COMPARISON EVALUATION OF PARAMETERS WITH AND WITHOUT ATTACK IN MANETS USING ALERT ROUTING PROTOCOL

DISSERTATION

Submitted in partial fulfillment of the
requirement for the award of the
Degree of

MASTER OF TECHNOLOGY
IN
Electronics and Communication Engineering

By

LOHIT KUMAR

Under the Guidance of

VISHALI SHARMA (ASSISTANT PROFESSOR)
PROJECT SUPERVISOR

LOVELY PROFESSIONAL UNIVERSITY

PHAGWARA (DISTT. KAPURTHALA), PUNJAB

School of Electronics and Communication
Lovely Professional University,
Punjab

DECEMBER 2014

CERTIFICATE

This is to certify that the Thesis titled “**Comparison evaluation of parameters with and without attack in MANETS using ALERT routing protocol**” that is being submitted by “***Lohit Kumar***” is in partial fulfillment of the requirements for the award of MASTER OF TECHNOLOGY DEGREE, is a record of bonafide work done under my guidance. The contents of this Thesis, in full or in parts, have neither been taken from any other source nor have been submitted to any other Institute or University for award of any degree or diploma and the same is certified.

Vishali Sharma
Supervisor
Lovely Professional University

Objective of the Thesis is satisfactory / unsatisfactory

Examiner I **Examiner II**

ACKNOWLEDGEMENT

I acknowledge with gratitude the tremendous inputs of my guide Asst. Professor **Vishali Sharma**, Lovely Professional University, for both initiating and motivating me in to research. It has been excruciating at times, as I have had to dwell upon the unheard and the unknown essential vitals to this research.

I am also grateful to **Prof. Bhupinder Verma,** Dean - Electronics and Communication Engineering, Lovely Professional University, Punjab for providing the facilities required for accomplishment of my Dissertation work at the university.

I am also grateful to the faculty of department of electronics and communication for continuous support, guidance and inspiration for effective and successful completion of this rewarding research.

I am also grateful to my parents and my friends who supported me in all my efforts.

Lohit Kumar
Reg. No.: 11200623

CERTIFICATE

This is to certify that Lohit Kumar bearing Registration no. 11200623 has completed objective formulation of thesis titled, **“Comparison evaluation of parameters with and without attack in MANETS using ALERT routing protocol”** 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 thesis has ever been submitted for any other degree at any University.

The thesis is fit for submission and the partial fulfillment of the conditions for the award of Degree of **Master of Technology** in **Electronics & Communication Engineering**.

Vishali Sharma
Assistant Professor
Lovely Professional University
Phagwara, Punjab.

Date:

DECLARATION

I, **Lohit Kumar**, student of **Master of Technology** under Department of Electronics and Communication Engineering of Lovely Professional University, Punjab, hereby declare that all the information furnished in this Dissertation report is based on my own intensive research and is genuine.

This thesis does not, to the best of my knowledge, contain part of my work which has been submitted for the award of my degree either of this university or any other university without proper citation.

Lohit Kumar
Registration No.: 11200623

Date:

ABSTRACT

Wireless Local Area Networks are the networks in which hundreds of computers are interconnected to share useful information. They come under the category of small scale networks. In WLAN users can be mobile while using the wireless network that means they can move anywhere within the range of network without getting disconnected with the network. WLAN operates in two different modes, infrastructure mode and ad hoc mode. Infrastructure mode contains special nodes called access points. These access points can interact with wireless nodes as well as with wired network. Ad hoc mode does not need any fixed infrastructure. Nodes communicate directly with each other. MANET is one type of ad hoc network which consists of a collection of mobile nodes which communicate without any centralized access point. Due to the limited transmission range of wireless network interfaces, multiple hops may be needed to exchange data between nodes in the network. Devices are free to join or leave the network and they may move randomly, possibly resulting in rapid and unpredictable topology changes. They highly support the situation where fixed infrastructure is not needed.

Aim of this dissertation is to add a new routing protocol and to evaluate the effect of implemented attack by comparing the parameters such as throughput and energy consumption. In this dissertation new routing protocol named proposed ALERT has been implemented which partitions the mobile nodes horizontally and vertically. This systematic partitioning of nodes prevents the mobile nodes from colliding with each other. Wormhole attack has been implemented on the network. Both these implementations have been done on back end. Two tcl files name wormhole and isolate have been created. In the wormhole tcl file attack has been implemented due to which the node starts to drop packets as shown in network animator screenshots. In the isolate file the attack has been countered due to which the packets will not drop as shown in network animator screenshots. Towards the end the results parameters such as throughput and energy consumption of both the files have been compared. Network Simulator-2 is proposed to be used as simulation tool to simulate results.

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ALERT	Anonymous Location-Based Efficient Routing Protocol
CPU	Central Processing Unit
CSMA/CA	Carrier Sense Multiple Access With Collision Avoidance
DARPA	Defense Advanced Research Projects Agency
DOS	Denial of Service
IPv4	Internet Protocol Version 4
IPv6	Internet protocol Version 6
LOS	Line of Sight
MAC	Medium Access Control
MANET	Mobile Ad hoc Network
PRNET	Packet Radio Network
QOS	Quality of Connection
SURAN	Survivable Radio Network
WLAN	Wireless Local Area Network
WSN	Wireless Sensor Network

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW OF WIRELESS SENSOR NETWORKS

Wireless Sensor Network consists of numerous tiny sensors deployed at high density in regions requiring surveillance and monitoring [1]. The sensors are deployed at a cost much lower than the traditional wired sensor system. A large number of sensors deployed will enable for accurate measurements. A Sensor Node consists of one or more sensing elements such as temperature, pressure etc., a battery, low power radio trans-receiver, microprocessor, mobilizer and a position finding system. With integration of information sensing, computation, and wireless communication, the sensor nodes can sense physical phenomena, process rough information, and report them to the sink [2]. Compared with the traditional Ad hoc networks, the energy of each sensor node is limited in wireless sensor networks [3]. Many design challenges that arise in sensor networks are due to the limited resources they have and their deployment in hostile environment. Sensor nodes are deployed in environments where it is impractical for humans to monitor them. The unattended nodes may affect the efficiency of many military and civil applications such as target field imaging, distributed computing, tactical surveillance, inventory control, disaster management and detecting ambient conditions. Some applications require sensors to be small in size and have short transmission ranges to reduce the chances of detection. These size constraints cause further constraints on CPU speed, amount of memory, RF bandwidth and battery lifetime. Therefore, efficient communication techniques are essential for increasing the lifetime and quality of data collection and decreasing the communication latency of such wireless devices.

Unlike the mobile ad hoc networks, sensor nodes are stationary for the entire period of their lifetime. Though the sensor nodes are fixed, still the topology of the network can change. When the nodes are low on activity, they can go to inactive sleep state to conserve energy. When some nodes run out of battery power and die, new nodes may be added to the network. Even though all nodes are initially equipped with equal energy, some nodes may experience higher activity because of region they are located in. An important property of sensor networks is the need of the sensors to reliably circulate the data to the base station within a time interval that allows the user to respond to the information in a timely manner, as out of date information is of no use and may lead to fatal results. Another important attribute is the scalability to the change in network size and topology. Sensor networks are very dense and slow when compared to mobile ad hoc and wired networks. This arises from the fact that the sensing range is lesser than the communication range and hence more nodes are required to achieve sufficient sensing coverage. Sensor nodes are required to be resistant to failures and attacks. Information routing is a very challenging task in Distributed Sensor Networks due to the inherent characteristics that distinguish these networks from other wireless or ad hoc networks. The sensor nodes deployed in an ad hoc manner need to be self-organizing as this kind of deployment requires system to form connections and cope with the resultant nodal distribution. Another important issue while designing sensor networks is that sensor networks are application specific. Hence the application scenario demands the protocol design in a sensor network. Also, the data collected by sensor nodes is often redundant and needs to be exploited by routing protocols to improve energy and bandwidth utilization. The proposed routing protocols for sensor networks should consider all the above issues for it to be very efficient. The algorithms developed need to be very energy efficient, scalable and increase the life of the network in the process. The multitudes of design challenges imposed on Sensor Networks tend to be quite complex and usually defy the analytical methods that are quite effective for traditional networks. At current stage of technology very few Sensor Networks have come into existence. Although there are many unsolved research problems in this domain, actual deployment and study is infeasible. The only practical alternate to study Sensor Networks is through simulation, which can provide better insight to behaviour and performance of various algorithms and protocols.

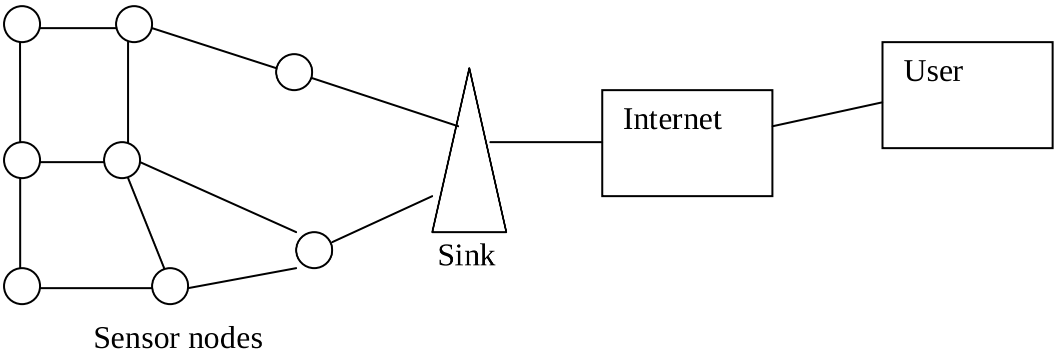


Figure 1.1: Wireless Sensor Network Structure.

If the node is not able to communicate with other through direct link, i.e. they are out of coverage area of each other; the data can be sent to the other node by using the nodes in between them. This property is referred as multi-hoping [4]. All sensor nodes work cooperatively to serve the requests. Generally WSNs are not centralized one as there is peer-to-peer communication between the nodes. So there is no requirement of prior established infrastructure to deploy the network. WSN gives flexibility of adding nodes and removing the nodes as required. But this gives rise to many drastic changes to deal with in the network topology such as updating the path, or the network tree, etc. In a WSN the node that gathers the data information is referred as a sink. The sink may be connected to the outside world through internet where the information can be utilized within time constraints [4]. The sensor nodes are small and inexpensive so they are deployed in large number. The resources are limited because sensor nodes are small, limited energy, bandwidth, and computational speed. The battery is limited so the life time of sensor nodes are also limited and the lifetime of sensor network is limited. Thus energy efficiency is a major issue for sensor networks [5].There are two types of WSNs: structured and unstructured. An unstructured WSN is one that contains a dense collection of sensor nodes. Sensor nodes may be deployed in an ad hoc manner into the field. Once deployed, the network is left unattended to perform monitoring and reporting functions. In an unstructured WSN, network maintenance such as managing connectivity and detecting failures is difficult since there are so many nodes. In a structured WSN, all or some of the sensor nodes are deployed in a pre-planned manner. The advantage of a structured network is that fewer nodes can be deployed with lower network maintenance and management cost. Fewer nodes can be deployed now since nodes are placed at specific locations to provide coverage while ad hoc deployment can have uncovered regions. Unlike traditional networks, a WSN has its own design and resource constraints. Resource constraints include a limited amount of energy, short communication range, low bandwidth, and limited processing and storage in each node. Design constraints are application dependent and are based on the monitored environment. The environment plays a key role in determining the size of the network, the deployment scheme, and the network topology. The size of the network varies with the monitored environment. For indoor environments, fewer nodes are required to form a network in a limited space whereas outdoor environments may require more nodes to cover a larger area. An ad hoc deployment is preferred over pre-planned deployment when the environment is inaccessible by humans or when the network is composed of hundreds to thousands of nodes. Obstructions in the environment can also limit communication between nodes, which in turn affects the network connectivity. [6]

1.1.1 Background of Sensor Network Technology

Researchers see WSNs as an ‘‘exciting emerging domain of deeply networked stems of low-power wireless motes2 with a tiny amount of CPU memory and large organized networks for high-resolution sensing of the environment’’ [7]. Sensors in WSN have many purposes, functions, and capabilities. The radar networks used in air traffic control, the national electrical power grid and nationwide weather stations deployed over a regular topographic mesh are all examples of early-deployment sensor networks but all of these systems use specialized computers and communication protocols and are very expensive. Much less expensive WSNs are now being planned for unique applications in physical security, healthcare and commerce. Sensor networking is a multidisciplinary area that involves, among others, radio and networking, signal processing, artificial intelligence, database management, systems architectures for operator-friendly infrastructure administration, resource optimization, power management algorithms, and platform technology (hardware and software, such as operating systems) [8]. Earthquake-oriented sensors in buildings can locate potential survivors and can help assess structural damage; tsunami-alerting sensors are useful for nations with extensive coastlines. Sensors also find extensive applicability on the battlefield for reconnaissance and surveillance.

Power efficiency in WSN is accomplished in three ways:

- Low duty cycle operation.
- Local-network processing to reduce data volume (and hence transmission time).
- Multi hop networking reduces the requirement for long-range transmission since signal path loss is an inverse exponent with range or distance. Each node in the sensor network can act as a repeater thereby reducing the link range coverage required and in turn the transmission power [9]

1.1.2 Types of Sensor Networks

There are five types of WSNs: terrestrial WSN, underground WSN, underwater WSN, multi-media WSN, and mobile WSN.

- **Terrestrial WSNs**

  They typically consist of hundreds to thousands of inexpensive wireless sensor nodes deployed in a given area, either in an ad hoc or in a pre-planned manner. In ad hoc deployment, sensor nodes can be dropped from a plane and randomly placed into the target area. In pre-planned deployment, there is grid placement, optimal placement, 2-d and 3-d placement models. In a terrestrial WSN, reliable communication in a dense environment is very important. Terrestrial sensor nodes must be able to effectively communicate data back to the base station. While battery power is limited and may not be rechargeable, terrestrial sensor nodes however can be equipped with a secondary power source such as solar cells. In any case, it is important for sensor nodes to conserve energy. For a terrestrial WSN, energy can be conserved with multi-hop optimal routing, short transmission range, in-network data aggregation, eliminating data redundancy, minimizing delays, and using low duty-cycle operations.

- **Underground WSNs**

  They consist of a number of sensor nodes buried underground or in a cave or mine used to monitor underground conditions. Additional sink nodes are located above ground to relay information from the sensor nodes to the base station. An underground WSN is more expensive than a terrestrial WSN in terms of equipment, deployment, and maintenance. Underground sensor nodes are expensive because appropriate equipment parts must be selected to ensure reliable communication through soil, rocks, water, and other mineral contents. The underground environment makes wireless communication a challenge due to signal losses and high levels of attenuation. Unlike terrestrial WSNs, the deployment of an underground WSN requires careful planning and energy and cost considerations. Energy is an important concern in underground WSNs. Like terrestrial WSN, underground sensor nodes are equipped with a limited battery power and once deployed into the ground, it is difficult to recharge or replace a sensor node’s battery. As before, a key objective is to conserve energy in order to increase the lifetime of network.

- **Underwater WSNs**

  They consist of a number of sensor nodes deployed underwater. As opposite to terrestrial WSNs, underwater sensor nodes are more expensive and fewer sensor nodes are deployed. Autonomous underwater vehicles are used for exploration or gathering data from sensor nodes. Compared to a dense deployment of sensor nodes in a terrestrial WSN, a sparse deployment of sensor nodes is placed underwater. A challenge in underwater communication is the limited bandwidth. Another challenge is sensor node failure due to environmental conditions. Underwater sensor nodes must be able to self-configure and adapt to harsh ocean environment. Underwater sensor nodes are equipped with a limited battery which cannot be replaced or recharged. The issue of energy conservation for underwater WSNs involves developing efficient underwater communication and networking techniques.

- **Multi-media WSNs**

  They have been proposed to enable monitoring and tracking of events in the form of multimedia such as video, audio, and imaging. Multi-media WSNs consist of number of low cost sensor nodes equipped with cameras and microphones. These sensor nodes interconnect with each other over a wireless connection for data retrieval and process. Multi-media sensor nodes are deployed in a pre-planned manner into the environment to guarantee coverage. Challenges in multi-media WSN include high bandwidth demand, high energy consumption, quality of service provisioning, data processing. Multi-media content such as a video stream requires high bandwidth in order for the content to be delivered. As a result, high data rate leads to high energy consumption. Transmission techniques that support high bandwidth and low energy consumption have to be developed.

- **Mobile WSNs**

  They consist of a collection of sensor nodes that can move on their own and interact with the physical environment. Mobile nodes have the ability sense, compute, and communicate like static nodes. A key difference is mobile nodes have the ability to reposition and organize itself in the network. A mobile WSN can start off with some initial deployment and nodes can then spread out to gather information. Information gathered by a mobile node can be communicated to another mobile node when they are within range of each other. Another key difference is data distribution. In a static WSN, data can be distributed using fixed routing or flooding while dynamic routing is used in a mobile WSN. Challenges in mobile WSN include deployment, localization, self-organization, navigation and control, coverage, energy, maintenance, and data process. [6]

1.1.3 Advantages of Wireless Sensor Networks

There are some advantages of wireless sensor network over wired ones.

- **Ease of Deployment**

  The wireless sensor networks can be deployed at the interested site without any pre organization. Thus saving the installation cost and increasing the flexibility

- **Extended range**

  One huge wired sensor can be replaced by many small wireless sensor networks for the same cost. One sensor can sense only small area whereas network of small sensors can be distributed over a wider region.
- **Fault tolerant**

  Since sensor networks are mostly unattended, they should possess fault tolerant capability. If one sensor fails then it doesn’t affect the network operation much because there are other nodes also collecting the same data. The data accuracy may be reduced.
- **Mobility**

  Since wireless sensors are equipped with battery, they have limited mobility. Thus if a region becomes unmonitored the nodes can re arrange themselves to distribute evenly which means that these nodes can be made to move towards the area of interest. [10]

1.1.4 Applications of Sensor Networks

Traditionally sensor networks have been used in the context of some high-end applications such as radiation and nuclear-threat detection systems over-the-horizon weapon sensors for ships, biomedical applications and seismic monitoring. Most recently the interest has been focusing on networked biological and chemical sensors for national security applications. Furthermore evolving interest extends to direct consumer applications. Existing and important applications of sensor networks includes military sensing, physical security, air traffic control, traffic surveillance, video surveillance, industrial and manufacturing automation, process control, inventory management, distributed robotics, weather sensing, environment monitoring, national border monitoring, and building and structures monitoring [11]. A short list of applications is as follows:

1.1.4.1 Military applications

- Monitoring enemy forces.
- Monitoring friendly forces and equipment.
- Military or battlefield surveillance.
- Targeting.
- Battle damage assessment.
- Nuclear, biological, and chemical attack detection.

1.1.4.2 Environmental applications

- Microclimates.
- Agriculture Research.
- Forest fire detection.
- Flood detection.

1.1.4.3 Health applications

- Remote monitoring of physiological data.
- Tracking and monitoring doctors and patients inside a hospital.
- Drug administration.
- Elderly assistance.

1.1.4.4 Home applications

- Home automation.
- Instrumented environment.
- Automated meter reading.

1.2 INTRODUCTION TO WLAN

Wireless technology has eased the networking by enabling multiple computers to simultaneously share the resources in home or at office. Wireless networking enables the same capabilities and comparable speeds of a wired network without many difficulties like laying wire, drilling into walls or stringing Ethernet cables throughout an office building.

Reasons to choose wireless networking over traditional wired networks are:

- Introducing additional wires or drilling new holes in home or at office could be prohibited or too expensive.
- Flexibility of location and data ports is required.
- Roaming facility is desired; e.g. connectivity should be maintained from almost anywhere inside a home or office.

An interesting usage of computers networks is in office and educational institutions, where hundreds of personal computers are interconnected to exchange the information. These privately owned networks are known as local area networks (LAN). They come under the category of small scale network. Such type of wire free network is called wireless local area network (WLAN).

1.2.1 Wireless LAN Standards

There are several wireless LAN solutions available today, with varying levels of standardization and interoperability. The solution that currently leads the industry is Wi-Fi. The 802.11 technologies enjoy wider industry support and are targeted to solve enterprise, home and even public hot spot wireless LAN needs.

IEEE released the 802.11 specification in July 1999 which uses 2.4GHz frequency and maximum data rate of 1-2 Mbps. In late 1999 two new specifications were released. The 802.11b specification increased the data rate up to 11Mbps in range of 2.4GHz while 802.11a uses 5GHz range and uses data rate up to 54Mbps.Unfortunately these new specifications were incompatible because they used different frequencies. This incompatibility force the creation of new specification known as 802.11g which supports up to 54Mbps and can use the information of 802.11b.[12]

- **802.11a**

  802.11a operates in 5-6GHz range with data rates in 6Mbps, 12Mbps, and 24Mbps range.802.11a uses orthogonal frequency division multiplexing standard therefore data rate can be as high as 54Mbps.As it operates on 5 GHz band which is relatively unused. It gives 802.11a a significant advantage. The disadvantage of 802.11a is that its signals are absorbed more readily by walls and other solid objects due to their smaller wavelength and as a result they cannot penetrate as far as those of 802.11b.
- **802.11b**

  802.11b standard operates in 2.4GHz range up to 11Mbps data rate.802.11b uses complementary code keying modulation. 802.11b devices experience interference from other products operating in the 2.4 GHz band. Some of the devices which operate in the 2.4 GHz range are microwave ovens, Bluetooth devices and cordless telephones.
- **802.11g**

  It operates at 2.4GHz with data rate 54Mbps over a limited range. It is fully compatible with 802.11b.It uses orthogonal frequency division multiplexing scheme.
- **802.11n**

  802.11n operates on 2.4GHz and 5GHz is optional. It is a slight improvement of 802.11 and uses multiple-input-multiple-output antennas.[13]

1.2.2 Types of WLAN

Wireless LAN has two modes of operation: ad hoc mode and infrastructure mode.

1.2.2.1 Ad hoc Mode

Ad hoc mode does not rely on pre existing infrastructure, such as routers in wired networks or access point in wireless networks. Instead, each node participates in routing by forwarding data for other nodes. The nodes transmit peer to peer that is directly to each other without the involvement of any base station or access point..An example of ad hoc mode is mobile ad hoc networks.

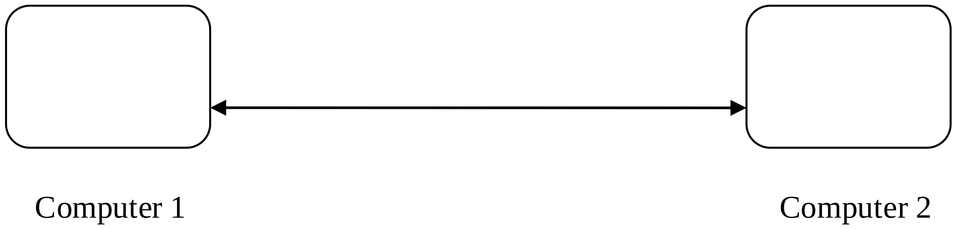


Figure 1.2: Peer to Peer.

1.2.2.2 Infrastructure Mode

In infrastructure mode nodes communicate through an access point which serves as a bridge to other nodes. Setting up an infrastructure mode network requires at least one access point. This access point is connected to the devices like computers, laptops, smart phones.

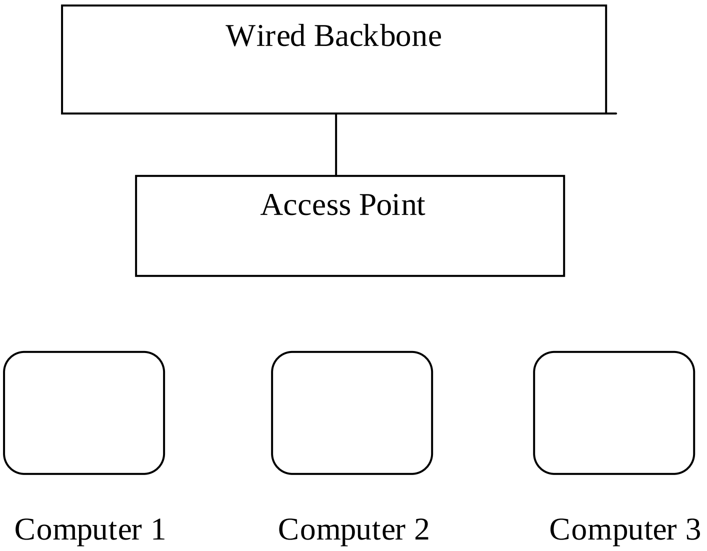


Figure 1.3: Infrastructure Mode.

1.2.3 Issues in WLAN

Users of wireless network will want same services as that of wired network. But to meet these objectives wireless networks faces some issues which are-

1.2.3.1 Frequency Allocation

Operation of a wireless network requires that all users operate on a common frequency band. Frequency bands for particular uses must typically be approved and licensed in each country, which is a time-consuming process due to the high demand for available radio spectrum.

1.2.3.2 Interference and Reliability

Interference in wireless communications can be caused by simultaneous transmissions by two or more sources sharing the same frequency band. Collisions are typically the result of multiple stations waiting for the channel to become idle and then beginning transmission at the same time. Collisions are also caused by the "hidden terminal" problem, where a station, believing the channel is idle, begins transmission without successfully detecting the presence of a transmission already in progress. Interference is also caused by multipath fading, which is characterized by random amplitude and phase fluctuations at the receiver.

1.2.3.3 Security

In a wired network, the transmission medium can be physically secured, and access to the network is easily controlled. A wireless network is more difficult to secure, since the transmission medium is open to anyone within the geographical range of a transmitter. Data privacy is usually accomplished over a radio medium using encryption. While encryption of wireless traffic can be achieved, it is usually at the expense of increased cost and decreased performance.

1.2.3.4 Power Consumption

Typically, devices connected to a wired network are powered by the local 110 V commercial power provided in a building. Wireless devices, however, are meant to be portable and/or mobile, and are typically battery powered. Therefore, devices must be designed to be very energy-efficient, resulting in "sleep" modes and low-power displays, causing users to make cost versus performance and cost versus capability trade-offs.

1.2.3.5 Mobility

Unlike wired terminals, which are static when operating on the network, one of the primary advantages of wireless terminals is freedom of mobility. [14]

1.2.4 Uses of WLAN

Wireless computer networks are capable of offering many functionalities. WLANs are very flexible and can be configured in a variety of topologies based on the application. Some of the uses of WLANs are mentioned below.

- Users can surf the internet, check e-mails on the move.
- There are many historic buildings where there is need to set up computer networks. In such places wiring man not be permitted. WLANs are very good solution in such places.
- In the areas affected by earthquake or any other disaster, no suitable infrastructure may be available on the site. WLANs are handy in such locations.

Table 1.1: Difference between cellular network and ad hoc network.

Cellular Network	Ad hoc Network
Fixed infrastructure based.	Infrastructure less.
Single hop wireless link.	Multi hop wireless link.
Centralized routing.	Distributed routing.
Circuit switched.	Packet switched.
Seamless connectivity.	Frequent path breaks.
High cost and time of deployment.	Quick and Cost effective deployment.
Easier to achieve time synchronization.	Time synchronization is difficult.

1.3 INTRODUCTION TO MANET

The field of wireless and mobile communications has experienced an unmatched growth during the past decade. Now a day’s mobile users can use their cellular phone to check their email and browse the Internet. Recently, an increasing number of wireless local area network (LAN) hot spots is emerging, allowing travellers with portable computers to surf the Internet from airports, railways, hotels and other public locations. Broadband Internet access is driving wireless LAN solutions in the home for sharing access between computers. However, all these networks are conventional wireless networks, conventional in the sense that as prerequisites, a fixed network infrastructure with centralised administration is required for their operation, potentially consuming a lot of time and money for set-up and maintenance. Furthermore, an increasing number of devices such as laptops, tablet PCs, smart phones, MP3 players, digital cameras, etc. are provided with short-range wireless interfaces. In addition, these devices are getting smaller, cheaper, more user friendly and more powerful. This evolution is driving a new alternative way for mobile communication, in which mobile devices form a self creating, self-organising and self-administering wireless network, called a mobile ad hoc network. [15]

MANET consists of a collection of mobile nodes forming a dynamic autonomous network. Nodes communicate with each other without any centralized access points or base stations. Applications of MANET can be found in situations such as emergency search and-rescue operations, meetings or conventions (in which users wish to quickly share information), and data acquisition operations in hostile terrain. In situations like battlefields or major disaster areas, ad hoc networks need to be deployed immediately without base stations or wired infrastructure [16]. In such a network, each node acts as a host, and may act as a router.

Security is a major concern to mobile ad hoc networks because a MANET system is much more vulnerable to malicious things than a wired network. Unlike wired networks where an attacker must gain physical access to the network wires or pass through several lines of defence at firewalls, attacks on a wireless network can come from any directions and can be targeted on any node.

Damages can include leaking secret information and message contamination. This means that a wireless ad-hoc network will not have a clear line of defence, and every node must be prepared for encounters with an enemy directly or indirectly. The mobile nodes are autonomous units that are capable of moving independently which means that nodes with inadequate physical protection have threat of being captured and hijacked. Tracking down a particular mobile node in a large scale ad hoc network is very difficult task whereas attacks by a compromised node from within the network are far more damaging and much harder to detect.

Due to the limited transmission range of wireless network interfaces, multiple hops may be needed to exchange data between nodes in the network. Due to frequent changes in the network topology and limited network resources, routing in MANET experiences link failure more often. Mechanisms which are used to describe the QOC for extracting the links connecting the pair of best stable nodes over time from the network point of view, uses degree of connectivity as the criteria for preferred neighbour election [17].

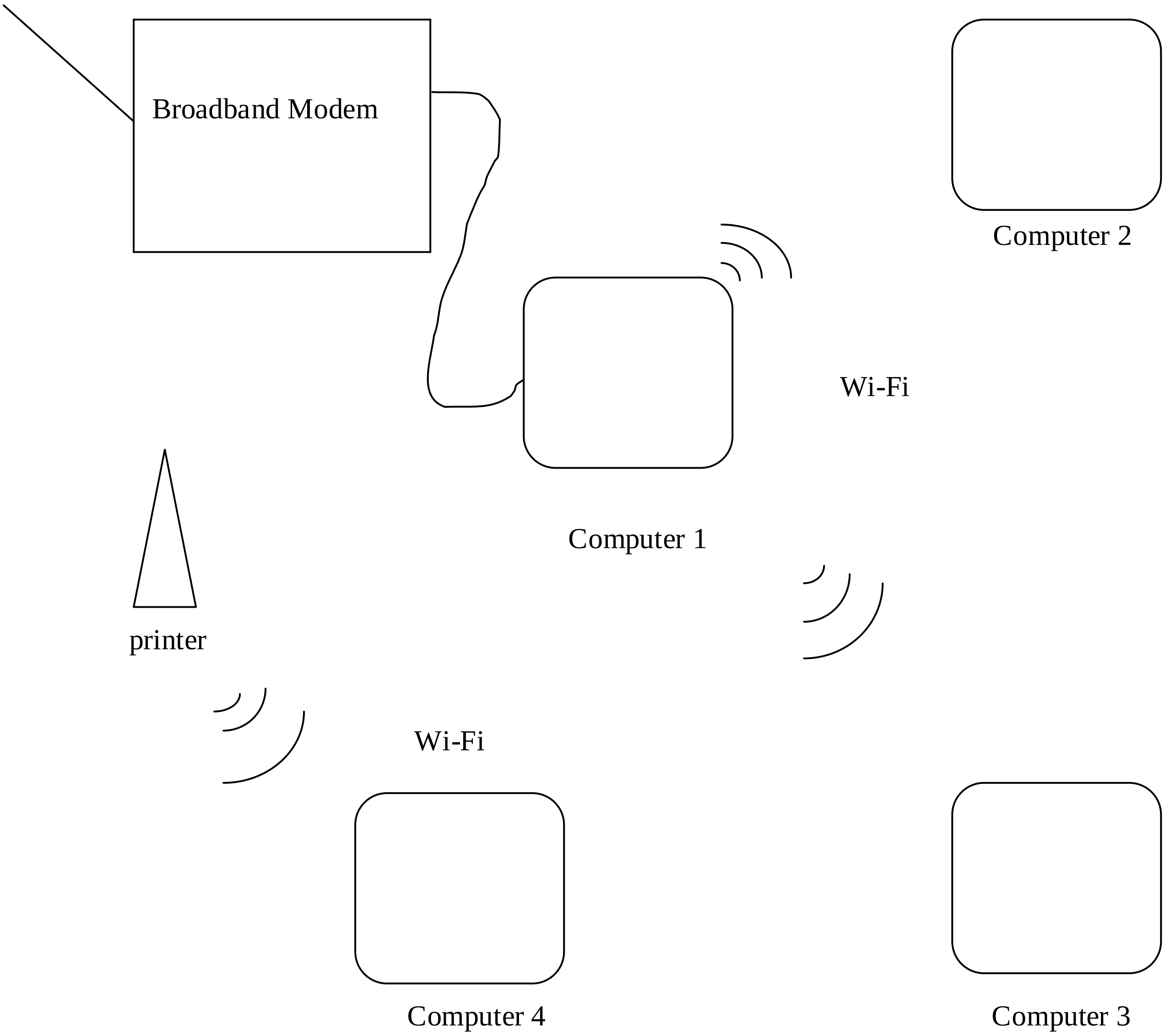


Figure 1.4: MANET Structure.

Nodes that lie within each other's send range can communicate directly and are responsible for dynamically discovering each other. In order to enable communication between nodes that are not directly within each other's send range, intermediate nodes act as routers that relay packets generated by other nodes to their destination. These nodes are often energy constrained— that is, battery-powered— devices with a great diversity in their capabilities. Furthermore, devices are free to join or leave the network and they may move randomly, possibly resulting in rapid and unpredictable topology changes. In this energy-constrained, dynamic, distributed multi-hop environment, nodes need to organise themselves dynamically in order to provide the necessary network functionality in the absence of fixed infrastructure or central administration [15].

1.3.1 MANET Evolution

Historically, mobile ad hoc networks have primarily been used for tactical network related applications to improve battlefield communications/ survivability. The dynamic nature of military operations means that military cannot rely on access to a fixed pre-placed communication infrastructure in battlefield. Pure wireless communication also has limitation in that radio signals are subject to interference and radio frequency higher than 100 MHz rarely propagate beyond LOS. Mobile ad hoc network creates a suitable framework to address these issues by providing a multi-hop wireless network without pre-placed infrastructure and connectivity beyond LOS. Early ad hoc networking applications can be traced back to the Packet Radio Network (PRNET) project in 1972 which was primarily inspired by the efficiency of the packet switching technology, such as bandwidth sharing and store and forward routing, and its possible application in mobile wireless environment. By using multi-hop store-and-forward routing techniques, the radio coverage limitation is removed, which effectively enables multi-user communication within a very large geographic area. Survivable Radio Networks (SURAN) was developed by DARPA in 1983 to address main issues in PRNET in the areas of network scalability, security, processing capability and energy management. The main objectives were to develop network algorithms to support a network that can scale to tens of thousands of nodes and withstand security attacks, as well as use small, low-cost, low-power radios that could support sophisticated packet radio protocols. This effort results in the design of Low-cost Packet Radio technology in 1987 which features a digitally controlled spread-spectrum radio with an integrated Intel 8086 microprocessor-based packet switch. In addition, a family of advanced network management protocols was developed and hierarchical network topology based on dynamic clustering is used to support network scalability. Other improvements in radio adaptability, security, and increased capacity are achieved through management of spreading keys. Towards late 1980s and early 1990s, the growth of the Internet infrastructure and the microcomputer revolution made the initial packet radio network ideas more applicable and feasible. Several networking designs were explored; for example Wireless Internet Gateways deploys a flat peer-to-peer network architecture. Tactical Internet implemented by US Army at 1997 is by far the largest-scale implementation of mobile wireless multi-hop packet radio network. Direct-sequence spread-spectrum, time division multiple access radio is used with data rates in the tens of kilobits per second ranges, while modified commercial internet protocols are used for networking among nodes. It reinforces the perception that commercial wire line protocols were not good at coping with topology changes as well as low data rate and high bit error rate wireless links. In 1999 Extending the Littoral Battle space Advanced Concept Technology Demonstration was another MANET deployment exploration to demonstrate the feasibility of Marine Corps war fighting concepts that require over the horizon communications from ships at sea to Marines on land via an aerial relay. Approximately 20 nodes were configured for the network Lucent s Wave LAN and VRC-99A were used to build the access and backbone network connections. In the middle of 1990, with the definition of standards commercial radio technologies begun to appear on the market, and the wireless research community became aware of the great commercial potential and advantages of mobile ad hoc networking outside the military domain. Most of the existing ad hoc networks outside the military arena have been developed in the academic environment, but recently commercially oriented solutions started to appear. [18]

1.3.2 Technical issues

Some of the properties of MANET impose challenges to network protocol. The physical layer must deal with rapid changes in link characteristics. The MAC layer needs to allow fair channel access, minimise packet collisions and deal with hidden and exposed terminals. At the network layer, nodes need to cooperate to calculate paths. The transport layer must be capable of handling packet loss and delay characteristics that are very different from wired networks. Applications should be able to handle possible disconnections and reconnections [15].

1.3.2.1 Routing

As mobile ad hoc networks are characterised by a multi-hop network topology that can change frequently due to mobility, efficient routing protocols are needed to establish communication paths between nodes, without causing excessive control traffic overhead or computational burden on the power constrained devices. A number of proposed solutions attempt to have an up-to-date route to all other nodes at all times. To this end, these protocols exchange routing control information periodically and on topological changes. These protocols which are called proactive routing protocols are typically modified versions of traditional link state or distance vector routing protocols encountered in wired networks, adapted to the specific requirements of the dynamic mobile ad hoc network environment. Most of the time, it is not necessary to have an up-to-date route to all other nodes. Therefore, reactive routing protocols only set up routes to nodes they communicate with and these routes are kept alive as long as they are needed. Combinations of proactive and reactive protocols, where nearby routes are kept up-to-date proactively, while far-away routes are set up reactively, are also possible and fall in the category of hybrid routing protocols. A completely different approach is taken by the location-based routing protocols, where packet forwarding is based on the location of a node's communication partner [15].

1.3.2.2 Services and Resource Discovery

MANET nodes may have little or no knowledge at all about the capabilities of or services offered by each other. Therefore service and resource discovery mechanisms which allow devices to automatically locate network services and to advertise their own capabilities to the rest of the network are an important aspect of self-configurable networks [19]. In directory less service nodes request services when needed or they announce their service to others. In directory based service services are registered and services are handled.

1.3.2.3 Addressing and internet connectivity

If the nodes need to communicate in the ad-hoc network then they must require an address. An internal address organization with prefixes is hard to maintain in mobile ad-hoc network due to node mobility. One solution is based on the assumption (and restriction) that all MANET nodes already have a static, globally unique and pre-assigned IPv4 or IPv6 address. This solves the whole issue of assigning addresses [15].

1.3.2.4 Security and node cooperation

In mobile ad hoc network if the malicious node is within the radio range of other nodes then it can easily communicate with those nodes and can join the network automatically. MANETs are exposed to various security attacks. In passive attacks the attacker just listens to the channel for some important information. This type of attack is hard to detect because it does not add any new traffic to network. In active attacks the attacker ruins the normal ongoing operations in the network. Preventive mechanisms include among others authentication of message sources, data integrity and protection of message sequencing [15].

1.3.2.5 Limited Power Supply

The nodes of MANETs are restricted to limited power supply which creates a lot of problem. Since the malicious node knows that the target node has limited power either it can continuously send additional packets to the target and ask it routing those additional packets, or it can induce the target to be trapped in some kind of time-consuming computations. In this way, the battery power of the target node will be exhausted by these meaningless tasks, and thus the target node will be out of service to all the benign service requests since it has run out of power [19].

1.3.3 Security solution to MANET

1.3.3.1 Availability

Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it [20].

1.3.3.2 Integrity

Integrity is mainly of two types-malicious alerting and accidental alerting [21]. A message can be removed by malicious node with malicious goal which is known as malicious alerting. If the content of message is changed due to transmission error in communication then it is known as accidental alerting.

1.3.3.3 Confidentiality

Confidentiality means that particular information is accessible to those who are authorized to access it. No one can access that information except the authorized person. Data encryption can be done to keep the data confidential

1.3.4 Different types of attacks on MANET

1.3.4.1 Passive Attacks

A passive attack does not disturb the operation of the network. In this the attacker generally gathers the information about the network. Detection of this attack is difficult because it does not affect the data traffic of the network. An example of passive attack is snooping, discussed below.

- **Snooping**

  Accessing other person's data in an unauthorized way is known as snooping. Watching other person's email and watching what other person is typing are some of the examples of snooping. The attacker use snooping to capture password and login information.

1.3.4.2 Active Attacks

Active attack disturbs the normal functioning of the network. Active attacks are classified into two categories-external attacks and internal attacks. External attacks are carried out by the nodes which are not authorized to the network whereas internal attacks are carried out by the nodes which are part of the network. Since the nodes are part of the network in internal attacks this attack is hard to detect and severe.

- **Wormhole Attack**

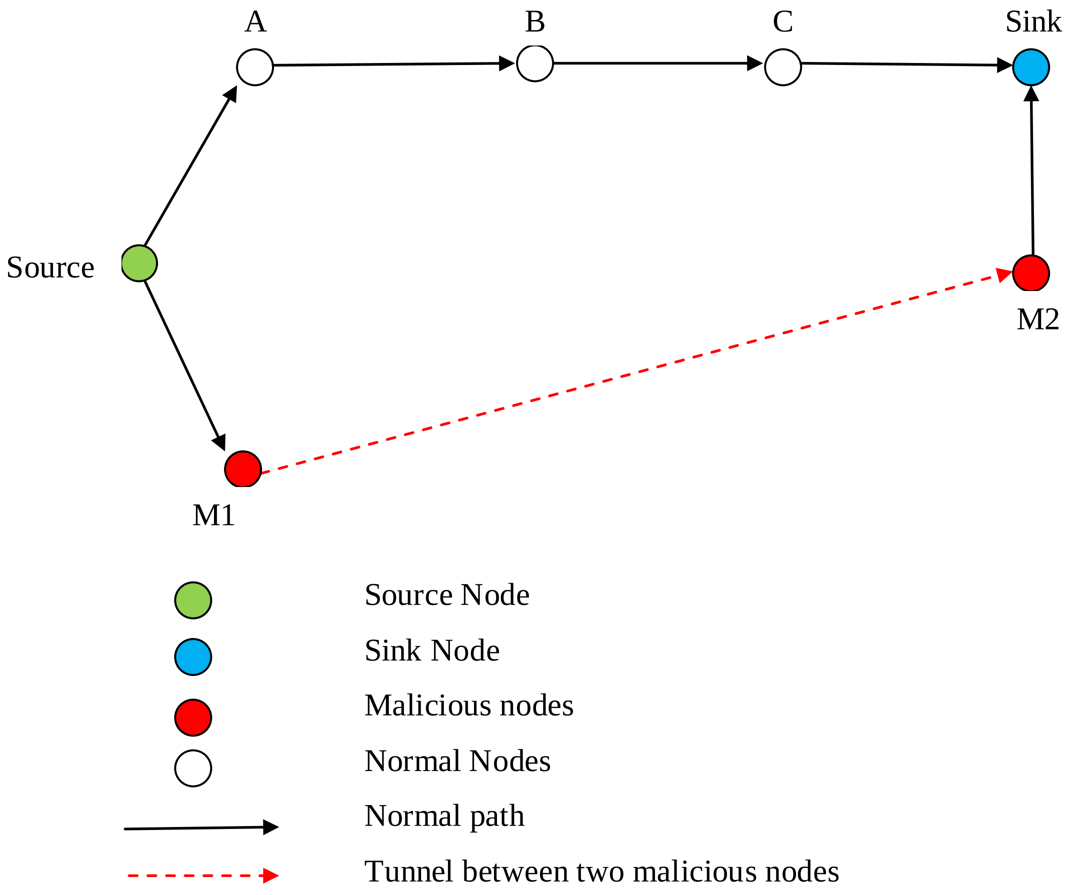


Figure 1.5: Wormhole Attack.

When the malicious node receive packet at one location and tunnels them to the other malicious node at another location. From there these packets are again resend to the network. Due to this the replica of packets are created. This tunnelling between malicious nodes is known as wormhole.

- **Blackhole Attack**

  In blackhole attack the attacker listens to the route and as soon as it receives the request for route to the destination node it sends reply to the source node. If the malicious reply reaches the source node then the actual reply then fake route will be created. After this the malicious node will drop all the packets to disturb the whole network.

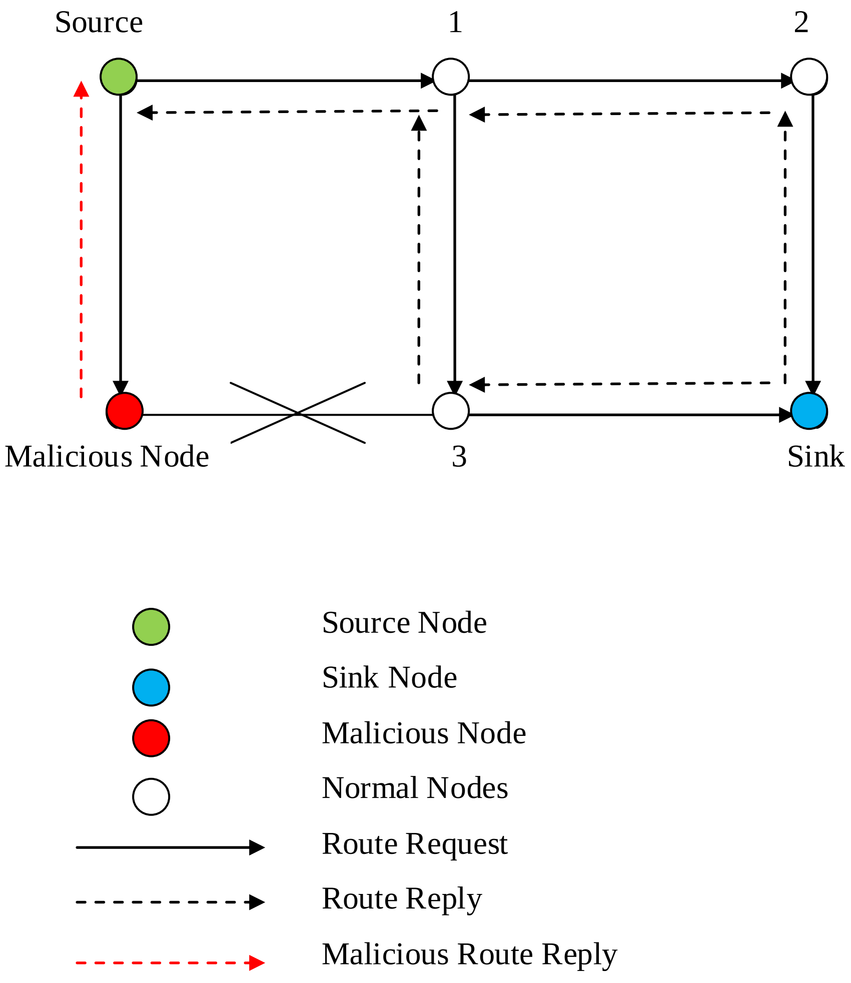


Figure 1.6: Blackhole Attack.

- **Information Disclosure**

  During the communication process the private information must be protected. Important data on nodes may contain location of node, detail of node, password etc. This data must be protected from unauthorized access

- **Resource Consumption Attack**

  In this the attacker tries to waste the limited resources like battery power, of other nodes which are there in the network.

- **Routing Attacks**

  Various attacks are there which are based on routing and they disturb the normal functioning of network. Some of the attacks based on routing are:

➢ **Routing Table Overflow**

It prevents new routes from being created by creating enough routes. In reactive routing algorithm we find the route only when it is needed whereas in proactive routing algorithm we need to know the routing information even before it is needed. Its basic goal is to prevent new routes and cause an overflow of routing table.

➢ **Routing Table Positioning**

In routing table poisoning, the compromised nodes present in the networks send fictitious routing updates or modify genuine route update packets sent to other authorized nodes. Routing table poisoning may result in congestion in portions of the network, or even make some parts of the network inaccessible [16].

➢ **Packet Replication**

In packet replication the malicious node sends the duplicate packets to the network. This consumes lot of power of the nodes and cause confusion in routing.

➢ **Rushing Attack**

When the malicious node receive the route request packet from the initiating node it quickly reply to that message by flooding the packets in the network before the other nodes which also receive the same route request packet. Any route discovered by source node will contain malicious node as one of the intermediate node. Due to this the source node will not be able to fin secure route.

- **Denial of Service Attack**

  In this type of attack, an attacker attempts to prevent legitimate and authorized users from the services offered by the network. DOS attack can be carried out in many ways. The classic way is to flood packets to any centralized resource present in the network so that the resource is no longer available to nodes in the network, as a result of which the network no longer operating in the manner it was designed to operate. This may lead to a failure in the delivery of guaranteed services to the end users [23].

1.3.5 Advantages of MANET

- Highly supports the situation where fixed infrastructure is not needed
- They can be rapidly deployed with minimum user interference because of their self creating and self organising capability.
- No need for planning any base station installation.
- When connected to internet other devices can also connect with it therefore making its service available to other users as well.

1.3.6 MANET applications

• Tactical networks	Military communication and operations Automated battlefields
• Emergency services	Search and rescue operation Disaster recovery Supporting doctors and nurses in hospitals
• Commercial environment	Electronic payment any time any where Transmission of weather condition, taxi cab network Shopping malls
• Home and enterprise networking	Home/office wireless networking Conferences, meeting rooms

• Education	Universities and campus setting Meeting and lectures in campus
• Entertainment	Multiuser games Robotic pets

1.3 TERMINOLOGY

- **Wireless sensor network**

  These are distributed autonomous sensors which consist of number of nodes which are used to monitor environmental conditions such as temperature, pressure etc.

- **Sensor node**

  Sensor node is a node in a wireless sensor network that is capable of gathering sensory information and communicating with other connected nodes in the network.

- **Sink node**

  It is also known as base station. Sensor nodes monitor a geographical area and collect sensory information and that information is communicated to sink node.

- **Wireless local area network**

  In this tens and hundreds of computers are interconnected, in a limited area, to share useful information.

- **Ad hoc mode**

  The nodes communicate directly with each other without any access point.

- **Infrastructure mode**

  The nodes communicate with the help of an access point and it acts as a bridge between two nodes.

- **Access point**

  It is a device that allows wireless devices to connect to wired network. Access points are useful for larger networks, and they are particularly well-suited for adding wireless capability to an existing wired network.

- **Cellular network**

  It is a wireless network distributed in the form of cell where each cell has at least one base station.

- **Mobile ad hoc network**

  It is an infrastructure less network consist of self configuring nodes which communicate without any access point.

- **Routing**

  Process of sending the data from source to destination through best possible path in the network.

- **Protocol**

  Set of instructions used to perform a specific task.

CHAPTER 2

LITERATURE REVIEW

Abhay Kumar Rai et.al [22] proposed their work on different types of attacks on integrated MANET-Internet communication. They consider most common types of attacks on mobile ad hoc networks and on access point through which MANET is connected to the Internet. Specifically, they studied how different attacks affect the performance of the network and found out the security issues which have not solved until now.

Rashid Sheikhl et.al [24] discussed in their work basic properties of the MANET, the vulnerabilities in it, different types of attacks, secure protocols and how SMC solutions can be used for privacy preservation during computation. The solution to SMC problems in MANET can be found with the modification of the data inputs or with some anonymization technique.

Sudhir Agrawal et.al [25] presented an overview of the routing protocols, the known routing attacks and the proposed countermeasures to these attacks in various works observed that although active research is being carried out in this area, the proposed solutions are not complete in terms of effective and efficient routing security. There are limitations on all solutions. They may be of high computational or communication overhead (in case of cryptography and key management based solutions) which is detrimental in case of resource constrained MANET, or of the ability to cope with only single malicious node and ineffectiveness in case of multiple colluding attackers. Some solutions may require special hardware such as a GPS or a modification to the existing protocol. Furthermore, most of the proposed solutions can work only with one or two specific attacks and are still vulnerable to unexpected attacks.

K. Sivakumar et.al [26] analyzed the security problems in MANET and presented a few promising research directions. On the prevention side, various key and trust management schemes were developed to prevent external attacks from outsiders, and various secure MANET routing protocols were proposed to prevent internal attacks originated from within the MANET system. On the intrusion detection side, a new intrusion detection framework has been studied especially for MANET. Both prevention and detection methods will work together to address the security concerns in MANET.

Das Prashanta Kumar et.al [12] analyzed the impact of proactive protocols by growing the density of nodes in network and keeping source node fixed and movable destination node and lastly, keeping the destination node fixed and move source node. In all three cases, behaviour of the routing protocol has been analyzed to progress and choose efficient and proficient routing protocol for network setup. The performance matrix contains delivery fraction, packet loss and end-to-end delay.

Haiying Shen et.al [27] proposed in their work an Anonymous Location-based Efficient Routing protocol (ALERT). ALERT dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non traceable anonymous route. In addition, it hides the data initiator/receiver among many initiators/receivers to strengthen source and destination anonymity protection. Thus, ALERT offers anonymity protection to sources, destinations, and routes. It also has strategies to effectively counter intersection and timing attacks. ALERT features a dynamic and unpredictable routing path, which consists of a number of dynamically determined intermediate relay nodes.

Bo Zhu et.al [28] proposed in their work an Anonymous Secure Routing (ASR) protocol that can provide additional properties on anonymity, i.e. Identity Anonymity and Strong Location Privacy, and at the same time ensure the security of discovered routes against various passive and active attacks which ensure both the anonymity and security of the routing protocol.

Sk. Md. Mizanur Rahman et.al [29] proposed in their work a new position-based routing protocol which keeps routing nodes anonymous, thereby preventing possible traffic analysis. To this end, a time variant Temporary Identifier Temp ID is computed from time and position of a node and used for keeping the node anonymous. Only the position of a destination node is required for the route discovery, and Temp ID is used for establishing the route for sending data: a receiver hand shake scheme is designed for determining the next hop on-demand with use of the Temp ID. AODPR prevents the target-oriented attack and explained the details of the routing procedure, which is applicable to any node density in a network. AODPR ensures node privacy, route anonymity and location privacy and also strong against most known attack.

Karim El Defrawy et.al [30] proposed in their work an anonymous routing framework (ALARM). It uses nodes current locations to construct a secure MANET map. Based on the current map, each node can decide which other nodes it wants to communicate with. ALARM takes advantage of some advanced cryptographic primitives to achieve node authentication, data integrity, anonymity and untraceability (tracking resistance). It also offers resistance to certain insider attacks. ALARM had strong privacy and strong security properties. By privacy properties we mean node anonymity and resistance to tracking. Whereas security properties include node/origin authentication and location integrity.

Hemant Dandotiya et.al [31] proposed a method which, works in two phases; first is signal strength based AODV if this approach is not work then it switch to second phase means work like as normal AODV, In signal strength based AODV protocol measures signal strength between nodes and compare with RSSI threshold values if it is greater than threshold value then it is accepted for further processing otherwise it is discarded if it is not find any route between source and destination then it switch to normal AODV which select route on the basis of minimum hop count . The benefit of this scheme is by selecting a strong route to the destination we can increase the lifetime of the network.

P. I. Basarkod et.al [32] proposed a method to find the stability factor of the node by considering self and neighbour nodes mobility. The steps in finding the stability factor of a node are as follows-firstly all the nodes in MANET find the self stability, i.e. when the node is moving to a new position with respect to its previous position. Secondly find neighbours stability of all the nodes in MANET by considering the neighbours self stability, and thirdly each node in the MANET will compute the stability factor based on self stability and neighbours stability. The stability factor of a node may be used to establish a path from the source to the destination. The stable nodes in the path will provide higher packet delivery ratio and lower latency.

Dr. K. Kathiravan et.al [33] analyzed in their work the vulnerabilities of PUMA (Protocol for Unified Multicasting through Announcements) and MAODV (Multicast Ad-hoc on-demand Distance Vector routing) against various possibilities of internal attacks. They also identify MA (Multicast Announcement) packet fabrication type of internal attacks in PUMA. It is very difficult to detect this attack efficiently when it changes its behaviours arbitrarily. They propose multicast activity-based overhearing technique to identify this attacker node in the multicast group. They have proposed a solution for MA fabrication and data packet drop attacks and also observed that this solution responds effectively with less cost.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 OBJECTIVE OF THE STUDY

- Add a new routing protocol in the NS-2 environment.
- Deployment of nodes as per requisite routing protocol.
- Add attack to the network of the proposed simulation.
- Evaluate and analyse the results for with and without attack and further compare the results on the basic parameters like throughput and energy consumption.

3.2 APPROACH TO STUDY

Anonymous routing protocols are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. Anonymity in MANETs includes identity and location anonymity of data sources (i.e. senders) and destinations (i.e., recipients), as well as route anonymity. Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption and redundant traffic. Many approaches cannot provide all of the aforementioned anonymity protections.

ALERT dynamically partitions the network field horizontally and vertically and choose a node for communication with all the other nodes. All the remaining nodes form clusters and the chosen node communicates with the clusters of nodes one by one.

In this approach proposed ALERT has been implemented on 49 nodes and wormhole attack has been implemented. Two tcl files name wormhole and isolate have been created. In the first tcl file wormhole attack has been implemented at 110 seconds of simulation. So due to wormhole attack after 110 seconds node 7 will start to drop the packets which is shown in network animator screenshots. In second tcl file wormhole attack has been countered. So after 110 seconds of simulation node 7 will still communicate with the other nodes which are shown in network animator screenshots. We have used if condition here. If malicious=true then drop packets and if detector=true then malicious=false. Parameters such as throughput and energy consumption have been compared from both the files.

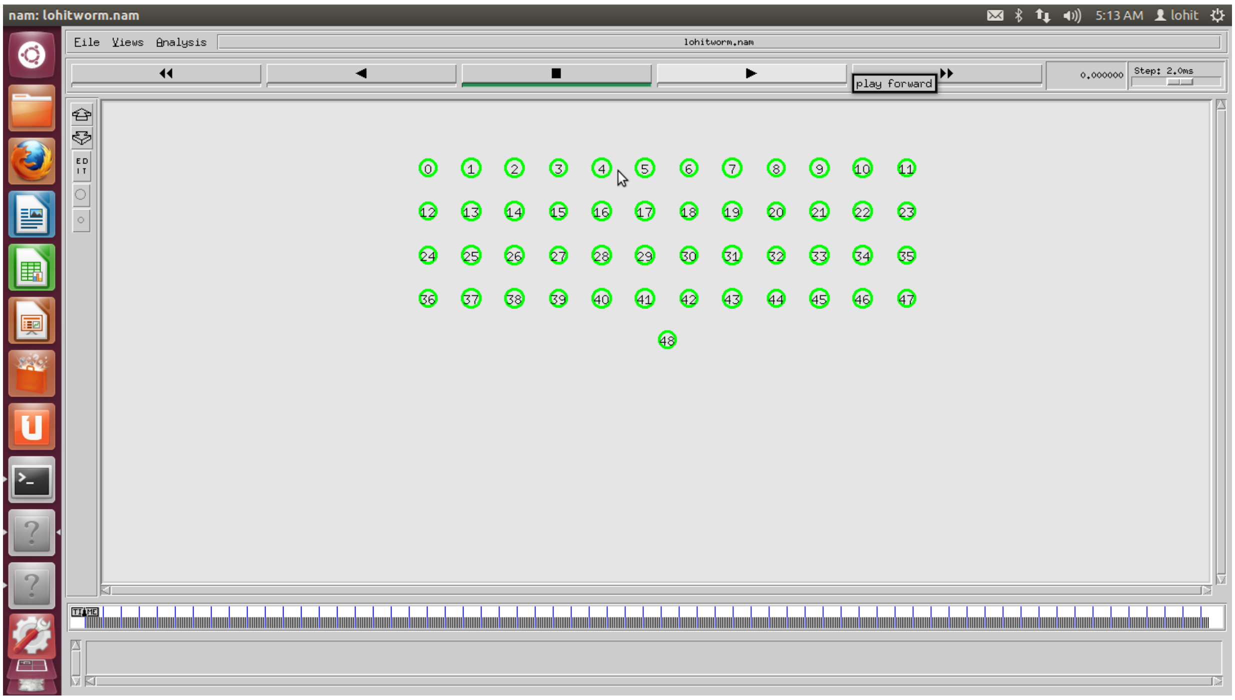


Fig 3.1: Initial position of nodes.

Figure 3.1 show the initial positioning of nodes. There are total 49 nodes from 0-48.

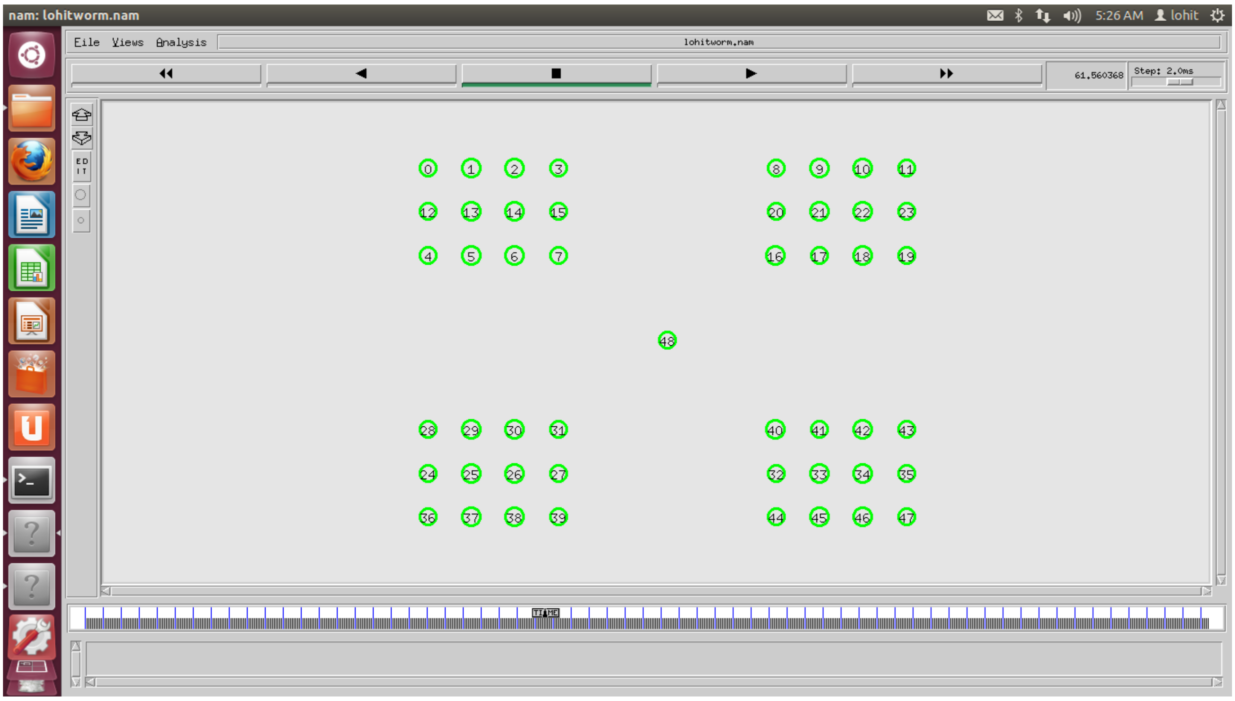


Fig 3.2: Partition of nodes.

Figure 3.2 show the partitioning of nodes horizontally and vertically after applying ALERT. Now node 48 will communicate with all the clusters one by one.

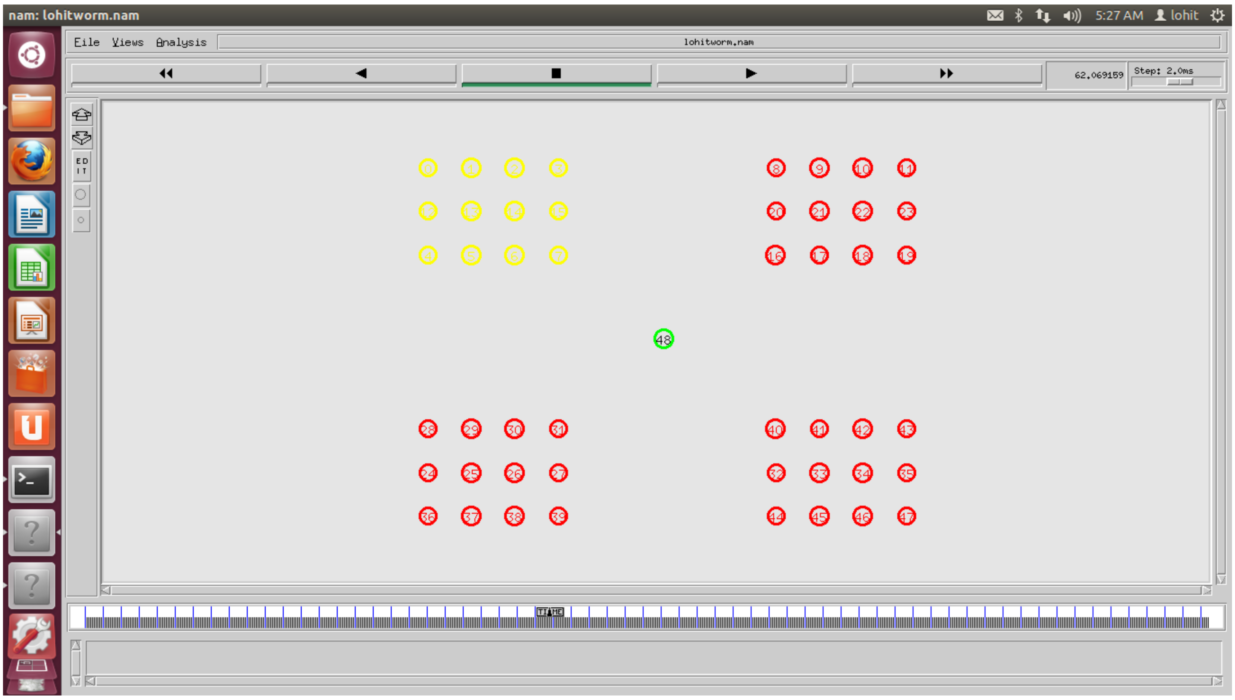


Fig 3.3: Node 48 approaching cluster 1.

Figure 3.3 show that node 48 is approaching cluster 1 for the communication. The cluster to which node 48 will approach will change its colour from red to yellow.

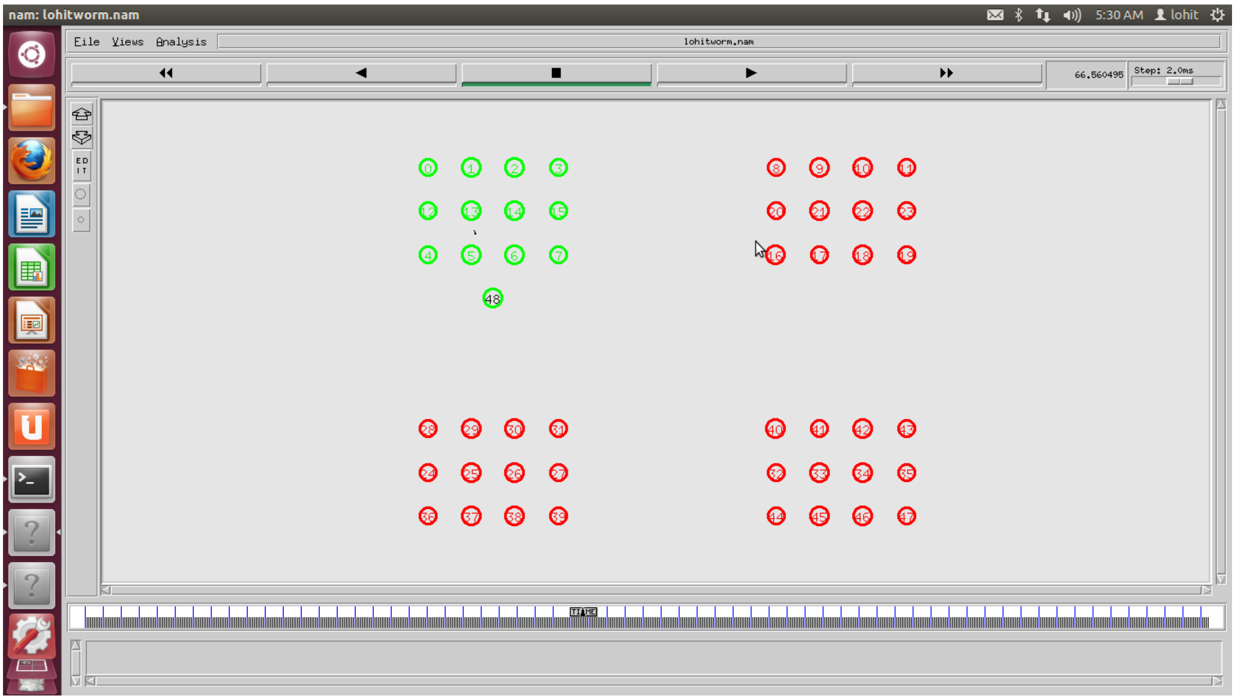


Figure 3.4: Node 48 communicating to cluster 1.

Figure 3.4 show that node 48 is communicating to cluster 1 and since it is communicating to only cluster 1 the colour of cluster 1 will change from yellow to green.

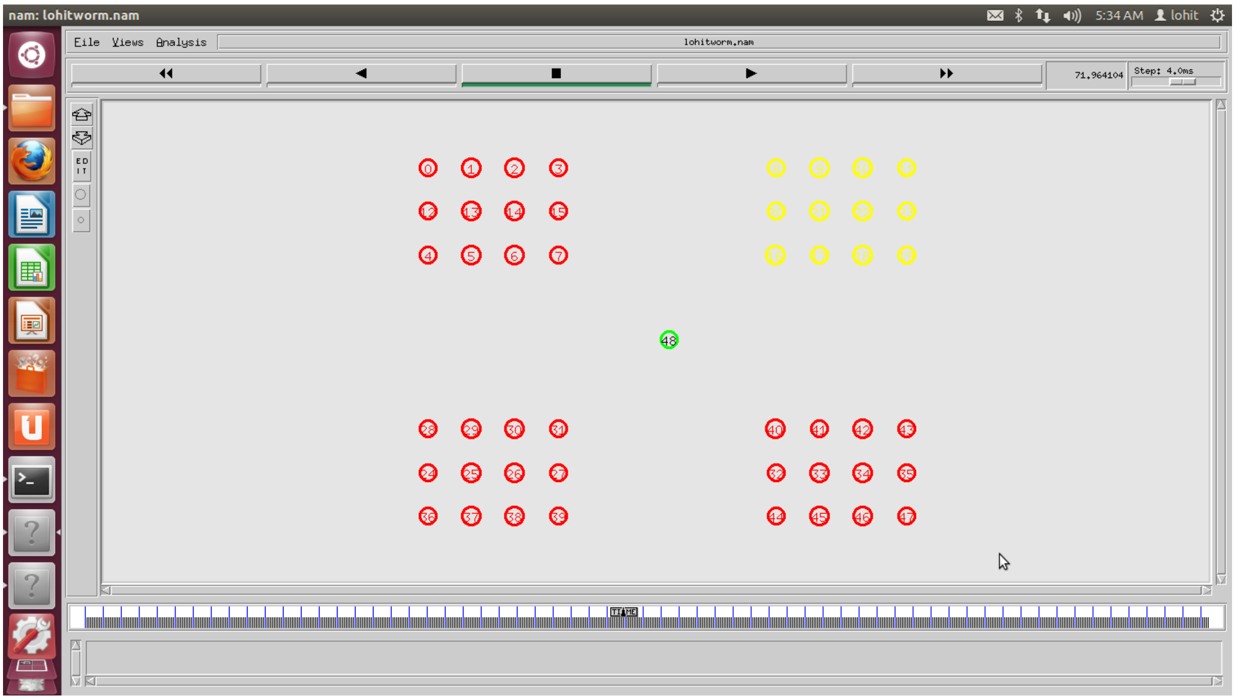


Fig 3.5: Node 48 approaching cluster 2.

Figure 3.5 show that node 48 is approaching cluster 2 for the communication. The cluster to which node 48 will approach will change its colour from red to yellow.

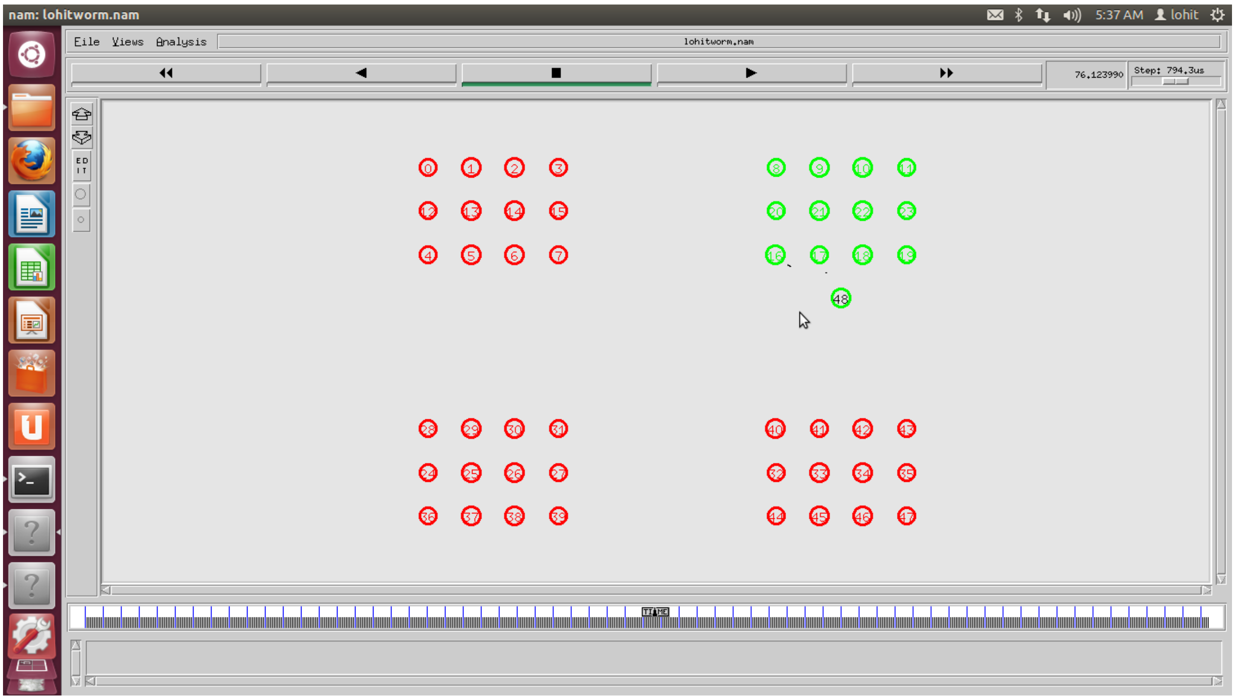


Figure 3.6: Node 48 communicating with cluster 2.

Figure 3.6 show that node 48 is communicating to cluster 2 and since it is communicating to only cluster 2 the colour of cluster 2 will change from yellow to green.

The same process will be repeated for cluster 3 and cluster 4. After communicating from cluster 2 node 48 will approach cluster 3 and will communicate with it. After completing the communication with cluster 3 node 48 will approach cluster 4 and will communicate with it. After completing the communication with all four clusters node 48 will come back to its initial position.

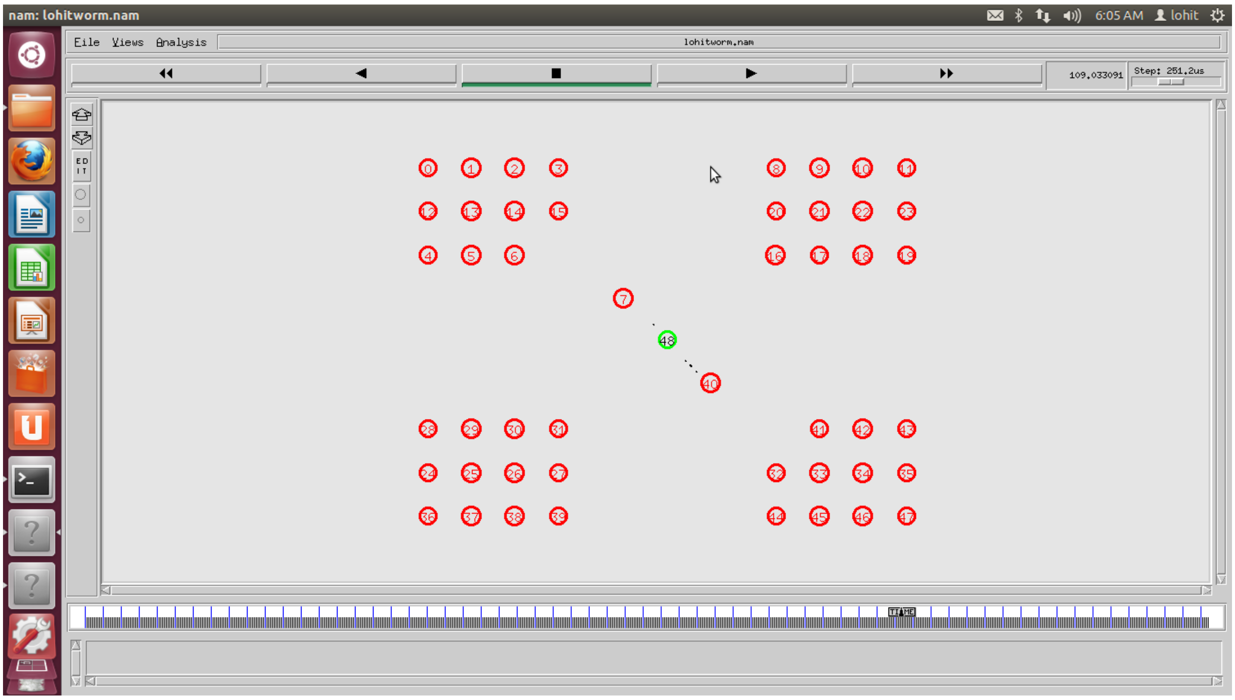


Figure 3.7: Node 48 communicating to cluster heads of cluster 1 and 3.

In this figure node 7 and node 40 will act as cluster heads of cluster 1 and cluster 3 respectively and will come out from their respective clusters and will communicate with node 48 till 110seconds.

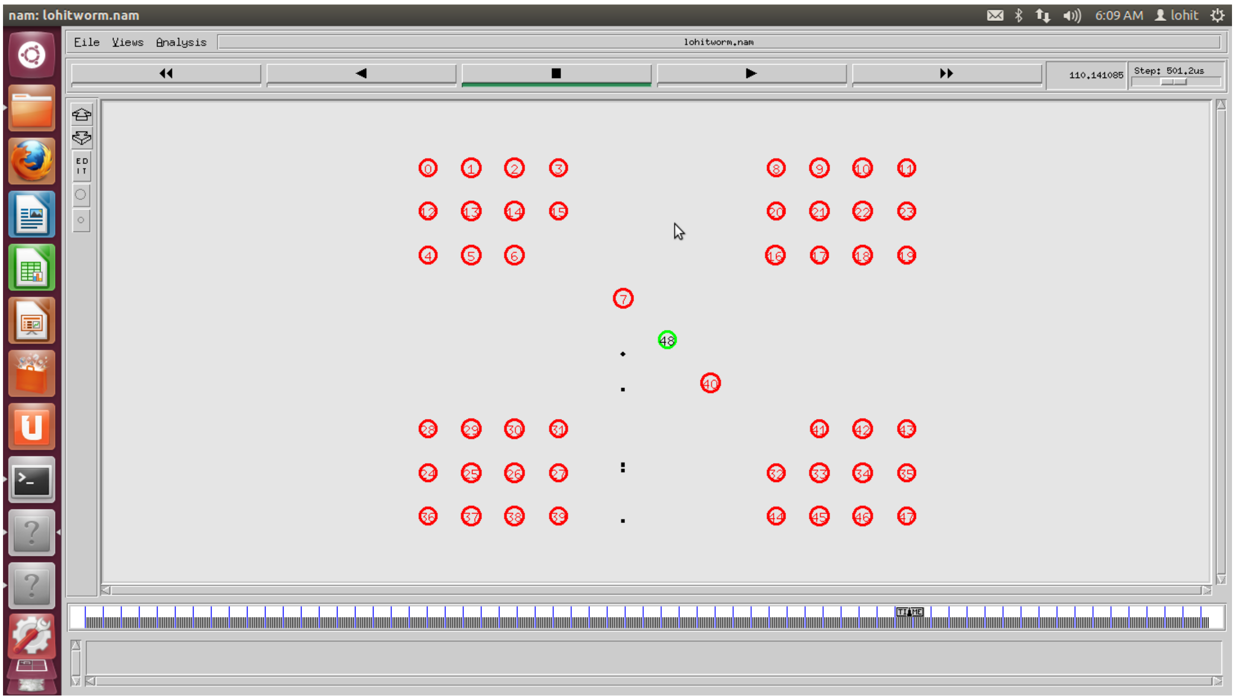


Figure 3.8: Node 7 dropping packets due to wormhole attack.

After 110 seconds wormhole attack will become active on node 7 and it will start to drop packets because of wormhole attack. After 110 seconds till the end of simulation packets will continue to drop.

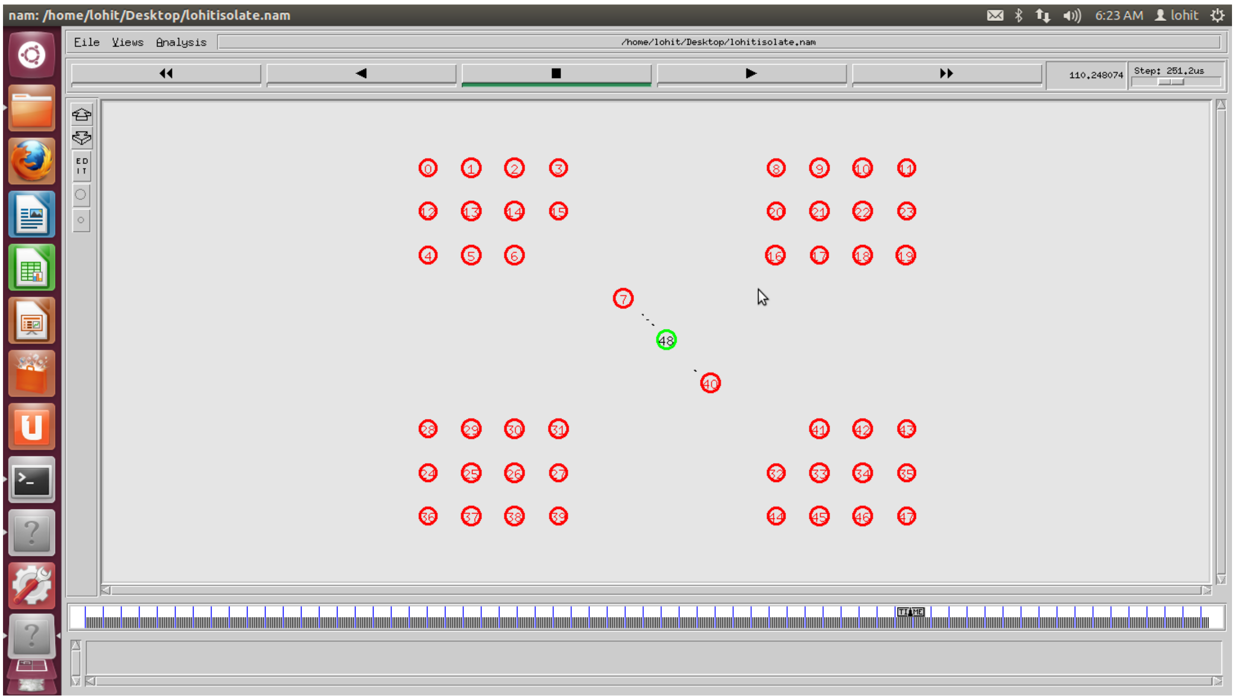


Figure 3.9: Node 7 communicating to cluster heads of cluster 1 and 3.

This figure is from 2nd tcl file where we have counter the wormhole attack and communication is possible between node 7 and node 48 after 110 seconds.

3.3 RESEARCH METHOD

In this research, a new routing protocol has been implemented. In order to proceed research; literature survey must be done. Literature survey is to exploit the research and gather information about methods to approach. After doing literature survey next step is to formulate the hypothesis which can lead to better results and then formulate the problem based on the analysis

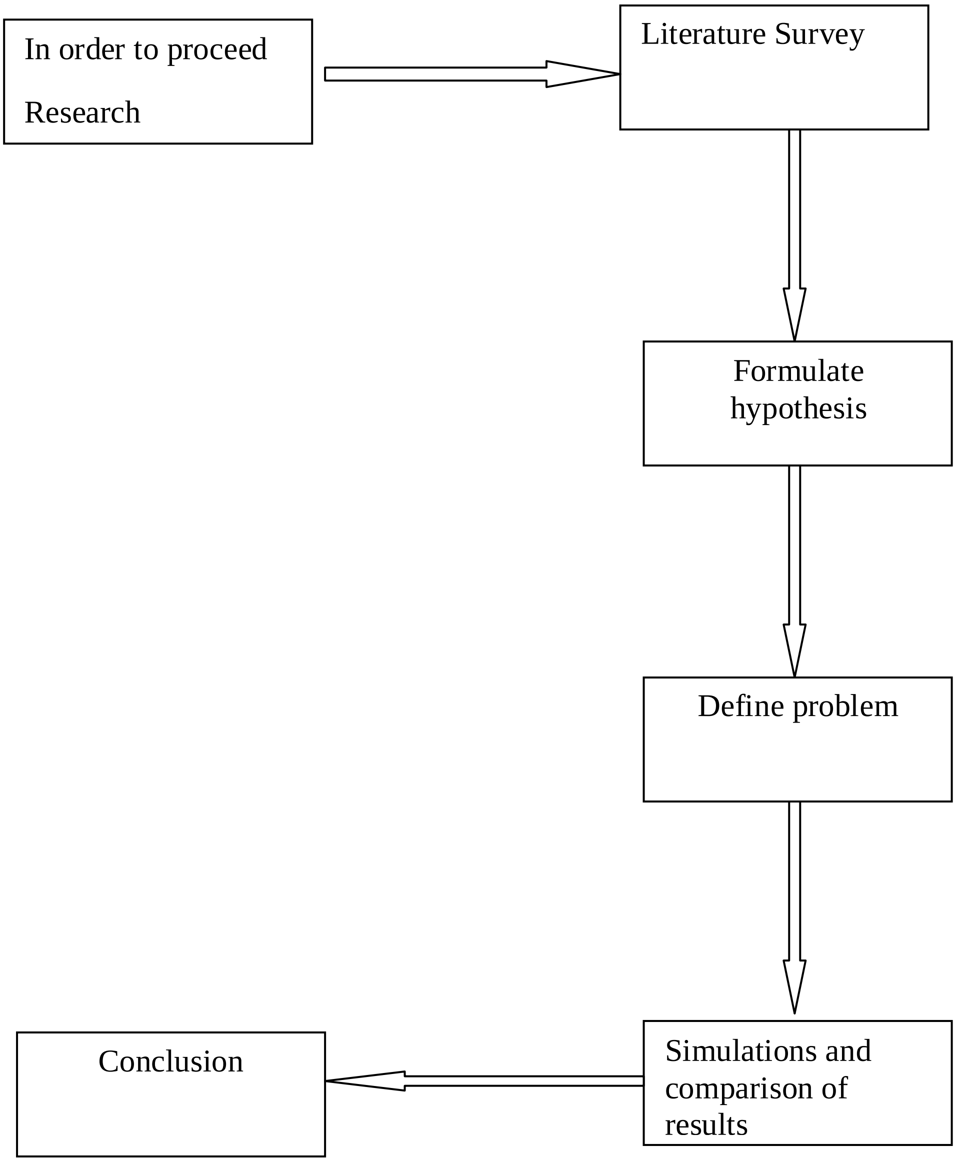

In order to proceed Research
Literature Survey
Formulate hypothesis
Define problem
Simulations and comparison of results
Conclusion

Figure 3.10: Flowchart of Research Methodology.

3.4 STEP WISE EXECUTION OF METHODOLOGY

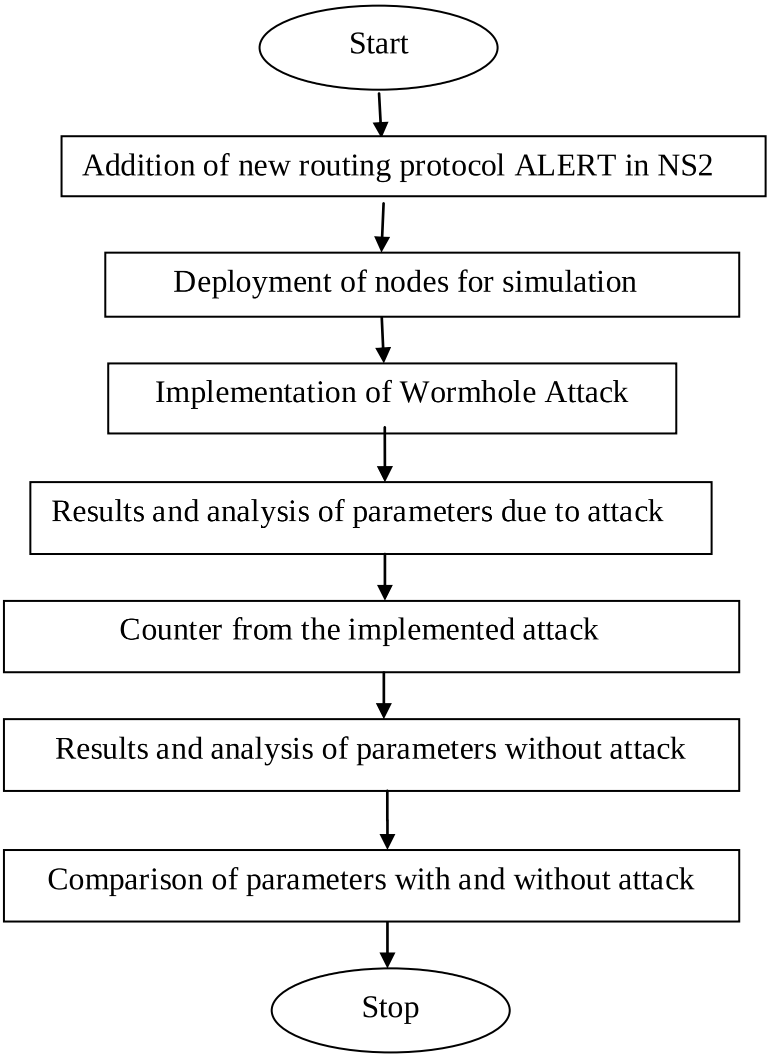

Start
Addition of new routing protocol ALERT in NS2
Deployment of nodes for simulation
Implementation of Wormhole Attack
Results and analysis of parameters due to attack
Counter from the implemented attack
Results and analysis of parameters without attack
Comparison of parameters with and without attack
Stop

Figure 3.11: Flowchart of approach and applicability of methodology followed.

The flowchart shows the steps towards approach and applicability of the methodology followed. Firstly new routing protocol ALERT is added. Then nodes are deployed for simulation. Then wormhole attack is implemented. Results and analysis have been done with attack. Counter from implemented attack has been done. Results and analysis have been done without attack. Finally parameters such as throughput and energy consumption have been compared with and without attack.

CHAPTER 4

RESULTS AND SIMULATION

4.1 THROUGHPUT WITH ATTACK

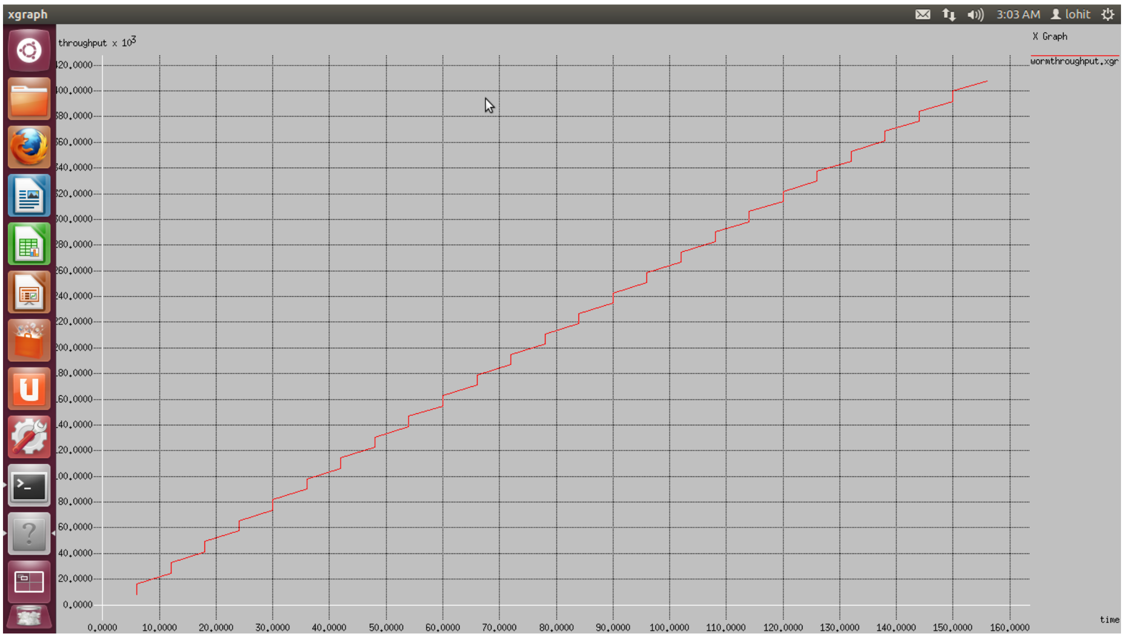


Figure 4.1 Throughput with attack.

Figure 4.1 shows the throughput with attack. In this graph y-axis shows the throughput and x-axis shows the time. The maximum value of throughput at 150 sec. is around 399750.

4.2 THROUGHPUT WITHOUT ATTACK

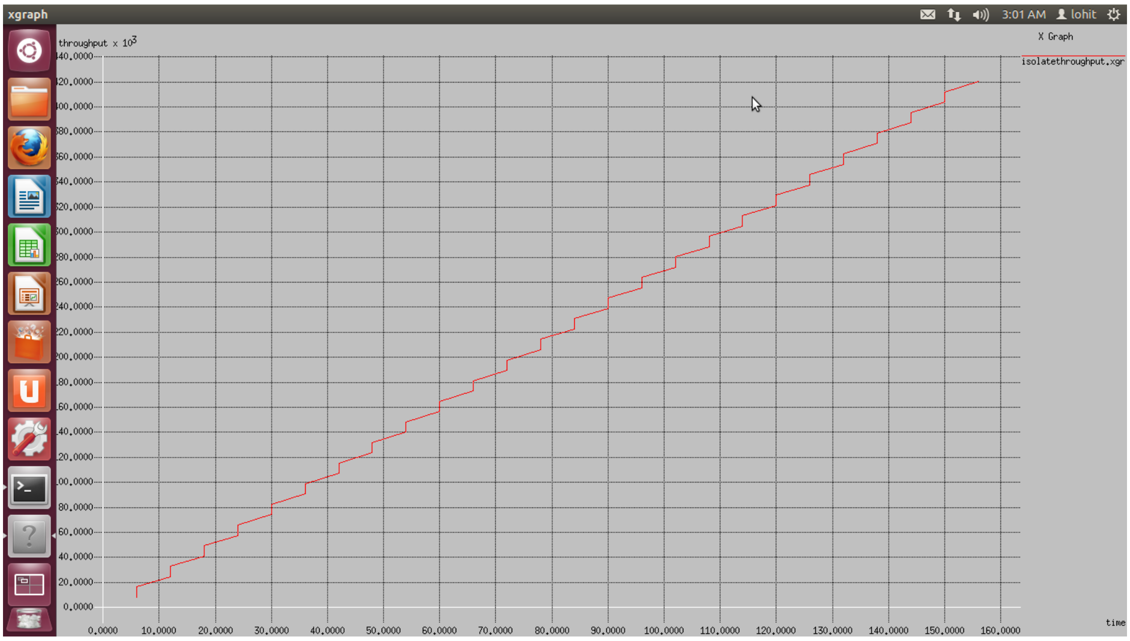
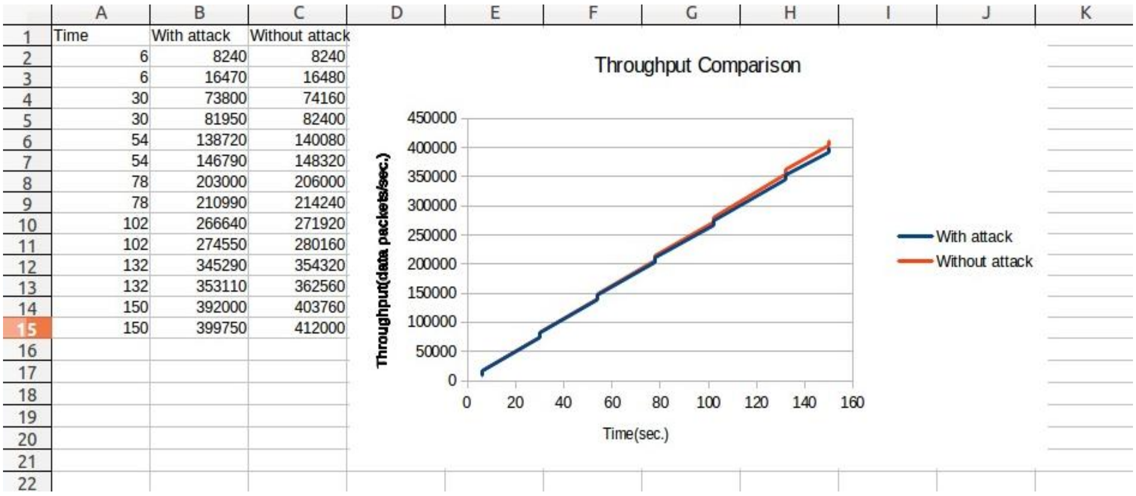


Figure 4.2 Throughput without attack.

Figure 4.2 shows the throughput without attack. In this graph y-axis shows the throughput and x-axis shows the time. The maximum value of throughput at 150 sec. is 412000

4.3 THROUGHPUT COMPARISON



Time	With attack	Without attack
6	8240	8240
6	16470	16480
30	73800	74160
30	81950	82400
54	138720	140080
54	146790	148320
78	203000	206000
78	210990	214240
102	266640	271920
102	274550	280160
132	345290	354320
132	353110	362560
150	392000	403760
150	399750	412000

Figure 4.3: Throughput comparison (with and without attack).

Figure 4.3 shows the throughput comparison (with and without attack). In this graph y-axis shows the throughput and x-axis shows the time. Blue line represents the throughput with attack while orange line represents throughput without attack. It can be clearly seen from the table and graph that the throughput of the network without attack is greater than throughput of the network with attack.

4.4 ENERGY CONSUMPTION WITH ATTACK

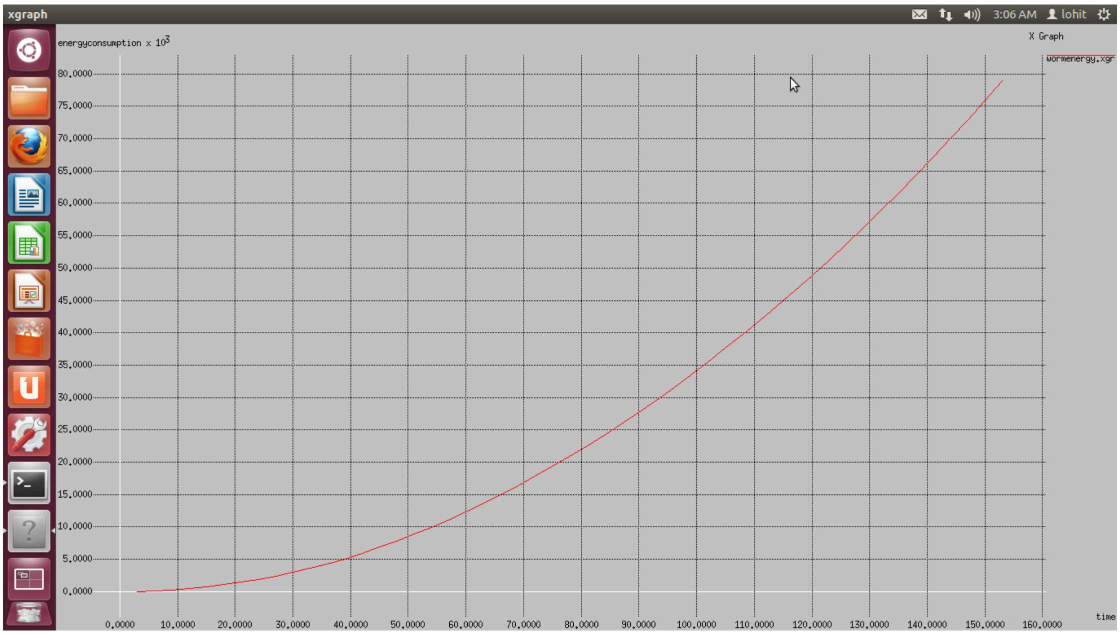


Figure 4.4: Energy consumption with attack.

Figure 4.4 shows the energy consumption with attack. In this graph y-axis shows the energy consumed by the nodes and x-axis shows the time. The value of energy consumption at 150 sec. is 75873J.

4.5 ENERGY CONSUMPTION WITHOUT ATTACK

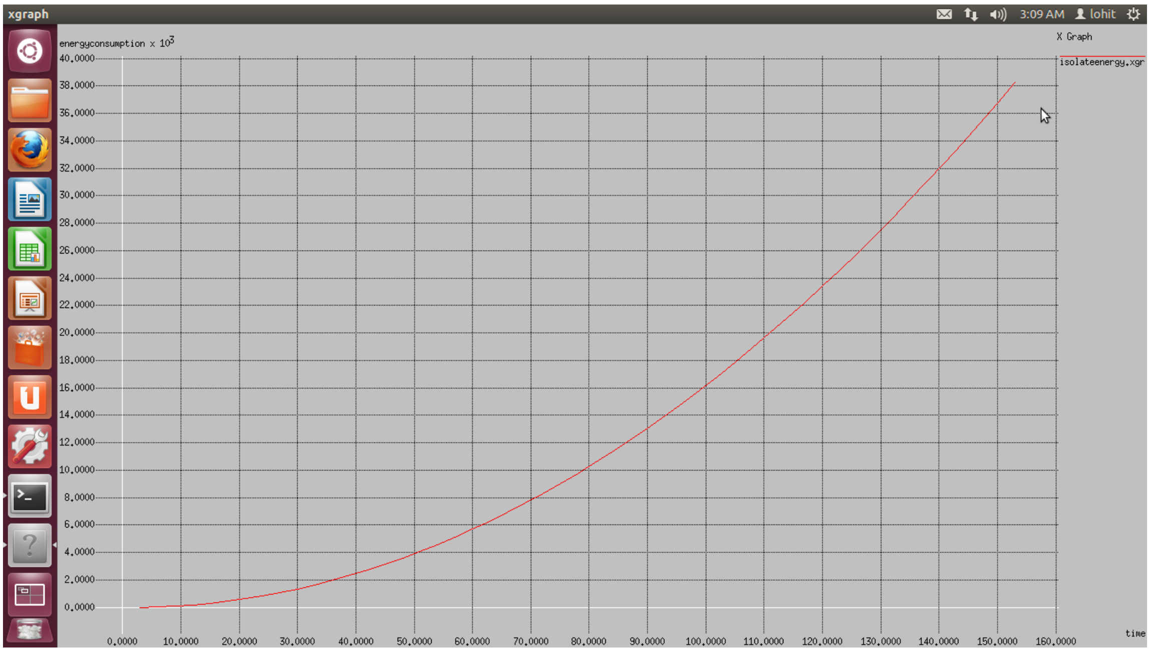
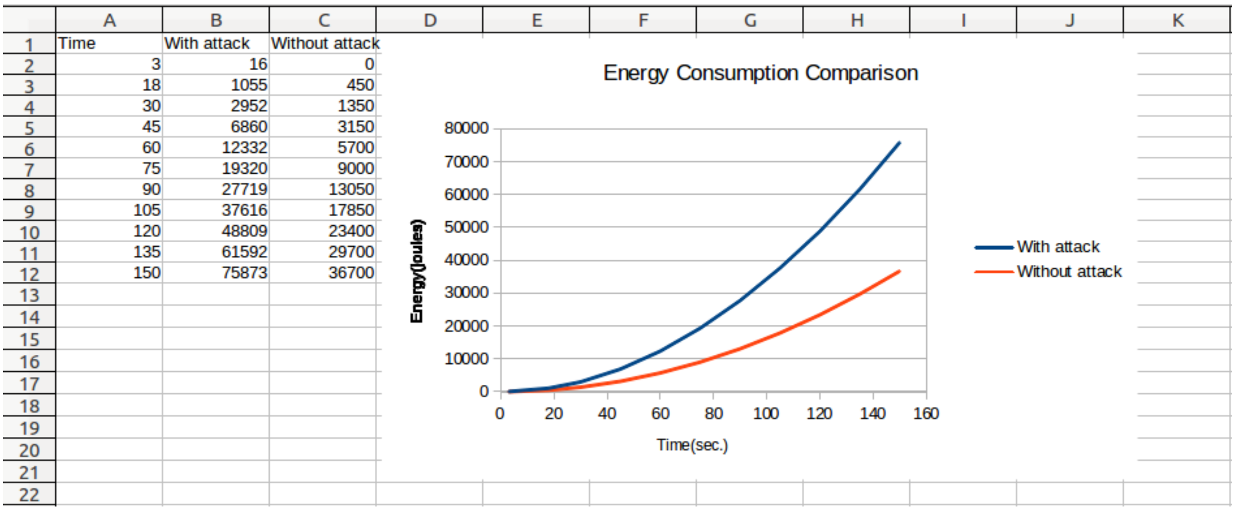


Figure 4.5: Energy consumption without attack.

Figure 4.5 shows the energy consumption without attack. In this graph y-axis shows the energy consumed by the nodes and x-axis shows the time. The value of energy consumption at 150 sec. is 36750.

4.6 ENERGY CONSUMPTION COMPARISON



Time	With attack	Without attack
3	16	0
18	1055	450
30	2952	1350
45	6860	3150
60	12332	5700
75	19320	9000
90	27719	13050
105	37616	17850
120	48809	23400
135	61592	29700
150	75873	36700

Figure 4.6 Energy consumption comparisons (with and without attack).

Figure 4.6 shows the energy consumption comparison with and without attack. In this graph y-axis shows the energy consumed by the nodes and x-axis shows the time. Blue curve represents energy consumption of nodes with attack while orange line represents energy consumption of nodes without attack. It can be clearly seen from the table and graph that the energy consumption of network without attack is less than the energy consumption of network with attack.

CHAPTER 5
CONCLUSION AND FUTURE SCOPE

5.1 CONCLUSION

In the present work, two tcl files named wormhole and isolate have been created consisting of 49 number of nodes ranging from 0-48. Proposed ALERT has been implemented and parameters have been compared for both the files. In wormhole file, wormhole attack is implemented which stops the communication between two nodes after 110 seconds of simulation and the packets starts to drop. Then wormhole attack has been countered in another tcl file known as isolate. Due to counter of wormhole attack packets will not drop even after 110seconds of simulation. Finally, two parameters that are throughput and energy consumption with respect to time have been calculated for both the files and the result of both the files have been compared. The results and analysis show that the throughput of the network without attack is better than throughput of the network with attack as the value of throughput of the network with attack at 150 seconds is 399750 data packets/sec whereas for without attack at 150 seconds is 412000 data packets/sec. With attack the energy consumed by network at 150 seconds is 75873J whereas the energy consumed by the network without attack at 150 seconds is 36700J.

5.2 FUTURE SCOPE

For the future research new attack can be implemented on the network and various parameters like throughput, energy consumption etc. can be compared. New routing protocol can be added and then results can be compared.

REFRENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. (2002) “Wireless Sensor Networks: A Survey”. Computer Networks, 38:pp.393–422

[2] Samaneh Alikhanzadeh, Mohammad Hossein Yaghmaee (2010) “A Learning Based Protocol for Bidirectional Congestion Control in Wireless Sensor Network” International Conference on information, Networking and Automation.

[3] Zilong Li, Weixia Zou, Tao Qi (2011) “A cross-layer congestion control strategy in wireless sensor network” Proceedings of IEEE IC-BNMT.

[4] Sudhanshu Pant, Naveen Chauhan (December 2010), “Effective Cache based Policies in Wireless Sensor Networks: A Survey” International Journal of Computer Applications (0975 – 8887) vol.11– No.10, pp. 975-8887.

[5] Ewa Hansen, Jonas Neander, Mikael Nolin and Mats Bjorkman, “Efficient Cluster Formation for Sensor Networks”.

[6] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal (2008),Department of Computer Science, University of California, Davis, CA 95616, United States, "Wireless sensor network survey" 52 pp.2292–2330.

[7] M. Welsh, D. Malan, B. Duncan, T. Fulford-Jones, S. Moulton, (2004) ‘‘Wireless Sensor Networks for Emergency Medical Care,’’ GE Global Research Conference.

[8] J. Kurose, V. Lesser, E. de Sousa e Silva, A. Jayasumana, B. Liu, Sensor Networks Seminar, CMPSCI 791L, University of Massachusetts, Amherst, MA, Fall 2003

[9] Kazem Sohraby, Daniel Minoli, Taieb Znati (2007) “WIRELESS SENSOR NETWORKS Technology, Protocols, and Applications” John Wiley & Sons,inc.,Publication

[10] Carlos de Morais Cordeiro and Dharma P. Agarwal, “Mobile Ad hoc Networking”, OBR Research Center for Distributed and Mobile Computing, ECECS University of Cincinnati, Cincinnati, OH 45221-0030-USA.

[11] C.-Y. Chong, S. P. Kumar, ‘‘Sensor Networks: Evolution, Opportunities, and Challenges,’’ Proceedings of the IEEE, Vol. 91, No. 8,(2003), pp. 1247ff.

[12] Das Prashanta Kumar, Robin Singh Bhadoria, Deka Ganesh Chandra, Praveen Mudgal, “Comparative Study of Proactive Protocol of Mobile Ad-Hoc Network”, 2013 International Conference on Communication Systems and Network Technologies, 2013 IEEE, pp. 243-247.

[13] http://en.wikipedia.org/wiki/IEEE_802.11

[14] Brian P. Crow, The MITRE Corporation, Indra Widjaja (1997), “IEEE 802.11 Wireless Local Area Networks “, Fujitsu Network Communications, Jeong Geun Kim, University of Arizona Prescott T. Sakai, Cypress Semiconductor, IEEE Communications Magazine, pp.116-126.

[15] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester Department of Information Technology(INTEC),Ghent University – IMEC vzwSint Pietersnieuwstraat 41, B-9000 Ghent,Belgium.

[16] N. Nikaein and C. Bonnet, ”Improving routing and network performance in mobile ad hoc networks using quality of nodes”, In Proceedings of Wireless Optimization (WiOpt), Sophia-Antipolis, France, 2003.

[17] E. Royer, T. Chai-Keong, “A review of current routing protocols for ad hoc mobile wireless networks”, IEEE Personal Communications, Vol. 6, No.2, pp.46-55, 1999.

[18] Imrich Chlamtac , Marco Conti , Jennifer J.-N. Liu (2003), “Mobile ad hoc networking: imperatives and challenges”, Ad Hoc Networks, pp. 13–64.

[19] Wenjia Li and Anupam Joshi "Security Issues in Mobile Ad Hoc Networks".

[20] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

[21] Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Data_integrity 9

[22] Abhay Kumar Rai, Rajiv Ranjan Tewari and Saurabh Kant Upadhyay "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3) pp.265-274.

[23] L. Zhou and Z. J. Haas. “Securing Ad Hoc Networks”. IEEE Network Magazine, Volume. 13, no. 6,pp. 24-30, December 1999

[24] Rashid Sheikhl Mahakal Singh Chandee, Durgesh Kumar Mishra, “Security Issues in MANET: A Review” IEEE 2010

[25] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, “A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks”, journal of computing, volume 3, issue 1, january 2011,pp.41-48.

[26] K. Sivakumar, Dr. G. Selvaraj, “Overview of various attacks in MANET and countermeasures for attacks” International Journal of Computer Science and Management Research, Vol. 2 Issue 1 January 2013,pp. 1366-1372.

[27] Haiying Shen and Lianyu Zhao "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs" IEEE transactions on mobile computing, Vol. 12, no. 6, JUNE 2013.pp.1079-1093.

[28] Bo Zhu, Zhiguo Wan, Mohan S. Kankanhalli, Feng Bao, Robert H. Deng "Anonymous Secure Routing in Mobile Ad-Hoc Networks" 29th Annual IEEE International Conference on Local Computer Networks.

[29] Sk. Md. Mizanur Rahman, Masahiro MAMBO, Atsuo INOMATA, Eiji OKAMOTO "An Anonymous On-Demand Position-based Routing in Mobile Ad Hoc Networks "Proceedings of the 2005 Symposium on Applications and the Internet.

[30] Karim El Defrawy and Gene Tsudik "ALARM: Anonymous Location-Aided outing in Suspicious MANETs",School of Information and Computer Science" (2007)

[31] Hemant Dandotiya, Rachit Jain, Rinkoo Bhatia "Route Selection in MANETs by Intelligent AODV",2013 International Conference on Communication Systems and Network Technologies.

[32] P. I. Basarkod, S. S. Manvi, D.S.Albur "Mobility Based Estimation of Node Stability in MANETs",2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology

[33] Dr. K. Kathiravan,A. Menaka Pushpa "Secure Multicast Routing Protocol against Internal Attacks in Mobile Ad Hoc Networks",2013 IEEE GCC Conference and exhibition, November 17-20.

BIOGRAPHY

Name:	Lohit Kumar
Father's Name:	Mukesh Kumar
Date of Birth:	March 2,1990
Place of Birth:	Delhi
Nationality:	Indian
Marital Status:	Un-Married
Permanent Address:	Block C-15/Y-1, Dilshad Garden, Delhi-110095
Email ID:	lohitkumarec@gmail.com

Academic Qualifications

Bachelor of Technology	Electronics and Communication Engineering, Rajasthan Technical University, Kota, Rajasthan(Year 2012)
Master of Technology	Electronics and Communication Engineering Lovely Professional University, Phagwara, Punjab(Year 2014)