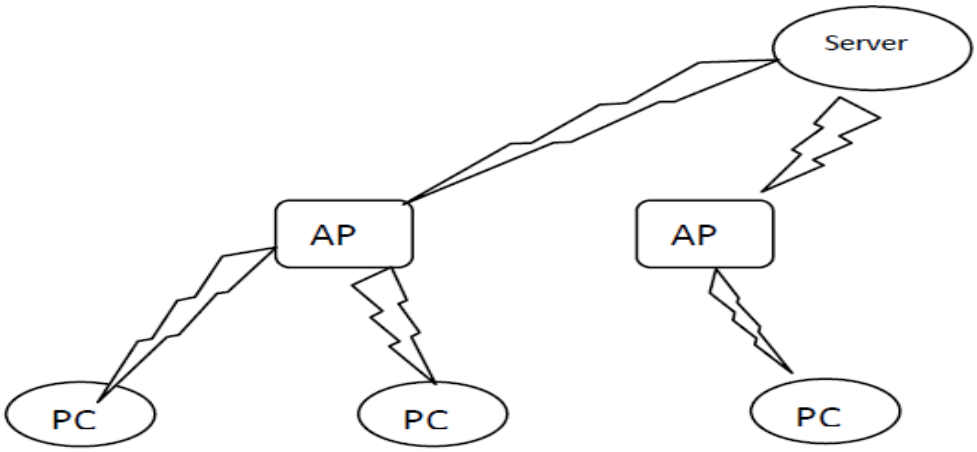

Figure 3: Infrastructure Less Network

Infrastructure less Network do not need any pre-constructed infrastructure to communicate with one another. Infrastructure less network can be used to communicate with one another during emergencies. There are many types of infrastructure less network available but the study mainly focuses on MANET.

Types of infrastructure less or Adhoc Network:

There are mainly three types of infrastructureless or Adhoc networks available. These are as following:

- MANET (Mobile Ad-Hoc Network)
- Wireless Sensor Networks (WSN)
- Wireless Mesh Networks (WMS)

1.2MANET (Mobile AD-HOC Network)

MANET or Mobile Adhoc Network is a self-organized and self-maintain wireless network consisting of mobile nodes. MANET wireless communication system can be deployed rapidly on the fly. It is very significant example include establishing survivable, efficient, dynamic communication in case of disaster operations, relief efforts, military networks and emergencies. In MANET network scenarios cannot rely on centralized and organized connectivity. MANET network is autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Mobile network topology may change rapidly and unpredictably from time to time. MANET or Mobile Adhoc Network is decentralized type of network where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves. The application of mobile ad hoc network constrained by power sources, to large-scale, mobility, high dynamic networks. The design of network protocol for this network is complex issue. Mobile Adhoc Network has used different distributed algorithms to determine the network, link scheduling and routing. In the mobile ad hoc network, nodes find the shortest path between the source and destination which is usually the optimal route. MANET is set of mobile nodes which communicate over radio and do not need any fixed infrastructure. This type of network is very flexible and suitable for several situations and applications as it is infrastructureless. Due to the limited transmission range of wireless interface the communication traffic has to relay over several intermediate nodes to enable the communication between the nodes. MANET complete the functionality of hosts but each node also be router to forwarding packets for other nodes.

As MANETs are illustrate by limited bandwidth and node mobility, there is demand to take into account the energy efficiency of the nodes, topology changes and unreliable communication in the design. There are many types of protocol are available in Mobile Adhoc Network. The protocols available are as follows:

1.2.1 Routing Protocols in MANET:

Routing protocols are developed to define the route from one device to another. It helps to search shortest route from source to destination. There are mainly three types of routing protocol available. These are as following:

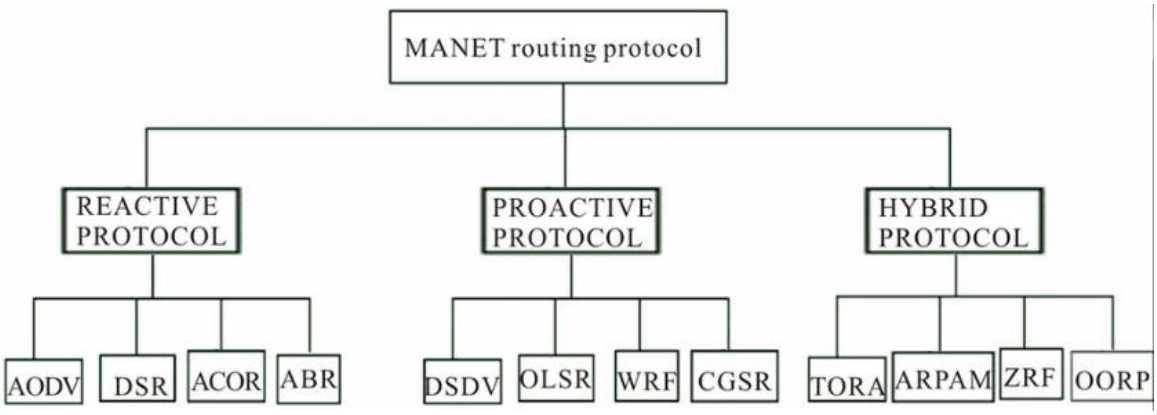

Figure 4: MANET Routing Protocols*[1]*

- **Proactive Routing Protocol:**

  Proactive protocol is the type of protocol that does not always create new route when a source request the route to destination instead it will check its routing table and finds the route. Proactive Routing protocol works faster than the Reactive protocol. It is also known as table driven protocol. Some examples of proactive protocol are DSDV, OLSR.

- **Reactive Routing Protocol:**

  Reactive Protocol is other type of protocol which always build a new route when source requested a route to the destination. Reactive protocol is a lazy protocol. Reactive Protocol is also known as on demand protocol. Some main reactive protocols are AODV, DSR etc.

- **Hybrid Routing Protocol:**

  Hybrid Routing Protocol is the combines the functionality of both proactive routing protocol as well as reactive routing protocol. Hybrid routing protocol uses the route discovery functionality of reactive routing protocol and table maintenance functionality of proactive routing protocol. Hybrid routing protocol divides the network into the zones and perform routing. It is mainly suitable for large network. One of the main example of hybrid routing protocol is ZRP i.e. Zone Routing Protocol.

1.2.2 Applications of the MANET:

As the moveable devices in wireless communication increases, ad-hoc networking is become widespread applications. Anywhere where there is small or no communication infrastructure is exist or the existing infrastructure is inconvenient or expensive to use. Ad hoc networking allows the devices can be simply adding and removing devices to and from the network and to keep connections to the network also. MANET is become very vast in these days by increase its scalability, provide mobility, become dynamic in nature etc. The application of MANET is as follows:

- **Emergency Services**:

  It can be used in emergency operation where nature disaster occur or any accident, flood, earthquake where no existing network exits to provide them reliefs. It collected information from effected area to the people for their help or to any local control posts. As soon as the control post comes to know about situation they give responsibilities to works to help them as soon as possible and provide doctors and other help which they wants at that time.

- **Military Battlefield:**

  Military equipment contains some kind of computer equipment. Military take advantage of common place network technology to keep an information network between the vehicles, soldier and military information headquarters using adhoc networks. From this field the basic techniques of ad hoc network came.

- **Entertainment and Local level**:

  Ad hoc networks can also link temporary multimedia network palmtop computers to share and spread information among participants at conference and classroom using notebooks, laptops and computers. It can be used as home networks where devices can communicate to exchange information directly [2]. It can be used as peer to peer networking and multi user game and in theme parks.

- **Commercial Environments**:

  It can be used for the purpose of business in dynamic databases and mobile offices. In the field of E-commerce it can help in the purchasing like we can be

purchase anything from anywhere and electronic payments can be made. In vehicular service it can be used to transmit the information of road accident, inter vehicles network and road transmission. In sports stadium, taxicab adhoc networks also help.

- **Personal Area Network (PAN):**

  The interconnection between short ranges devices like mobile, PDA, laptops are comes under PAN communication in adhoc networks. The wired system is replaced by the wireless communications. It extends the internet scalability to access the internet with the help of Wi-Fi LANS, GPRS, and EDGE. It has greater scope in future.

1.2.3 Advantages of Manet

The main advantages of the Adhoc networks are as follows:

- In MANET there is no need of centralized network. It can be setup anywhere as the nodes are mobile.
- No need of pre-constructed network setup.
- Nodes act as router forwarding data from one to another.
- MANET is very flexible type of network.
- Last but not the least, In MANET you can scale up and down the network anytime.

1.2.4 Disadvantages of Manet

The disadvantages of MANET are as following:

- One of the main disadvantage is regular changing topology.
- No centralized access.
- Lack of resources.
- Different protocols for Adhoc Network
- Detecting of malicious node is very difficult without central access.

1.2.5 Challenges to MANET

The main challenges to MANET are as following:

- Routing is one of the main challenge to MANET because of regular changing topology.
- Security and Reliability is other challenge to MANET due to neighbor relying packets.
- Providing the Quality of Service in constantly changing environment.
- Design a protocol for location-aided routing in MANET.
- Remove the hidden and exposed terminal problem.
- Remove the problem of link failure due to constant movement of mobile nodes.
- Last but not the least Power Consumption is also another challenge to MANET because MANET rely on battery power.

1.3AODV ROUTING PROTOCOL

AODV is an ad-hoc on demand distance vector routing protocol that establishes route to the destination when it is desired by the source node. It maintains these routes as when needed by the source node. It offers quick adoption to dynamic link conditions, low processing, memory overhead, low network utilization, and determines unicast routes to the destinations within the ad-hoc network [1paper]. Route Request (RREQ), Route Reply (RREP), Route Error (RERR) messages are three control packets that are used in AODV. RREQ and RREP are used in route discovery process and RERR is used in maintenance phase. AODV also maintains destination sequence number for each routing table entry. AODV protocol firstly discover the route by using route discovery process, In route discovery process firstly, source node broadcast a Route Request Packet (RREQ) to all its neighbors, and they transmits packet to their neighbors until and unless they find a valid route to the destination. After receiving Route Reply (RREP) messages, source node check its table and selects the route with the highest sequence number. If a link breaks, neighbors of that link broadcast Route Error Message (RERR) through the network to alert other nodes about this failure [2].

AODV protocol does not provide a complete view of network topology to the nodes. In AODV protocol each node only knows about only its neighbors. AODV protocol is not a secure protocol in MANET. The security of AODV protocol is compromised due to presence of the malicious nodes in the network. The malicious node can be a Black hole as well as it can be a Gray hole node.

The standard AODV protocol cannot detect malicious node in the network due to its nature of finding the new routes to destination every time a source request to transfer the data packets.

In AODV protocol the source node will floods the route request messages to all its neighbor node to discover the route from the source to destination node. Destination node also broadcast the route reply message for the source node.

In the below figures the process of discovering the routes followed by the AODV protocol is shown.

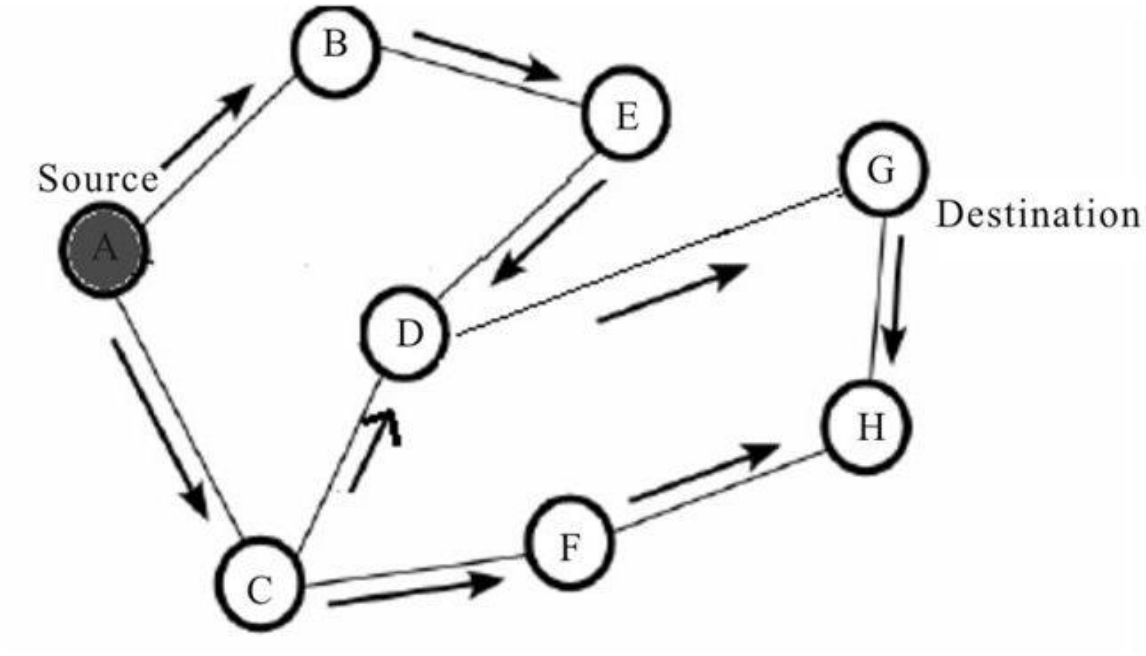

Figure 5: AODV Route Request*[1]*

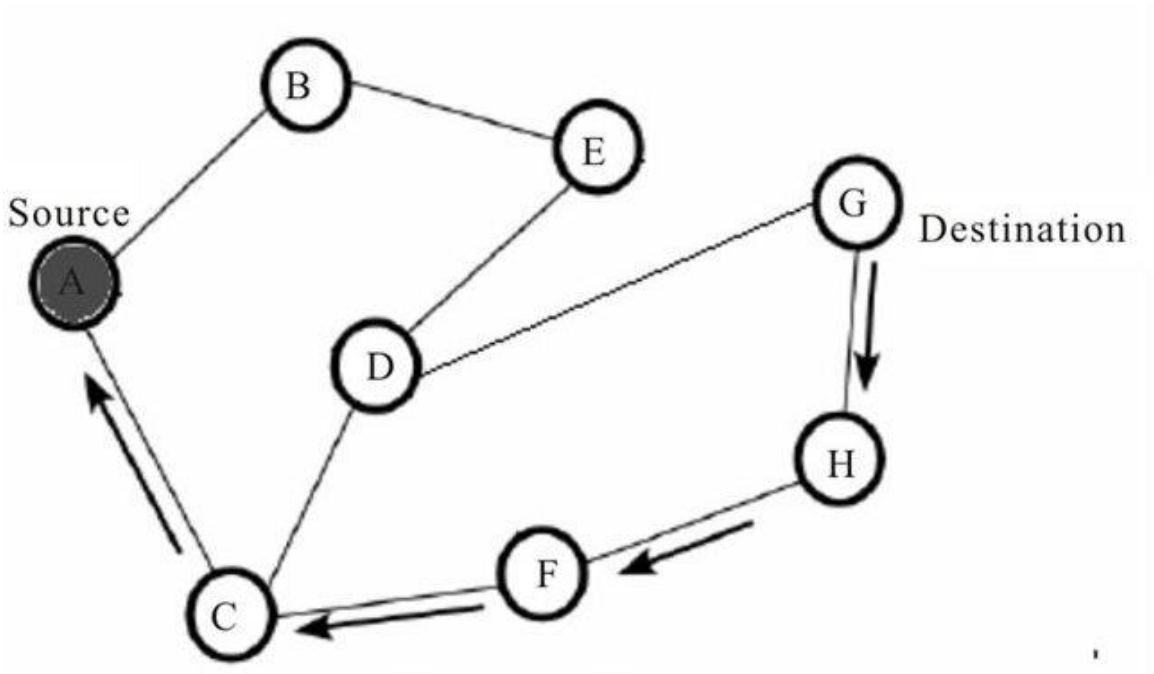

Figure 6: AODV Route Reply*[1]*

1.3.1 Black Hole Attack in AODV Protocol

Black hole attack is one of most frequent attack that happened in the network. In black hole attack the malicious node falsely advertise that it has the shortest path to the destination. The reason behind such malicious activity is to stop the destination from receiving the packets. In Black hole attacker introduced itself as the destination or it has the shortest path to the destination by replying with a high sequence number RREP message. The source node selects the high sequence RREP message and ignores all other RREP message including the correct ones and starts transmitting the data packets to the malicious node. The malicious node will not forward any data packet to other nodes instead it will drop all the data packets. This type of attack is very severe to detect and we proposed a technique to detect and to prevent black hole attack in Mobile Adhoc Network [2].

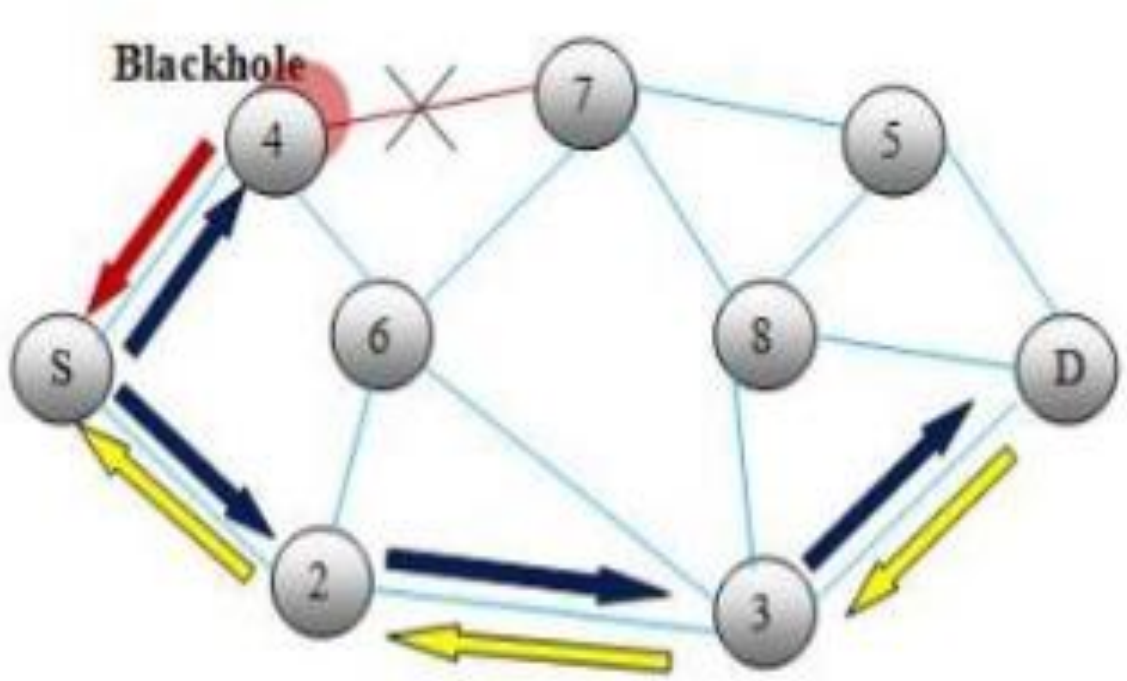

Figure 7: Black Hole Attack*[3]*

1.3.2 Gray Hole Attack in AODV Protocol

Gray hole attack is bit similar to black hole attack with a small variation where the malicious node does node drop the whole packets instead it will drop some selective packets. In Gray hole attack, a node which is member of the network, gets RREQ packets and create a route to destination. After creating the route, it drops some of data packets. Gray hole attack is very difficult to detect because malicious node do not drop data packets regularly but instead it will drop the data packets occasionally. Therefore sometimes node will act normal node and sometime node switch to malicious node. Gray hole attacks are more frequent in AODV routing protocols and are bit hard to detect and can cause disruption in the network without being detected.[2]

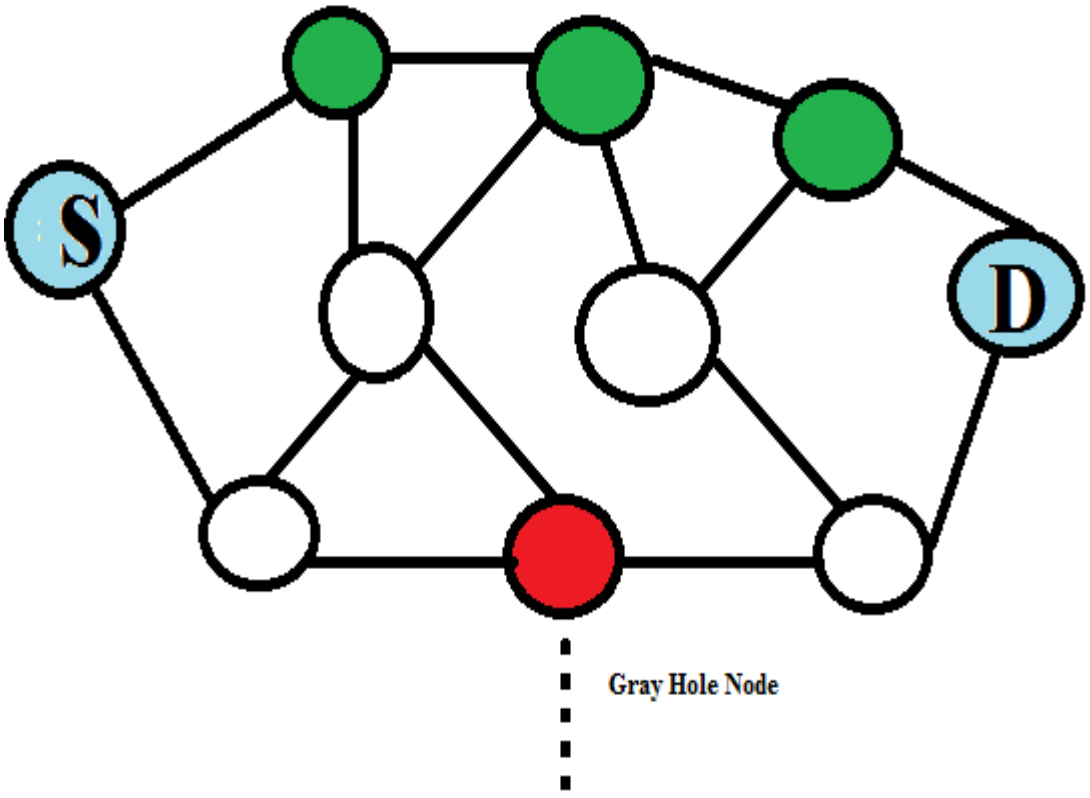

Figure 8: Gray Hole Attack

CHAPTER 2

REVIEW OF LITERATURE

This chapter reviews the literature about the previously proposed techniques for detecting and preventing Black and Gray hole attack.

Marti et.al (2000) proposed a technique to trace malicious nodes using watchdog. This protocol works by checking the routing table of next node that the node forwards the packet or not. In this technique when a node forwards the data packet to its neighbor node than node's watchdog verifies that next node forward the data or not. If the neighbor node does not forward the data packet in a defined threshold time than it will blame the next node as malicious node [4].

Sukla Banerjee (2008) proposed a technique for detection and removal of Black and Gray hole in MANET. In this technique firstly the source node will divide all data packets into K equal parts, after source node sends a message to destination informing about the number of packets. If destination node does not receive total number announced packet than it starts removing the malicious node from the network. Also, neighboring node uses a counter for counting the data packet of its neighbors [5].

S. Ramaswamy et.al (2003) proposed a technique that uses Data Routing Information table. The DRI table uses two fields named as 'from' and 'through'. From nodes is that from which the node getting the data packets and through node is that sends the message to current node. The mechanism will check the value of 'from' and 'through' fields. This protocol uses RREQ and RREP packets [6].

Priyanka Goyal et.al (2011) have introduced the elementary problems of ad hoc network by giving its background which is related to its work including the concept, status, features and vulnerabilities of MANET. This paper presents summarized study of the routing protocols. Different types of Routing protocol like reactive, proactive and hybrid routing protocol and their subcategories all are mentioned in this paper[7].

Hizbullah Khattak et.al (2013) introduced a mechanism that is based on Optimal Path and Hash Based Scheme. The proposed solution choose the second shortest path by discarding the first shortest path. This solution also embed the technique of hash algorithm which maintains the integrity of the data [8].

Harmandeep Kaur et.al (2014) proposed a mechanism that will integrate the Data Routing Information table (DRI) with Ant Colony Optimization (ACO). The proposed mechanism send a promiscuous mode activation message to all neighbor nodes and checks the DRI table of all nodes and after that find all available path from source to destination using ACO table[9].

Kurosawa, Satoshi et.al (2007) introduced a new algorithm that is based on the limit of sequence number. The proposed algorithm will check the RREP packets number with the threshold value of that route, if the RREP sequence number is higher than the node, source will enter the node ID in the block list and broadcast the node as malicious node [10].

Sen, Jaydip et.al (2011) proposed a four step method for the detection of gray hole in the network. The first step is Data Collection of neighbors in which every node will gather the information of its neighbor and enters in its DRI table, in next step which is 'local anomaly detection' source selects a Cooperative Node (CN) by checking the DRI table of that node. Source node forwards a RREQ packet to CN and asks it if it receives the packet or not, if not it will increase its maliciousness. Third step is Cooperative Anomaly Detection is done to avoid the mistake in the detection of malicious node. Last step is 'Global Alarm Sending' in which source broadcast the node as gray hole node [11].

Alem et.al (2010) proposed a technique based on Intruder Detection using Anomaly Detection. IDAD monitored the activities of nodes and collect the audit data. IDAD compare the activity of each node with audit data and find the malicious node and isolate it from the system [12].

Yang, Shu et.al (2006) proposed the two combine method technique to prevent the Mobile Adhoc Network i.e. local collaboration of neighboring nodes to monitor each other and cross validation method in which each node cross verify the next node and monitor overheads transmission. The technique improves the security of Mobile Adhoc Network to some extend but in some case this technique break [13].

P. Agarwalet.al (2008) proposed a technique for detecting cooperative malicious black and gray hole nodes in mobile Adhoc networks. The technique initially establishes a trustful backbone network of strong nodes over ad hoc network. Each strong nodes are assumed to be a trustful one. These strong trustful nodes detect the malicious nodes between the regular nodes. The backbone network of trusted strong nodes carry out end-to-end checking to determine whether the data reached the destination or not. If result fails then the backbone network initiates a protocol to detect the malicious node in the network [14].

G. Carofiglio et.al (2009) proposed a technique that improve routing efficiency of Mobile Adhoc Network by selecting the most stable path so as to reduce the latency and overhead. The selection of path depends on mobility patterns of nodes in the network and these mobility pattern depends on the movement of nodes with respect to other nodes in the Mobile Adhoc Network [15].

Sung-Ju Lee et.al proposed a new type of technique known as AODV-BR. The proposed technique is based on backing up the alternate routes to the destination. The technique uses mesh structure and alternate paths. The scheme can be merged with any ad hoc on demand routing protocol. The backed up alternate routes can be used when data packets cannot delivered using primary routes. The proposed technique will improve the efficiency of the network [16].

CHAPTER 3

PRESENT WORK

3.1 PROBLEM FORMULATION

Mobile ad hoc network (MANET) is a self-organizing, self-configuring wireless network consisting of mobile nodes. It do not require any centralized access point. There is no need for any fixed infrastructure for nodes to communicate between themselves. Manet is vulnerable to various attacks due to lack of centralized monitoring and regular changing topologies. Security has become one of the challenging issue to protect MANET from various malicious attack and provide secure communication between the nodes.

Routing in Mobile Adhoc Network has become a challenging task due to regular changing topology. The mobility feature of MANET make it difficult to securely route the packet from source to destination. In MANET, there is no restriction on nodes to join or leave the network, therefore any node can leave or join the network at anytime. This property of MANET makes it very difficult to secure the MANET from various type of attacks including Black & Gray hole attacks.

There is lot of research has been done on MANET previously, but I however believe that there is still lots of security issue in MANET such as Black and Gray hole attacks.

The study mainly focuses on the problem of Black hole and Gray attacks in the Mobile Adhoc Networks.

The main challenge of our study is to prevent the discovered problem of Black and Gray hole attacks in a AODV based Mobile Adhoc Network by providing a new technique which is capable of detecting and preventing the AODV based Mobile Adhoc Network from Black and Gray hole attacks and to improve the efficiency of Mobile Adhoc Network.

3.2 OBJECTIVES OF THE STUDY

When we deals with the web MANET much security is required because MANET do not depend on pre-constructed infrastructure and in MANET nodes are free to join and leave the network any time so while looking at appropriate security schema the objectives of our work are as following:

- The study focus on enhancing the security of MANET by analyzing the Black and Gray hole attack and its consequences.
- The aim is to introduce a new technique which is able to detect and prevent the black hole and gray hole nodes in the network.
- To reduce the congestion from network due to black hole and gray hole nodes.
- To make the Adhoc network more reliable in terms of security.

3.3 PROPOSED METHODOLOGY

Black hole node will drop all data packets whereas Gray-hole node will drop selective data packets. Here our task is to prevent the black hole attack as well as Gray-hole attack. Here we will use a novel approach which will based on the basis of some threshold values. This novel technique will helps to prevent Black hole attack as well as Gray hole attack at single time.

.

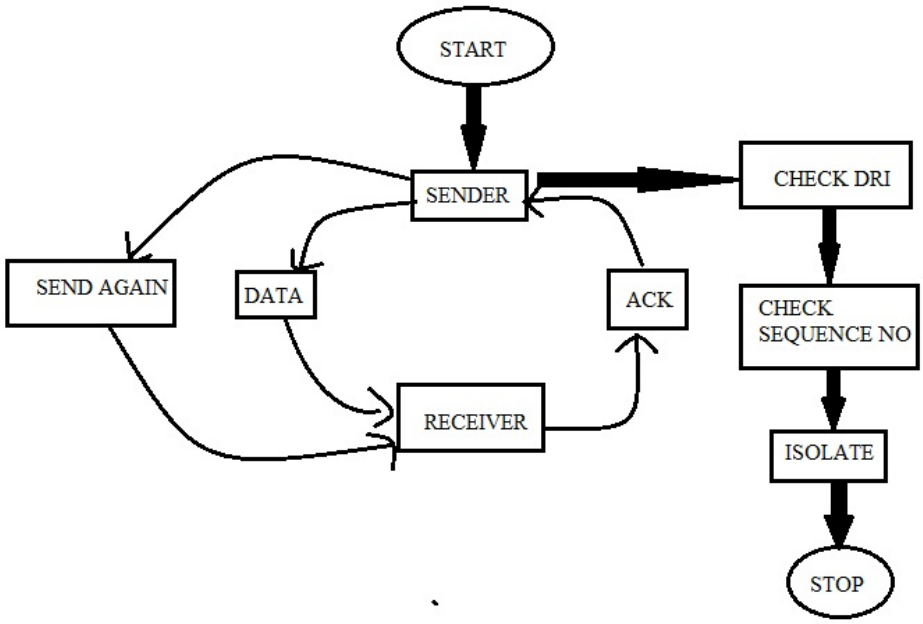

Figure 9: Flow Chart

For that technique we will consider some assumptions and some threshold values like:

Threshold of packet received at destination: T_{rec}=500

Threshold of dropped packet received at destination: T_{D_rec}=20

Threshold of packet lose: T_{PL}=300

Timer =3

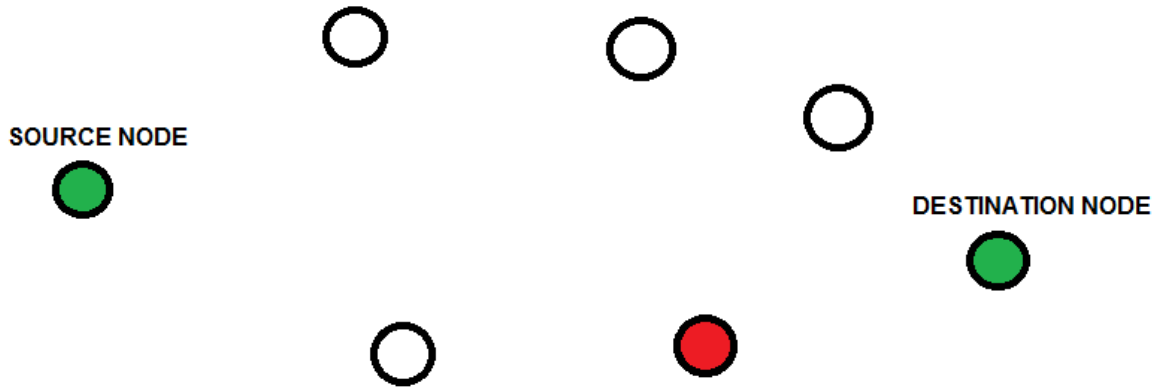

Figure 10: Proposed Network

Here the network has been created source and destination nodes were selected now we are considering the black hole attack.

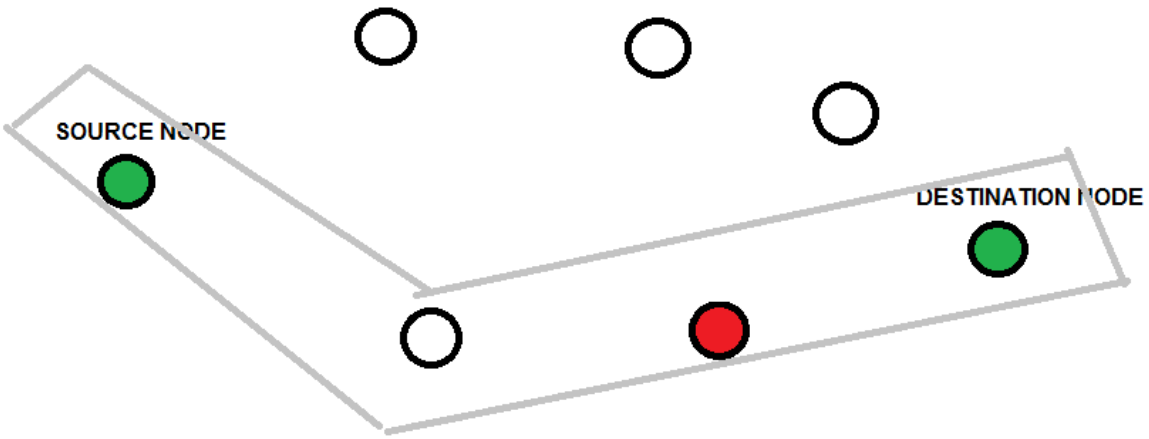

Figure 11: Black Hole Node

Suppose on the basis of AODV the path has been selected and the path contains black-hole node. Now here we will use TCP protocol for data transmission. Here TCP will work on the basis of threshold values.

- Source node will start transmitting packets to destination node.
- Destination node will receive packets and when its received packet value will be equal to T_{rec}it will send ACK to source node.
- After getting ACK it will check the T_{PL} and find out that how much packets were lost in the path.
- If the value of T_{PL}>300 then it will consider a malicious node in network because black hole and gray hole both nodes are used to do packet drop.
- Else If the value of T_{PL}<= 300 then it will consider that packet-loss can be cause of congestion in the network.
- Now it will again send lost data packets 3 time each using timer.
- Now after getting T_{D_rec}value receiver will again send ACK and the whole procedure will be repeated again.
- If all the packets are delivered successfully then the transmission will be continues.
- Else it will declare a malicious node into the network.
- It will temporary block the path and will check DRI values of each node.
- In promiscuous mode we can check DRI tables of node. Promiscuous mode is a mode which is caused to generate and receive all traffic through node. DRI table is which contain dynamic routing information. It contains all values of THROUGH and FROM. If the node is normal and passing all traffic through it then the value of its THROUGH table is 1 and if it's malicious then the THROUGH table contain value 0. So to check whether the node is malicious or not we will use DRI tables. So in our scenario before communication source node broadcast RREQ packets with fake destination address. All the normal nodes will pass this message through them but black hole nodes will drop this packet after this source node will request for promiscuous mode activation message to all nodes and requests and requests them to show there DRI tables and the nodes contain 0 value of THROUGH are considered as black-hole nodes. After that will

choose the path in which all nodes are having FROM and THROUGH values 1,1. The nodes are having value 0 will be isolated for communication

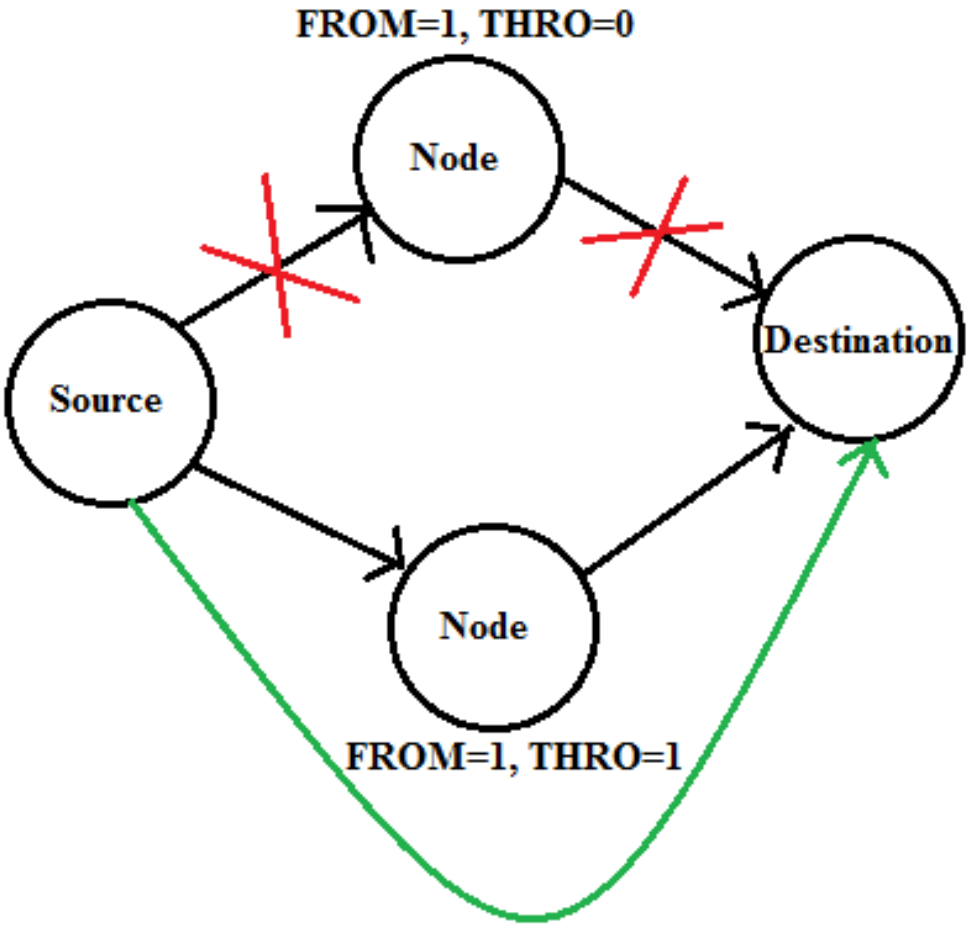

Figure 12: DRI Table

- Now to detect gray hole node we will apply cross verification method. In cross verification method the source node will send rough data through all nodes and verifying through the next hope that either the data passed through node or not. If any node is responsible for high packet loss means almost near to half of the total packets then it will be considered as gray hole node

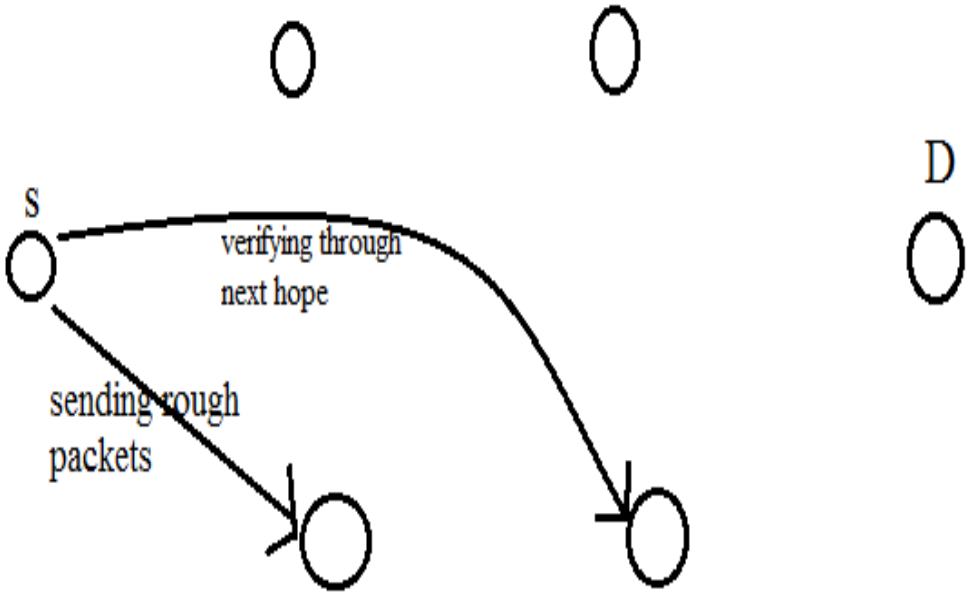

Figure 13: Gray Hole Detection

CHAPTER 4

RESULTS AND DISSCUSSIONS

MANET security is one of the major concerns because of the lack of centralized access and regular changing topologies. One of the major task is to design a security effective protocol that will help to avoid the attacks and provide a secure communication between the nodes. In a group communication security issues become worst because there are number of senders and number of receivers. So I am going to propose a new threshold based technique that will be more efficient against the Black and Gray hole attacks and helps to detect and prevent the attacks. The proposed work will also enhance the performance of the network.

The simulation of the proposed technique is done using network simulator (NS-2.34). Here the attack and proposed technique is implemented by taking wireless nodes and the results are plotted in terms of throughput, packet drop and congestion in the network. The comparison between the scenarios is shown in the form of graphs. The following parameters have been taken to perform the simulation:

Table 1: Simulation Parameters

Network	Wireless
Antenna	Omni directional
Routing Protocol	AODV
No of Nodes	11
Mac Type	802.11
Pause Time	2.0
Simulation Time	10 s
Application Traffic	CBR

4.1 SIMULATION

The simulation of the proposed methodology is done using the network simulator (NS2). The network is deployed with eleven mobile nodes.

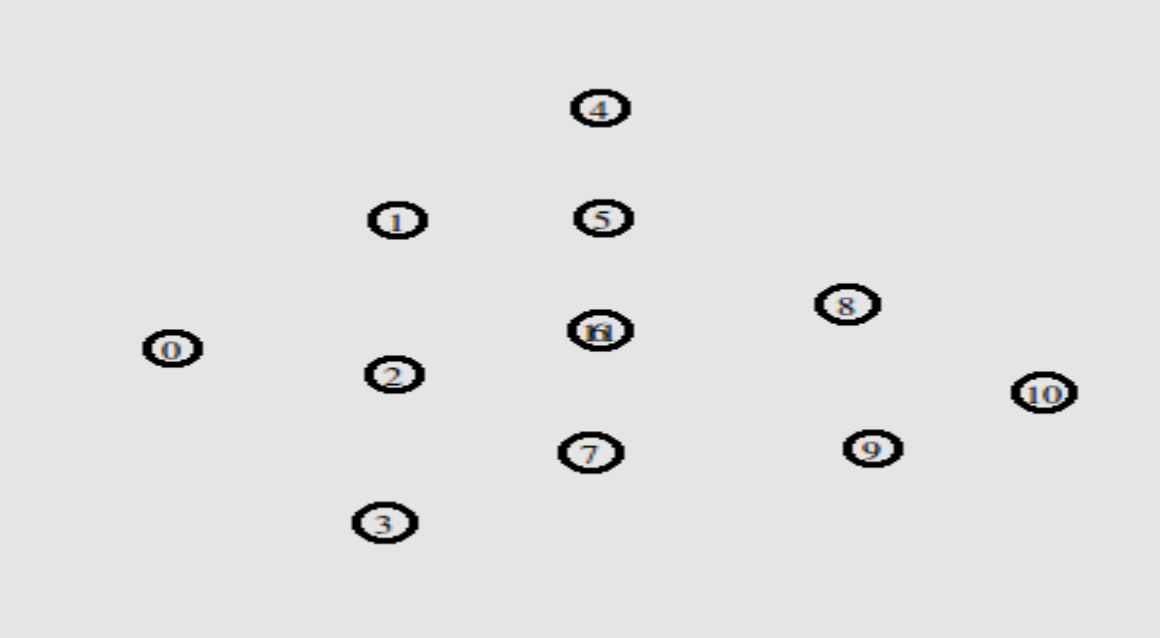

Figure 14: Network Deployment

After deploying the network source and destination nodes are selected. Source node is the node which will send the data packets while the destination node is the one which will receive the data packets.

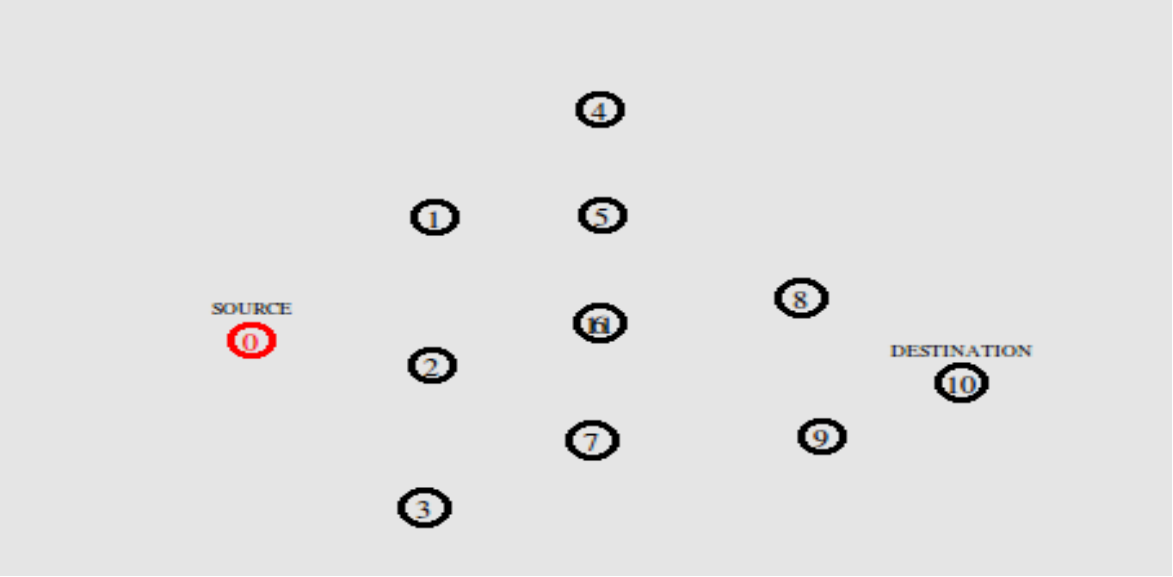

Figure 15: Source and Destination Nodes Selection

Source node starts discovering the route to destination. The route to the destination is discovered using AODV protocol by flooding the route request (RREQ) packets to all its neighbor nodes which contains the address of the destination node. Every node will forward the route request packets to its neighbor node till the route request packet reach the destination.

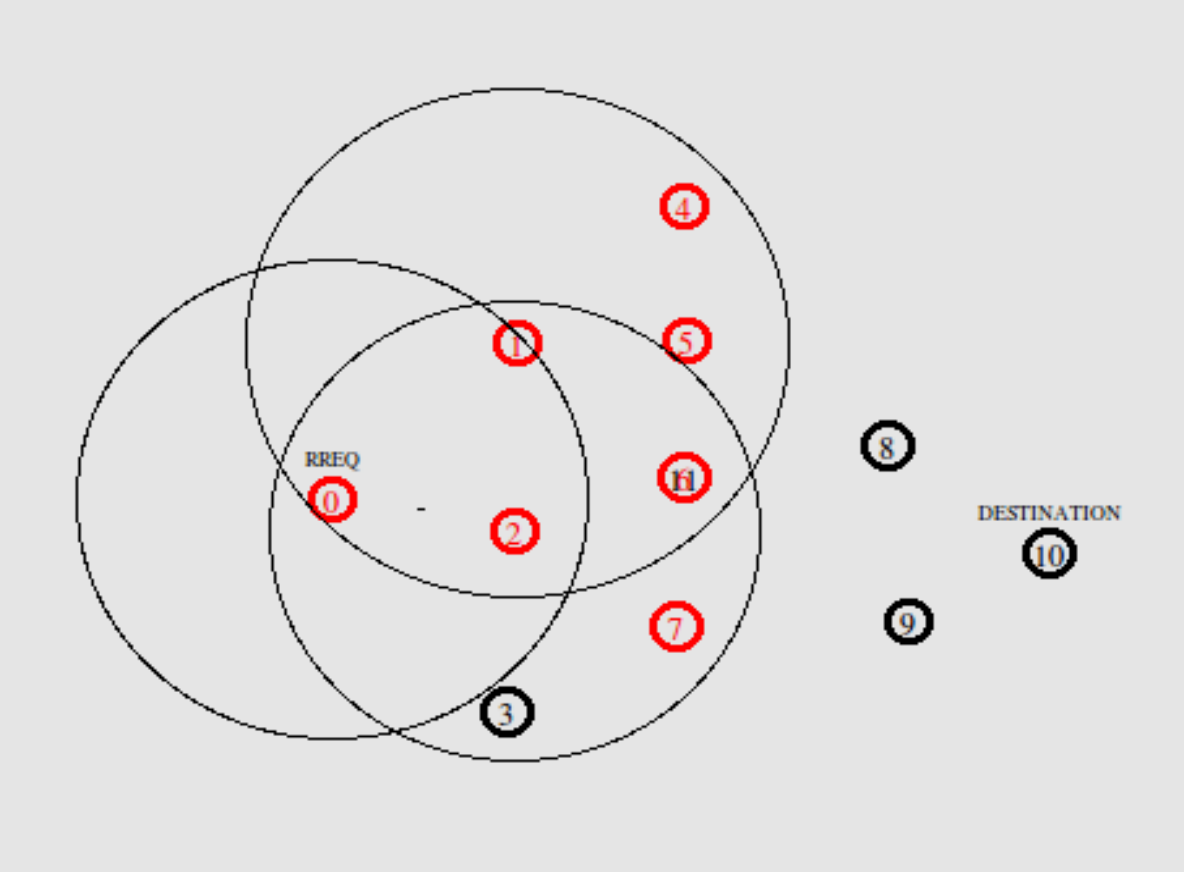

Figure 16: Route Request Process

After receiving the route request (RREQ) packets from source node, destination node will flood the route reply (RREP) packets to the source node. Destination node will send back the packets containing the route from source to destination to the source node.

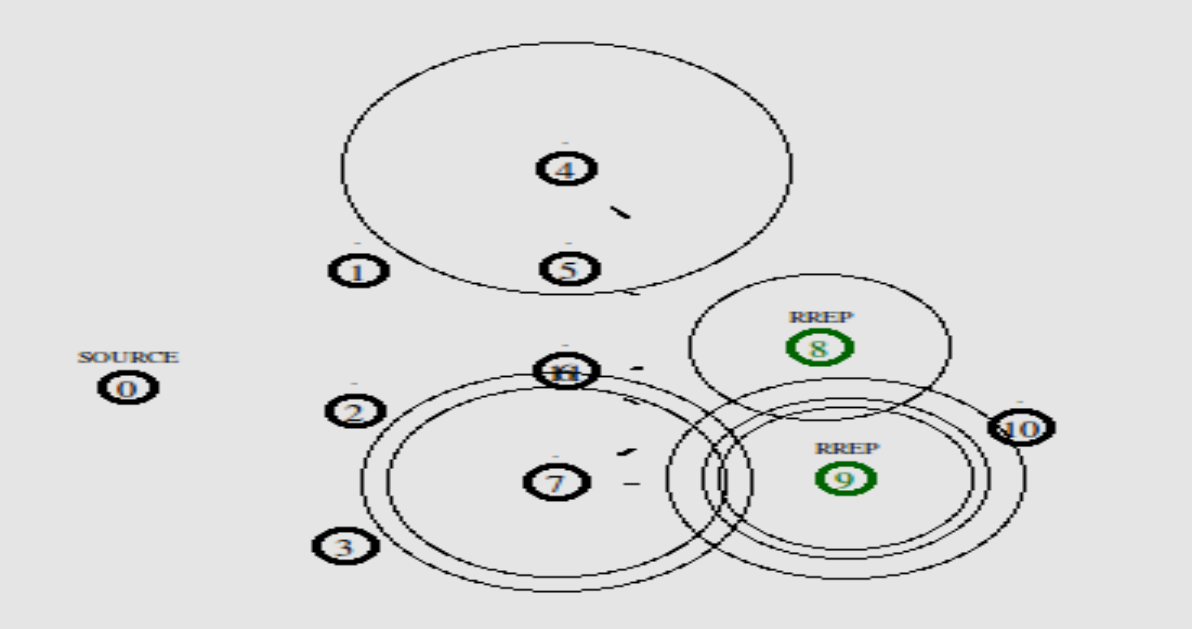

Figure 17: Route Reply Process

Source node will receive the route reply packets from the destination node and select the shortest path from source to destination node. Shortest route contains less number of intermediate node.

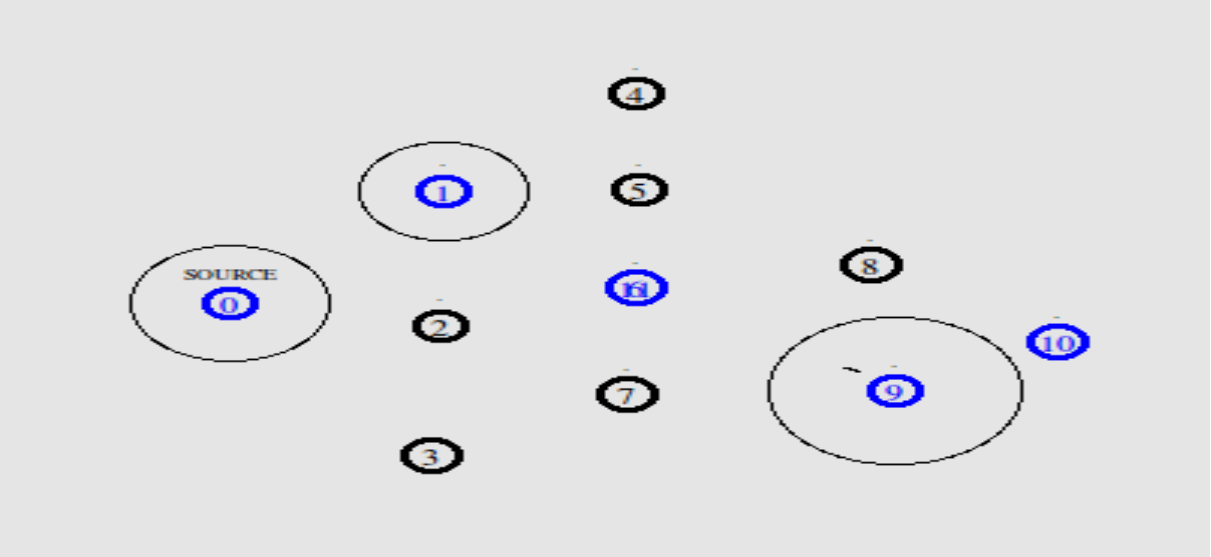

Figure 18: Route Reply Process

Source node will starts the transmission of data to the destination node. In transmission the black hole node will not transmit the data to neighbor node instead it will start dropping the data packets.

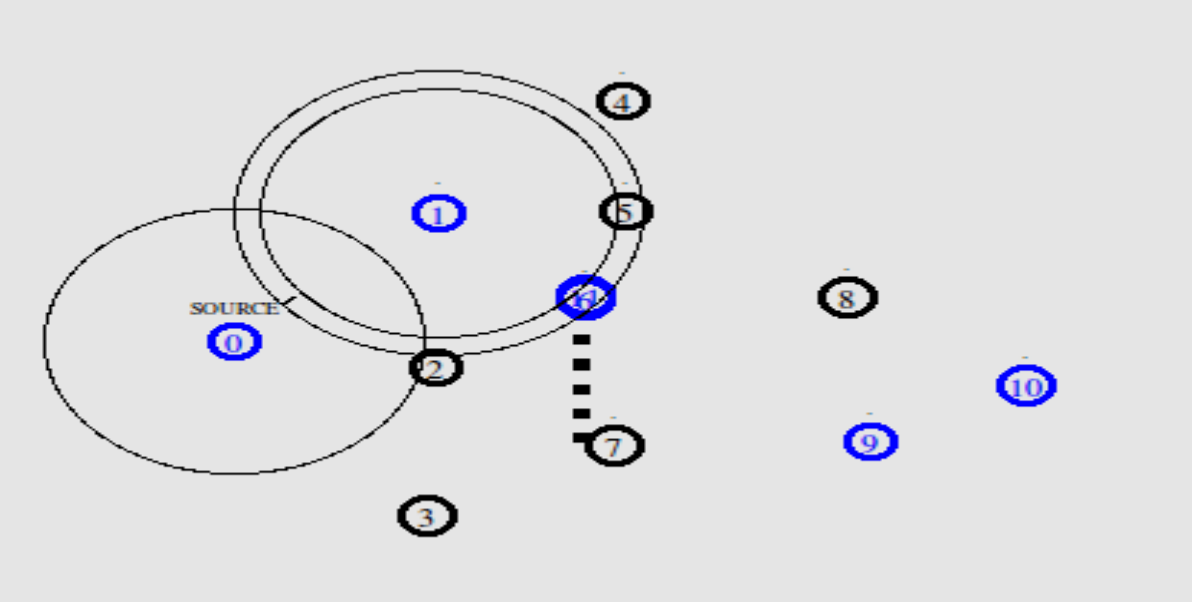

Figure 19: Black Hole Node Dropping Packets

After sending the minimum 500 data packets to the destination source node will starts the promiscuous mode and check the DRI values of all the nodes. If any node finds with 0 through value then the node will consider as malicious node and isolated in the network.

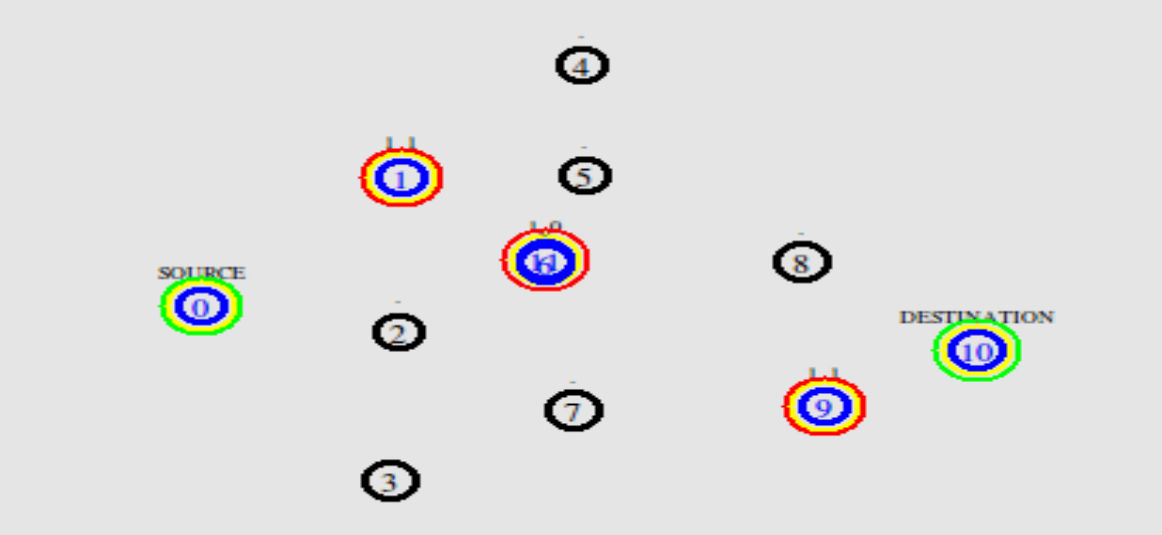

Figure 20: Promiscuous Mode

Here the node which is dropping the data packets rather than sending it to its neighbor node is consider as the malicious node. Therefore malicious black hole node is isolated from the network and path is also blocked due to the presence of black hole node.

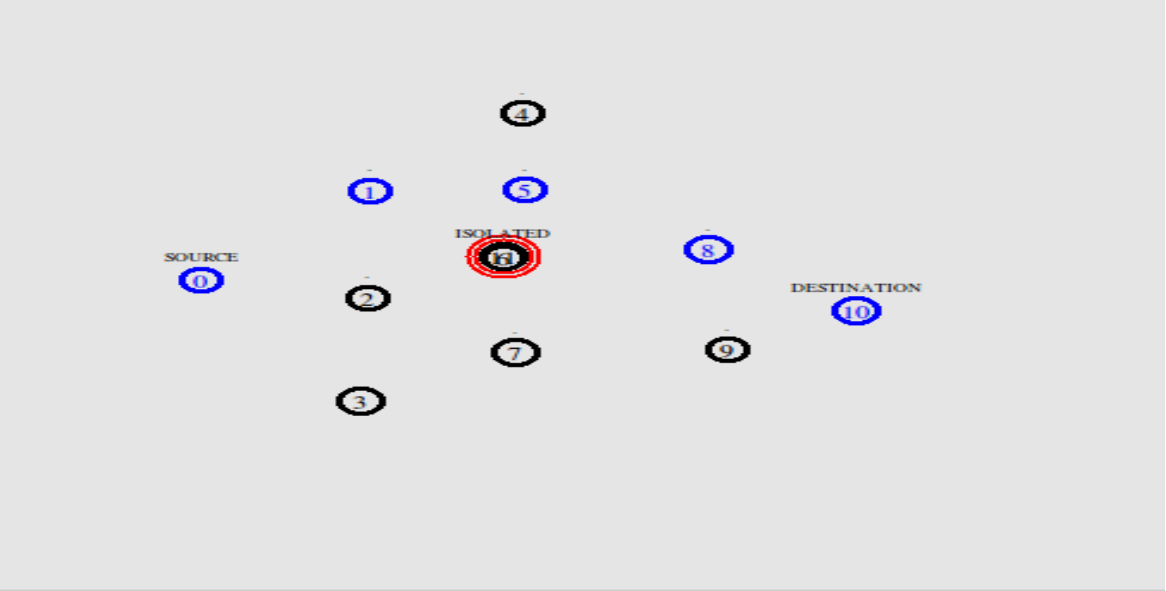

Figure 21: Isolated Black Hole Node

Now the source node will select the new route and starts sending of data packets with the new route. Source node firstly send some rough data and verify it using cross checking mode.

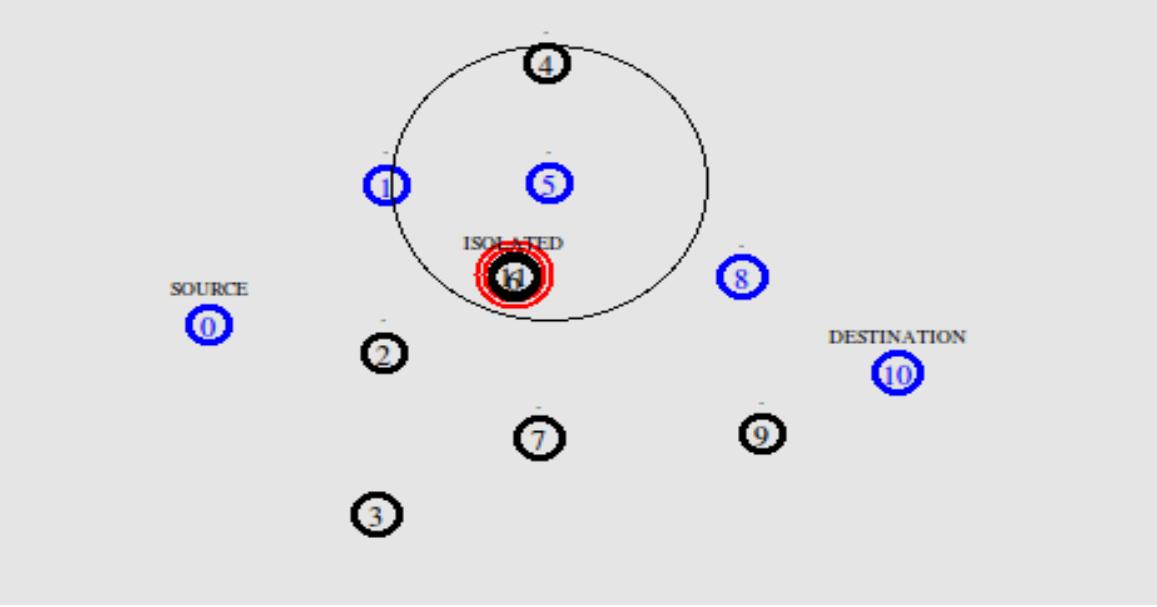

Figure 22: New Selected Path

Source node will send the rough data to the destination node to verify the new path. Rough data contains 50 data packets that source node will transmit to destination node. The verification of the path is done using a technique called cross checking.

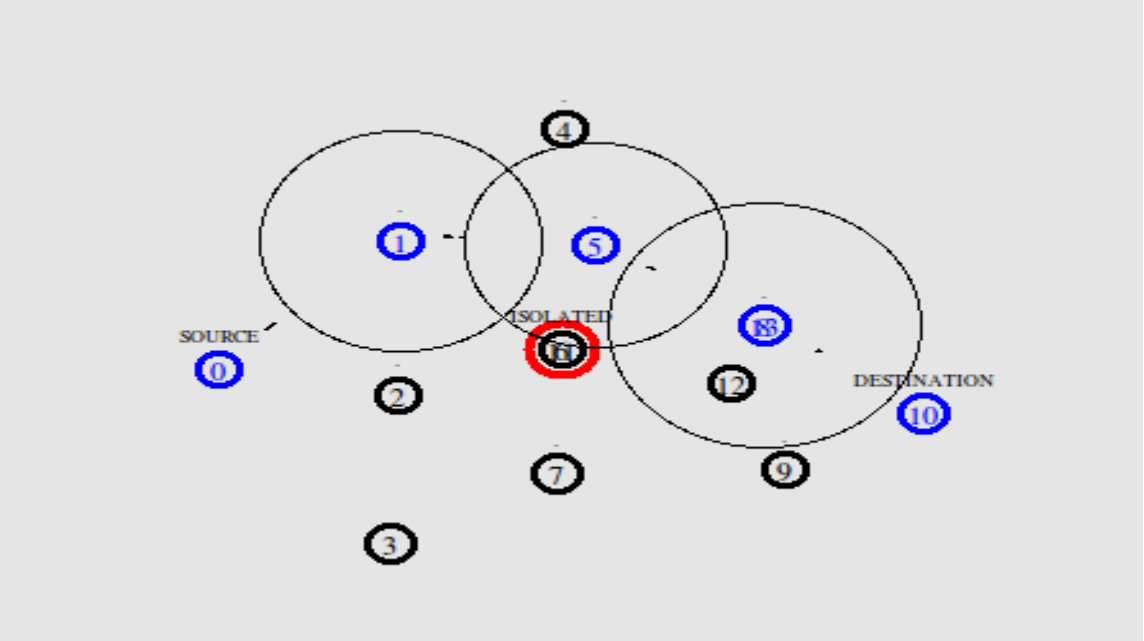

Figure 23: Rough Data Transmission

After sending the 50 rough data packets to the destination node, source node will enable the cross checking mode. Cross checking mode is the one in which the source node will send some rough data to the destination and verify it with the other nodes present in the network. If any node receiving more number of data packets and forwarding very less number data packets will consider as malicious gray hole node. Now in the below figure, source node starts cross checking the node 1 with the node 2. Source node will verify the number of data packets received by the node 2 and number of data packets forward by the node 2.

Node 2 shows that it has received 50 data packets and also forward the 50 data packets. Source node will verify the node 2 as normal node because node 2 forwards all data packets it has received.

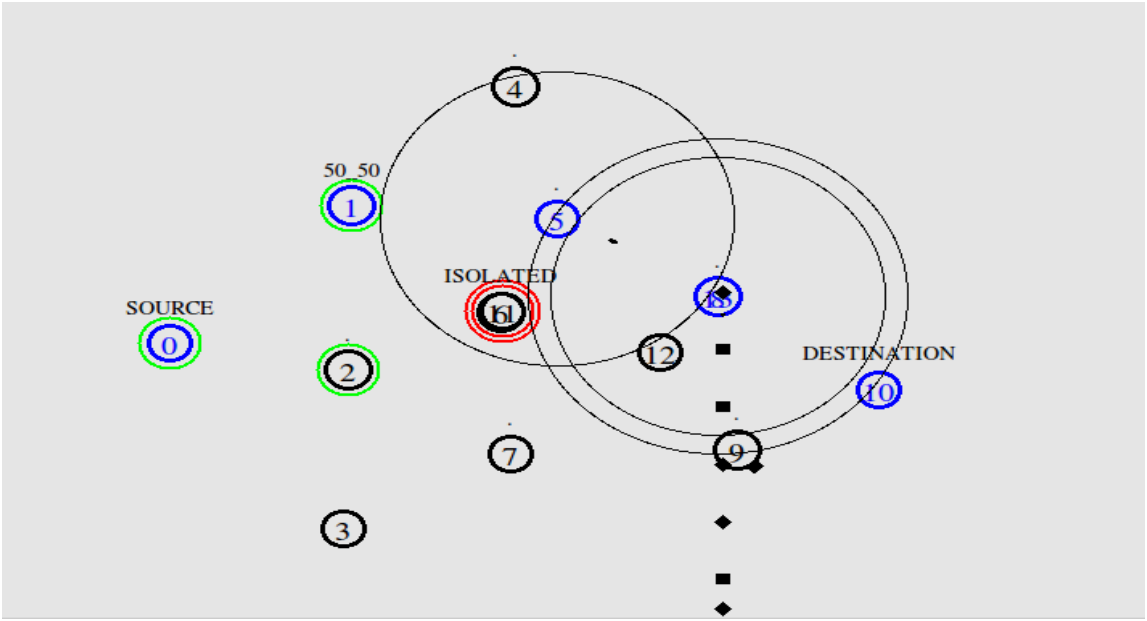

Figure 24: Cross Verification of Node 1

After cross verifying node 1, source node will cross verify the next node present in the selected path. Source node will verify node 5 using node 4. Source node will follow the path of node 2 and node 4 to cross verify node 5.

Node 5 shows that it has received a total number of 50 packets and forward total number of 46 packets to next node. Source node will compare the number of data packets and verify node 5 as normal node because node 5 is dropping very less number of data packets that can be due to presence of congestion in the network.

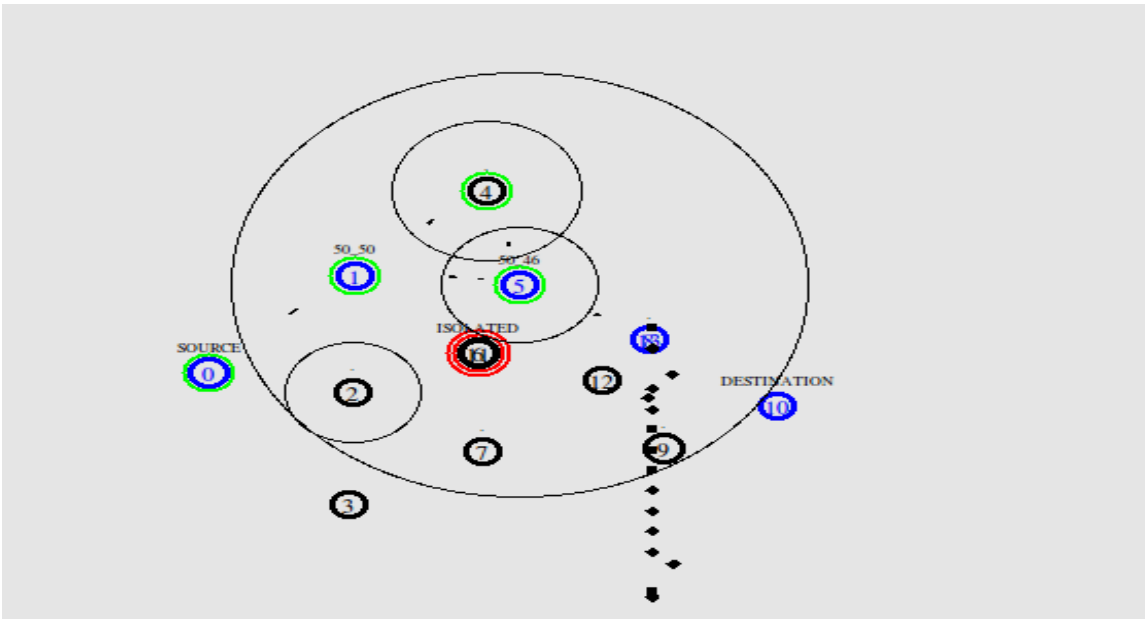

Figure 25: Cross Verification of Node 5

Source node will cross check the next node i.e. node 8. Source node will verify the node 8 using node 12. The path source node will use to cross check node 8 is through node 2 and node 7.

Source node checks that node 8 is receiving total number of 50 data packets but only forwarding the total number of 20 data packets. Node 8 is dropping 30 data packets which is very heavy data dropping rate. The packet dropping ratio of node 8 is almost equal to 60%. Therefore source node will declare the node 8 as malicious gray hole node because node 8 is only forwarding selective data to the destination node and dropping all the other data.

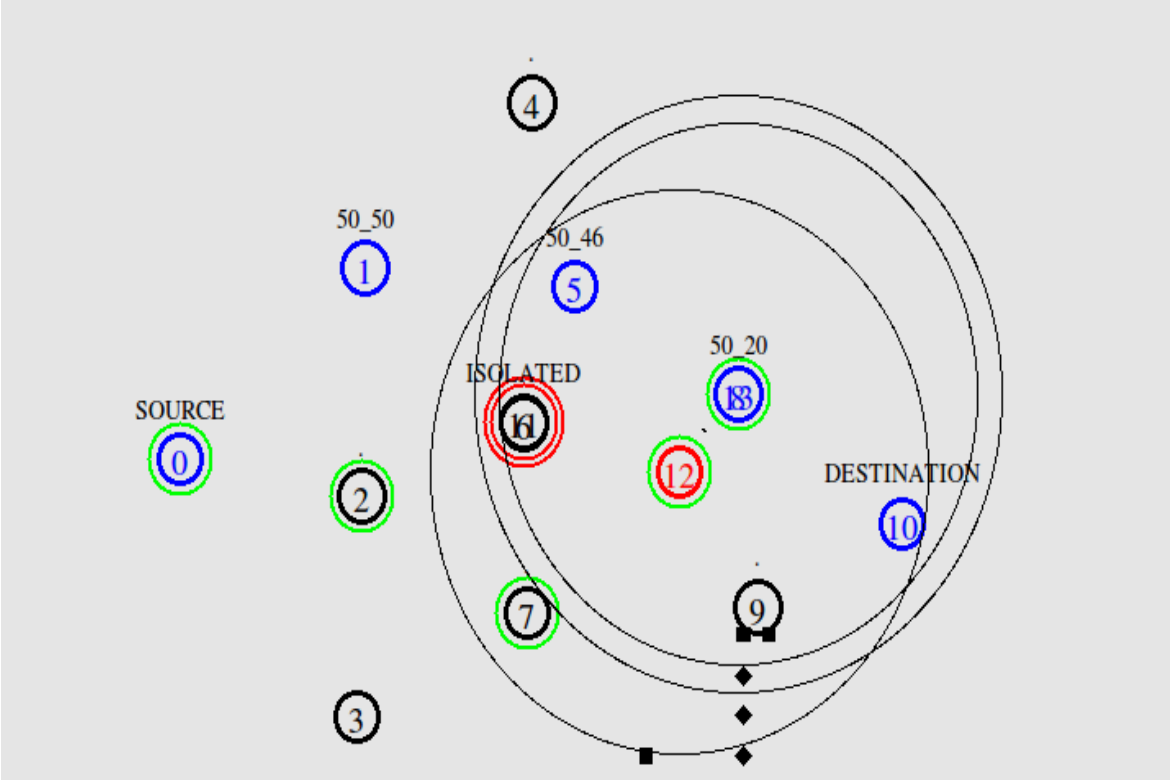

Figure 26: Cross Verification of Node 5

The below figure is showing the nature of gray hole node which will only forward selective data packets to the next neighbor node and drops all the other data packets. Gray hole node sometimes act as normal node and sometimes it act as an malicious node.

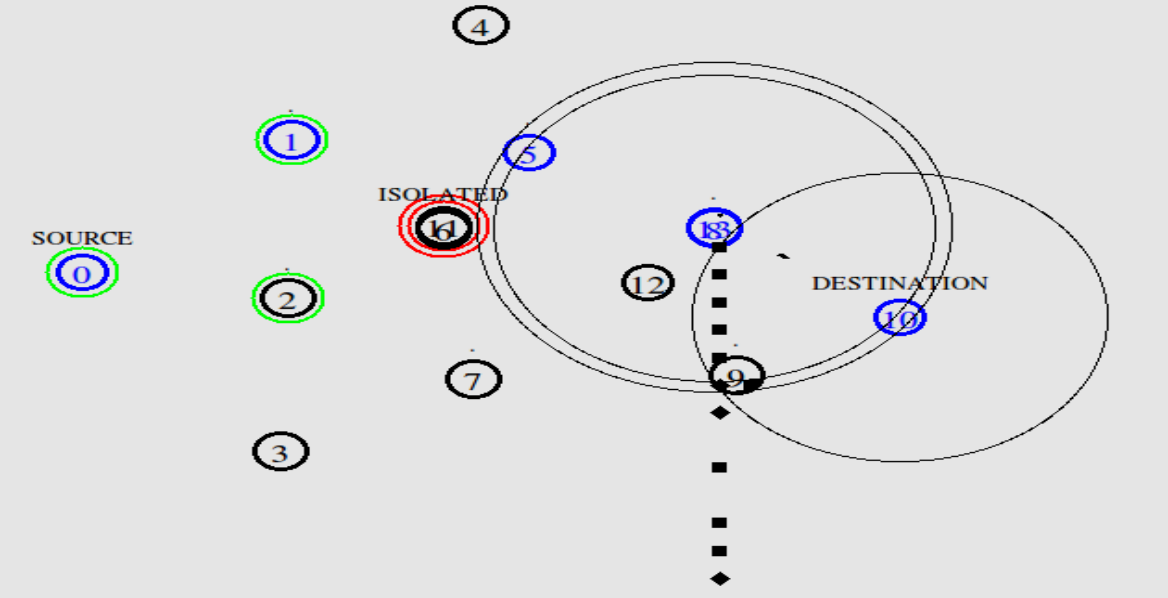

Figure 27: Gray Hole Node Forwarding and Dropping Data

Source node finds that node 8is only forwarding selective data packets to the destination node and dropping all other data packets and acting as a malicious node. Source node will isolate the node 8 in the network.

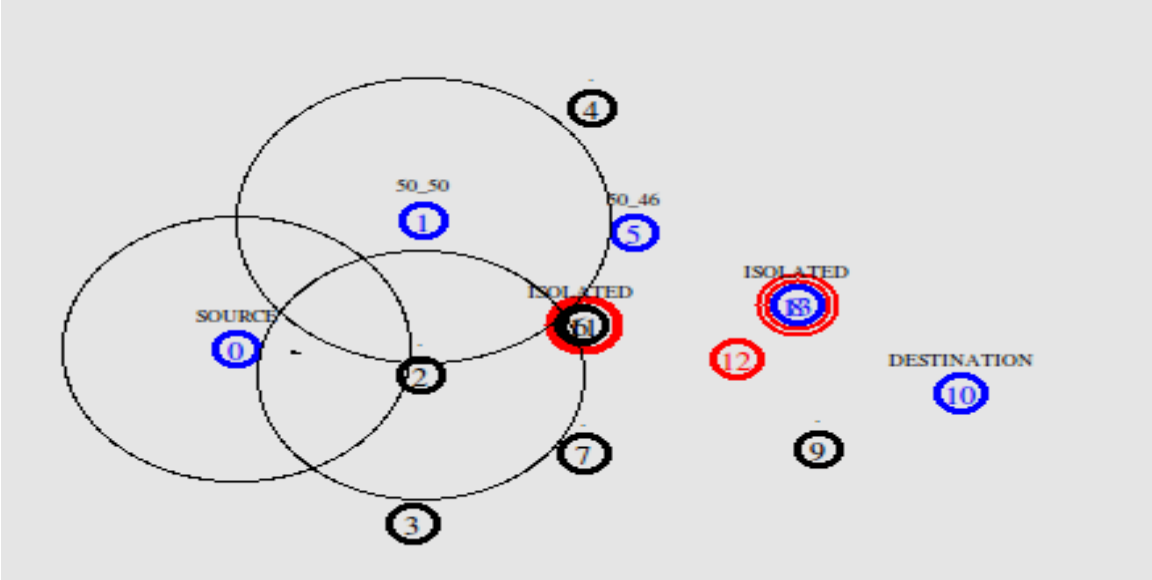

Figure 28: Isolated Gray Hole Node

Due to presence of malicious node in the previous path source node will select the new path to transmit the data to the destination. Source node select the path though node 2, nose 7 and node 9. Source node starts transmitting data through new path.

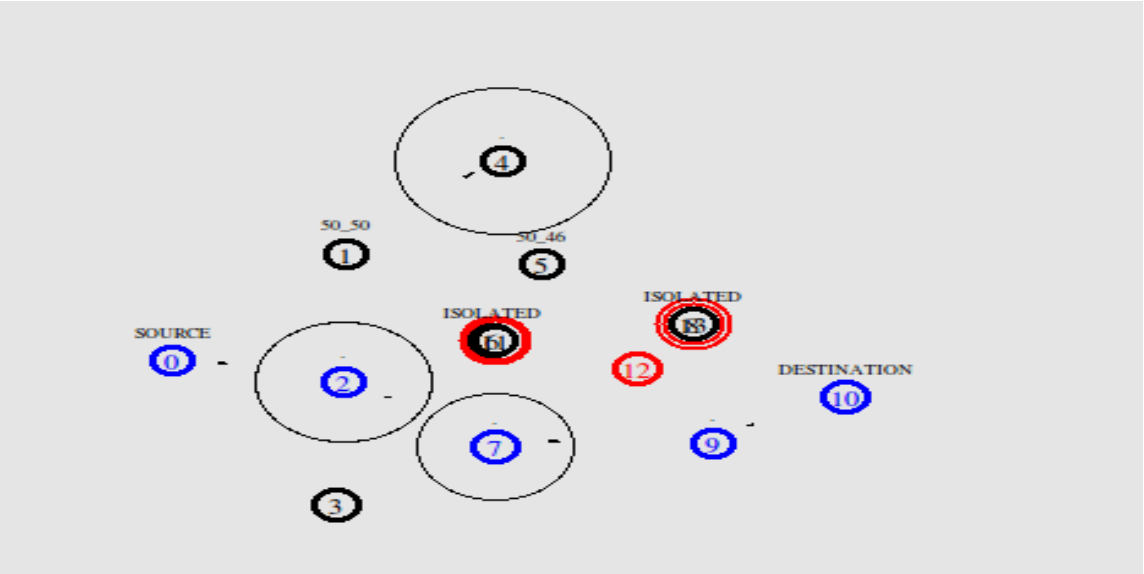

Figure 29: Selected New Path

Destination node will send the acknowledgement of the received data with another path so that no other malicious node can make changes in the acknowledgement. The new path destination node will follow is through node 12, node 5, node 1.

The way of sending acknowledgement with another path make the ad hoc network more secure and reliable.

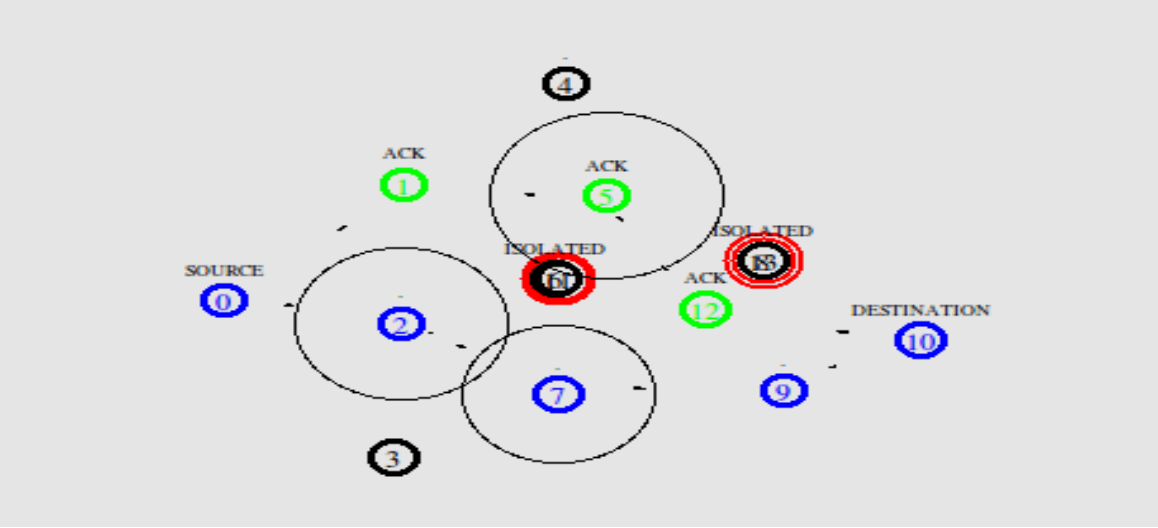

Figure 30: Acknowledgement of Transmitted Data

4.2 TABLES

Tables are used in the network for routing purpose and as well as detecting the malicious node in the network. In MANET every node has its routing table to route the data packets from source to destination. Also nodes have to maintain some additional tables such as DRI table, Malicious Node table to make the Adhoc network more secure and reliable.

4.2.1 Malicious Nodes Table

Malicious node table is used to detect the number of malicious node present in the network. Malicious node table will keep the record of every node present in the network. The table uses two values i.e. 0 and 1, 0 value refers to normal node while 1 value refers to malicious node. Initially each node will consider as normal node and have value 0 but as soon as any node behaving like malicious node the value will change to 1 and the node will be isolated from the network.

In the proposed scenario there are two malicious node present in the ad hoc network, one is the black hole node and the other one is the gray hole node.

Table 2: Malicious Node Table

NORMAL NODE = 0	MALICIOUS NODE =1
NODE 0	= 0
NODE 1	= 0
NODE 2	= 0
NODE 3	= 0
NODE 4	= 0
NODE 5	= 0
NODE 6	= 1
NODE 7	= 0
NODE 8	= 1
NODE 9	= 0
NODE 10	= 0
NODE 11	= 0

4.2.2 Data Routing Table (DRI)

Data Routing Information (DRI) table is also another most important table because DRI table is used to detect the malicious node in the network. DRI table will check the through and from values of all the nodes present in the route. DRI table contains two types of value i.e. 0 and 1. Here 0 in from table refers that node has not receive the data while in through table it refers that node has node send the data. On the other hand 1 in from table refers that node has successfully receive the data and in through table it refers that node has successfully send the data to next node. If any node find with 0 through value, the node will be consider as the malicious node and isolated from the network.

The proposed solution uses the DRI table for detecting the black hole node in the ad hoc network. The values of DRI table helps to detect the black hole node in the network.

Table 3: DRI Table

DRI TABLE

NODE ID	FROM	THROUGH
NODE 0	= 1	1
NODE 1	= 1	1
NODE 2	= 1	1
NODE 3	= 1	1
NODE 4	= 1	1
NODE 5	= 1	1
NODE 6	= 1	0
NODE 7	= 1	1
NODE 8	= 1	1
NODE 9	= 1	1
NODE 10	= 1	1
NODE 11	= 1	1

4.2.3 Black Hole Node Table

Black hole node table is used to indicate the number of black hole node present in the ad hoc network. Black hole node table display the node acting as malicious black hole node in the network. Black hole nodes are those nodes which drops all the data packets instead of forwarding it to the next neighbor nodes. The nodes acting as malicious black hole node will contain the value 1 and node performing as normal node contains the value 0.

The proposed ad network only contains a single black hole node in the ad hoc network. Node 6 is acting as black hole node therefore it holds the value 1 and all other nodes contains the value 0.

Table 4: Black Hole Node Table

NORMAL NODE = 0	Black Hole Node =1
NODE 0	= 0
NODE 1	= 0
NODE 2	= 0
NODE 3	= 0
NODE 4	= 0
NODE 5	= 0
NODE 6	= 1
NODE 7	= 0
NODE 8	= 0
NODE 9	= 0
NODE 10	= 0
NODE 11	= 0

4.2.3 Gray Hole Node Table

Gray hole nodes are those nodes which drops selective the data packets and forwards the other data packets to the next neighbor nodes. Gray hole node table is used to indicate the number of gray hole node present in the ad hoc network. Gray hole node table display the node acting as malicious black hole node in the network. The nodes acting as malicious gray hole node will contain the value 1 and node performing as normal node contains the value 0.

The proposed ad network only contains a single gray hole node in the ad hoc network. Node 8 is acting as black hole node therefore it holds the value 1 and all other nodes contains the value 0.

Table 5: Gray Hole Node Table

NORMAL NODE = 0	Gray Hole Node =1
NODE 0	= 0
NODE 1	= 0
NODE 2	= 0
NODE 3	= 0
NODE 4	= 0
NODE 5	= 0
NODE 6	= 0
NODE 7	= 0
NODE 8	= 1
NODE 9	= 0
NODE 10	= 0
NODE 11	= 0

4.3 PERFROMANCE COMPARISON GRAPHS

The Performance of the Networks are discussed below in the form of throughput, packet drops and delay in the network.

Throughput: In this graph throughput comparison between both scenarios is shown. Here the green curve is showing the throughput for old case and red curve is showing the throughput for new case. Due to the more packet loss in the old scenario the throughput is less and because of the prevention of attack in new case throughput rate is high.

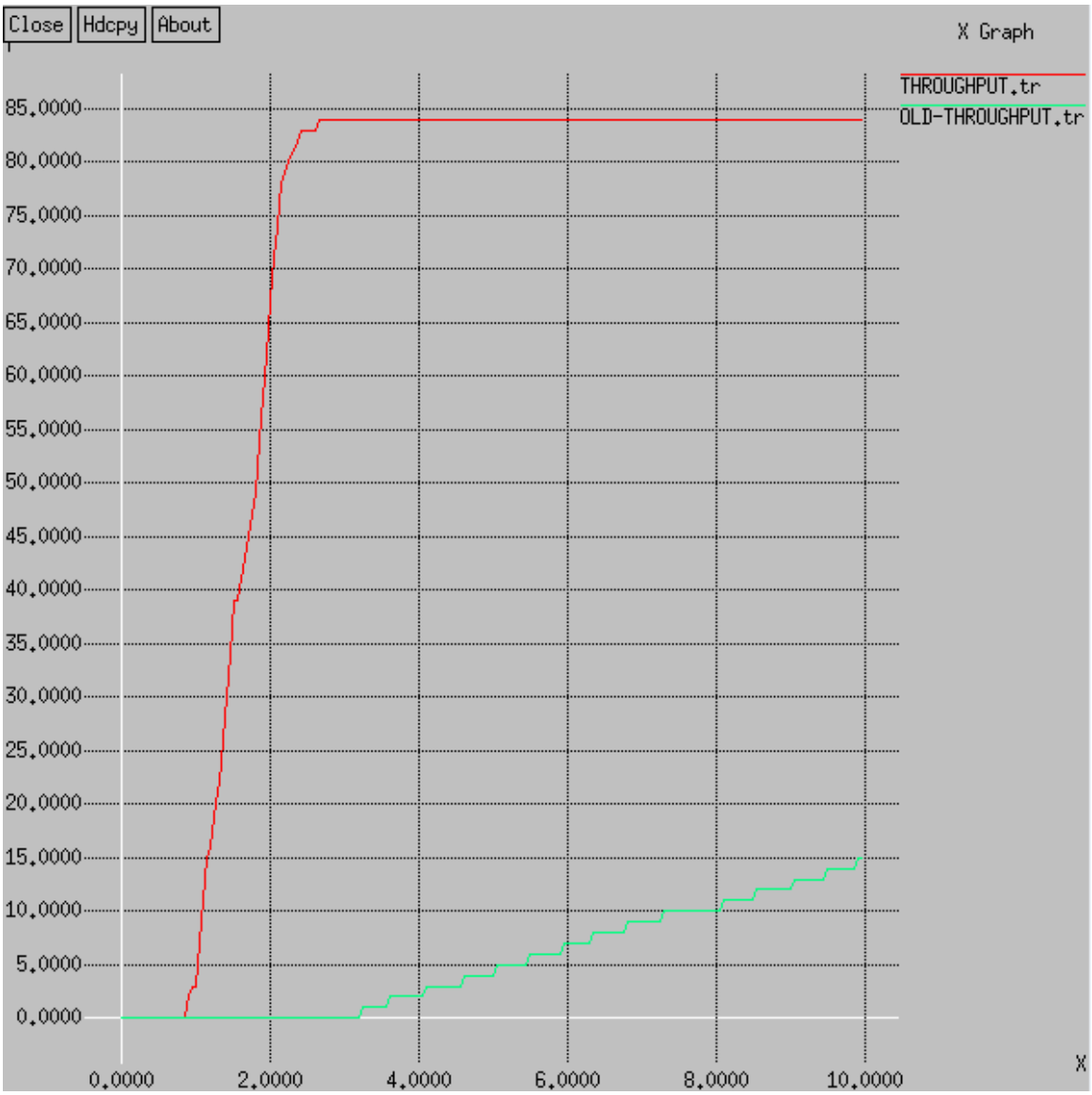

Figure 31: Throughput Graph

Congestion: Here the following graph is showing the congestion between both the scenarios. In the following graph the green curve is showing the congestion of the old case and the red curve is showing the congestion in the new case. In the old case due to the regular black and gray hole attacks in the network the congestion in the network increases because source node has to resend the data number of time but in new case because of the prevention of these Black and Gray hole attacks the congestion in the network gradually decreases.

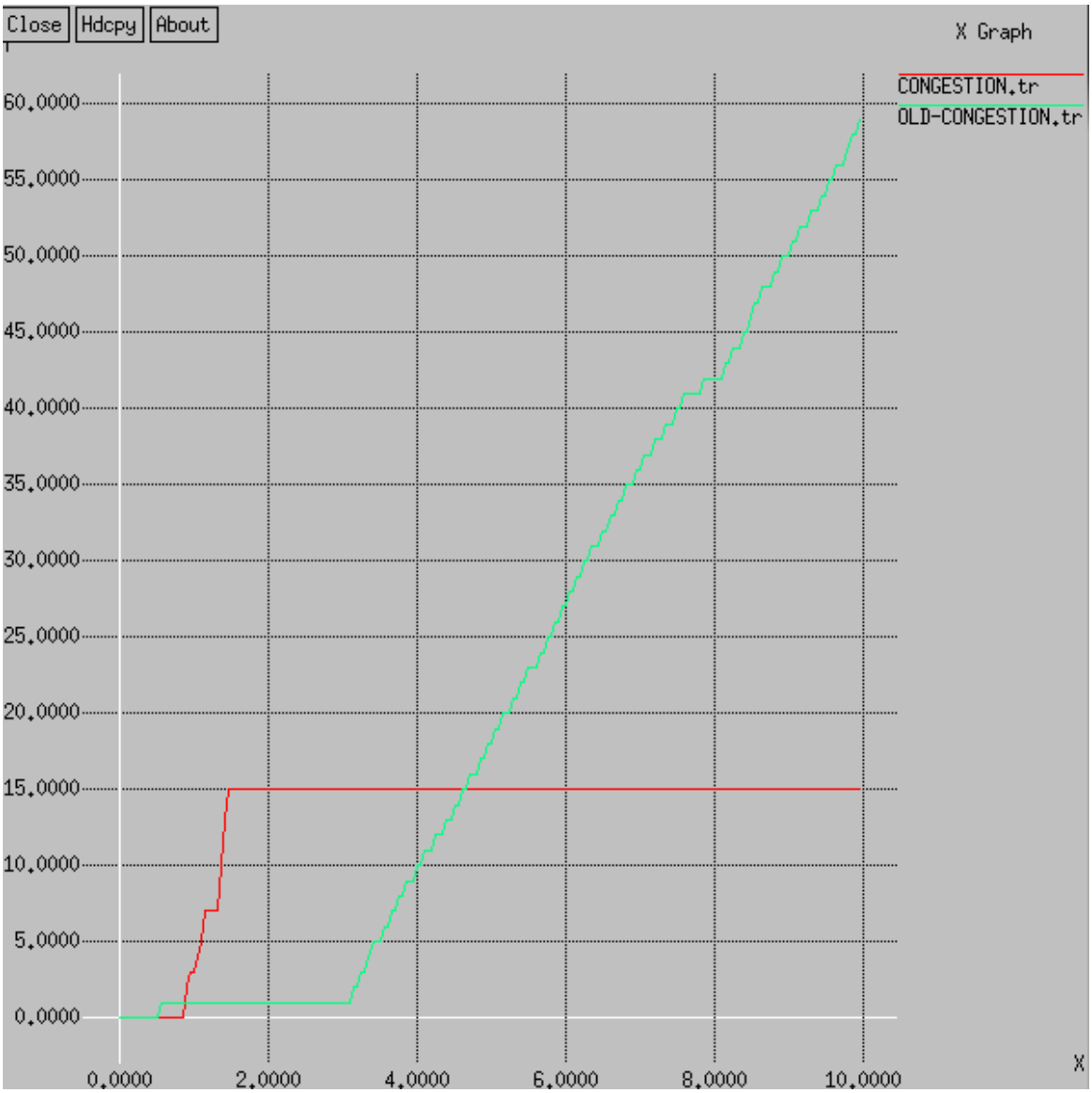

Figure 32: Congestion Graph

Packet Drop: In the following graph the comparison between of packet drop between both the scenarios is shown. The green curve shows the packet drop of the old case and the red curve shows the packet drop of the new case. Because of more congestion and regular Black and Gray hole attacks in the network the packet drop in the old case is very high but in new case because of the prevention of these Black and Gray hole attacks the packet drop in the network is less.

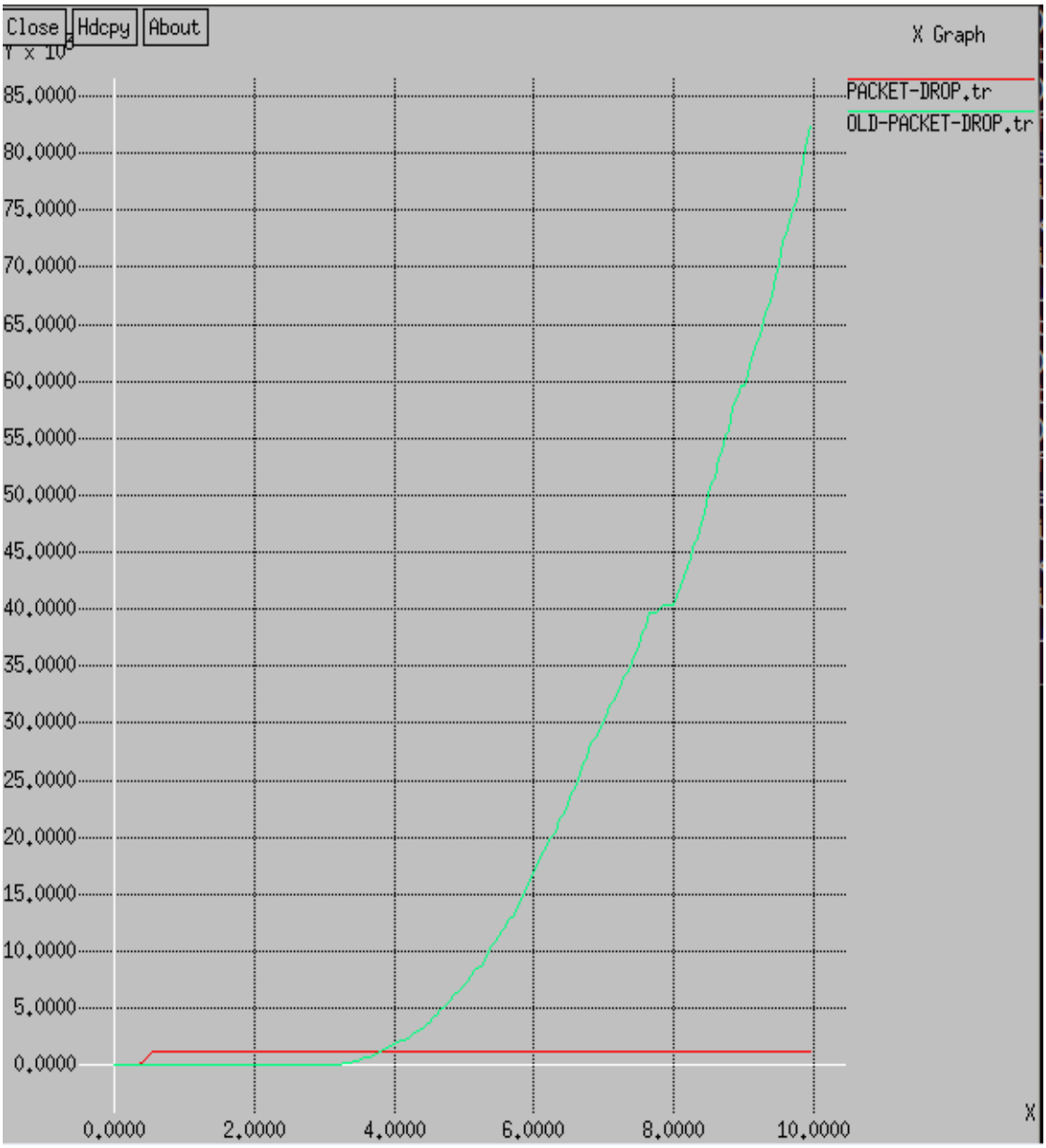

Figure 33: Packet Drop Graph

4.3.1 Basic AODV vs New Proposed Protocol Performance Comparison

The graph below is showing the comparison between the performances of basic AODV routing protocol with the new enhanced routing protocol with more reliable security mechanism. The graph compares the performance of basic AODV protocol with new improved protocol when the malicious gray hole node attacks in the network in terms of throughput. The basic AODV working normally but when malicious node attack in the network the performance of AODV decreases but on the other side improved protocol become stable and handled the attack very carefully.

The comparison shows that the designed enhanced protocol handled the attack very intelligently without any falls in the performance.

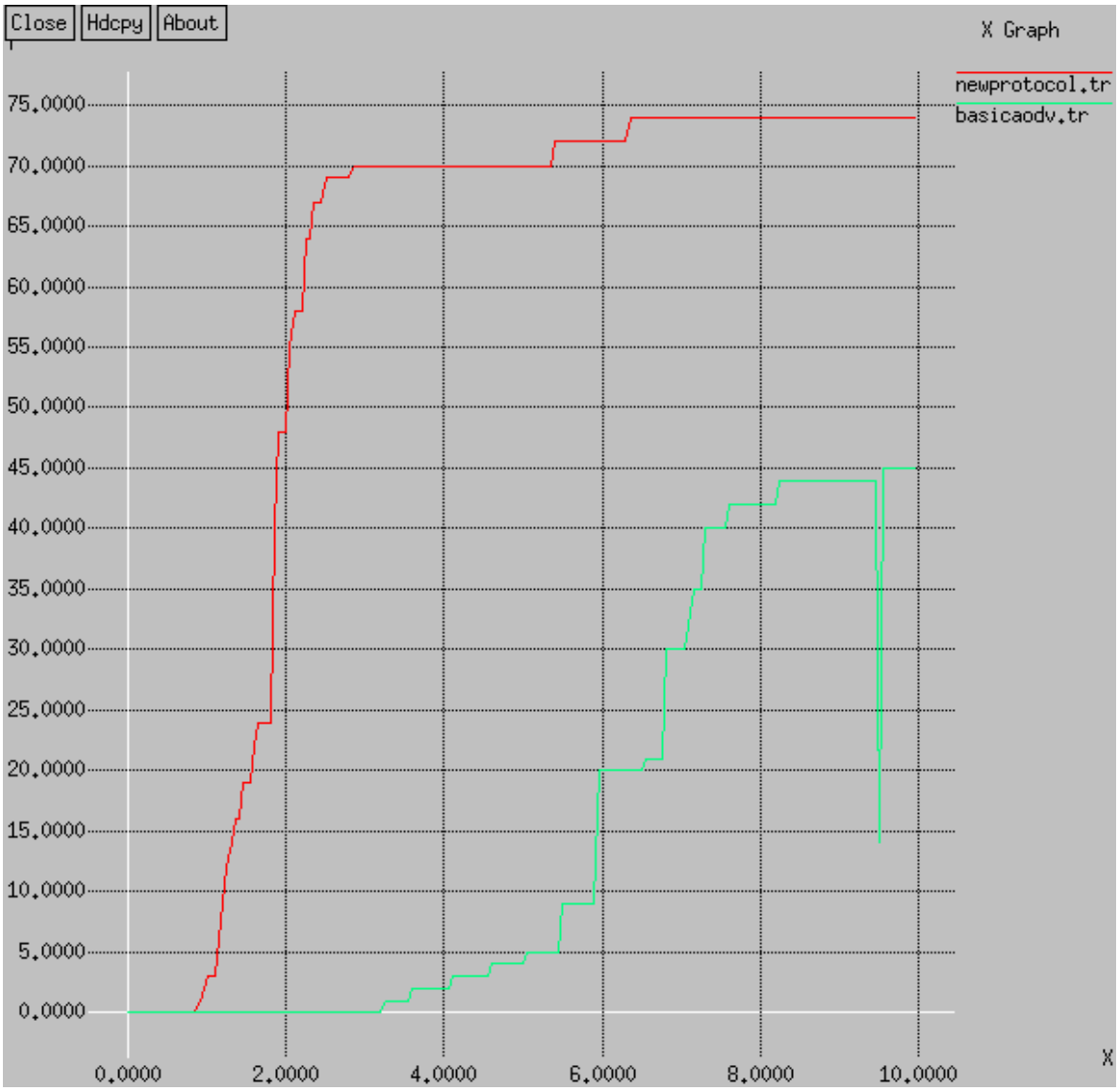

Figure 34: Basic AODV vs Changed AODV

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

Mobile Adhoc Network is a self-organizing type of network which can be made on the fly. In Mobile Adhoc Network nodes are free to join or leave the network at any time. This property of MANET makes it more vulnerable to attacks therefore security has become one of the major limitation of MANET. Security of MANET depends on how much secure route is available to route the data packets from source to destination. Black and Gray hole attack is one of the major attack that will held on MANET. Black hole nodes will drop all the packets whereas Gray hole node will drop selective data packets. The misbehaving and the malicious node can cause a severe damage to the Mobile Adhoc Network if they are not taken care of. In this study we have implemented both Black hole and Gray hole attacks and also showed how our proposed technique can be helpful for detecting and preventing such types of attacks. In this study we analyzed the effects of black and gray hole attacks in an AODV based MANET. For this purpose we have modified and implemented AODV protocol. The simulation is done using network simulator (NS2). From our simulations we can easily find out that normal AODV has very less packet drop, congestion and high throughput but after including the malicious nodes in the network throughput decreases drastically and packet drop increases very highly. When include the proposed technique for Black and Gray hole attacks, it is observed that the throughput of the network again increases and packet loss decreases at very high rate. The result show that using the proposed technique with AODV protocol will increase the efficiency of the network and make it more secure for the communication.

The future work of the research is to enhance proposed technique to detect the cooperative black hole attacks in the network. Also the technique will be tested in more mobility environment where the nodes can move more freely in the ad hoc network and where the number of nodes are very less. In further implementations, we will increase the number of mobile nodes and evaluate the proposed scheme under this scenario.

REFERENCES

[1] B. G. A. A. Meghna Chhabra, "A Novel Solution to Handle DDOS Attack in MANET," *Journal of Information Security*, pp. 165-179, 2013.

[2] M. ARORA, "A Review of Detection & Prevention Techniques," *International Journal for Research in Applied Science & Engineering*, vol. Volume 2 , no. Issue XI, pp. 470-473, 2014.

[3] K. Prajapati, "Slideshare," [Online]. Available: http://www.slideshare.net/Kunal1194/study-of-security-attacks-in-manet. [Accessed 28 March 2015].

[4] S. G. T. J. L. K. &. B. Marti, "Mitigating routing misbehavior in mobile ad hoc networks," *ACM*, pp. 255-265, 2000.

[5] S. Banerjee, "Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks," in *proceedings of the world congress on engineering and computer science*, 2008.

[6] S. e. a. Ramaswamy, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks," in *International Conference on Wireless Networks*, 2003.

[7] P. V. P. a. R. R. Goyal, "Manet: Vulnerabilities, challenges, attacks, application."," *IJCEM International Journal of Computational Engineering & Management* , pp. 32-37, 2011.

[8] H. N. N. a. F. K. Khattak, "Preventing black and gray hole attacks in AODV using optimal path routing and hash," in *10th IEEE International Conference*, 2013.

[9] H. K. a. R. Singh, "A NOVEL APPROACH TO PREVENT BLACK HOLE ATTACK IN WIRELESS SENSOR NETWORK," *IJARET*, 2014.

[10] S. e. a. Kurosawa, " Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method," *J Network Security*, pp. 338-346, 2007.

[11] J. S. K. a. A. U. Sen, "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks," in *Second International Conference on IEEE, 2011*, 2011.

[12] Y. F. a. Z. C. X. Alem, "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection," in *2nd International Conference on. Vol. 3. IEEE*, 2010.

[13] H. e. a. Yang, "SCAN: self-organized network-layer security in mobile ad hoc networks." Selected Areas in Communications," *IEEE Journal*, pp. 261-273, 2006.

[14] R. G. S. K. D. Piyush Agarwal, "Cooperative Black and Gray Hole Attacks in Mobile Adhoc Networks," in *2nd International conference on Ubiquitous Information Management and Communication*, Suwon,Korea, 2008.

[15] C. C. M. G. E. L. G. Carofiglio, "Route stability in MANETs under the random direction mobility model," in *Mobile Computing, IEEE Transactions on 8, no. 9*, 2009.

[16] M. G. Sung-Ju Lee, "AODV-BR: Backup routing in ad hoc networks," in *Wireless Communications and Networking Confernce, 2000. WCNC. 2000 IEEE. Vol. 3.*, 2000.

[17] M. e. a. Abdelhaq, "A local intrusion detection routing security over MANET network," in *IEEE Conference* , 2011.

[18] E. t. E. D. A. o. P. O.-d. R. Protocols, "Taneja, Sunil, and Amandeep Makkar".

[19] A. H. B. Mohamed, "Analysis and Simulation of Wireless Ad-Hoc Network Routing Protocols," *Universiti Putra Malaysia*, 2004.

[20] B. e. a. Wu, "A survey of attacks and countermeasures in mobile ad hoc networks," *Springer US*, pp. 103-135, 2007.

[21] E. G. a. K. S. Nilsson, "Ad Hoc Networks and Mobile Devices in Emergency Response–a Perfect Match," *Springer Berlin Heidelberg*, pp. 17-33, 2010.

[22] J. e. a. Hoebeke, "An overview of mobile ad hoc networks: Applications and challenges," *Journal-Communications Network*, pp. 60-66, 2004.