SECURE MESSAGE TRANSMISSION DURING HANDOFF IN WIRELESS MESH NETWORKS

Project report submitted in partial fulfillment of the requirement for the degree of Bachelor of Technology

In

Computer Science and Engineering

By

Pankaj Thakur (151417)

Pragya Chakshoo Saklani (151418)

Under the supervision of

Dr. Geetanjali Rathee

To

Department of Computer Science & Engineering

Jaypee University of Information Technology Waknaghat, Solan-173234, Himachal Pradesh

CANDIDATE'S DECLARATION

I hereby declare that the work presented in this report entitled **"Secure Message Transmission During Handoff in Wireless Mesh Networks(WMN)"** in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering/Information Technology** submitted in the department of Computer Science & Engineering and Information Technology**,** Jaypee University of Information Technology Waknaghat is an authentic record of my own work carried out over a period from August 2018 to December 2018 under the supervision of **Dr. Geetanjali Rathee**(Assistant Professor (Senior Grade) in the department of Computer Science and Engineering at Jaypee University of Information Technology, Waknaghat, Solan, INDIA).The matter embodied in the report has not been submitted for the award of any other degree or diploma.

(Student Signature)	(Student Signature)
Pankaj Thakur, 151417	Pragya Chakshoo Saklani, 151418

This is to certify that the above statement made by the candidate is true to the best of my knowledge.

(Supervisor Signature)
Dr. Geetanjali Rathee
Assistant Professor (Senior Grade)
Computer Science and Engineering
Dated:

ACKNOWLEDGMENT

We have put a lot of effort into this project. But this was not possible without the kind support and help of many people. We thank all of them sincerely. **Dr. Geetanjali Rathee** is very grateful to us for providing leadership and continuous supervision as well as providing us with the necessary information about our project and for supporting our project completion. We would like to give special thanks and appreciation to our friends and colleagues who have given us time and attention.

Pankaj Thakur   Pragya Chakshoo Saklani

Dated:

TABLE OF CONTENTS

ANALYSIS

LIST OF ABBREVIATIONS

AODV	Ad hoc On-Demand Distance Vector
AMMNETs	Autonomous Mobile Mesh Networks
AS	Authentication Server
BFTR	Best effort fault Tolerant Routing
BS	Base Station
CCC	Common Control Channel
CRAHNs	Cognitive Radio Networks
CR	Cognitive Radio
CRN	Cognitive Radio Networks
DRI	Data Routing Information
ETT	Expected Transmission Time
ETX	Expected transmissions
FREQ	Following Route Request
IN	Intermediate Node
MAC	Media Access Control
MANETs	Mobile Ad Hoc Networks
MAPs	Mesh Access Points
MC's	Mesh Clients
MR's	Mesh Routers
MPs	Mesh Points
MGs	Mesh Gateways
NAM	Network Animator
NHN	Next Hop Neighbor
NS2	Network Simulator
OTcl	Object-oriented tool command language
PU	Primary User
QoS	Quality Of Service
RREP	Route reply
RREQ	Route request
RF	Radio Frequency

SAMER	Spectrum-aware mesh routing
SU	Secondary User
UML	Unified Modeling Language
VoIP	Voice over Internet Protocol
WMN	Wireless Mesh Networking

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Wireless Mesh Networking (WMN) is regarded as a promising key technology of the next generation. This is attractive or absurdly expensive in areas where the infrastructure already exists for its multi-hop, self-healing, self-organizing and dynamic properties. Progress in Network technologies have enabled companies to use the network for more than just sharing. resources, but also to store a large amount of data for analysis. Therefore, the security of this data is very high Whenever an MC moves outside the limits of your current service mesh router, thenthe corresponding signal-to-noise ratio (SNR) of this MR service falls due to the signal attenuation. A significant reduction in the SNR ratio causes the MC to search for a new mesh router have a good signal strength to continue their network services by activating the handover. Since, the nodes are dynamic, unstable and limited by security disputes with new Performance issues, a significant delay in handoff procedure may cause copious performance concerns such as network attacks and delay in the network. Therefore, during transmission it is a prerequisite that roaming customers have a comprehensive access authentication process in place that does not only with a short delay, but also with reinforcement for outpatient customers with handover networks. In addition, if a node is an inter-domain (communication between two domains), or Intra-domain (communication within a domain) wants to send some messages to its recipient the information is exchanged between several MRs. However, to prevent that Data exposure at each intermediate node, the messages should be encrypted by some security techniques or an ornate encryption technique that is required to ensure that even if the message is faked by an intruder, you may not be able to decrypt it anyway. Due to the dynamic character of the WMN, in which information about several hops or MR is transmitted, the time of data encryption is considered an important parameter. In addition, the most important factor that affects WMN performance is the type of basic routing protocols used to promote data packets. The presence of a malignant or misbehaving node within a routing path can interrupt network activity either by spoofing or by reducing data or by compromising the overall performance of the network.WMN is another developing field with its potential applications in to great degree erratic and dynamic situations. However, it is especially helpless because of its highlights of open medium, unique evolving topology, agreeable steering calculations. The article reviews the best in class in security for remote work systems. Right off the bat, we break down different conceivable dangers to security in

remote work systems. Secondly, we present some delegate arrangements to these dangers, including answers for the issues of key administration, secure system directing, and interruption location. We likewise give a correlation and talk of their individual benefits and disadvantages, and propose a few enhancements for these downsides. At long last, we additionally examine the remaining challenges in the zone.

Although the number of scientists/researchers has suggested various handover authentications procedures with message encryption and secure routing techniques, but the problems occur. By the intruders who encounter a variety of malicious nodes or threats to disrupt the network performance. In addition, by increasing one parameter that ensures security, other parameters (such as end-to-end delay, network throughput, packet delivery ratio) are affected drastically. Therefore, it is necessary to propose an efficient security technology with the following features reduced authentication delay, shorter encryption/decryption time and secure routing mechanism against routing layer attacks with the aim of optimizing the other network parameters. Security is therefore provided to ensure an efficient and secure communication process. Secured in three different aspects, e.g. authentication of Handoff clients, encrypted message transmission between source and destination and reliable route finding for routing of the transferred data packets. In the future, every MC that joins the network will have to be equipped with a unique key by the AS to identify the MC for authentication. Further studies that proposed algorithm is tested under high packet flow and large number of attackers (by taking into account black hole and wormhole attacks) and then their results are compared with those of various performances.

In mobile special networks (MANETs), the main requirement for establishing contacts between nodes is cooperation between nodes. When malicious nodes are present, this requirement can lead to serious security problems; for example, such nodes can disrupt the routing process. In this context, preventing or detecting malicious hosts launching grey hole or black hole attacks together is a complex task. This article attempts to solve this problem by developing a dynamic power supply (DSR) routing mechanism called a joint bait detection scheme (CBDS) that combines the benefits of both proactive and reactive protection. Our CBDS method implements a backtracking method to help you achieve your stated goal. Modeling results show that when attacked by malicious hosts, CBDS outperforms DSR, 2ACK and BFTR protocols (selected as benchmarks) in terms of packet delivery and routing costs (selected as performance metrics).

CHAPTER 1
INTRODUCTION

In this chapter we will get to know about what is WMN, what its role in our next generation, what is handoff and its types, why security is required in WNN, security goals and key challenges of WMN. We will also look forward about our problem statement and objective of our report.

1 WIRELESS MESH NETWORK

1.1 Introduction

Wireless Mesh Network (WMN) is an attractive and growing way of new communications because of low cost for the future, which is why it is becoming more popular in communications. In all kinds of networks, security is important for reliable, secure and robust communication. WMN networks are self-sufficient, configurable, and efficient. You do not have to mess with them after being demanded often, few jobs are needed to identify them, and they provide the best and most effective results you can achieve in your home. Network Solutions Fix a Specific Issue: covering large related areas, more than 1000 meters on one floor, especially where there is no Ethernet for use, to facilitate cable connections to have Wi-Fi router off, and wireless access point.

1.1.1 What is WMN?

A wireless network is any wireless network where data is transmitted through a network. The node present here sends as well as receives data, and also acts as a switch to other nodes and each node collaborates on data sharing across the network. Wireless networks can be considered as blocks of nodes where each network node is a router. Compare this with a Wi-Fi access point, where services can be provided in a range, and when it is off the connection is lost. The system hub works distinctively by sending the information to another piece that it is associated through an unfilled territory where the hub can be turned off. Figure 1 demonstrates one case for WMNs foundation. Work switch is commonly considerably more incredible than customer as far as calculation and correspondence abilities, and own a constant supply of power. Also, all of them regularly remain changeless as well as they provide associations and administrations to work with customers. The switches consequently set up and keep up work availability among them, making WMNs progressively self-sorted out and self-arranged systems. These highlights convey numerous advantages to WMNs, for example, low establishment cost, substantial scale arrangement, dependability, and self-administration. Despite the fact that there are many existing reported takes a shot at WMNs, there are a few difficulties should have been settled each one of the convention layers. Within the MAC layer, the difficulties are well heeled channel portion, productive range use among numerous radios, planning of streams for most extreme asset use, consistent versatility between heterogeneous WMNs, provisioning of various QoS measurements, and so forth. WMNs likewise require the improvement in MAC conventions in a multi-radio multi-channel design which fulfilled QoS measurements necessities, for example, end-to-end delay, parcel misfortune proportions, connect quality, impedance, and data transmission and defer jitter. The different research difficulties of steering convention for WMNs are referenced as pursues: propose present day directing measurements for new applications, structure multi-channel directing conventions that is versatile, productive, unwavering quality that fulfilled QoS measurements. Moreover, numerous applications require multi-throwing capacity. For instance, take a network system, in which video circulation is considered as a typical implementation. As of now; ample research work has taken place in multi-throwing over wired, however a touch of research has been done in multi-throwing wireless mesh networks for instance; stack adjusting calculation and multipath directing, security (validation and protection dependability), at last, decide and select the area of the extra work.

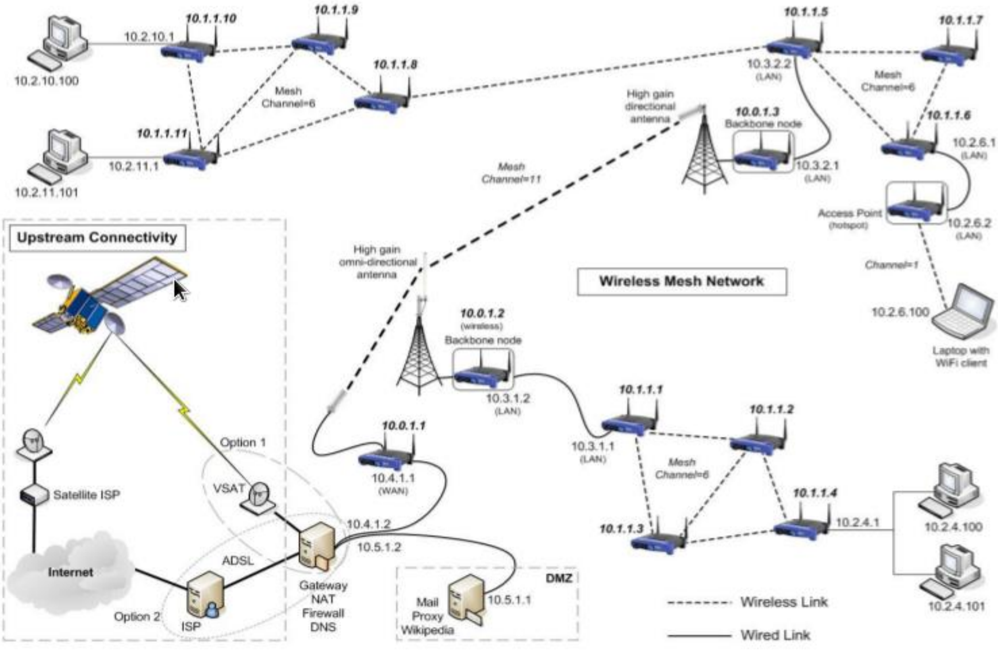


Figure 1.1 WMN Infrastructures

1.1.2 Handoff

Handoff means when a user from mobile used to travel from a single coverage area to another coverage area inside a call's duration then that call should transfer to the new coverage base station(BS). Or else, that call will lose its grip because the connection with the current BS begins to be weak as the mobile moves away. This caliber to shift call without dropping is referred to as automatic link transfer, handover, or handoff.

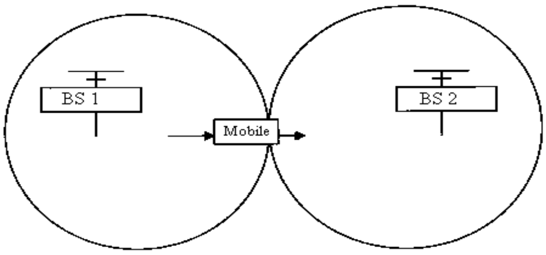


Figure 1 .2 Handoff

- **Types of Handoff**

a) Hard handoff

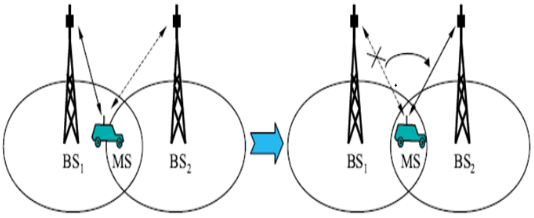


Figure1.3 Hard Handoff

b) Soft handoff

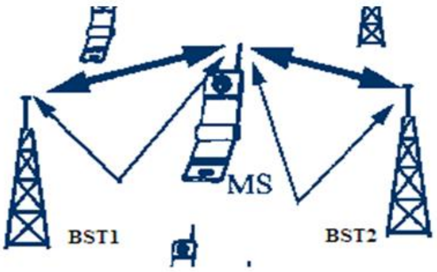


Figure 1.4 Soft Handoff

1.1.3 Need of security in WMN

Despite the ease of communication and the many advantages of network technology, it should be recognized that this technique of technology brings new risks. The reality for mobile network infrastructure is that mobile subscribers are likely to switch from one to another. Therefore, security issues become more important during the epidemic (customers can change their attachments while roaming). One of the biggest challenges for networking is to provide security as a key element in wireless communications. This is due to the fact that consumers are becoming more mobile. Due to the massive deployment of wireless technology that supports mobile mobility. A new generation of customers is trying to stay connected during their transition without the connection constraints. During the communication process, any network switch attempts to be completely transparent. Such requests increase the network exposure.

Authentication is an important step in predicting and combating WMN attacks. Authentication allows users who are eligible for network connections and prevent networkers from integrating and interrupting their work. An example of security mechanisms is a follow-up process to track attackers' signs and find out sources of threats, so procedures may be established to protect future anti-network networks. The rest of this section

1.1.4 Security Goals

For each program, the following common goals are required to ensure safety.

- **Confidentiality:** Communication between users is guaranteed, so the information cannot be disclosed to data theft.
- **Available:** The software must provide reliable DoS messages.
- **Authentication:** When the user sends a message, there are a number of process to identify the user to ensure that messages are sent by the sender, instead of being produced by someone else.
- **Robustness:** The whole route is protected to ensure that messages are not changed illegally or are not reposted during the transmission.
- **Permission:** Before a user does a specific job, there must be a mechanism to ensure that the relevant user has the right to do so.

1.1.5 Challenges

Along with the powerful and attractive features of the web, issues, challenges, and emerging opportunities that are addressed to find ways for network operators to offer innovative and unprecedented services. In this section we present various challenges to networking.

- **Mobility:** WMN cannot support more mobility for users. External layers need to change the frequency and adapt to the deceleration conditions normally attached to the phone's users.
- **Privacy:** User data traveling through multiple wireless devices on the wireless network. Customers will handle the secrecy of their information. User data must be protected from swallowing and reading by other users of the site.
- **Accounting and Bills:** WMNs require special accounting mechanisms and systems appropriate to the appropriate business model that take into account the benefits of mobile phone users and service providers. To ensure the availability and sustainability of the cross-border account accounting service, it is important for WMN.
- **Open and shared environment:** The radio spectrum is a shared resource in a wireless network where each node is connected through a multi-line connection to another node. This open atmosphere means the best target for the attacker.
- **Transparency:** WMN creates sections for broadcasting to many stores. So this type of network is transparent, it can use a high layer to provide efficient support for broader traffic and multiple channels, and even opt for the best route.
- **Justice:** This network must ensure fair sharing of the WMN bandwidth between consumers with the same rights. At the same time, WMNs need to balance each other to maintain the best service and ensure a stable connection.

1.2 Mobile Ad Hoc Networks (MANETs)

An ad-hoc wireless network is a combination of portable/semi-purpose hubs without pre-installation. Each hub has a wireless interface and communicates with each other by radio or infrared. Advanced collaborators PCs that specifically discuss with each others are a few cases of hubs in an ad-hoc network. The hubs of the ad hoc network are regularly portable. However, it may also include stationary hubs, for example, focusing on the web.

Semi-multi-purpose hubs can be used for the transfer of interest in territories where devolution is possible Figure 1.1 shows a basic ad hoc network with three hubs. The furthest hubs are not within the scope of the transmitter. However, the central hub can be used to advance bundles between the furthest hubs. The central hub serves as a switch and the three hubs have set up an ad-hoc network.

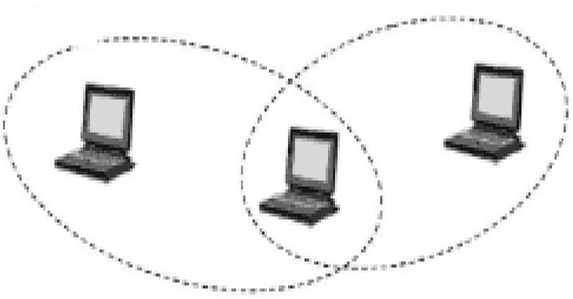


Figure 1.5: An Ad-Hoc Network

An ad hoc network does not use any concentrated administration. This is to ensure that the network will not fall out since one of the portable hubs moves outside the scope of the other's transmitter. The hubs should have the ability to enter or exit the network as they wish. Given the limited scope of the issuer of hubs, multiple bounce jumps could result in different hubs. Any hub that wants to support an interest in an ad hoc network has to transmit packets for different hubs. As a result, all platforms A hub can be considered as a conceptual element consisting of a router and an arrangement of associated portable hosts. Routers are substances that, in the addition of many other things manage a steering agreement. A hand-held host is only an IP-addressable host/element in the conventional operating system.

In addition, the ad hoc networks are well equipped to handle topology shifts and faults in hubs. It is resolved by reconfiguring the network. For example, if a hub is leaving the network and causing interface breakdowns, influenced hubs can, with no stretching, require new paths to be resolved. This has slightly widened the delay, but the network will be operational in any case.

Ad-hoc wireless networks take full advantage of the idea of wireless communication support. At the occasion of the end of the day on a wired network, its physical cabling is completed and the association is limited earlier. This enclosure is lacking in the wireless space and, given the fact that two hubs are within the range of the transmitter of each other, a prompt between them can be formed.

1.3 Problem Statement

The objective of this project is to discover black hole nodes in the network using a modified bait pattern, an prevent them by drawing up a blacklist and creating an optional pathway from source to destination which is not including every node of the black hole.

1.4 Objectives

The aim of this project is to develop a better and more secure system for MANETs, since MANETs are used in an extensive way. The security systems to prevent black hole attacks usually take a significant amount of time to determine the attack or have high calculation costs. We are offering a more efficient and simplified system for the detection as well as for the prevention of black hole attacks.

1.5 Organization of Report

This report is divided into 7 chapters.

CHAPTER 1: In this chapter we discussed the introduction of WMN and MANETs. Further the chapter discussed the handoff procedure in WMN, the security aspects during the WMN handoff. The need of the security during the communication in handoff with its goals and challenges is deliberated. Furthermore, the chapter introduces the problem statement and the objectives. Moreover the organization of entire report is presented in this chapter.

CHAPTER 2: In this chapter we discussed about the various analyses made by various analysts - their approach as well as the cessation they meet and also the upshots published so far. We also took a variety of framework of the project as well as the scope of the project.

CHAPTER 3: The main intention of this chapter is to introduce the readers to an architectural vision of NS2 as well as of our project. This section offers a concise introduction to NS2. In this chapter, we also saw a brief description of Software requirements, followed by Hardware requirements. In this chapter, we saw a brief description of Software Requirements, followed by Hardware requirements. The architecture of the system is shown in section 3.6 & data flow diagram is also shown in section 3.8.The functionality related to each component is also explained in briefly. At the end of this chapter provides detailed design of the project and further it explains the purpose and also the processing steps and brief explanation of the module.

CHAPTER 4: This chapter introduces the MANET networking concept and the other terms/methods/algorithms related to topic. It also provides you with information about MANET and attacks from the black hole and the existing methodologies used to detect and prevent black holes in MANET.

CHAPTER 5: In this chapter, we use a quantitative trial approach in which the trials were performed using the Network Simulator (version 2.34). This software was designed to run on ubuntu distribution of the Linux OS. Here experiments are done using NS2 platform. Further this chapter deals with various techniques that are used in the development of the project, beginning with the language and platform selection to explain the entire process of implementation steps.

CHAPTER 6: This chapter analyses the experiments carried out and the results obtained from these experiments. The delivery reports of the packages, the scope and the delay are calculated.

CHAPTER 7: This chapter shows that a modified bait plan will be effective in identifying and keep the attack on MANETs under control of the AODV protocol. The proposed algorithm will ensure the safety of the MANET topology and keep the black hole from the dynamic route. The offered work will be easy on weight and will provide the big throughput, a share of transportation of parcels with lower beam delays. Indeed, even within the visibility of black hole nodes, the reliability of the node holes the network stayed the same as a normal network. Based on the above results, we conclude that the proposed plan skillfully recognizes and prevents an attack on black holes in the mobile network (MANETs).

CHAPTER 2

LITERATURE SURVEY

In this chapter we discussed about the various analyses made by various analysts - their approach as well as the cessation they meet and also the upshots published so far. We also took a variety of framework of the project as well as the scope of the project.

The emergence over past few years of the ubiquitous computing technology has opened up larger and more promising possibilities to users living in rural, remote as well as developing countries. During the last decade, there has been greater progress in various new technologies like social networking, online gaming, Mobile Voice over Internet Protocol (VoIP), mobile cloud storage and video conferencing. All these technologies demand a very high speed communication Infrastructure that provides an efficient transportation system. Wireless Mesh Networks (WMNs) as well as Cognitive Radio (CR) technologies have become established as one of the most compelling high-speed wireless broadband solutions. The wireless mesh network is defined as a dynamic multi-shop network with the ability to organize and configure itself. The wireless mesh networks have conceptually grown from Mobile Ad Hoc Networks (MANETs) and have taken over the advancing as well as the self-configuration possibilities on or after the MANETs. At the same time, CR technology has been defined as a fully programmable wireless system capable of capturing its operating environment and intelligently adjusting its transmission parameters. Both these technologies can be combined to deliver the new generation of intelligent, frequency-switching and autonomous networks.

There are two main components of the WMN architecture, respectively the mesh routers (MRs) and the mesh clients (MCs). These mesh routers are linked to each other to create a multi-hop mesh backbone. The MCs usually comprise client machines like laptops and mobile devices that can access the Internet by using the MC backbone. According to their position and their functionalities, MCs are subdivided further into three kinds: the mesh routers that offer connectivity to end-users are called Mesh Access Points (MAPs) and are typically situated within the operator's grounds. MCs, which are located within the WMN backbone and which are responsible for transferring MC data, are called Mesh Points (MPs). The third type of MC located on the edges of the WMNs is called mesh gateways (MGs) and allows communication between WMNs backhaul and the Internet via a cabled medium. Such a communication network delivers such benefits as low implementation and maintenance costs, reliability of the network and extended coverage. It also delivers opportunities which are designed to meet the ever-increasing requirements of end users, such as need of scalability, data rate and mobility support. But scalability and bandwidth are constrained by the character of wireless media and the availability of a limited spectrum. For these WMN constraints, CR provides an additional communication solution that can boost the capabilities of traditional WMN networks.

Its design and architecture increases the use of the radio frequency (RF) band by permitting unauthorized users to detect and access licensed frequency bands at will. But the Authorized Primary User (PU) must be protected from the interference. As a result, adjusting WMNs to the use of CR technology can be expected to substantially improve performance gains for efficient use of spectrum and network capacity. In a multi-hop system situation, the communication is dependent on the reliability of the network connectivity. However, a reliable and robust connection relies on the efficiency and effectiveness of a routing strategy employed. Therefore, both mesh routers with client nodes have a key role in routing decision making. Therefore, the implementation and optimization of an efficient routing protocol is still a significant part of the CR-WMN Ad hoc wireless network researchers have anticipated a series of routing procedures to expand the act of multi-hop cognitive radio systems. Newer work has been focusing on routing in both traditional ad hoc mobile networks and ad hoc cognitive radio networks (CRAHNs). They have tackled the specific problems and issues arising from the modification from stationary to self-motivated access to band. The suggested structures and protocols are grounded on inimitable or else similar project and optimization objectives, such as dodging PU interfering, decreasing end-to-end delays, get the most out of achievable bandwidth and increasing throughput rates.

The creators planned a receptive Cognitive Ad Hoc On-Demand Distance Vector (CAODV) convention for CRAHN. Their effort advances directing convention dependent on keeping away from the locales of primary user’s exercises, joint way, and frequency determination at each sending hub. It likewise misuses numerous channels to enhance the system execution. Notwithstanding, the proposed CAODV convention depends on a common control channel (CCC) procedure that makes added test in powerful cognitive radio networks (CRN) condition. The supposition of having the CCC may not be practical due to nondeterministic channel accessibility.

The creators in proposed an area based steering convention to address an issue of different control movement streams in the system. At the point when the way determination and channel choices are made consecutively, higher steering overhead happens. Moreover, in, a Spectrum-aware mesh routing (SAMER) convention as a steering answer for multi-hop intellectual radio work systems was proposed. The convention artfully chooses the channels with higher range accessibility likelihood and quality while adjusting between long haul course soundness (i.e., course dependent on most stable channels) and momentary crafty execution.

Creators in proposed a directing plan that processes source-goal way by thinking about the exercises of the PUs. The proposed calculation makes utilization of the likelihood of abusing different frequencies in the meantime between two SU hubs. The proposed plan depends on joint steering and range choice criteria that process the in all probability way that fulfills the necessities expressed by the application. In any case, it actualizes simultaneous different channel communicate technique, which makes an overhead on every accessible channel, bringing about wasteful usage of the transmission capacity.

Other prominent directing conventions for multi-hop CRN situations incorporate the plans proposed in. Most directing methods proposed endeavor to address the wasteful aspects in course disclosure components, utilization of CCC, instruments to lessen steering overhead, and distinctive approaches to manage availability disappointment because of discontinuous PU exercises.

1) **Detection and Removal of Black Hole Attack in Mobile Ad-Hoc Networks:**
   The article proposes a system to differentiate between malignant nodes by isolating all information in estimated small squares. The destination receives a message about the blocking of the source and sends a postlude message in response. This strategy is divided into two stages. At the beginning of the scene it manages the misfortune of the information and the second phase manages the detection of the malicious hub. In the first stage, along with receiving a postlude message, the reference node checks the information misery. During the transfer of

   Parcels, the node is inside the limit run. If not, the second step is started. Source hub sends a message with questions that include day and age to each of your neighbors to identify and throw away a harmful hub. If exceeding the time limit results in a message being sent or if the hub is harmful, the message has been received at the following address the source hub. At this point, the source hub attaches this hub to the final table and find malicious table.

Limitations:

- This technique can only be activated if there is an actual transmission of information taking place.
- This plan needs an additional preparation of the source hub to separate the traffic, and moreover to handle precluding -postlude messages.
- It is ineffective in the event of traffic congestion.

2) Prevention of cooperative black hole attack in wireless ad hoc networks:

The paper proposes a technique for identifying a number of black hole nodes that work together as a group by using the slightly modified AODV protocol through the introduction of the Data Routing Information (DRI) Table and cross-checking.

This solution consists of two bits of additional data from the nodes, which are based on the RREQ of Source node. In the DRI table, 1 stands for 'true' and 0 stands for 'false'. The first bit "From" means information. The second bit "Through" means information about the routing of data packets through the node (in the Node field).

Any time an intermediate node (IN) responds to an RREQ, it will send the ID of its next hop neighbor (NHN) and DRI entry for NHN on the source node. If IN is not reliable for the source, the source sends the following route request (FREQ) to NHN. NHN, in its turn, replies with a FREP message containing the following DRI entry for IN, the next hop node of the actual NHN and the DRI entry for the next NHN Hop.

If the NHN node is a trusted node, the source checks if the IN is a black hole or not by using the DRI entry for the IN answered NHN, and in the case of NHN, answered IN. These are consistent if the IN is not malignant. If the NHN is uncertain, then the same cross-check will be continued with the next NHN hop node. This cross Loop checking lasts until a trusted node is found.

Limitations:

- This solution is not able to accommodate the attack of gray holes in which nodes move alternately between malignant and normal behavior.

CHAPTER 3

SYSTEM DEVELOPMENT

The main intention of this chapter is to introduce the readers to an architectural vision of NS2 as well as of our project. This section offers a concise introduction to NS2. In this chapter, we also saw a brief description of Software requirements, followed by Hardware requirements. In this chapter, we saw a brief description of Software Requirements, followed by Hardware requirements. The architecture of the system is shown in section 3.6 & data flow diagram is also shown in section 3.8.The functionality related to each component is also explained in briefly. At the end of this chapter provides detailed design of the project and further it explains the purpose and also the processing steps and brief explanation of the module.

3.1 Tool

Network Simulator (Version 2), broadly recognized as NS2, is basically an event-based model software device that has proven to be advantageous for researching the changing environment of the communication networks. Simulation of both wired as well as wireless network features and procedures (e.g., routing algorithms, TCP, UDP) can be done with NS2. In many cases, NS2 allows users to define and simulate these network protocols. In additions, NS2 also provides users with a way to specify and simulate such network protocols.

3.2 Basic Architecture

NS2 includes two main languages: Object-oriented tool command language (OTcl) and C++ . The C++ describes the backend appliance of the model, the OTcl defines the frontend. The C++ and OTcl are binded to one another by TclCL. When plotted to a C++ object, variables in OTcl fields are a lot called handles. Abstractly, a handle is just a string-like "_o10" in the OTcl domain and does not have any functionality. Rather, the functionality (e.g. getting a packet) is defined in the Mapped C++ object directive . In the OTcl field, a handle acts as a frontend that acts in interaction with users and other OTcl objects. It may determine their procedures as well as variables in order to improve interaction. The procedures and variables of members in the OTcl domain are referred to as the instance procedures (instprocs) and instance variables (instvars), respectively.

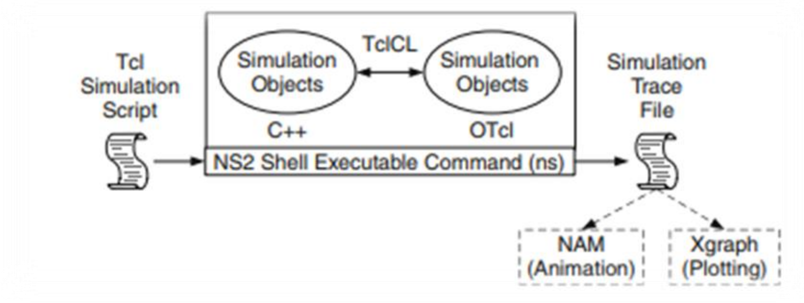
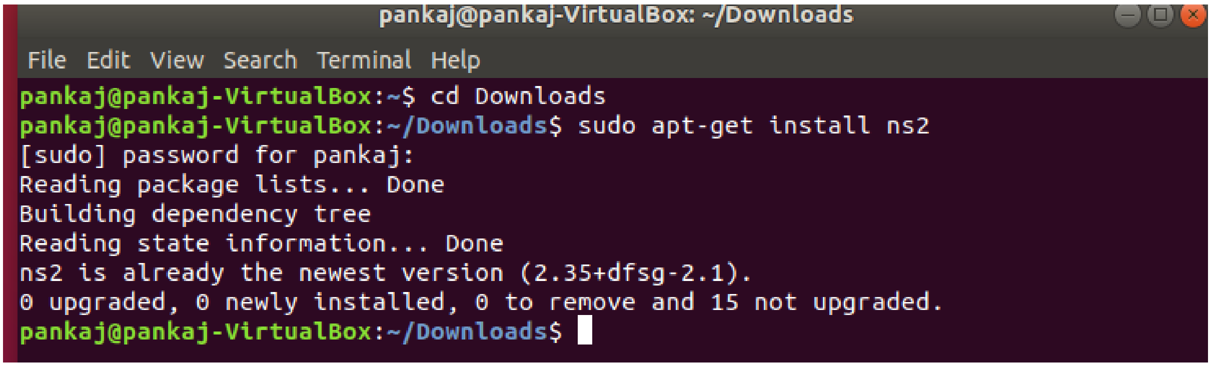


Figure 3.1Basic architecture of NS

NS2 has a amount of fixed C++ classes. Basically it is recommended that you use C++ classes to make a model via a Tcl simulation script. The forward-looking users, on the other hand, may perhaps discover these items to be lacking. They want to build their peculiar C++ classes so that they can use an object-oriented tool command language interface to put collected objects that are instantiated from this class.

As the simulation is done, network simulator produces a text-based simulation output. In order to graphically and interactively understand these effects, we use gears such as NAM (Network Animator) and XGraph. When analyzing a particular network performance, the users can extract a meaningful sub-set of text-based information and convert it into a more understandable representation.

- Introduce NS-2 utilizing this direction :
  sudo apt-get install ns2



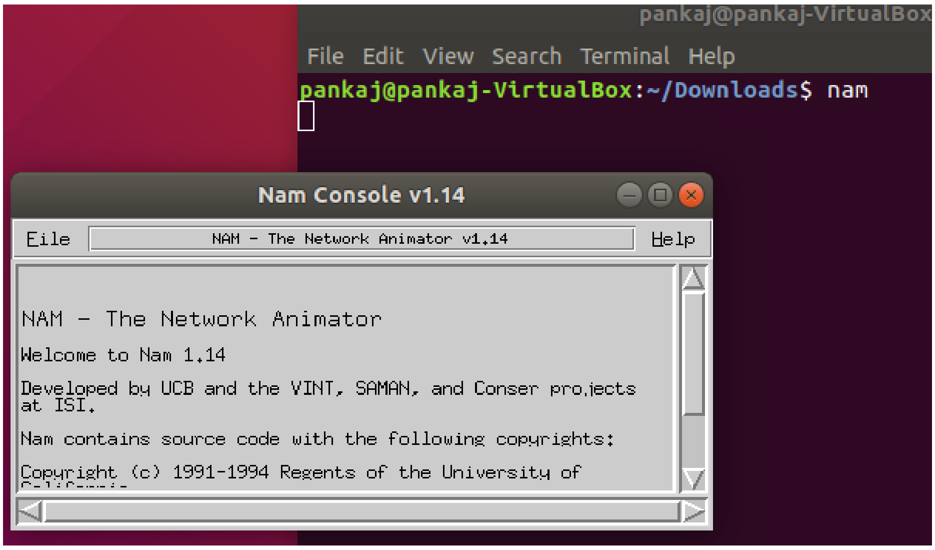
pankaj@pankaj-VirtualBox: ~/Downloads
File Edit View Search Terminal Help

```
pankaj@pankaj-VirtualBox:~$ cd Downloads
pankaj@pankaj-VirtualBox:~/Downloads$ sudo apt-get install ns2
[sudo] password for pankaj:
Reading package lists... Done
Building dependency tree
Reading state information... Done
ns2 is already the newest version (2.35+dfsg-2.1).
0 upgraded, 0 newly installed, 0 to remove and 15 not upgraded.
pankaj@pankaj-VirtualBox:~/Downloads$
```

Figure 3.2 Installing NS2

- Furthermore, Nam is supposed to enter. Nam (Network Animator) is a moving mechanism to talk graphically to system. Use the command:

sudo apt-get install nam


pankaj@pankaj-VirtualBox
File Edit View Search Terminal Help
Nam Console v1.14
File
NAM - The Network Animator v1.14
Help

```
pankaj@pankaj-VirtualBox:~/Downloads$ nam
```

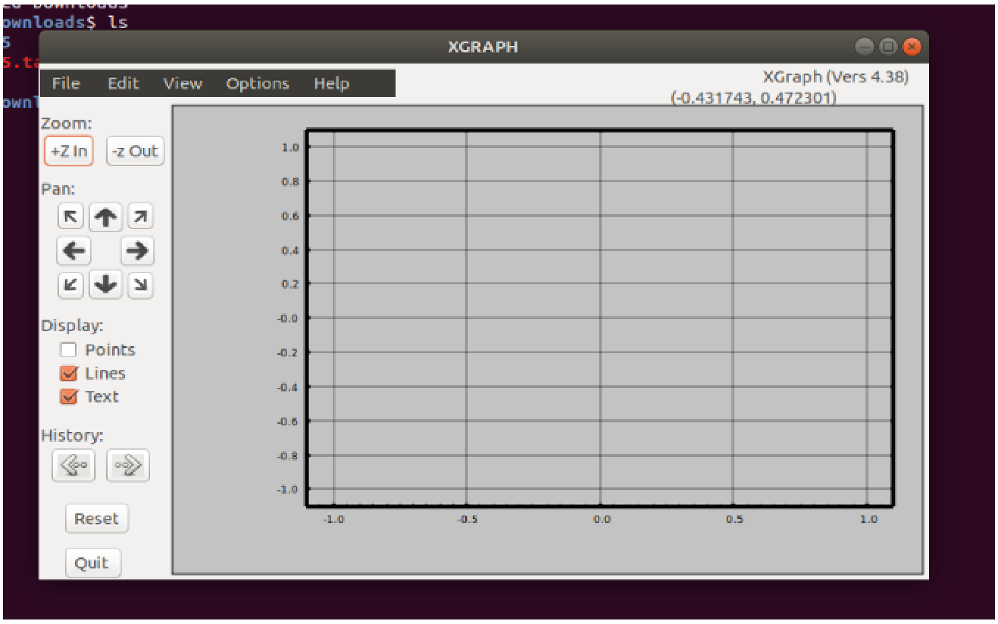
```
NAM - The Network Animator
Welcome to Nam 1.14
Developed by UCB and the VINT, SAMAN, and Conser projects
at ISI.
Nam contains source code with the following copyrights:
Copyright (c) 1991-1994 Regents of the University of
California
```

Figure 3.3: NAM Console

- XGRAPH is a broadly useful x-y information plotter with intelligent catches for panning, zooming, printing, and choosing show alternatives. It can be used to plot information from a wide number of records on a similar diagram and can deal with boundless informational index sizes and any number of information documents. To install XGRAPH, unzip:

  tarxyfz

  xgraph_4.38.tar.gz



```
ownloads$ ls
```

Figure 3.4: XGRAPH

3.3 Operating Environment

As part of this project, we have developed an approach model for the dynamic allocation of resources in a wireless environment and assessment of the stability of the system under consideration. Users can focus on specific actions such as design issues at system level, without worrying about low levels of design and infrastructure. Linux as an operating system that is an open system. The hardware and software requirements are as follows:

Hardware Requirements:

- Processor: Any processor with speed above 500 MHz
- RAM: 512Mb (minimum).
- Input Devices: Standard Keyboard and Mouse.
- Output Devices: High Resolution Monitor.

Software Requirements:

- Operating system: Linux
- Programming tool: NS 2.34

3.4 Applications

The applications for the project are:

- This system can be used for military operations.
- This system can be used secure and fast communication during law enforcement operations.

3.5 Advantages

This system has the following advantages:

- Reduces the network overhead and vulnerabilities by applying bait procedure from each and every node that is within its radio range.
- High Throughput and Less Delay in MANET Using Bait Procedure.

3.6 System Architecture

The aim of the architectural scheme is to describe a set of significant decisions about the software system including the choice of structural elements and interfaces that make up the system.

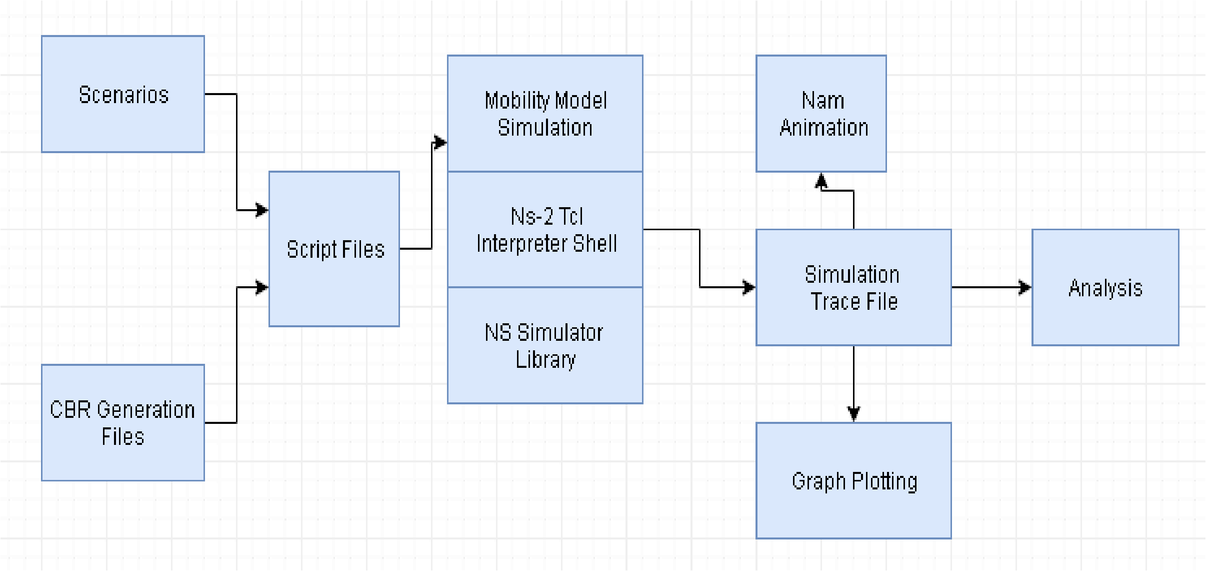


Figure 3.5: System Architecture

At the modeling level, NS uses OTcl (Object Oriented Command Language) programming Language for interpreting user simulation scripts. OTcl is an object-oriented extension of Tcl. While the content of OTcl is being deciphered, NS is at the same time producing two main research reports as records.
The NAM (Network Animator) question is asked in order to demonstrate a visual animation. The simulation and protest of the "Trace" case shows that a significant number of articles have been preserved in the a simulation. The previous ".nam" document is used by the NAM programming that connects the NS. Then it is ".tr". The writing, which contains all simulations, takes place in the content layout. The ".tcl" documents inthe content manager compiles and breaks the effects of the ".tr" record using "feline", "awk" , "wc" and "grep" to the Unix operating system.

In relation to the quality achieved in the simulation, a diagram is drawn. X-graph is utilized and the order gnu plot is utilized to draw a chart. The chart is followed by a comparison between the proposed demonstration and the current model.

3.7 Sequence Diagram

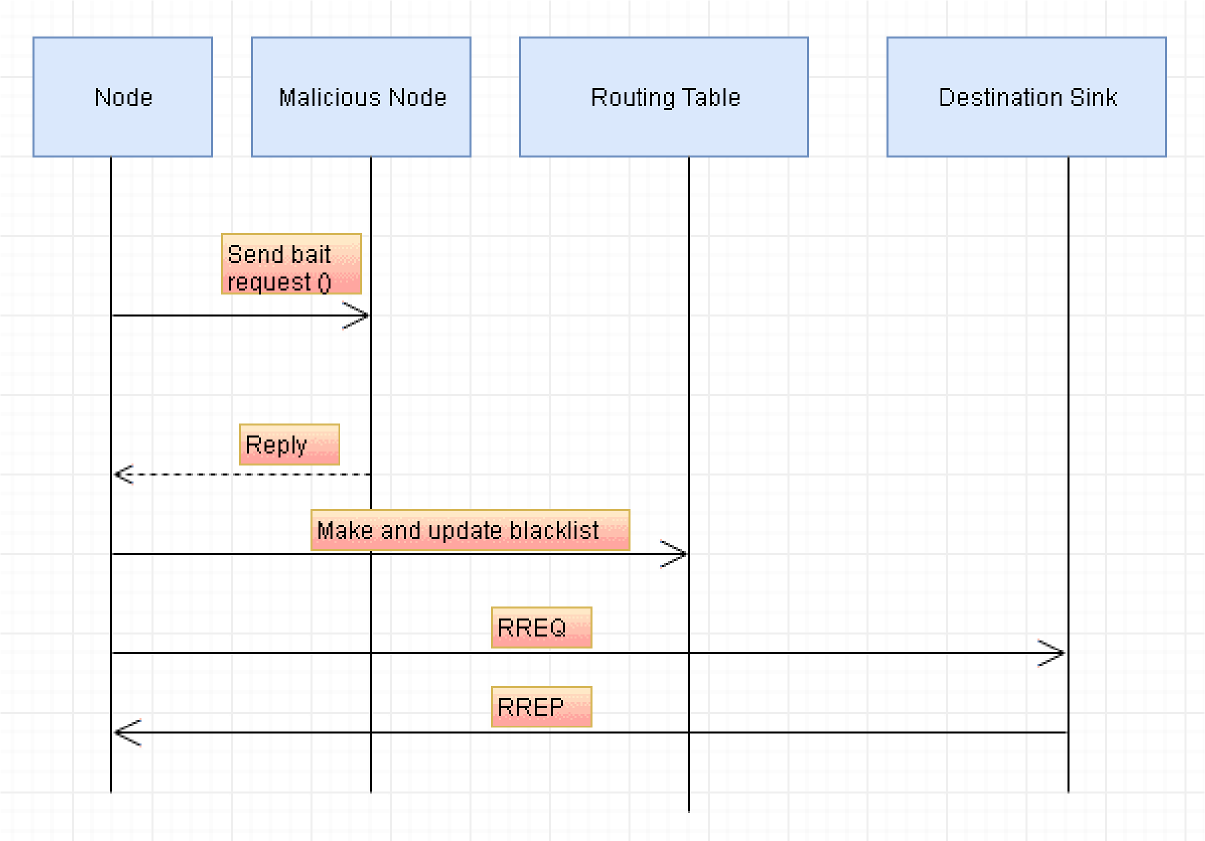


Figure 3.6: Sequence Diagram

A succession graph or sequence model in a Uniform Modeling Language (UML) is a type of interface a graph that shows each component as a protest, how they interact with each other and in what way to organize. The arrangement scheme has parallel vertical lines talking to lifeguards speaking to each question life savers. It shows all the information traded between these articles. The chart showing the distribution speaks for itself.

The network has a total of 60 nodes. The multiples of 4 and 5 are malicious.

The black list is declared an array length of 20. The array length can be increased or decreased accordingly.

3.8 Flow Diagram

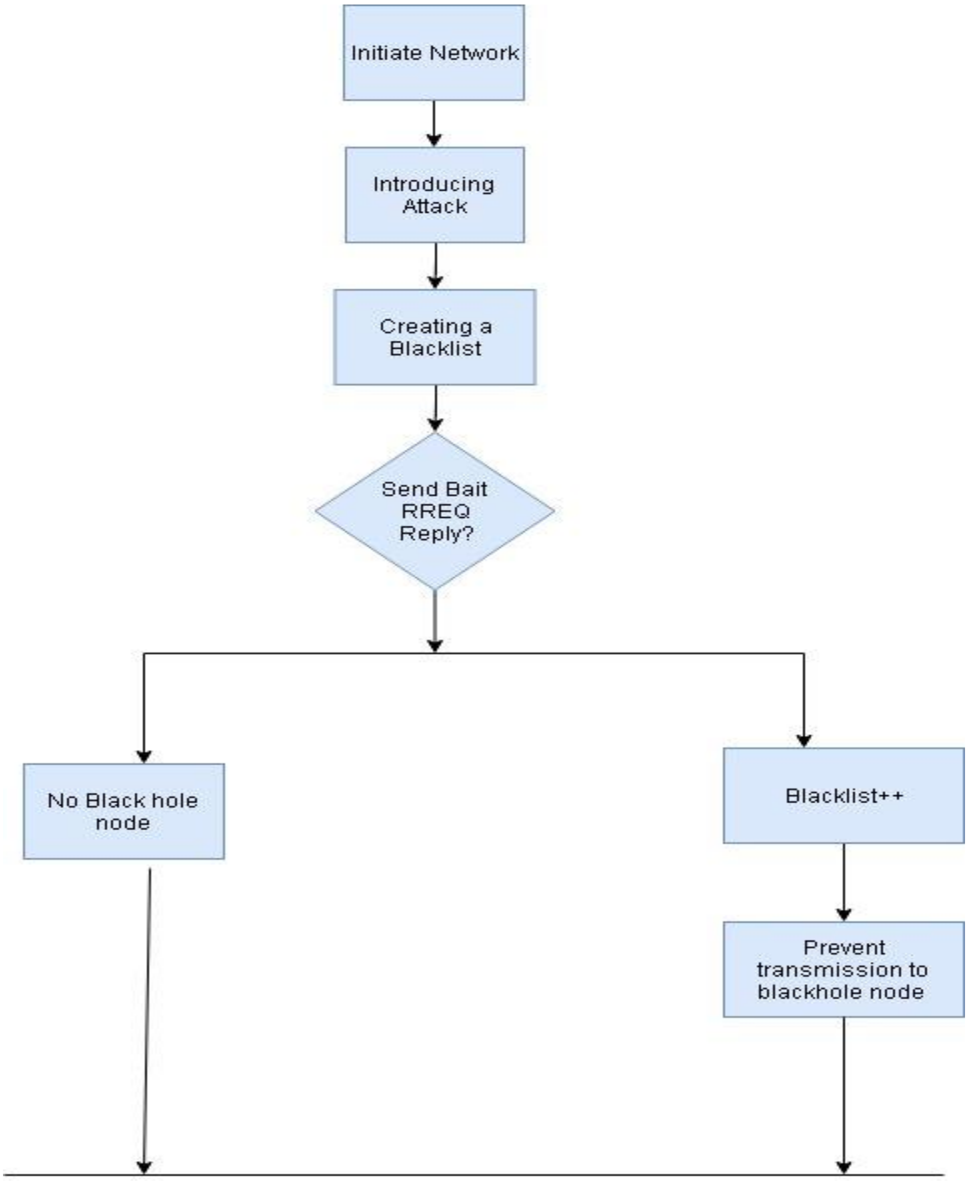


Figure 3.7: Flow Chart of the proposed system

The following are mentioned in the Fig 3.7:

1) **Initiate Network: -**The MANET network is established by using the ns2 network simulator version 2.34. The network consists of mobile and randomly distributed nodes.
2) **Introducing Attack: -**Introducing a black hole attack by configuring some of the nodes as malignant in the network**.**

3) **Create a Blacklist: -**Allocate an array of a specified length to which we will be adding the index of the black hole nodes present in the network.
4) **Send bait RREQ: -** Source node will send a request for RREQ bait to the adjacent node with the destination node that is not in the network.
5) **Receive a reply RREP :-**If a response is received, the index of the node sending a response to previously send RREQ, the index of that node is added to the blacklist to make sure that there are no packages sent to this malicious node.
6) **No reply received: -**If no response is received, it means that there are no blackhole nodes in the network and therefore the delivery of the packets takes place as a normal operation.
7) **Prevent transmission to black hole nodes: -**Whenever a source node wants to send a package to a destination, it avoids sending the package to a black hole node by referring to the blacklist.
8) **Successful Packet delivery: -**After detection and prevention of black hole nodes, the package is as follows delivered successfully.

3.9 Processing Steps

In order to prevent the black hole attack inside the network we will use modified bait Scheme. The steps associated in the processing are given below:

Step 1: MANET network is created with the help of ns2 network simulator version 2.34. The network created consists of mobile and randomly distributed nodes, each of which acts as a host and router.

Step 2: We present a black hole attack by configuring multiple hosts on the network as malicious. These are malicious hosts that forward routing packets, but do not forward them to their neighbors.

Step 3: In this step we assign an array of a certain length to which the black hole node index is added, those present in the network.

Step 4: Source node sends a request for RREQ bait to a neighboring node with a target node index that is not on the network. The RREQ' bait is initiated when the bait is used for initial routing and then wait for an answer.

Step5: When the RREQ' is received by the malignant node, it will respond with a fake RREP and then we can use this false reaction to detect the malignant node.

Step6: If no response is received, it means that there are no black hole nodes in the network and that the packet supply takes place in the normal way.

Step7: After discovering and eliminating black hole nodes, the package is successfully delivered.

3.10 Modified Bait Scheme

1. Start making blacklist array.
2. Then send bait request.
3. After that check for nodes that give RREQ.
4. Keep in mind the index values of the nodes and then add them to the blacklist.
5. Later send the blacklist to the routing table.
6. At the end prevent transmission of the data from or to these nodes.

CHAPTER 4

ALGORITHMS

This chapter introduces the MANET networking concept and the other terms/methods/algorithms related to topic. It also provides you with information about MANET and attacks from the black hole and the existing methodologies used to detect and prevent black holes in MANET.

- **AODV(Ad hoc On-demand Distance Vector):**

Ad hoc On-demand Distance Vector is a standout amongst most famous directing conventions, which is a straightforward and proficient on-request MANET steering convention. The ideas of AODV that makes it alluring for MANETs with restricted transfer speed incorporate the accompanying:

a) Less space complexity: The above algorithm assures that nodes which are not in the current path will not maintain information on this route. When a node gets the route request (RREQ) message and establishes an opposite route to its routing table while propagating the RREQ message with its neighbors, if it receives no route reply (RREP) message by its neighbors at this request, it erases the routing data it has stored.

b) Maximum bandwidth utilization: The highest result of the algorithm can be considered. Because the protocol will not require periodic global advertisements, the available bandwidth demand is lower. All the intermediate routes on an activated path update its routing tables while ensuring maximum use of the bandwidth. Because, these routing charts will be used over and over again if that node gets a RREQ from some other source to the same target.

c) Simple: It's easy to do, with every node acting as a router, holding a very simple routing table, and source node initializing the route detection query, causing the entire network to be started dynamically.

d) The most efficient routing information: When a node propagates an RREP message, and the node gets RREP with small hop-count, it will update its routing information to this improved path and propagates it.

e) Loop-free routes: This algorithm sustains loop-free paths applying the straightforward logics used by nodes and then drops the packets for the same broadcast ID.

f) Highly scalable: The above algorithm is very scalable because of its minimal space complexities and transmissions will be avoided.

- **2ACK-Scheme:**

The 2ACK plan implicitly improves the locating instrument 2ACK scheme details. 2ACK plan is a systematic layered method used to discover interfaces and palate their things. It can be done as an addition to existing road conventions for MANET, for example OLSR and other steering systems.. In the 2ACK plan, a decent behavior is found by using a different kind of affirmative package called2ACK.

A 2ACK pack is defined in a fixed way by two jumps (three nodes) in the reverse direction to the way information flows. The 2ACK is a systemic layered method to differentiate between malicious activities and moderate their stuff. You can update it as an addition to your existing plan management of MANET conventions, such as OLSR. The 2ACK schedule recognizes malice by using another kind of supportive package called 2ACK. A 2ACK pack is determined in a fixed two-stage course is reflected (three nodes) in the other direction of the information traffic course. It can be updated as follows in addition to the existing MANET road conventions, for example OLSR and several other steering conventions.

This 2ACK plan will find decent performance when using another type of affirmative packet called 2ACK. A 2ACK packet is defined in a fixed way by two bounces (Figure 4.1) against the information heading the way it moves. At the N1, each ID will remain on the record for ’t’ seconds, the rest for 2ACKcollection. Just in case that the 2ACK groups co-coordinating this database in front of the clock the letter, the ID will be taken out of the file. In addition, the ID will be removed from the rest of the record and the counter called Cmis will be enlarged. If it is not possible for N3 to receive at this point, determined if he needed to send a 2ACK packet to N1.The specific final objective is to cut the additional reason for the overheads of the 2ACK framework, namely vulnerability in the information package will be recognized as a multi-band package. Such a loophole is called Affirmative range, Rack. As the rack evolves, we can gradually adjust the overall cost of Many-Hop packet transmissions. The N1 client comments on the N2→N3 connection for the session of Time tobs.

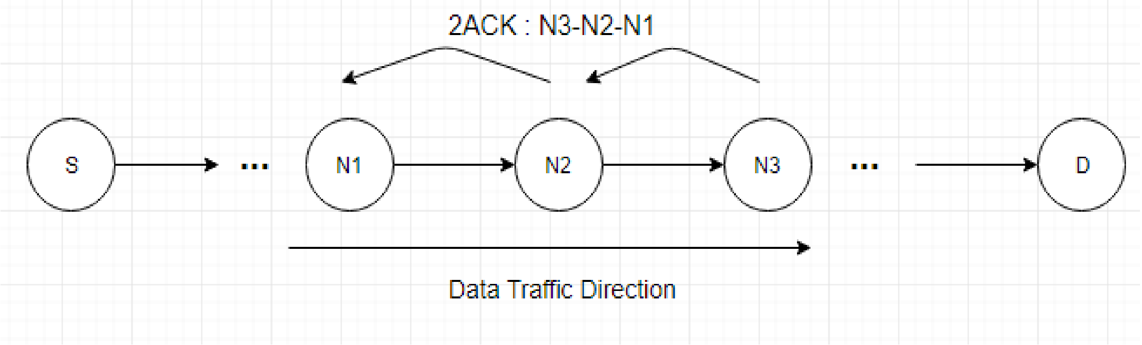


Figure 4.1: Settled way of two jumps in 2ack

For the remainder of the session, N1 decides on the degree of loss of 2ACK packets as Cmis/Cpkts and contrasts with it and limit the Rmis. In case the scope is more notable than a Rmis, the following should be combinedN2→N3 is declared troublesome, and a particular connection is excluded from guiding table. As only partitions in the get information package are recognized, the Rmis can split.Rmis> 1-Rack ignores false warnings by using this method mainly for affirmative purposes. Every customer obtaining such a packet 2ACK comments on the N2→N3 connection as upstream and passes it to Dark records of such actors are part of what he controls. The moment the client starts his work its own information activities, it will then refrain from using such upstream interfaces as a piece of its own way.

- **Best effort fault tolerant routing:**

The aim of the BFTR plan is to ensure a high proportion of transport in packages managed by public administrations, and Low overhead costs in close proximity to existing hubs. BFTR operates in a redundant network without one point failure (Figure 4.2). Instead of assessing whether the road is great or dreadful, i.e. whether it is the BFTR assesses the credibility of the management system based on its conclusion to the final implementation (e.g. proportion of parcel transport and deferral). Persistently observing the BFTR powerfully processes packets in the most convenient way. The BFTR gives an efficient and uniform response to a wide range of malicious activities in the facility that is few in number of safety. BFTR calculations are assessed both in the context of an investigation and in the context of extensive leisure activities. The results show that the BFTR significantly improves the specially designated guidance system executing within sight of creating problem nodes.

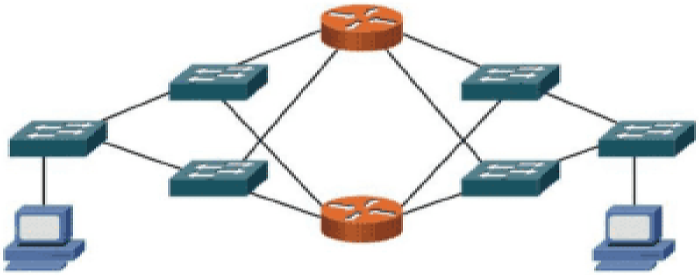


Figure 4.2: Redundant network with no single point of failure

- **Cooperative Bait Detection Scheme :**

The CBDS conspiracy consists of three stages:

a) The starting draw step.
b) The invert following advance,
c) The moved to responsive barrier step.

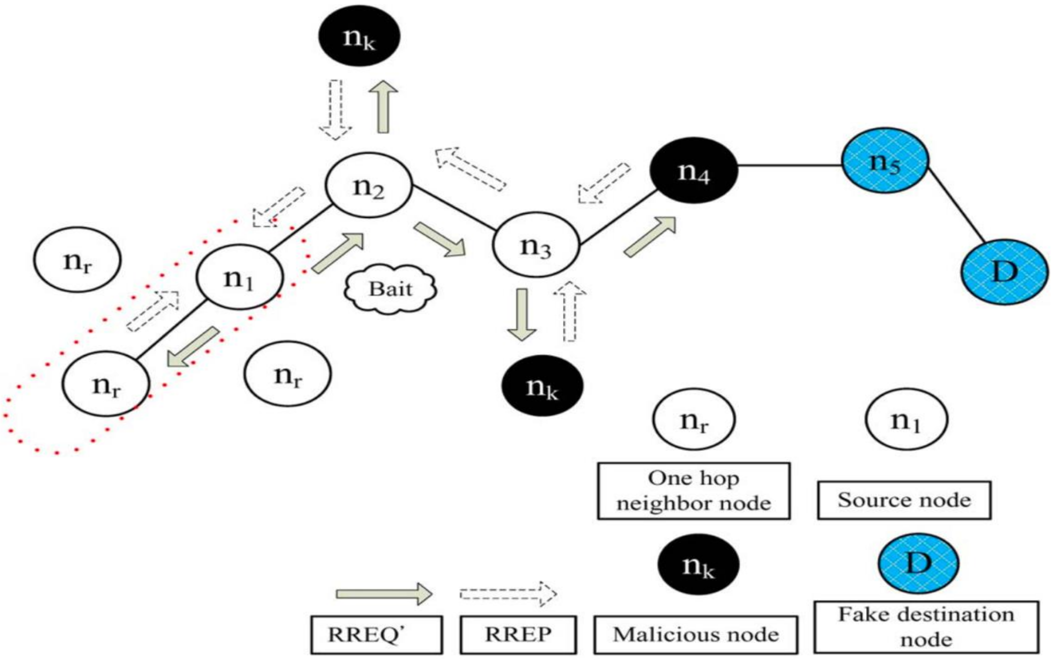


Figure 4.3: Random Selection of Cooperative baits

Initial Bait Step:

The purpose of good mastermind is to lure the damaging central point to answer a RREP response by sending the RREQ catch that it used to develop at the moment into the most concise way to a central point which limits the packages that have been modified. In order to achieve that objective, it is necessary to run with the system, it is proposed to make the territory in which the RREQ draw takes place objective. The middle point of the source therefore selects the adjacent center (Fig. 4.5).

Reverse Tracing Step:

Reversal after progress is used to perceive acts that threaten the centers through a course response to the RREQ message'. In case a toxic focal point gets a RREQ', then it is going to answer with a fake RREP. In a similar way, the switch that follows the project will be composed for RREP Tolerant Centre, whose purpose is to identify questionable information and out of the blue confined in the zone during the course.

Reactive Defense Step:

When the above proactive shield (stages 1 and 2) is activated, the DSR course revelation process begins. Precisely when a course is set and when at the destination it turns out that the proportions of packet transport are as follows in general terms, falls, if possible, the sitting project would be re-initiated in order to perceived as continuous aid and constant profitability of the response. Benefit is a differentiated incentive in terms of the scope that can be adapted by the current viability framework.

CHAPTER 5

TEST PLAN

In this chapter, we use a quantitative trial approach in which the trials were performed using the Network Simulator (version 2.34). This software was designed to run on ubuntu distribution of the Linux OS. Here experiments are done using NS2 platform. Further this chapter deals with various techniques that are used in the development of the project, beginning with the language and platform selection to explain the entire process of implementation steps.

The performance is evaluated on the basis of following parameters:

1. **End-to-end latency:** time taken to send a packet from source to destination node across a network.

   Latency = n * (transmission + propagation + processing + queuing)

   Where n = No. of hops.

2. **Throughput:** measure of data processed in a given amount of time by the system, calculated in bits per second (bps).

   Throughput = efficiency * bandwidth.

3. **Packet delivery ratio:** Ratios of no. of packets send by sender node to the no. of packets received by the receiver node.

   PDR = packet send by source / packet received by destination

4. **AODV:** Ad Hoc On-Demand Distance Vector (AODV) is a routing protocol specifically designed for wireless and mobile networks. It establishes routes to destinations on demand and supports unicast and multicast routes. It was jointly developed by the Nokia Research Center, the University of California, Santa Barbara and Cincinnati University in 1991.

   AODV control convention is ready for use by compact central points in an exceptional selected frame. It provides quick adaptation to dynamic connection conditions, Low planning and memory, low framework utilization and choose unicast courses to achieve your goals within the structure of the framework. Use objective collection numbers to ensure that the circle constant adaptability (despite the anomalous transmission of a coordinated control), avoiding problems linked to the traditional conventions of separation vectors.

5. **Routing Overhead:** Updating of actual information about network routes, routing algorithms generate small packets called routing packets. One example of such packets is the HELLO packet, which is used to check the activity of a neighboring node. Note that the routing packets do not contain any applications like data packets.

   Both the routing and the data packets should have the same network bandwidth most of the time, and therefore routing packets are considered to be network overhead. These overheads are called routing overheads. For a good routing protocol, there should be less routing overhead.

6. **Black-hole attack**: In the organization of the network, storming by packet dropping or ambushing through black holes is a kind of Denial of assault with benefits, where the center that is supposed to issue the packages is more likely to arrange for their transfer.

   This usually comes from a hub that is able to trade with different types of goods. One of the reasons mentioned in the study is to refuse benefits when attacking a router Using the well-known DDoS tool. Since packets are usually removed from the framework with losses that a packet drop attack is difficult to recognize and verify.

   A malignant router can also perform a similar ambush, e.g. by dropping

   packages for a specific framework purpose, at a specific time, a package for each n group or every second or a randomly picked piece of bundle. This is quite a dark interval. If toxic changes attempt to discard all incoming packets, the attack may actually be as follows are quickly detected, for example, by means of typical framework administration tools, trace. In addition, when the distinctive switches see that the traded switch is falling, everyone in general, they will begin to displace this change from their original tables and, finally, they will not the movement will flow to the attack. In any case, if the poisonous switch starts to reset the groups. On a certain day and age or every n bundle, it is usually harder to tell. The report also argues that some actions are still directly relevant to the framework.

5.1 Implementation

Implementation is an important stage in the development cycle. This stage involves the translation of the requirements and specifications of the system in the working model in order to fulfill the services in real time. The key functions identified at the design stage are transformed into functions that can be performed using relevant programming languages.

Therefore, the implementation phase is always followed by major decisions regarding the choice of language, choice of platform, etc. These decisions are impacted by a number of factors, such as response time required, security and data management issues, among others. These decisions also concern affects how well the end product functions.

Implementation steps:

1. The network setup runs on the default AODV protocol.
2. Then the black hole node is implemented into the network which results in packet drop.
3. After this black hole detection step is employed.
4. At last we apply prevention methodology that results in successful delivery of data.

5.2 Programming Language Selection

When you are implementing a software system, the choice of programming language is one of the most important decisions which must be made. As there are so many programming languages to choose from, it is easy to get lost in the details of everyone. The selection of the programming language, however, depends on a variety of factors. Some of the factors that should be considered when choosing the programming language are:

- Skill of programming language of each team member working in the project.
- Platform support & portability.
- Applicability to the domain of the problem,
- Availability of the necessary libraries to setup the whole environment.

By considering all the above factors, we decided to choose ns2 for simulation. Ns2 consists the libraries that were required for the creation of networking environment. Also ns2 was only an application with which everyone in the team was completely comfortable with. The ns2 version which is used for better support and lesser bugs is 2.34.

5.3 Platform Selection

We used Linux platform for our project because of the following reasons:

1. **Flexibility**

   This comes at the same time from the desktop, because Linux is an unbelievably flexible operating system framework it is wrong to limit the adaptability to the desktop alone. The thing is: With Linux, there's always more than one approach to dealing with an errand. In addition, there is the ability to get the extremely imaginative with your critical thinking, and you have the prerequisites for a far unrivaled framework. Windows is as rigid as a working framework can be.

2. **Shell Scripting**

   Shell scripting is better because of these following reasons:

   - You can write a script to initialize something when booting the system, so that it can't be performed manually.
   - It is easy to kill as well as start multiple applications together.
   - Automation is also better.

3. **Command Line**

   This is something else where I shouldn't have to state fundamentally more than the title. The Linux request line can do about anything you need to work in the Linux working system. Really, you require a contact of data to do this, anyway comparative stays consistent for the Windows order line. The best refinement is the aggregate you can do when met with just the charge line. In case that you needed to oversee two machines through the request line just, you would quickly observe precisely how preferable the Linux CLI is over the unfathomably underpowered Windows CLI.

5.4 Implementation Steps

Ad Hoc On-Demand Distance Vector (AODV) is a routing protocol specifically designed for wireless and mobile networks. It establishes routes to destinations on demand and supports unicast and multicast routes. It was jointly developed by the Nokia Research Center, the University of California, Santa Barbara and Cincinnati University in 1991.

AODV control convention is ready for use by compact central points in an exceptional selected frame. It provides quick adaptation to dynamic connection conditions, Low planning and memory, low framework utilization and choose unicast courses to achieve your goals within the structure of the framework. Use objective collection numbers to ensure that the circle constant adaptability (despite the anomalous transmission of a coordinated control), avoiding problems linked to the traditional conventions of separation vectors.

In AODV, the framework is quiet until the time when associations develop.

The points of the framework centre that need associations put forward the demand for the association. Whatever remain AODV centers send a message and record the central point that has requested the association. Accordingly, they take short courses back to the requesting central point. The center that receives such messages and paves the way to the desired center sends a regressive signal through and the occasional courses towards the nodal center. The training centre, which is now in demand, uses a course containing

the minimum number of jumps over different nodes. Extracts that are not used as part of the director tables are reused after a while. If there is a possibility that the connection will be interrupted. The direction error is transmitted back to the sending center and the procedure is repurposed.

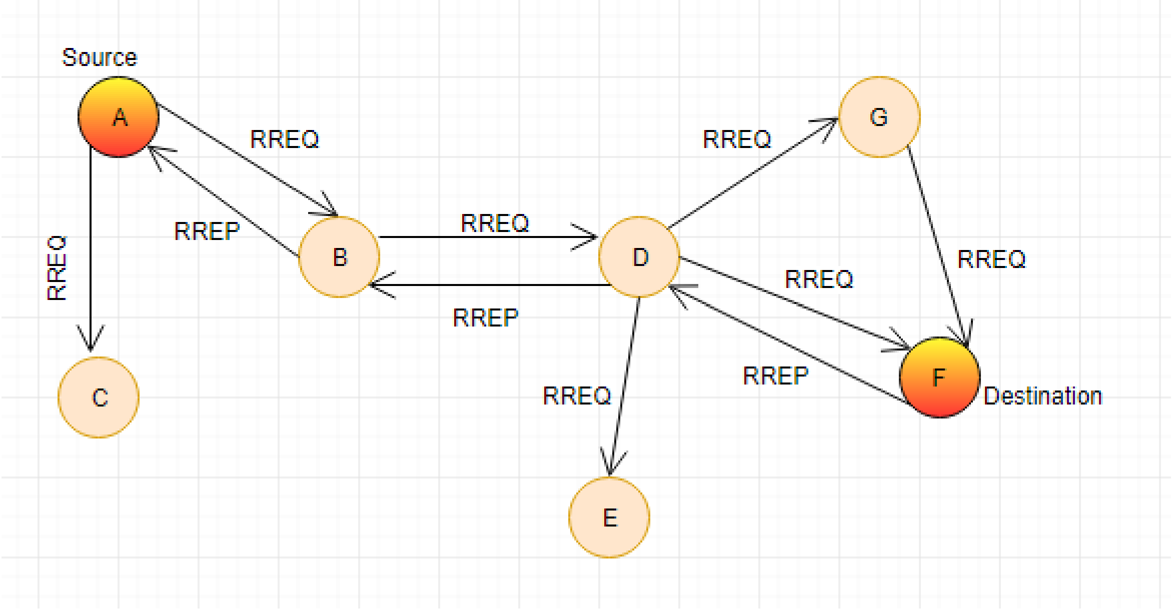


Figure 5.1: Simple AODV

5.5 Introduce Black hole Node

The black hole nodes are introduced into the system. The black hole attack is one of the threats to security in that the traffic is redirected to a node that does not actually exist in the network, so that the data instead of being received at the destination (Fig 5.2). It is an analogy of the real world to the black hole in the universe where things disappear. The node is presented in such a way as to the knot that can attack other knots and nets knowing that it has the shortest path. Figure below shows a black-hole attack:

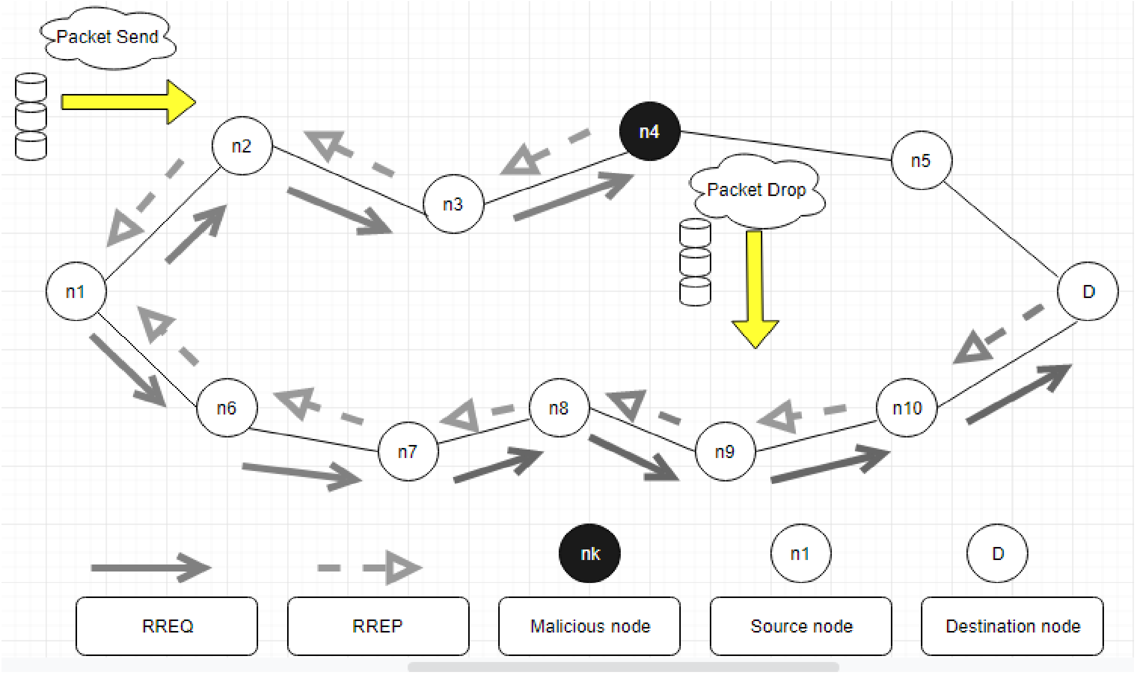


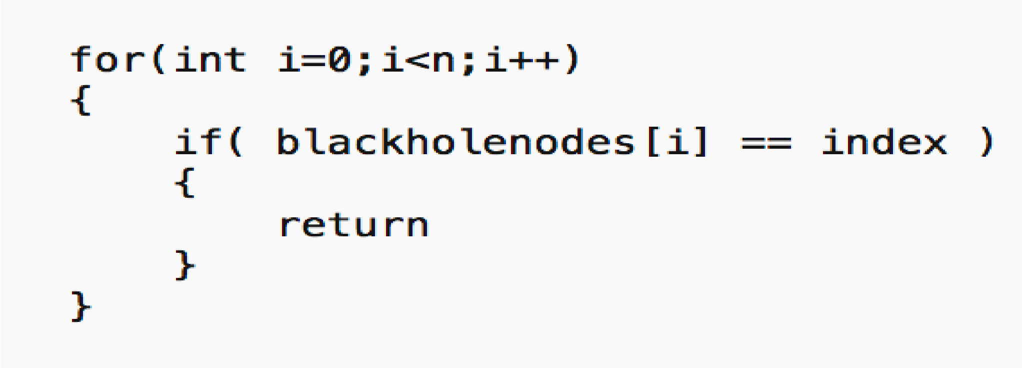
Figure 5.2: Data packet drop by Black hole node n4

5.6 Detection Of black Hole Attack

A request for the bait route (RREQ) is sent. The RREQ bait has been assigned a node that is not present on the network. Normally, the RREQ receives a route response/reply (RREP) under normal conditions. Only if a specific node is present in the network and the node sending RREP must have the shortest distance from the source to the destination. But here, if it receives RREP, we can confirm that the node that sends RREP is a malicious node.

5.7 Prevention of black hole Attack

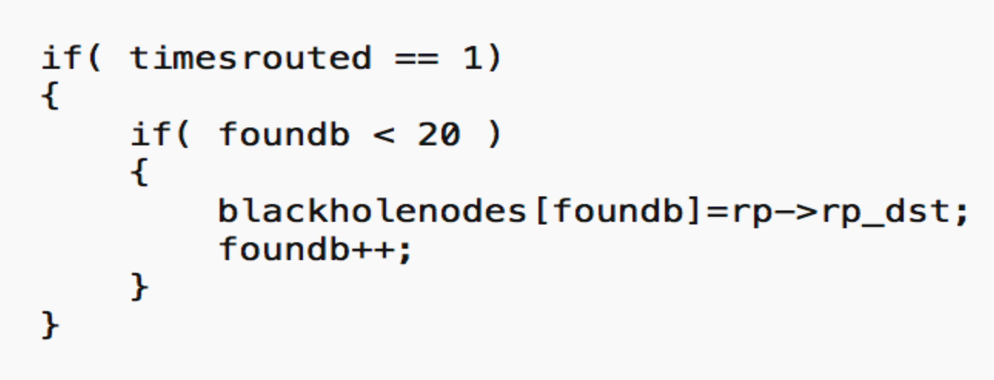
Creating list which consists of all black-hole nodes.



```
for(int i=0;i<n;i++)
{
        if( blackholenodes[i] == index )
        {
                return
        }
}
```

Figure 5.3: Creating the blacklist

Nodes that respond to the bait RREQ is added to the blacklist.



```
if( timesrouted == 1)
{
        if( foundb < 20 )
        {
                blackholenodes[foundb]=rp->rp_dst;
                foundb++;
        }
}
```

Figure 5.4: Addition of black hole nodes to the blacklist

After following these steps, indices of blacklisted nodes are sent to the routing tables of nodes to stop packet transmission to and from these blacklisted nodes.

CHAPTER 6

RESULTS AND PERFORMANCE ANALYSIS

During this simulation, we initially set up a Mobile Ad Hoc network consisting of 60 nodes. In the very first simulation test we linked the "defaultaodv" file to aodv.cc file. As soon as the link is established, we run the tcl-script which is followed by a simulation that will show that there is no packet transfer between source and destination in the presence of black-hole nodes in the network.

For the next simulation test, we will connect the black hole AODV file, which contains a modified aodv.cc scheme, to aodv.cc. When the link is established, we will execute the tcl-script, followed by a simulation showing that the nodes have chosen an alternative path from source to destination that does not contain any of the black-hole nodes in the network. Therefore, the anticipated outcome matches the true outcome and the simulation test has been passed. This chapter analyses the experiments carried out and the results obtained from these experiments. The delivery reports of the packages, the scope and the delay are calculated.

6.1 Simulation Testing

To check how the transmission takes place between different aodv routing files, we do a simulation.

Simulation Test 1:

Simulation Test Case ID	Test Case 1
Description	Testing the default aodv routing protocol in the presence of black hole nodes.
Input	Link aodv.cc file to point to default aodv
Expected Output	No transmission of packet takes place.
Actual Output	No packet transmission takes place.
Remarks	Passed

Table 6.1: Simulation Test Case 1

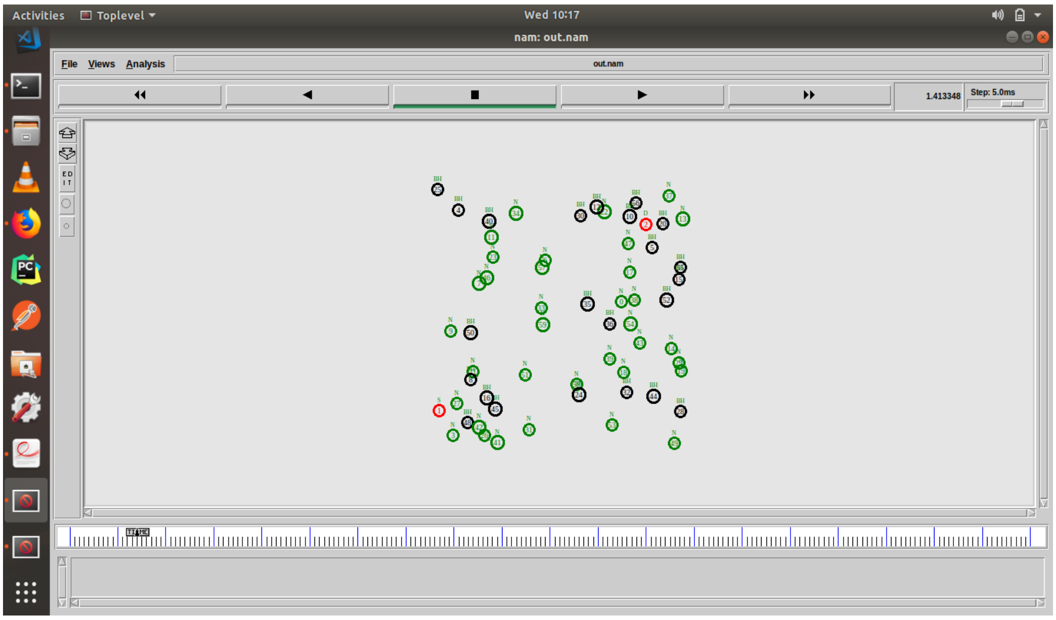


Figure 6.1: Simulation Diagram for Test Case 1.

Simulation Test 2:

Simulation Test Case ID	Test Case 2
Description	Testing aodv.cc file to point to blackhole_aodv which has modified bait algorithm.
Expected Output	Nodes should find an alternate path to the destination and packets must be sent from source to the destination.
Actual Output	Nodes found out an alternate path from source to destination and most of the packets from source were received at destination.
Remarks	Passed

Table 6.2: Simulation Test Case

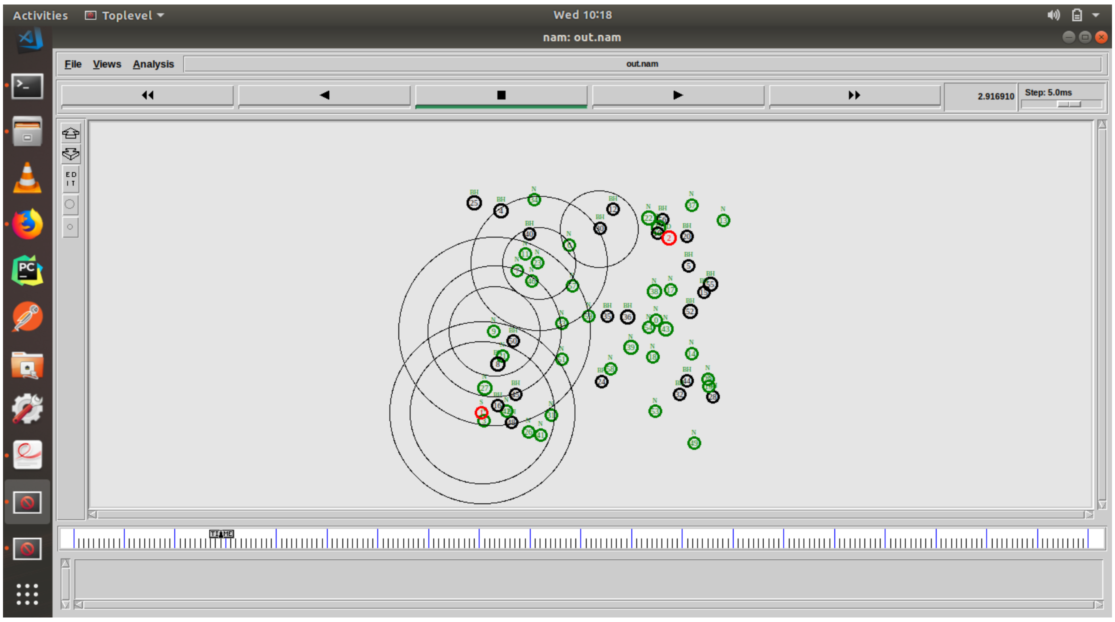


Figure 6.2: Simulation Diagram for Test Case 2

6.2 Simulation Result

Like we have mentioned before in the simulation, we initially simulate the "standard aodv"(SimpleAodv), Fig 7.1, routing protocol and the agenda is that no packet should be delivered from source to destination. This is done because no paths can be set due to the presence of black hole nodes in the network. Initial simulation is as follows:

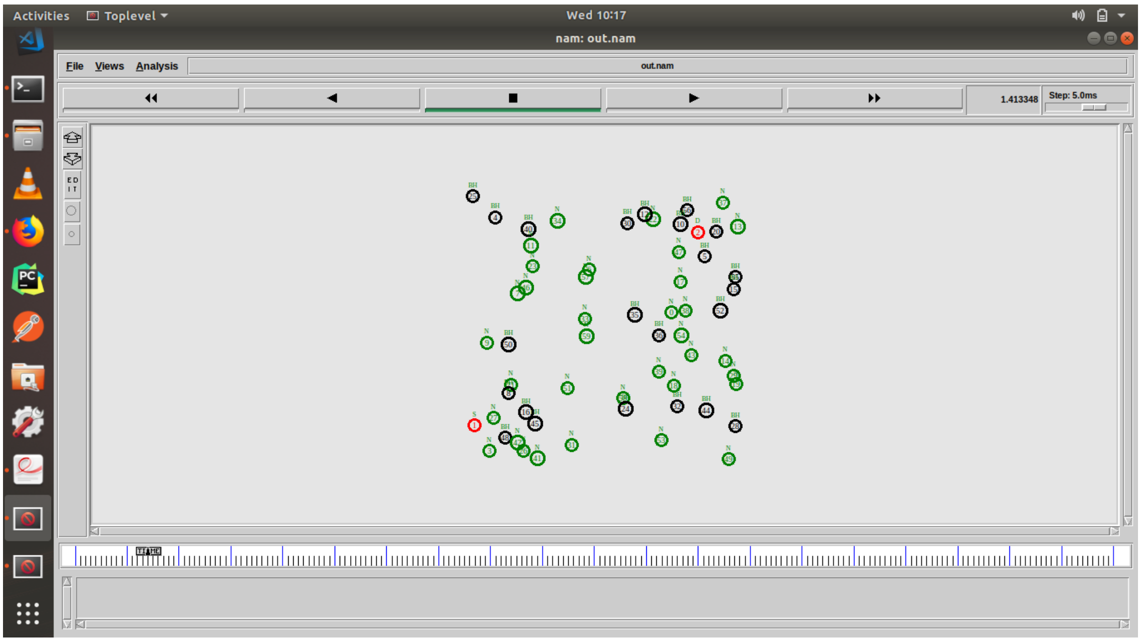


Figure 6.3: Simple AODV transmission with black hole

As we already mentioned in the simulation, in the next simulation test we simulate the "blackhole aodv" (Fig 6.3) routing protocol and the agenda is that the nodes must find an alternative path from source to destination without including the blackhole nodes in the network. Also all data packages should be delivered from source to destination in the newly set path. This is done because we blacklist all nodes responding to the bait request and while determining the path, we make sure that none of the nodes are included in the black list. The simulation is as follows:

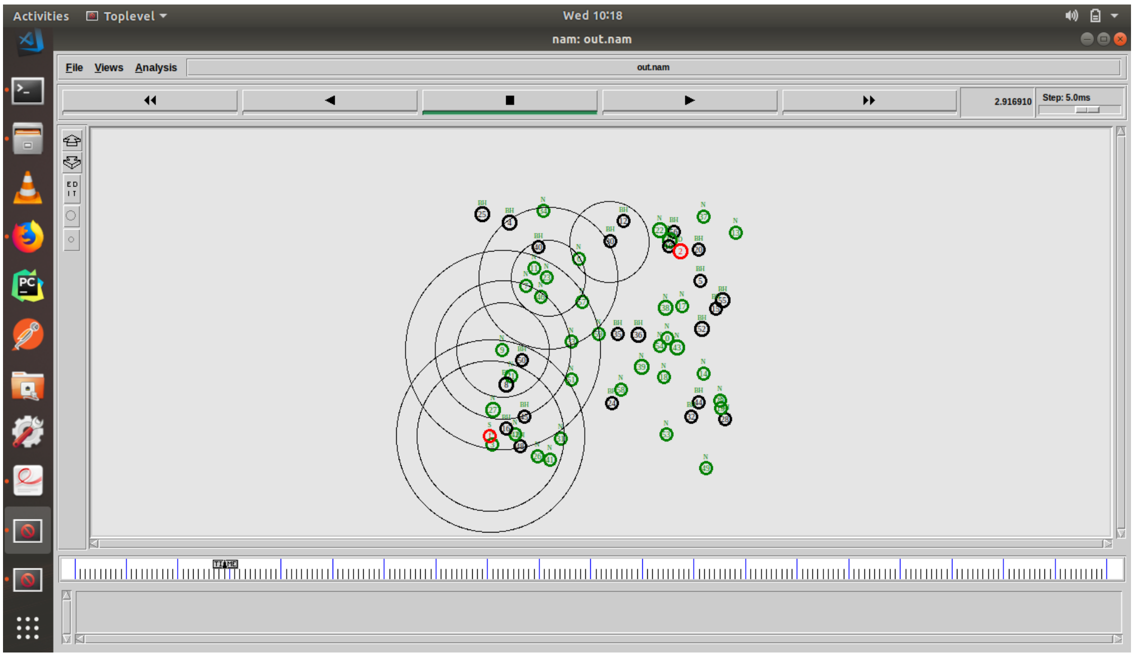


Figure 6.4: Transmission after applying Modified Bait

- **Throughput:** It is the number of data packets that were sent successfully from source to destination.

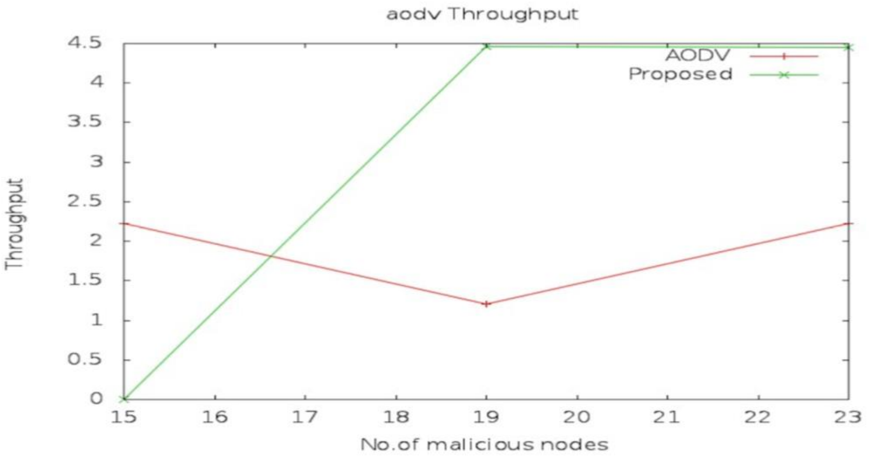


Figure 6.5: Graph plotted for throughput against number of malicious nodes.

In the throughput graph, we can see that the throughput for the "default aodv" is nearly constant because there is no transmission between source and destination. In the case of the proposed modified bait scheme, the throughput increases with the increase in the number of malicious nodes, which indicates the effectiveness of the proposed approach.

- **Delay**

  Delay is the latency occurred in the round trip of data packets. There shouldn’t be any delay in the default aodv because no transmission of data packets takes place.

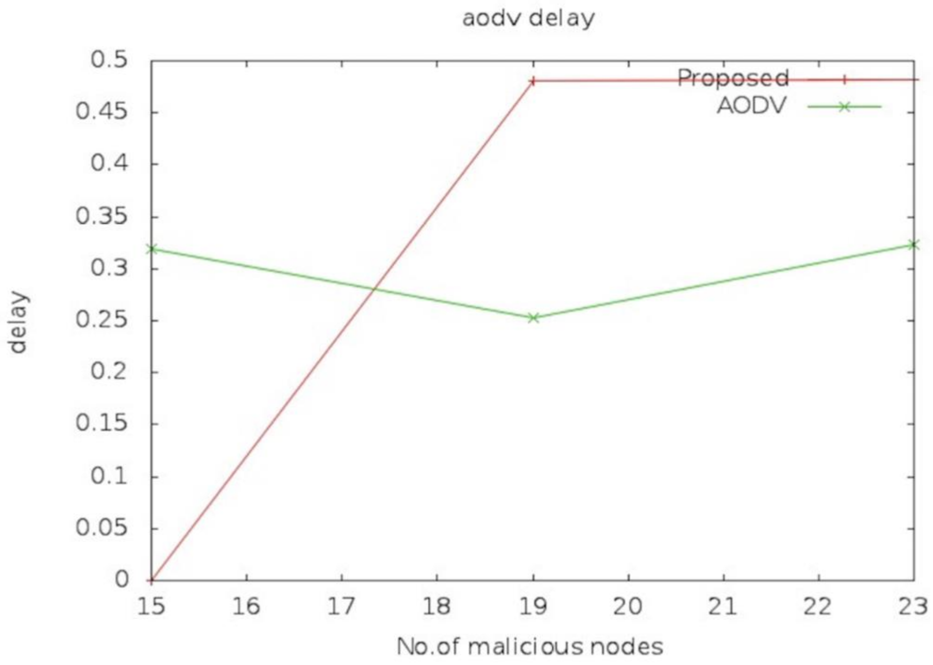


Figure 6.6: Graph plotted for delay against number of malicious nodes

As you can see in the delay graph, the delay for the routing protocol "by default aodv" is almost constant, because there is no data transfer between the source and the recipient. In the case of modified bait aodv (proposed) scheme, this delay will increase as the number of malicious nodes increases. This is because when the number of malicious nodes increases, it takes time to establish the route between the source and destination nodes.

- **Routing Overhead**

Routing overhead tells how many data packets are required for the communication in a network to take place. It is ratio of packets that is sent to packets received.

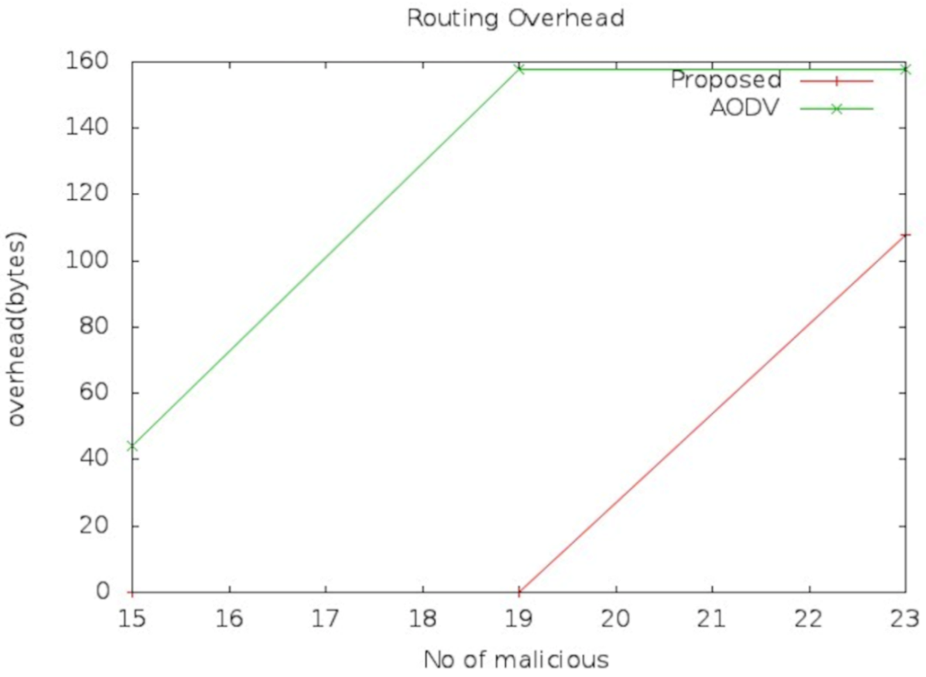


Figure 2.7: Graph plotted for routing over head against number of malicious nodes.

In the Routing over head, since we see that the routing costs for the "standard aodv" are very high compared to the modified bait scheme, this is due to the presence of malicious nodes in the standard aodv. It is very difficult for it to establish the path between the source and the final destination, which increases the overhead of routing. And with a modified bait scheme, as we have blacklisted all the nodes in the blacklist, establishing a route between the source and destination becomes easier.

CHAPTER 7

CONCLUSIONS

The above graph shows that a modified bait plan will be effective in identifying and keep the attack on MANETs under control of the AODV protocol. The proposed algorithm will ensure the safety of the MANET topology and keep the black hole from the dynamic route. The offered work will be easy on weight and will provide the big throughput, a share of transportation of parcels with lower beam delays. Indeed, even within the visibility of black hole nodes, the reliability of the node holes the network stayed the same as a normal network. Based on the above results, we conclude that the proposed plan skillfully recognizes and prevents an attack on black holes in the mobile network (MANETs).

7.1 Assumption

We are going to examine an ad-hoc wireless network with a set of nodes and assume that there is a possibility of one or more nodes of the attacker. Thus, we will implement our proposed algorithm to prevent and remove the attacker's node from the network.

7.2 Limitations

We used only one of the parameters to detect black hole nodes, and this parameter is nothing more than the answer to the bait request. Whatever nodes respond to the bait request, they will be pushed back into blacklist. We can also consider other parameters as well.

7.3 Future Enhancement

- This implementation can also be improvised to take into account other network parameters to detect and blacklist malicious nodes.
- This approach focuses solely on bait requests and the detection of malicious hosts, and thereby blacklisting them.
- This technique can be implemented for networks that are more robust for more efficient routing.
- This may be accomplished for Autonomous Mobile Mesh Network (AMMNETs) to prevent network partitioning.

REFERENCES

1) IEEE 802.11s-2011 Standard for Information Technology. Telecommunicationsand Information Exchange between Systems. Local and Metropolitan AreaNetworks. Specific Requirements. Part 11: Wireless LAN Medium AccessControl (MAC) and Physical Layer (PHY) Specifications. Amendment 10: Mesh Networking (IEEE, New York, 2007).

2) IEEE P802.11i/D10.0. Medium Access Control (MAC) Security Enhancements, Amendment 6 to IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks - Specific requirements - Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications. April, 2004.

3) IEEE Standard 802.1X-2001. IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control. June, 2001.

4) Jian-MingChang,Po-ChunTsou,IsaacWoungang,Han-ChiehChao,andChin-FengLai,"Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait DetectionApproach,"IEEESYSTEMSJOURNAL,MARCH2015

5) Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments, "Wireless Pers. Commun., vol. 29,pp. 367–388,2004.

6) K.Liu, D.Pramod ,K.Varshney, and K.Balakrishnan ,"An Acknowledgement based approach for the detection of routing misbehavior in MANETs, "IEEE Trans. Mobile Comput., vol. 6,no. 5,pp. 536–550, May 2007.

7) W. Wang, B. Bhargava, and M. Linderman, "Defending against collaborative packet drop attacks on MANETs," in Proc. 28th IEEE Int. Symp. Reliable Distrib. Syst., New Delhi, India, Sep. 2009.

8) L.Himral, V.Vigand N.Chand, "Preventing AODV Routing Protocol from Black Hole Attack", International Journal of Engineering Science and Technology(IJEST)Vol. 3,No. 5,2011.

9) Z. Alishahi, J. Mirabedini and M. K. Rafsanjani, "A new method for improving security in MANETs AODV Protocol",Management Science Letters2(2012)2271–2280.

10) Tariq Siddiqui and Tanveer Farooqui, "A Survey on Malicious Node Detection in MANET," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 12, December2014.

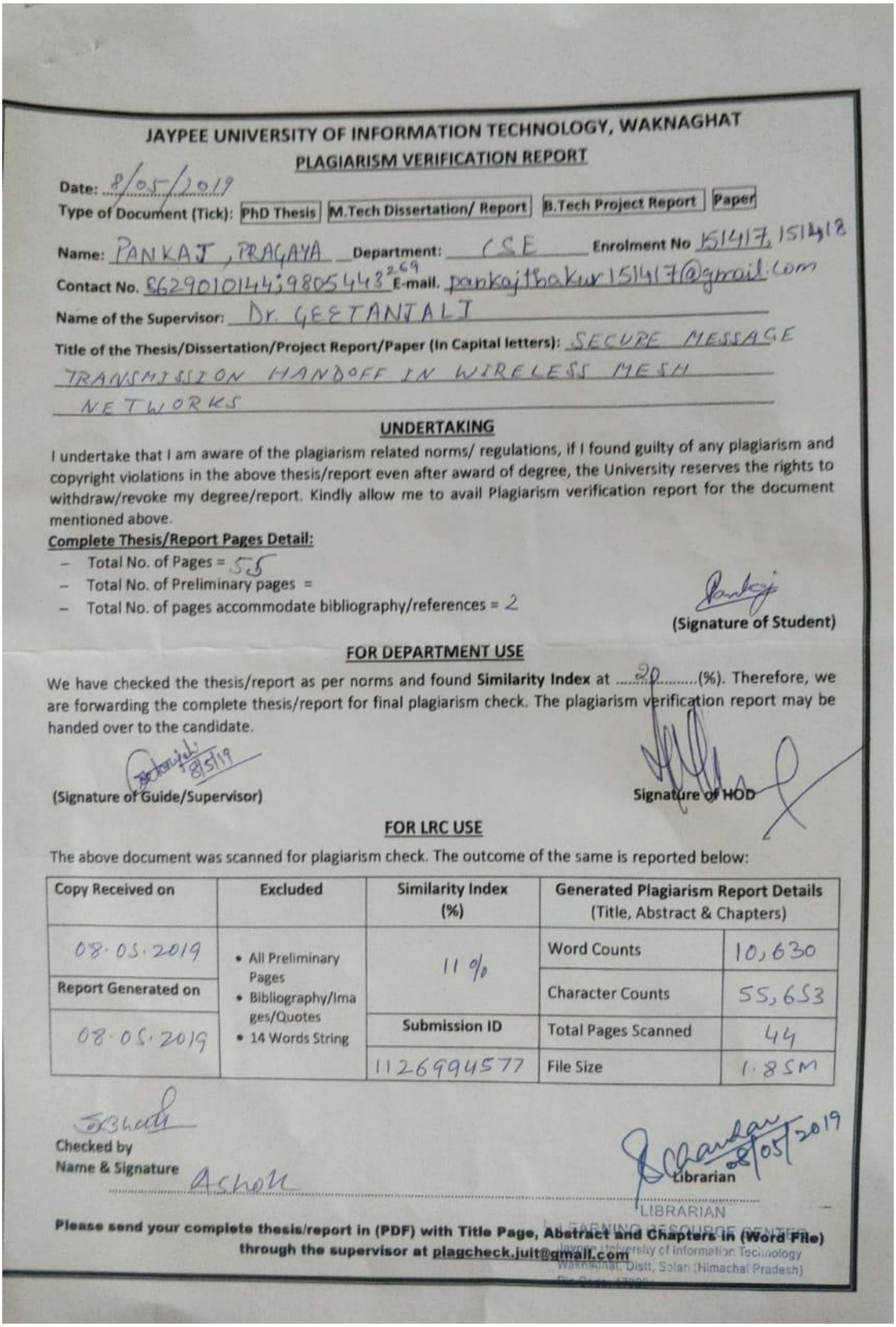
11) W. Kozma and L. Lazos, “REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits,” In Proceedings of the second ACM conference on Wirelessnetworksecurity,pp.103-110,2009.

12) P.-C.Tsou,J.-M.Chang,H.-C.Chao,andJ.-L.Chen,“CBDS:A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture,” in Proc. 2nd Intl. Conf. Wireless Commun., VITAE, Chenai, India, Feb. 28–Mar., 03, 2011.

13) S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in Proc. 6th Annu. Intl. Conf. MobiCom, 2000.

14) S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, “Prevention of cooperative blackhole attacks in wireless ad hoc networks,” in Proc. Int. Conf. Wireless Netw., Jun. 2003.

15) C. Perkins, E. B. Royer and S. Das, “Ad hoc On Demand Distance Vector (AODV) Routing, Internet Draft,” RFC 3561, IETF Network Working Group, July 2003.



JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

PLAGIARISM VERIFICATION REPORT

Date: 8/05/2019

Type of Document (Tick): PhD Thesis | M.Tech Dissertation/ Report | B.Tech Project Report | Paper

Name: PANKAJ , PRAGAYA Department: CSE Enrolment No 151417, 151418

Contact No. 8629010144;9805443269 E-mail. pankajthakur151417@gmail.com

Name of the Supervisor: Dr. GEETANJALI

Title of the Thesis/Dissertation/Project Report/Paper (In Capital letters): SECURE MESSAGE TRANSMISSION HANDOFF IN WIRELESS MESH NETWORKS

UNDERTAKING

I undertake that I am aware of the plagiarism related norms/ regulations, if I found guilty of any plagiarism and copyright violations in the above thesis/report even after award of degree, the University reserves the rights to withdraw/revoke my degree/report. Kindly allow me to avail Plagiarism verification report for the document mentioned above.

Complete Thesis/Report Pages Detail:

- Total No. of Pages = 55
- Total No. of Preliminary pages =
- Total No. of pages accommodate bibliography/references = 2

Pankaj

(Signature of Student)

FOR DEPARTMENT USE

We have checked the thesis/report as per norms and found **Similarity Index** at ...20.........(%). Therefore, we are forwarding the complete thesis/report for final plagiarism check. The plagiarism verification report may be handed over to the candidate.

Geetanjali 8/5/19

(Signature of Guide/Supervisor)

Signature of HOD

FOR LRC USE

The above document was scanned for plagiarism check. The outcome of the same is reported below:

Copy Received on	Excluded	Similarity Index (%)	Generated Plagiarism Report Details (Title, Abstract & Chapters)	
08.05.2019	• All Preliminary Pages • Bibliography/Images/Quotes • 14 Words String	11 %	Word Counts	10,630
Report Generated on			Character Counts	55,653
08.05.2019		Submission ID	Total Pages Scanned	44
		1126994577	File Size	1.85M

Checked by
Name & Signature Ashok

RChandan 08/05/2019
Librarian

Please send your complete thesis/report in (PDF) with Title Page, Abstract and Chapters in (Word File) through the supervisor at plagcheck.juit@gmail.com