ANALYZING THE PERFORMANCE OF VARIOUS TOPOLOGIES IN PRESENCE OF MAN IN THE MIDDLE ATTACK

PROJECT REPORT
PHASE II

Submitted by

YUVASRI.G
Register No: 15MAE013

in partial fulfillment for the requirement of award of the degree of

MASTER OF ENGINEERING

in

APPLIED ELECTRONICS

Department of Electronics and Communication Engineering

KUMARAGURU COLLEGE OF TECHNOLOGY
(An Autonomous Institution Affiliated to Anna University, Chennai)
COIMBATORE – 641 049

ANNA UNIVERSITY, CHENNAI 600 025

APRIL 2017

BONAFIDE CERTIFICATE

Certified that this project report titled **"ANALYZING THE PERFORMANCE OF VARIOUS TOPOLOGIES IN PRESENCE OF MAN IN THE MIDDLE ATTACK"** is the bonafide work of **YUVASRI.G [Reg. No. 15MAE013]** who carried out the research under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form part of any other project or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

SIGNATURE

Dr.s.Umamaheswari

Project Supervisor

Department of ECE

Kumaraguru College of Technology

Coimbatore-641 049

SIGNATURE

Mr.K.Ramprakash

Head of PG Programmes

Department of ECE

Kumaraguru College of Technology

Coimbatore-641 049

The candidtae with University **Register No.15MAE013** was examined by us in the project viva-voice examination held on .....

INTERNAL EXAMINER **EXTERNAL EXAMINER**

ACKNOWLEDGEMENT

First, I would like to express my praise and gratitude to the Lord, who has showered his grace and blessings enabling me to complete this project in an excellent manner.

I express my sincere thanks to the management of Kumaraguru College of Technology and Joint Correspondent **Shri Shankar Vanavarayar** for his kind support and for providing necessary facilities to carry out the work.

I would like to express my sincere thanks to our beloved Principal **Dr.R.S.Kumar Ph.D.,** Kumaraguru College of Technology, who encouraged us with his valuable thoughts.

I would like to thank **Prof. K.Ramprakash M.E.,** Head of the Department, (PG Programme), Electronics and Communication Engineering, for his continuous encouragement and motivation throughout the course of this project work.

In particular, I wish to thank with everlasting gratitude to the project coordinator **Ms.S.Nagarathinam M.E., (Ph.D).,** Assistant Professor-III **,**Department of Electronics and Communication Engineering, for her expert counselling and guidance to make this project to a great deal of success.

I extend my heartfelt thanks to my project guide **Dr.S.Umamaheswari Ph.D.,** Associate Professor, for her immense contribution, guidance, support and constructive criticism not only during this project but also during this two years of master program.

Lastly, I would like to thank my friends and family for standing by me and encouraging me throughout the project.

ABSTRACT

In a densely deployed wireless sensor network ,a single node has numerous neighboring nodes with which direct communication would be possible when using moderate large transmission power this is however , not beneficial; high transmission power requires lot of energy .the recent area of WSNS has brought new challenges to developers of net-work protocols like Energy consumption ,network coverage ,node failures ,fault tolerance, network lifetime has to be preserved in wireless sensor network . In this paper, we propose a new scale free topology model which has both fault-tolerance against random faults and intrusion tolerance against selective remove attacks at the same time and a rectangular topology with design and implementation of a wireless sensor network, which consists of energy-efficient wireless sensor nodes with an integrated ultrasonic sensor, which establish a collision free data transmission in an emergency scenario. This review analyze the most popular and efficient topology arrangement and better performance for wireless sensor networks with man in middle attack based on the comparison of various metrics like network life time, energy efficiency, throughput ,end to end delay, packet delivery ratio

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS	NOMENCLATURE
WSNs	Wireless Sensor Networks
BA	Barabasi-albert
BA-E	Barabasi albert evolution model
QOS	Quality of service
EAEM	Energy aware evolution model
CHMM	Clustering hierarchy modularity measure
IPSN	Information processing in sensor networks
MIMA	Man-in-the-middle attacks
GPS	Global positioning system
MANETs	Mobile Ad Hoc Networks
GPRS	General packet radio service
RSSI	Received signal strength indication
PKG	Private key generation
ID-PKG	Identity private key generator
DOS	Denial of service

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW OF WIRELESS SENSOR NETWORKS

A wireless sensor network (WSN) of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" from a few to several hundreds or even thousands, where each node is connected to one sensor. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding. In computer science and telecommunications, wireless sensor networks are an active research area with numerous workshops and conferences arranged each year, for example IPSN, EWSN. The figure 1.1 represents the wireless sensor network

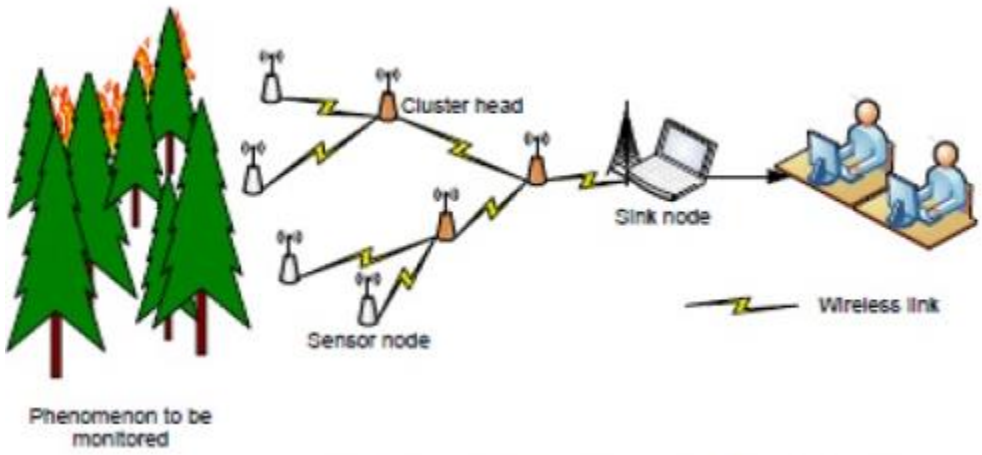

Figure 1.1 Wireless Sensor Network Architecture

1.2 APPLICATIONS

- Process Management
- Health care monitoring
- Environmental/Earth sensing
- Air pollution monitoring
- Forest fire detection
- Landslide detection
- Water quality monitoring
- Natural disaster prevention
- Industrial monitoring
- Machine health monitoring

1.3 CHARACTERISTICS

The main characteristics of a WSN include:

- Power consumption constraints for nodes using batteries or energy harvesting
- Ability to cope with node failures (resilience)
- Mobility of nodes
- Heterogeneity of nodes

- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use
- Cross-layer design

Cross-layer is becoming an important studying area for wireless communications. In addition, the traditional layered approach presents three main problems:

1. Traditional layered approach cannot share different information among different layers which leads to each layer not having complete information. The traditional layered approach cannot guarantee the optimization of the entire network.
2. The traditional layered approach does not have the ability to adapt to the environmental change.
3. Because of the interference between the different users, access confliction, fading, and the change of environment in the wireless sensor networks, traditional layered approach for wired networks is not applicable to wireless networks.

So the cross-layer can be used to make the optimal modulation to improve the transmission performance, such as data rate, energy efficiency, QoS (Quality of Service), etc.. Sensor nodes can be imagined as small computers which are extremely basic in terms of their interfaces and their components. They usually consist of a processing unit with limited computational power and limited memory, sensors or MEMS (including specific conditioning circuitry), a communication device (usually radio transceivers or alternatively optical), and a power source usually in the form of a battery. Other possible inclusions are energy harvesting modules, secondary ASICs, and possibly secondary communication interface (e.g. RS-232 or USB).The base stations are one or more components of the WSN with much more computational, energy and communication resources. They act as a gateway between sensor nodes and the end user as they typically forward data from the WSN on to a server. Other special components in routing based networks are routers, designed to compute, calculate and distribute the routing tables.

1.4 OUTLINE OF SCALE FREE AND RECTANGULAR TOPOLOGY

Wireless sensor networks (WSNs) have gained enormous attention for their wide range of applications. In many applications, it is impractical to replace the nodes as they work under harsh environment. However, the nodes in WSNs, which are deployed in harsh environments, are easy to break down because of energy depletion, hardware failure or invasion.On node failure, the network connectivity will be reduced greatly, and the entire network even to be paralytic. After classical BA model (Barabasi–Albert Model) was put forward, the = robustness of scale-free topology to node failure excited many scholars' widespread interest. The scale-free topology is a heterogeneous topology, that is, the degree distribution probability fulfills the power-law relation. The topological robustness is the ability of the topology to maintain its connectivity after node failures, meaning that the nodes remove. It has been shown that the method of removing failure nodes (randomly or selectively) changes topology functionality. In this context, the influence of random and selective node failures on the efficiency of scale-free topology is investigated.

Information gathering in tunnels, buildings, bridges, etc. during disasters is of vital importance in speeding up rescue efforts and for protecting the fire fighters. The collected data can be used by the emergency services in the planning of rescue operations and allocation of human resources at a local level. In this article we present design and implementation of a wireless sensor network, which consists of energy-efficient wireless sensor nodes with an integrated ultrasonic sensor in rectangular topology, which establish a collision free data transmission in an emergency scenario. The developed network was tested in a field experiment in an explosion within a building to confirm its functionality and reliability. The wireless sensor network was able to pass critical data to the emergency units to initiate the rescue procedures during this disaster scenario.

CHAPTER 2

LITERATURE REVIEW

2.1 TOPOLOGY MANAGEMENT TECHNIQUES FOR TOLERATING NODE FAILURES IN WIRELESS SENSOR NETWORKS: A SURVEY

In wireless sensor networks (WSNs) nodes often operate unattended in a collaborative manner to perform some tasks. In many applications, the network is deployed in harsh environments such as battlefield where the nodes are susceptible to damage. In addition, nodes may fail due to energy depletion and breakdown in the onboard electronics. The failure of nodes may leave some areas uncovered and degrade the fidelity of the collected data. However, the most serious consequence is when the network gets partitioned into disjoint segments. Losing network connectivity has a very negative effect on the applications since it prevents data exchange and hinders coordination among some nodes. Therefore, restoring the overall network connectivity is very crucial. Given the resource-constrained setup, the recovery should impose the least overhead and performance impact. This paper focuses on network topology management techniques for tolerating/handling node failures in WSNs. Two broad categories based on reactive and proactive methods have been identified for classifying the existing techniques. Considering these categories, a thorough analysis and comparison of all the recent works have been provided. Finally, the paper is concluded by outlining open issues that warrant additional research. Further classification is done within each category based on the system assumptions, required network state, metrics and objectives for the recovery process, etc. Under each category, we discuss several algorithms and highlight their strengths and weaknesses. Finally, we enumerate open research issues that are yet to be investigated by the research community.

2.2 THE SPREAD OF COMPUTER VIRUSES OVER A REDUCED SCALE-FREE NETWORK

Due to the high dimensionality of an epidemic model of computer viruses over a general scale-free network, it is difficult to make a close study of its dynamics. In particular, it is extremely difficult, if not impossible, to prove the global stability of its viral equilibrium, if any.

To overcome this difficulty, we suggest to simplify a general scale-free network by partitioning all of its nodes into two classes: higher-degree nodes and lower-degree nodes, and then equating the degrees of all higher-degree nodes and all lower-degree nodes, respectively, yielding a reduced scale-free network. We then propose an epidemic model of computer viruses over a reduced scale-free network. A theoretical analysis reveals that the proposed model is bound to have a globally stable viral equilibrium, implying that any attempt to eradicate network viruses would prove unavailing. As a result, the next best thing we can do is to restrain virus prevalence. Based on an analysis of the impact of different model parameters on virus prevalence, some practicable measures are recommended to contain virus spreading. The work in this paper adequately justifies the idea of reduced scale-free networks. We suggest to simplify the topology of a general scale-free network by partitioning all nodes in the network into two classes: higher-degree nodes and lower-degree nodes, assuming that the degrees of all higher-degree nodes are equal to their average degree and that the degrees of all lower-degree nodes are equal to their average degree. As with general scale-free networks, we assume that a node in the simplified network is connected to a k-degree node with a probability that is proportional to the value of k. Thus, a reduced scale-free network is formed. The major objective of this paper is to understand the spread of computer viruses on a reduced scale-free network. For that purpose, we propose a novel epidemic model of computer viruses. Our theoretical analysis reveals that this model always admits a globally stable viral equilibrium.

2.3 TOPOLOGY AND VULNERABILITY OF THE IRANIAN POWER GRID

In this paper we investigated the structural properties of the ultrahigh voltage power transmission network of Iran. We modeled the power grid as a network with 105 nodes and 142 connection links. We found that the Iranian power grid displays a relatively moderate clustering coefficient – much larger than that of corresponding random networks – and small characteristics path length comparable to that of corresponding random networks; i.e. the power grid is a small-world network with exponential degree distribution. Global efficiency was considered as an indicator of grid's performance and the influence of random and intentional nodal failures on the efficiency was investigated. We also studied the influence of cascaded failures on the largest connected component of the network. The power grid was vulnerable against cascaded failures, which should be considered serious in redesigning the network topology. Complex dynamical

networks have a vital role in our everyday life. It has been shown that many biological, technological and social networks lie between random and regular networks, with high clustering coefficient and small characteristics path length; they are indeed small-world networks. The idea that the dynamical behavior of complex systems could be strongly influenced by the structure of an underlying network was suggested first by Watts and Strogatz in their seminal work on small-world networks. In this context, the importance of the network structure became even more evident after a work by Barabasi and Albert on scale-free networks. The role of network structure is further emphasized by the presence of communities, correlations, patterns of weighted connections and other nontrivial structures in many real-world networks that had not been anticipated from the classical random graph theory of Erdos and Renyi. The first approach to capture the global properties of complex systems is to model them as graphs with nodes representing the dynamical units and links the interactions between them.

2.4 OPTIMAL NETWORK TOPOLOGY FOR STRUCTURAL ROBUSTNESS BASED ON NATURAL CONNECTIVITY

The structural robustness of the infrastructure of various real-life systems, which can be represented by networks, is of great importance. Thus we have proposed a tabu search algorithm to optimize the structural robustness of a given network by rewiring the links and fixing the node degrees. The objective of our algorithm is to maximize a new structural robustness measure, natural connectivity, which provides a sensitive and reliable measure of the structural robustness of complex networks and has lower computation complexity. We initially applied this method to several networks with different degree distributions for contrast analysis and investigated the basic properties of the optimal network. We discovered that the optimal network based on the power-law degree distribution exhibits a roughly ‘‘eggplant-like’’ topology, where there is a cluster of high-degree nodes at the head and other low-degree nodes scattered across the body of ‘‘eggplant’’. Additionally, the cost to rewire links in practical applications is considered; therefore, we optimized this method by employing the assortative rewiring strategy and validated its efficiency. In a recent work, the authors proposed a new measure, R, for network robustness under malicious attack on nodes, 15 which corresponds to the failure of the stressed nodes in physical networks. This new measure R, considers the size 16 of the largest connected cluster during the malicious attack. With this measure, they designed an algorithm, based on 17 greedy

algorithms to enhance the structural robustness of a given network by swapping its links while keeping its degree 18 distribution fixed. The R-optimized network has an ‘‘onion-like’’ topology consisting of a core of highly connected nodes 19 that are hierarchically surrounded by rings of nodes with decreasing degree. Moreover, the method based on greedy algorithm usually fails to find the global optima due to the complexity of 34 this kind of combinatorial optimization problem.

2.5 DESIGN OF FAULT TOLERANT WIRELESS SENSOR NETWORKS SATISFYING SURVIVABILITY AND LIFETIME REQUIREMENTS

Sensor networks are deployed to accomplish certain specific missions over a period of time. It is essential that the network continues to operate, even if some of its nodes fail. It is also important that the network is able to support the mission for a minimum specified period of time. Hence, the design of a sensor network should not only provide some guarantees that all data from the sensor nodes are gathered at the base station, even in the presence of some faults, but should also allow the network to remain functional for a specified duration. This paper considers a two-tier, hierarchical sensor network architecture, where some relay nodes, provisioned with higher power and other capabilities, are used as cluster heads. Given a distribution of sensor nodes in a sensor network, finding the locations to place a minimum number of relay nodes such that, each sensor node is covered by at least one relay node, is known to be a computationally difficult problem. In addition, for successful and reliable data communication, the relay nodes network needs to be connected, as well as resilient to node failures. In this paper, a novel integrated Integer Linear Program (ILP) formulation is proposed, which, unlike existing techniques, not only finds a suitable placement strategy for the relay nodes, but also assigns the sensor nodes to the clusters and determines a load-balanced routing scheme. Therefore, in addition to the desired levels of fault tolerance for both the sensor nodes and the relay nodes, the proposed approach also meets specified performance guarantees with respect to network lifetime by limiting the maximum energy consumption of the relay nodes.

2.6 Complex networks-based energy-efficient evolution model for wireless sensor networks

Based on complex networks theory, we present two self-organized energy-efficient models for wireless sensor networks in this paper. The first model constructs the wireless sensor

networks according to the connectivity and remaining energy of each sensor node, thus it can produce scale-free networks which have a performance of random error tolerance. In the second model, we not only consider the remaining energy, but also introduce the constraint of links to each node. This model can make the energy consumption of the whole network more balanced. Finally, we present the numerical experiments of the two models. Many energy-aware and fault-tolerant topology control algorithms for wireless sensor networks have been presented in recent years. In Ref., authors proposed an energy-efficient routing algorithm for gathering correlated data in sensor networks. Authors in Ref. proposed an approach to construct k-connected network for clustering sensors deployed in hostile environments. Authors in Ref. presented a mechanism to deduce fault-tolerant communication topology among the cluster heads. Several control algorithms considered in Ref. are to maintain network connectivity while improving network performance. Authors in Refs Have much related work about energy efficiency and fault tolerance. However, almost all the existing studies have not studied the performance of energy efficiency and fault tolerance in WSNs from the views of the network evolution and degree distribution. In this paper, we propose two evolving algorithms for wireless sensor networks-based on complex networks theory. The first model is to deduce energy-aware communication topology, and this model can produce scale-free networks which have a performance of random error tolerance.

2.7 A TOPOLOGY CONSTRUCT AND CONTROL MODEL WITH SMALL-WORLD AND SCALE-FREE CONCEPTS FOR HETEROGENEOUS SENSOR NETWORKS

Topology construction and control is a vital technique in wireless sensor networks. In this paper, based on small-world and scale-free concepts of complex network theory and considering the characteristics of wireless sensor network, a topology model with small world and scale-free concepts for heterogeneous sensor network is presented. This work is achieved by applying heterogeneous sensors and preferential attachment mechanism. Furthermore, the topology evolution algorithm is designed. Finally, we simulate the network characteristics, and simulation results are consistent with the theoretic analysis and show that topologies of wireless sensor network built by this model have small-world and scale-free feathers and can significantly improve energy efficiency as well as enhance network robustness, leading to a crucial improvement of network performance. Most topology models are based on some network

theories such as random graph theory and complex network theory. The complex networks widely exist in real world such as electrical power grids, global transport networks, co authorship and citation networks, and so on. As an interdisciplinary research area, complex networks arouse worldwide attention. Two most typical network models in complex network theory are small-world network and scale-free network. The small-world network has two independent structural features: (i) a small average shortest path length and (ii) a large clustering coefficient. By applying small-world theory in topology construction of WSNs, the network performance will be improved in querying data efficiency, energy efficiency, network lifetime, and so forth. A scale-free network is a network whose node's degree follows a power law distribution, and the scale-free topology characteristics have a higher robustness to endure the random failure.

CHAPTER 3

OVERVIEW OF FIRST TOPOLOGY

3.1 SCALE FREE TOPOLOGY

Over the past several years, researchers have uncovered scale-free structures in a stunning range of systems. When we studied the World Wide Web, we looked at the virtual network of Web pages connected to one another by hyperlinks. The figure 3.1 represents the birth of a scale free network. Researchers have also discovered that some social networks are scale-free collaborations between scientists from Boston University and Stockholm University, for instance, has shown that a network of sexual relationships among people in Sweden followed law: although most individuals had only a few sexual partners during their lifetime, a few (the hubs) had hundreds. A recent study led by Stefan of the University of Kiel in Germany concluded that the network of people connected bye-mail is likewise scale free. Sidney Redner of Boston University demonstrated that the network of scientific papers, connected by citations, follows a power law as well. And Mark New man of the University of Michiganat Ann Arbor examined collaborations among scientists in several disciplines, including physicians and computer scientists, and found that those networks were also scale-free, corroborating A study we conducted focusing on mathematicians and neurologists.

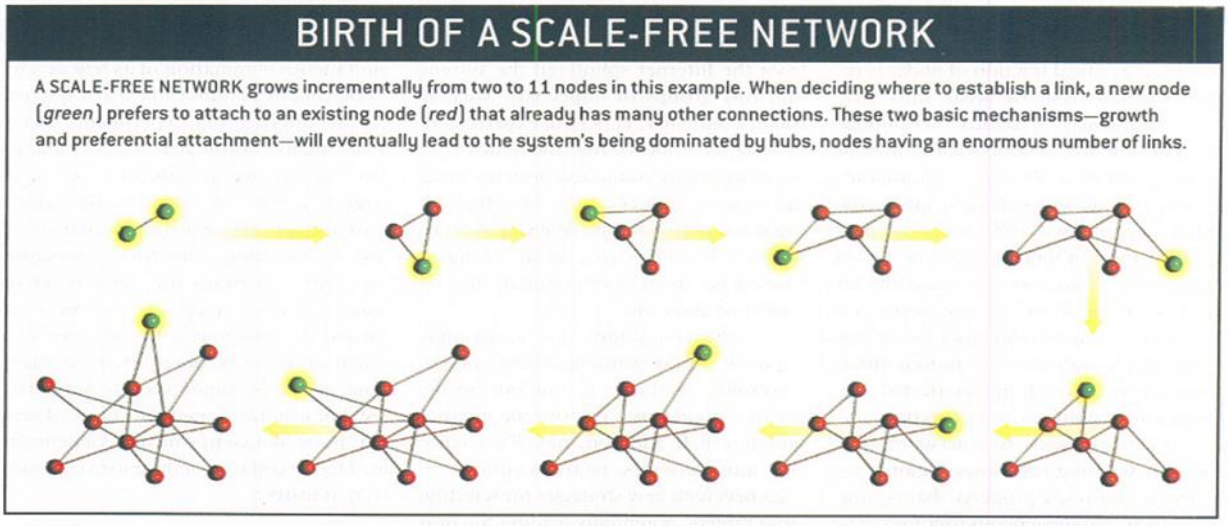

Figure 3.1 Birth of A Scale Free Network

Recent researches show that the scale-free topology is robust to random faults of the node but vulnerable to selective remove attacks of the node. This conclusion becomes more evident

after a deal of works by Barabasi and Albert on scale-free topology. So how to design and optimize the scale-free topology and how to make the scale-free topology have the strong capability of fault-tolerance to random faults and intrusion-tolerance to selective remove attacks simultaneously is particularly important and urgent. In order to improve the robustness of the scale-free topology against selective remove attacks on the basis of strong fault-tolerance, this paper proposes a new scale-free topology model BA-E (BA-Evolution) and obtains an optimal scale free topology.

3.2 EXISTING METHOD

In previous work, we used an EAEM (Energy-Aware Evolution Model) investigated how to build the energy efficient scale-free topology. It introduced the node residual energy to the preferential attachment mechanism, and improved the energy efficiency of the scale-free topology. It combined more characteristics of sensors, including residual energy, degree saturation and maximum communication radius. It considered the residual energy and the node fitness during the topology evolution, which made the scale-free topologies a good robustness against energy exhaustion and random faults. There are more constraints being added on the scale-free topology to make it accord with the characteristics of WSNs in varied applications, which are needed to optimize the topology robustness, but the scale-free topologies don't optimize the capability of intrusion-tolerance against selective remove attacks.

3.2.1 Disadvantages

- The scale-free topology is robust when confronted with random faults, but it is fragile when confronted with selective remove attacks.
- However, the nodes in WSNs, which are deployed in harsh environments, are easy to break down because of energy depletion, hardware failure or invasion.
- On node failure, the network connectivity will be reduced greatly, and the entire network even to be paralytic.

3.3 PROPOSED METHOD

In order to improve the robustness of the scale-free topology against selective remove attacks on the basis of strong fault-tolerance, this paper proposes a new scale-free topology model BA-E

(BA-Evolution) and obtains an optimal scale free topology which can assure the topological fault-tolerance against random faults and maximize topological intrusion tolerance against selective remove attacks. The proposed scale-free topology model BA-E has the adjustable scaling exponent for the degree distribution the figure 3.2 represents the architecture of scale free network. Two criterions of measuring the topological properties (i.e. one for fault-tolerance against random faults, the other for intrusion-tolerance against selective remove attacks) and the effect of topological degree distribution on these properties are discussed mathematically. Then the optimal parameter of the BA-E model is derived. The proposed BA-E model with the obtained optimal parameter is implemented through simulation for fault-tolerance against random fault and intrusion-tolerance against selective remove attacks.

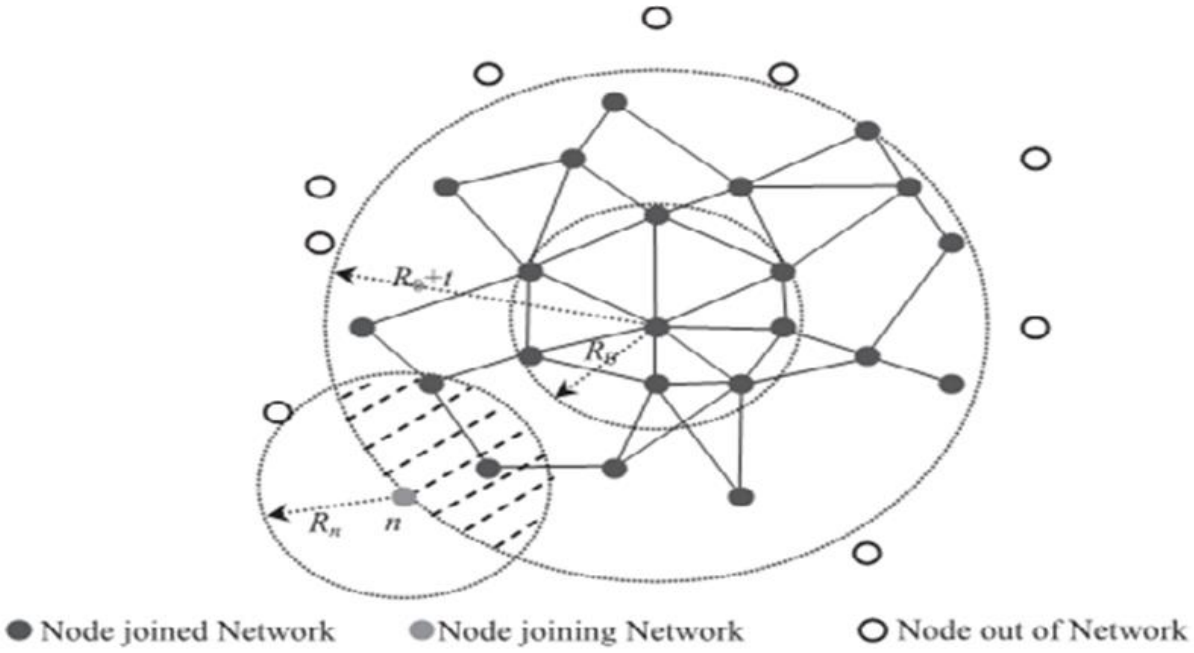

Figure 3.2 Architecture of a scale free network

3.3.1 Advantages

- The new scale-free topology model can keep the character that the scale-free topology has a stronger robustness to random faults.

- It improves the robustness of the scale-free topology against selective remove attacks on the basis of strong fault-tolerance and it also can reduce their fragility for selective remove attacks and further prolong its lifetime.

CHAPTER 4
OVER VIEW OF SECOND TOPOLOGY

4.1 RECTANGULAR TOPOLOGY

Long-term monitoring of critical infrastructure such as bridges, tunnels, dams, and skyscrapers is focused on detecting damages caused by static and cyclic loads during regular operation. The assessment of structural behavior and resulting lifetime predictions of these structures are also outlined in the planned work and still an active topic of research. Deployment of a wireless sensor network for monitoring the condition of the infrastructure in the event of a disaster is an approach since a decade.

The primary goal of an attack is to deny the access to a particular resource of a victim. The attacker, in order to hide the identity, often spoofs the source IP address of the packet. Such spoofing results in the impossibility of tracing back the attacker. Recently, IP spoofing prevention technique using Identity based cryptography has been proposed in which a signature scheme is used to achieve better security.

4.2 EXISTING METHOD

Previously used approaches for this purpose mostly employ wired communication systems, or use wireless sensor nodes where time-critical events are not considered in conjunction with wireless systems, e.g., environment; buildings; pipelines; mine tunnels; train- and road tunnel. Several publications were also reported in emergency situations in tunnels, mines and pipelines. Their major focus is on the explosions effects on the infrastructure. Few publications also reported on the data management of a disaster scenario. Extensive research in the area of wireless sensor networks has been frequently reported which includes research in energy-efficient wireless protocols in topology; in routing; in algorithms; in synchronization, in maximizing the lifetime and in position status determination.

4.2.1 DISADVANTAGES

- Using wireless sensor nodes in case of disasters in scenarios where there is no need for time critical aspects were discussed by previous works.
- The use of wireless sensor networks for the scenarios which includes the time-critical events has not been reported.
- And the time-critical aspects in disastrous situations is still not reported.

4.3 PROPOSED METHOD

Information gathering in tunnels, buildings, bridges, etc. during disasters is of vital importance in speeding up rescue efforts and for protecting the fire fighters. The collected data can be used by the emergency services in the planning of rescue operations and allocation of human resources at a local level. In this article we present design and implementation of a wireless sensor network, which consists of energy-efficient wireless sensor nodes with an integrated ultrasonic sensor, which establish a collision free data transmission in an emergency scenario. The developed network was tested in a field experiment in an explosion within a building to confirm its functionality and reliability. The wireless sensor network was able to pass critical data to the emergency units to initiate the rescue procedures during this disaster scenario.

In this paper, the drawbacks of True IP are addressed and a new architecture has been proposed to overcome them. In addition, all sorts of man-in-the-middle attacks (MIMA) are eliminated in our proposal.

In the presented work, we will focus on time-critical events monitoring using wireless sensor networks. For this purpose, a system of energy-efficient wireless sensor nodes has been developed to obtain information about the condition of the infrastructure in the event of a disaster. The wireless sensor nodes were placed in strategic positions to detect possible explosions occurring in the structure. The acquired information is transmitted wirelessly to a central unit, where emergency services were activated. Data from wireless sensor nodes provides the fire fighters and the related staff precise information about the infrastructure damages and possibility to detect the building collapse situation through this approach, efficient planning can be made to save lives.

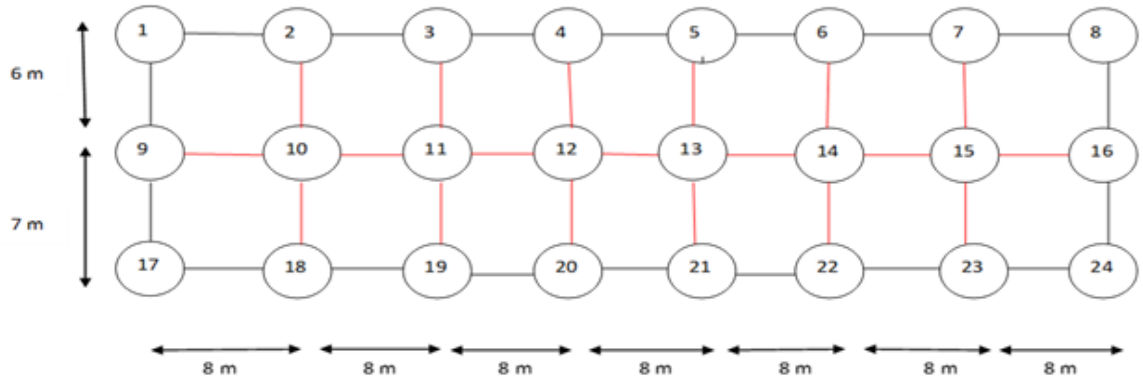

Figure 4.1 Architecture of rectangular topology

4.3.1 Advantages

- A novel application of the ID based signature scheme has been proposed to prevent IP spoofing and Man in-the-Middle Attack across a network.
- The proposed solution has been implemented with key generation, packet generation with signature, and signature verification modules.
- The implementation was tested at the application level and shown to prevent Man-in the-Middle attacks detecting the change in fields, viz., source IP address, destination IP address, packet data, and the appended signature within a network

CHAPTER 5

MODULE DESCRIPTION

5.1 MODULES OF SCALE FREE

- Scale-free topology model
- Degree distribution characteristics
- Mathematical optimization model

5.1.1 Scale-free topology model

In order to evolve the scale-free topology with the good performance of both fault-tolerance and intrusion-tolerance in WSNs, we can use the improved growth and preferential attachment to build the scale-free topology model with the local-area idea. Then the evolutional degree distribution of the model is discussed.

BA-E evolution model

In, BA model uses the method of growth and preferential attachment. In the growth process, the number of nodes in the network grows continuously. In the preferential attachment process, the probability of a new node to be linked to an existing node i depends on the degree k i of nod e i, and obeys the following rules

$$\prod(k_i) = \frac{k_i}{\sum_j k_j} \qquad (1)$$

The growth rule and preferential attachment rule above lead to a skewed degree distribution for topology, it constructs the BA scale-free topology whose degree distribution follows p(k)∝k −3. This BA scale-free topology has a good fault tolerance against random faults and a poor intrusion-tolerance against selective remove attacks. In order to improve the robustness of the scale-free topology against both random faults and selective remove attacks, the variable parameter p is introduced. When p varies from 1 to 0the topology changes from random topology to BA scale-free topology.

The BA-E model which is similar with the BA model can be divided into two steps: Growth: starting with a small number of nodes m0, at every time, a new node with m(m≤m0) links that will be connected to the nodes already exist in the network is added. Preferential attachment: when a new node comes into the network, it will choose some nodes in its local-area to connect. And the probability of the new node to be connected to node i depends on its degree k i and the preferential probability factor p, which is defined as

$$\prod_{local}(k_i) = \frac{(1-p)k_i+p}{\sum_{j\,\epsilon\,local}(1-p)k_j+p} \quad (0 < p \leq 1) \tag{2}$$

Where, the node i and j are within the local-area of the new node. The model evolves to BA scale-free topology when p=0, and it becomes an approximately random topology when p=1. For 0<p<1, we call this evolving model as BA-E. It is worthwhile to note that the adjustable degree distribution of BA-E model follows the power-law statistics of the scale free topology, which can improve the intrusion-tolerance of topology against selective remove attacks without breaking the strong fault-tolerance against random faults.

5.1.2 Degree distribution characteristics

The evolution of BA-E model the initial network consists of m0 nodes and e0 links. It is supposed that, node n joins the network at time t, R n is the communication radius of node n, R0 is the initial network radius, R0+t is the network radius at time t. Considering the degree distribution of BA-E model, the probability that the node n builds communication link in its local-area is decided by Eq. and m new links are formed during each time. According to the mean-field theory, we get

$$\frac{\partial k_i}{\partial t} = m \prod_{local}(k_{i)} \tag{3}$$

within [3 ,+∞) by adjusting the parameterp.Whenp→0, we can get p(k)~k−3, then the degree distribution of BA-E model is closing in on the BA scale-free topology which has the good capability of fault-tolerance against random faults; whenp→1, we can get p(k)∝e−k/m, then the degree distribution of BA-E model is closing in on the random topology which has the good

capability of intrusion-tolerance against selective remove attacks. So it can be concluded that the BA-E model has the power-law distribution that keeps its robustness of fault-tolerance, together with strong fault-tolerance, a strong intrusion-tolerance can also be obtained by adjusting the parameter p.

5.1.3 Mathematical optimization model

Based on the analysis of the degree distribution of BA-E model, the topology derived by BA-E model exist the optimal value p (which can withstand node failures, that is, the random faults and the selective remove attacks). In this section, we analyze the effect of degree distribution characteristics on topological fault-tolerance and topological intrusion tolerance, then find the optimal p. Base do n p, an optimal BA-E scale-free topology is derived which keeps the topological fault-tolerance and maximizes the topological intrusion-tolerance.

BA-E fault-tolerance index

Based on the percolation theory, Cohen et al. have studied the properties of the percolation phase transition, and found that there is a critical point removal ratio h_r, and hr can be used as the fault-tolerance strength criterion of the scale free topology. When the removal ratio of random nodes is more than hr, the topology will collapse into many smaller disconnected parts. And Ref. applied a general criterion for the existence of a spanning part, and this criterion can be written as

$$\frac{(k^2)}{(k)} = 2 \qquad (4)$$

When an h(0<h<1) ratio of nodes is randomly removed, for a node with initial degreek0chosen from an initial distribution p(k0), the connectivity distribution of the node is changed from the original distribution p(k0) to a new distribution ˜ p(k). The new distribution ˜ p(k)is given by

For the purpose of constructing the BA-E scale-free topology with stronger fault-tolerance, Eq. can be used as then topological fault-tolerance strength criterion. When m and λ

are constant, the smaller hr is, the less removal ratio of random nodes that topology can tolerate is, and the worse fault-tolerance the topology is.

BA-E intrusion-tolerance index

The heterogeneity of scale-free topology leads to paralysis when the topology is confronted with the selective remove attacks. In this section, we use the uniformity to measure the topological intrusion-tolerance. The authors in proposed the topology structure entropy which can well measure the heterogeneity of topologies. The topology structure entropy corresponds to the uniform topology when it is maximized and corresponds to the star topology when it is minimized. So, the optimization of topological intrusion-tolerance is equivalent to maximize the topology structure entropy of scale-free topology. The topology structure entropy is defined as follows:

$$E = -\sum_{i=1}^{N-1} l_i \ln I_i = -\frac{\sum_{i=1}^{N} k_i \ln k_i}{\sum_{i=1}^{N} k_i} + \ln \sum_{i=1}^{N} k_i \quad (5)$$

In Eq. the topology structure entropy E of BA-E scale-free topology can be expressed as the function of variables N and λ. When N and λ are constant, the topology structure entropy E can be used as the topological intrusion-tolerance strength criterion. The greater E is, the more uniform the topology is, and the stronger intrusion-tolerance the topology is. This means topology structure entropy E should be maximized if the stronger intrusion-tolerance of BA-E scale-free topology is needed.

Mathematical optimization model of BA-E for fault-tolerance and intrusion-tolerance

This section wants to construct an optimal intrusion-tolerance topology on the basis of strong fault-tolerance we use hr as the measure of the topological fault-tolerance strength criterion, and use E as the measure of the topological intrusion tolerance strength criterion. For hr>0.5, it means that the topology can tolerate more than half of all the nodes to randomly fail, and the topology has stronger fault-tolerance. So this optimization problem of intrusion-tolerance based on strong fault tolerance can be transformed into the following mathematical mode.

Under the condition of m=1, N=200,p≈0.27, we implement the BA-E model, the environment parameters are shown in Table 1, then we can evolve the optimal BA-E topology, as shown in Fig. Fig. represents the contrast of the theoretical value and actual value in the degree distribution of BA-E topology, and the straight line is the theoretical degree distribution

5.2 MODULES OF RECTANGULAR

- Initialization
- Monitoring Phase
- Attack detection & Data sharing

5.2.1 Initialization

In this module used to initialize the nodes in network topology. We used network topology and topography for our network animator window (nam window). We have syntax for create nodes in network animator window. Then we can create nodes in two types like random and fixed motions.

In random motion we fixed range for X and Y, fixed particular range then the nodes are randomly generate in that range of nam window. In fixed motion we give X and Y dimension position for all nodes then all the nodes are fixed in that particular dimension.

Sensor nodes are aware of their own positions. The position information may be based on a global or a local geographic coordinate system defined according to the deployment area. Determining the position of the nodes might be achieved using a satellite based positioning system such as global positioning system (GPS) or one of the energy-efficient localization methods proposed specifically for MANETs.

Every sensor node should be aware of the position of its neighbors. This information enables greedy geographic routing and can be obtained by a simple neighbor discovery protocol. The coordinates of a network center point has to be commonly known

by all sensor nodes. The network center does not have to be exact and can be loaded into the sensors' memories before deployment. The ring structure encapsulates the network center at all times, which allows access to the ring by regular nodes and the sink.

5.2.2 Monitoring Phase

We designed two different implementations of our system for centralized catastrophe management and monitoring services. The first implementation is dependent on the power limitations of the wireless sensor node and the router. In the second implementation the monitoring terminals and the wireless sensor nodes can be far away from each other. The already existing cellular communication network General Packet Radio Service (GPRS) is used to communicate between the monitoring center and the wireless sensor nodes. For instance, this system allows monitoring of multiple critical infrastructures that are in different geographical locations such as various cities or even countries. The monitoring data can be collected and evaluated at a single location which would eventually increase coordination efficiency and reduce the required time for the initiation of time critical activities.

In a network of interconnected wireless sensor nodes, efficient and collision-free data transmission is of vital importance, especially for the disaster management applications explained in this section. In terms of network topology the wireless sensor nodes are synchronized in this work using an adapted time-slot principle. For this purpose, the disaster area, e.g., tunnel or building, has a set S of wireless sensor nodes. In this work a uni-directional communication protocol was used, which is based on the channel access method TDMA. This protocol can be used in case of the time-critical application, e.g., explosion. In our application all wireless sensor nodes were in the range of both routers. This redundancy ensures that no data is lost in case of a break-down of one of the routers. In order to avoid data collusion, each wireless sensor node checks the Received Signal Strength Indication (RSSI). It transmits data if no other sensor node is currently active. The protocol, which was used in our application, is a deterministic protocol, i.e., the numbers of wireless sensor nodes is already known, and each of them sends in its own time slot.

5.2.3 Attack detection & Data sharing

The main idea of identity-based cryptography, proposed in this paper, is to use a publicly known identifier (ID) of a participant as its public key; it was first suggested by Shamir in. The IP address of the participant is used as the public key. A trusted authority operating an Identity Private Key Generator (ID-PKG) creates the corresponding private keys for the identities using the secret knowledge possessed only by the ID-PKG.

In our proposal, a system of n Private Key Generators (PKG) as shown in Figure 1 is considered. A PKG is installed in every network. Also a PKG is installed in a network present within a NAT. A master PKG (M-PKG) is responsible for guiding and coordinating the activities of all the other PKGs. It also sets the master secret key (msk) and public parameters (mpk) and distributes them securely to all other PKGs. Each user is associated with a PKG, to whom it makes a request for the Secret Key. Once secret keys are assigned through secure key distribution, users have to append a signature to every packet sent across the network. Verification of the signature is done using the public parameters of PKG by any intermediate router. Successful verification of the signature implies the authenticity of the packet.

CHAPTER 6
A SURVEY ON ATTACKS

Without security measures and controls in place, your data might be subjected to an attack. Some attacks are passive, meaning information is monitored; others are active, meaning the information is altered with intent to corrupt or destroy the data or the network itself. keeping data safe and secure in computers and networks became one of most interesting and challenging area in Network and Security. In spite of the fact, attackers try to achieve the sensitive and critical assets to take advantage of them. Due to many motivations, there are plenty of news about misusing information and attacking computers across the globe, which have done by intruders

6.1 VARIOUS KINDS OF ATTACK IN NETWORKING

6.1.1EAVESDROPPING:

Capturing and decoding unprotected application traffic to obtain potentially sensitive information (i.e). To listen secretly to the private conversation of others this is a passive attack, which occurred in the mobile ad-hoc network. The main aim of this attack is to find out some secret or confidential information from communication. This secrete information may be privet or public key of sender or receiver or any secrete data.

6.1.2 DATA MODIFICATION:

They occur when someone makes unauthorized modifications to data. An attacker can modify the data in the packet without the knowledge of the sender or receiver. Data modification is a control-data-attack, which is attacker modifies the control-flow of programs. That means it corrupt user characteristics, configuration and user input data or policy making data to achieve the attacker's goals.

6.1.3 IDENTITY SPOOFING

(IP Address Spoofing) creation of Ip packets with a forged source. purpose of it is to conceal the identity of the sender (or)impersonating another computing system. the

goal to flood the victim with overwhelming amount of traffic. It prevents an internet site (or) service from functioning efficiently or at all temporarily (or) indefinitely.

6.1.4 DENIAL-OF-SERVICE ATTACK

Denial-of-service (DoS) attacks typically flood servers, systems or networks with traffic in order to overwhelm the victim resources and make it difficult or impossible for legitimate users to use them DoS attack as an event that diminishes or attempts to reduce a network's capacity to perform its expected function. Denial of Service (DoS) is a class of attacks where an attacker makes some computing or memory resource too busy or too full to handle legitimate requests, thus denying legitimate users access to a machine. There are different ways to launch DoS attacks:

- Abusing the computers legitimate features.
- Targeting the implementations bugs.
- Exploiting the system's misconfigurations. DoS attacks are classified based on the services that an attacker renders unavailable to legitimate users.

6.1.5 WARM HOLE ATTACK

A wormhole is low latency link between two portions of a network over which an attacker replays network messages. This link may be established either by a single node forwarding messages between two adjacent but otherwise non neighboring nodes or by a pair of nodes in different parts of the network communicating with each other. The latter case is closely related to sinkhole attack as an attacking node near the base station can provide a one-hop link to that base station via the other attacking node in a distant part of the network.

6.1.6 BLACK HOLE ATTACK

A Black Hole attack is a type of routing attack in which malicious node advertise itself as having shortest path to destination in a network by sending fake route reply to the source node. The black hole attack is an active insider attack, it has two properties: first, the attacker consumes the intercepted packets without any forwarding. Second, the node exploits the mobile ad hoc routing protocol, to advertise itself as having a valid route to a

destination node, even though the route is spurious, with the intention of intercepting packets.

6.1.7 MAN-IN-THE-MIDDLE ATTACK

MITM attack works in such a manner that it makes the users difficult to understand if they are connected to the actual secure connection or to a similar non-secure connection. When the user tries to establish a connection with the network, the user first sends packets which include the information about the user device to the necessary network. The network then creates a digital certificate which includes the encrypted connection key and the user device address. Since the certificate that is being passed during the connection initialization is insecure, the attacker can easily gain access to the digital certificate and modify the information in the certificate leaving the approval of the certificate to the user. Many users do not have enough knowledge to check about the whereabouts of the forged and duplicate certificates and the attacks corresponding to them, thus they accept the certificates and allow connection to the non-secure network.

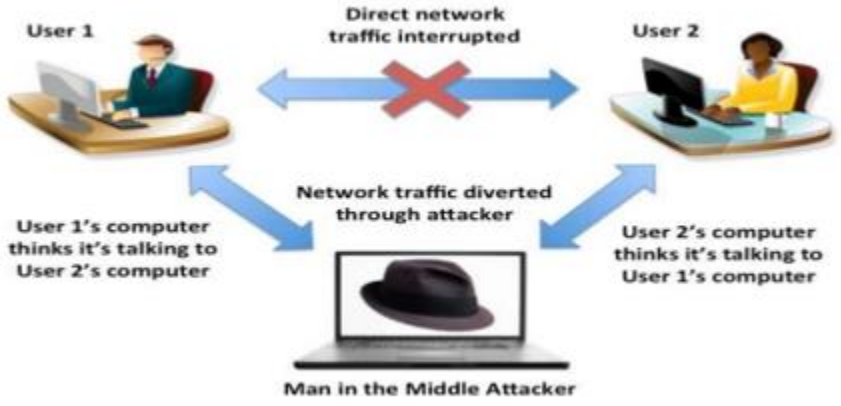

Figure 6.1 Architecture of Man in The Middle Attack

- It is found that the man in middle attack has quite interesting features compared to other attacks. The idea is to insert the man in middle attack in scale free topology and rectangular topology to analyze better performance based on metrics like throughput, packet delivery ratio, energy efficiency, end to end delay, network life time

CHAPTER 7

RESULTS

7.1 SIMULATION RESULTS OF SCALE FREE

This study used ns-2 as the network simulator and conducted numerous simulations to evaluate the propose result performance. All sensor nodes are randomly scattered with a uniform distribution. The location of the sink is randomly determined. This study evaluates the routing performance under scenarios with different numbers of sensor nodes

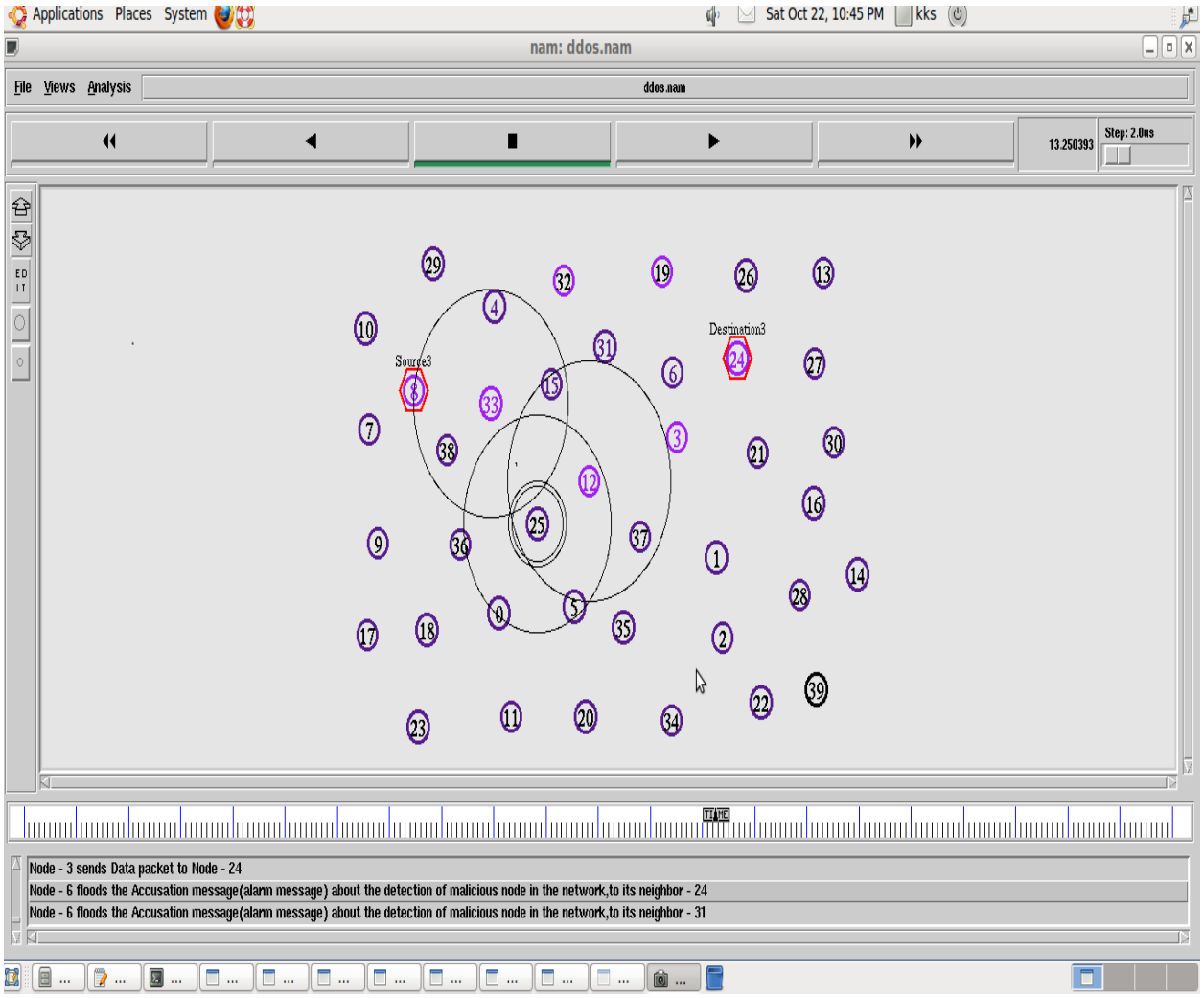

figure 7.1 node creation

The above figure 8.1 shows the collection of nodes in wireless sensor network (WSN). The source and destination are indicated by red color. The circle indicates the communication between neighboring nodes.

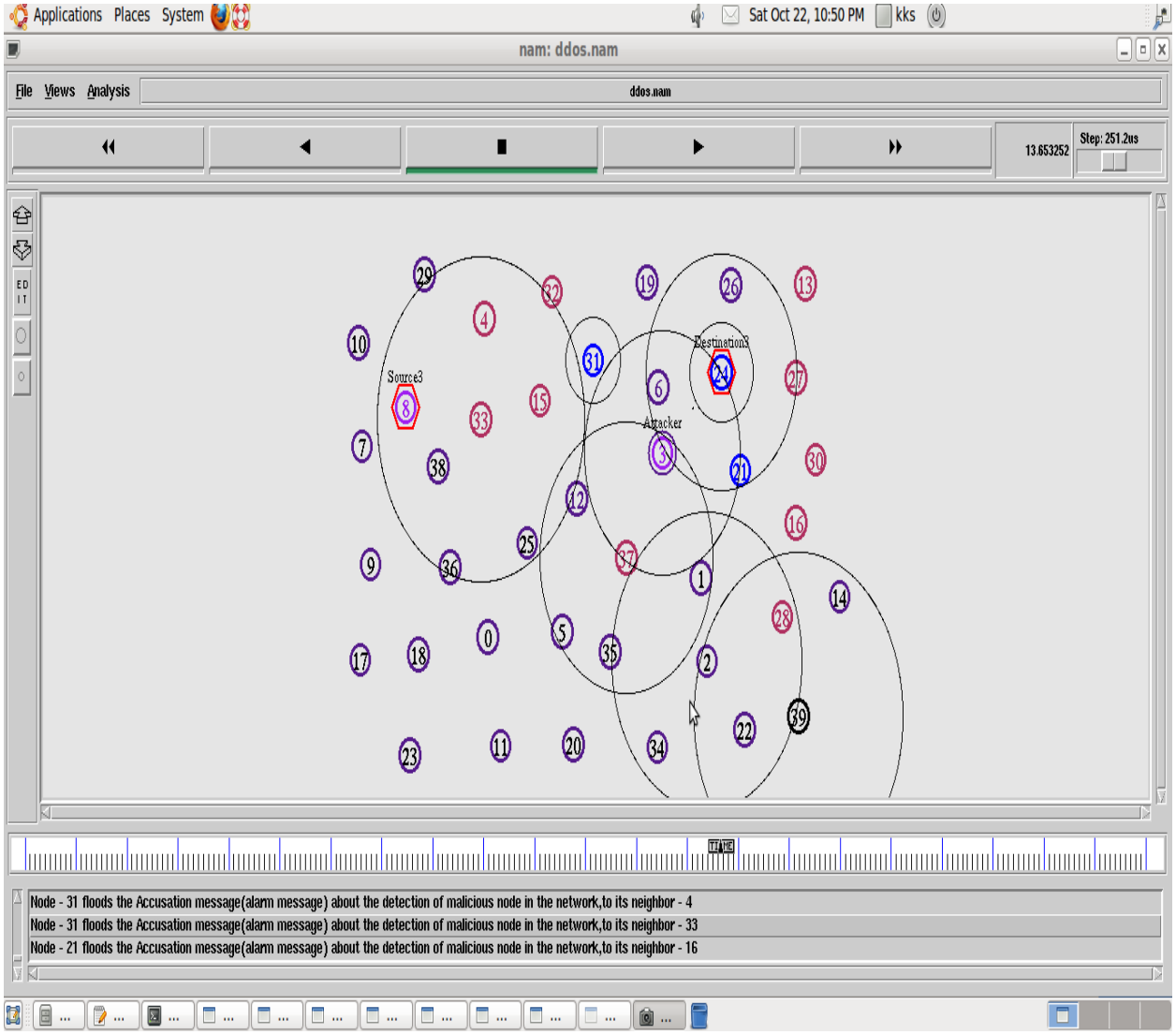

figure 7.2 Identification of attacker

The above simulation result of figure 8.2 indicates that the node 3 as an attacker which is shown in violet colour.the different way of data path which is shown in brown colour

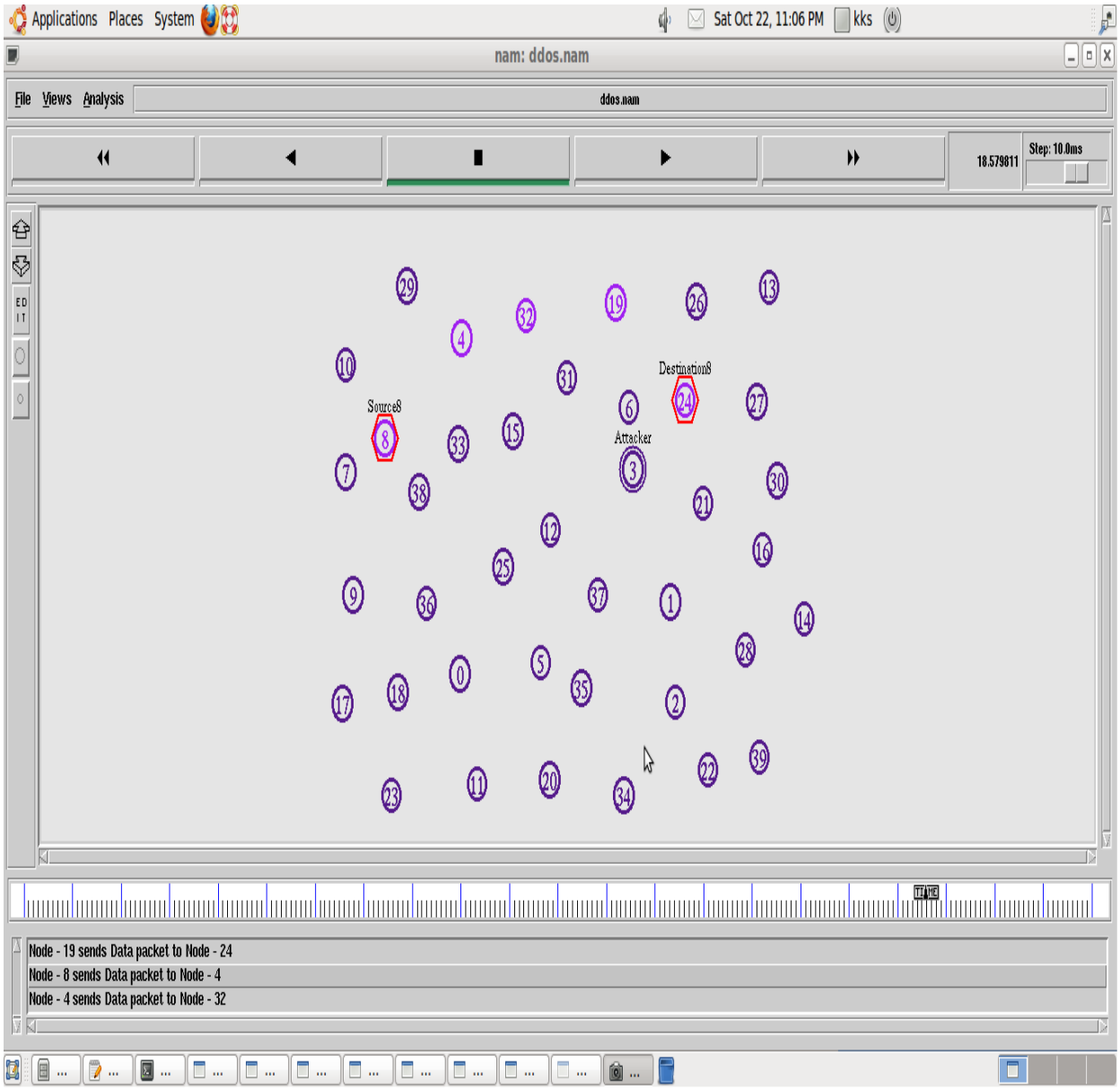

figure 7.3 Identification of best path for data transmission

The above simulation result of figure 8.3 indicates that the best path for reaching destination has been found and are indicated by violet color.

7.1.1 Packet drop

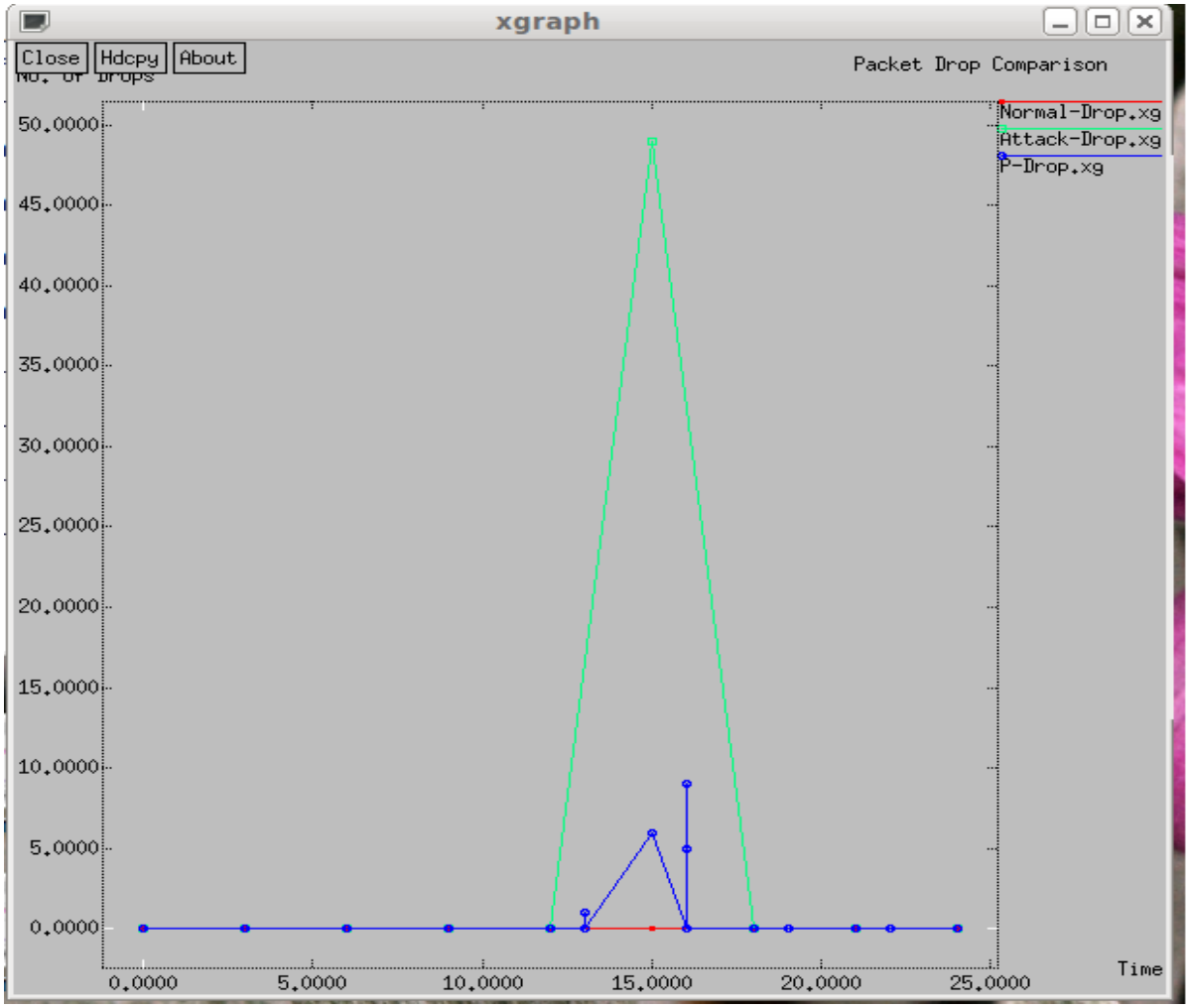

figure 7.4 Time vs No. of Nodes

The above figure 8.4 is the plot for time vs no of nodes. The red line indicates packet drop without attackers and the green line indicates packet drop with attackers and the blue line indicates the packet drop in proposed work. From the graph it is seen that the packet drop in proposed work is less when compared.

7.1.2 Throughput

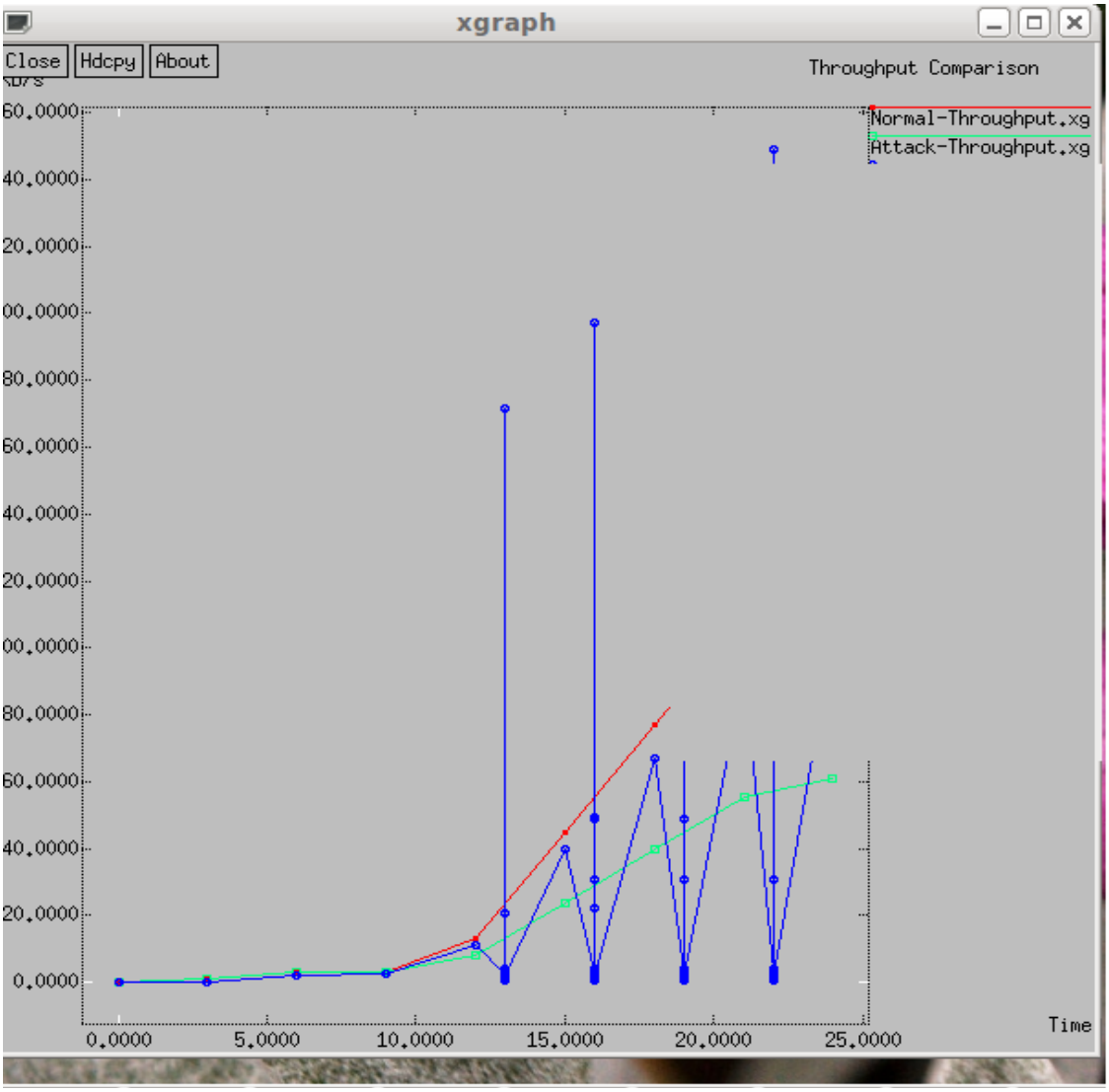

figure 7.5 Time vs No of packets

The above figure 8.5 is the plot for No. of nodes vs time the red line indicates the throughput without attack and the green line indicates the throughput with attack and the blue line indicates the throughput of proposed work. From the graph it is seen that the throughput of proposed work is high when compared.

7.1.3 Packet delivery

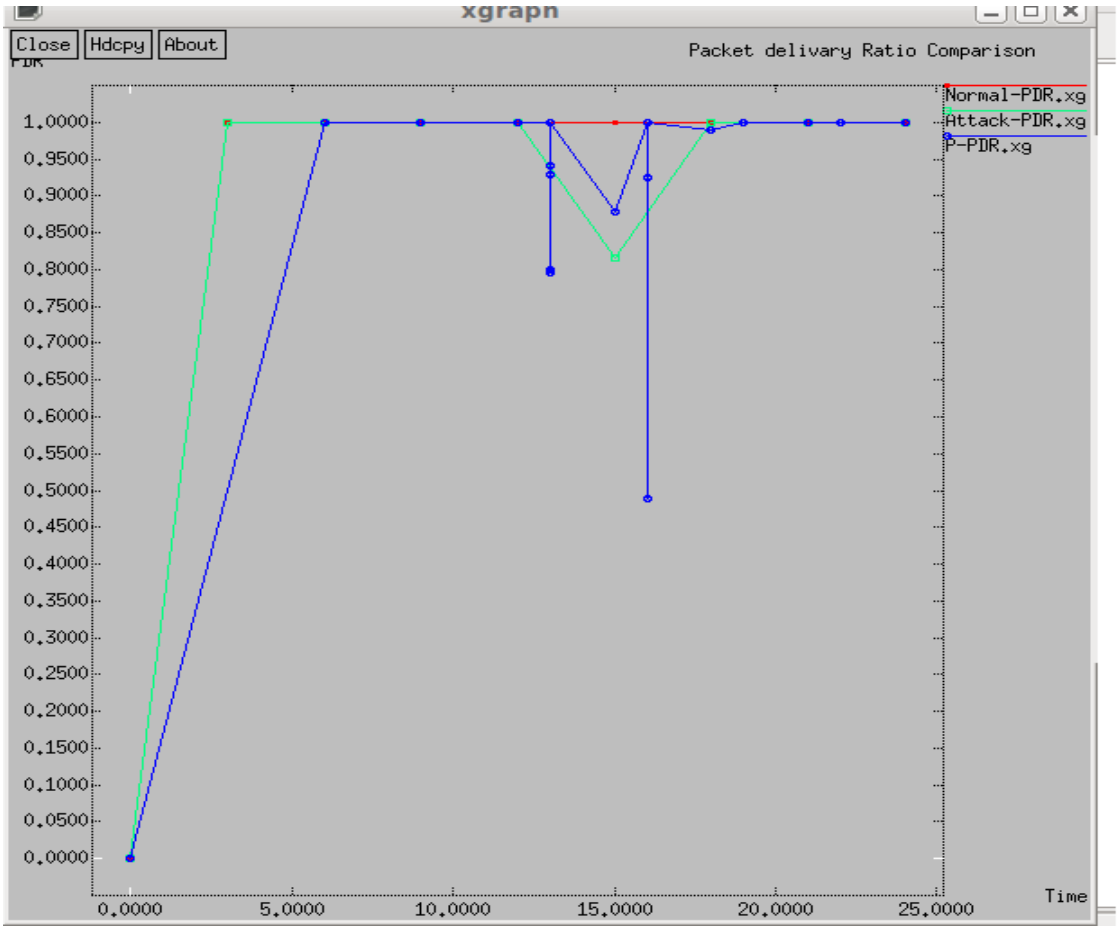

Figure 7.6 Time Vs Delay

The above figure 8.6 is the plot for time vs delay. The red line indicates the packet delivery without attackers and the green line indicates the packet delivery with attackers and the blue line indicates the packet delivery of proposed work. from the graph it is seen that the packet delivery of proposed work is high when compared.

7.1.4Energy efficiency ratio

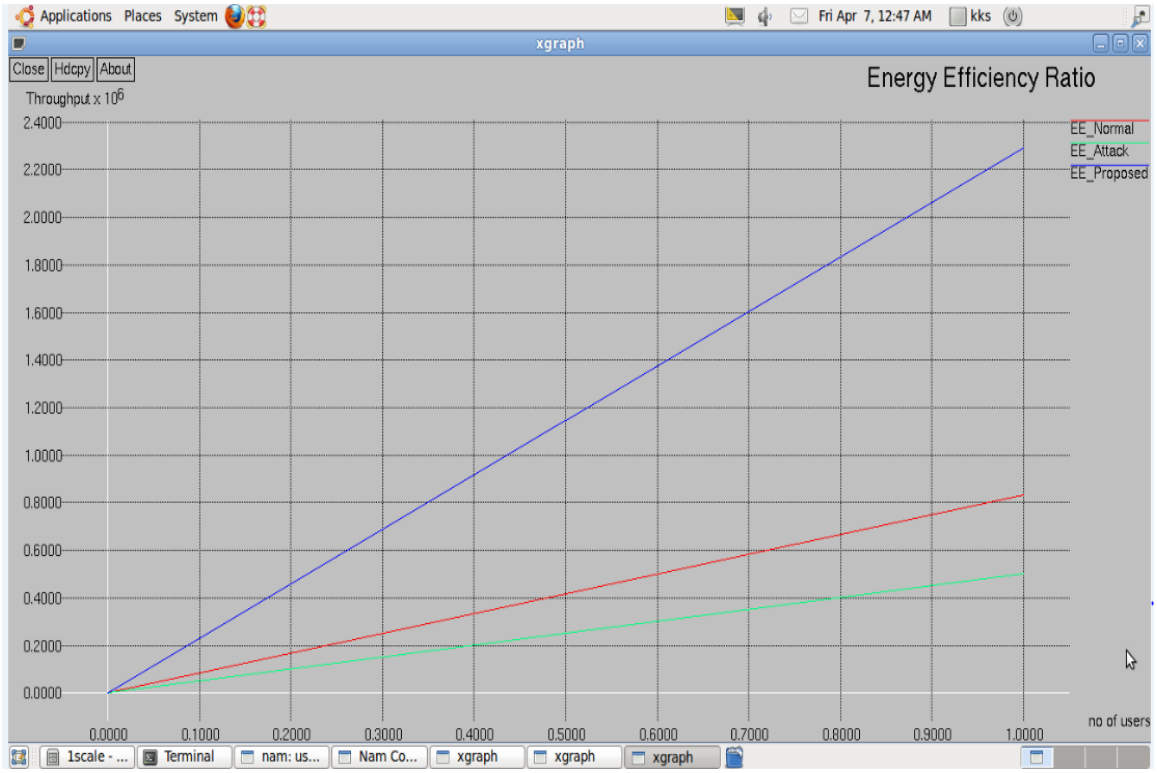

Figure 7.7 No.of users Vs Throughput

The above figure 7.7 is the plot for No.of users vs throughput. The red line indicates the efficiency of energy without attackers and the green line indicates the efficiency of energy with attackers and the blue line indicates the energy efficiency of proposed work. From the graph it is seen that energy efficiency of proposed work is very high in scale free .

7.1.5 Life time ratio

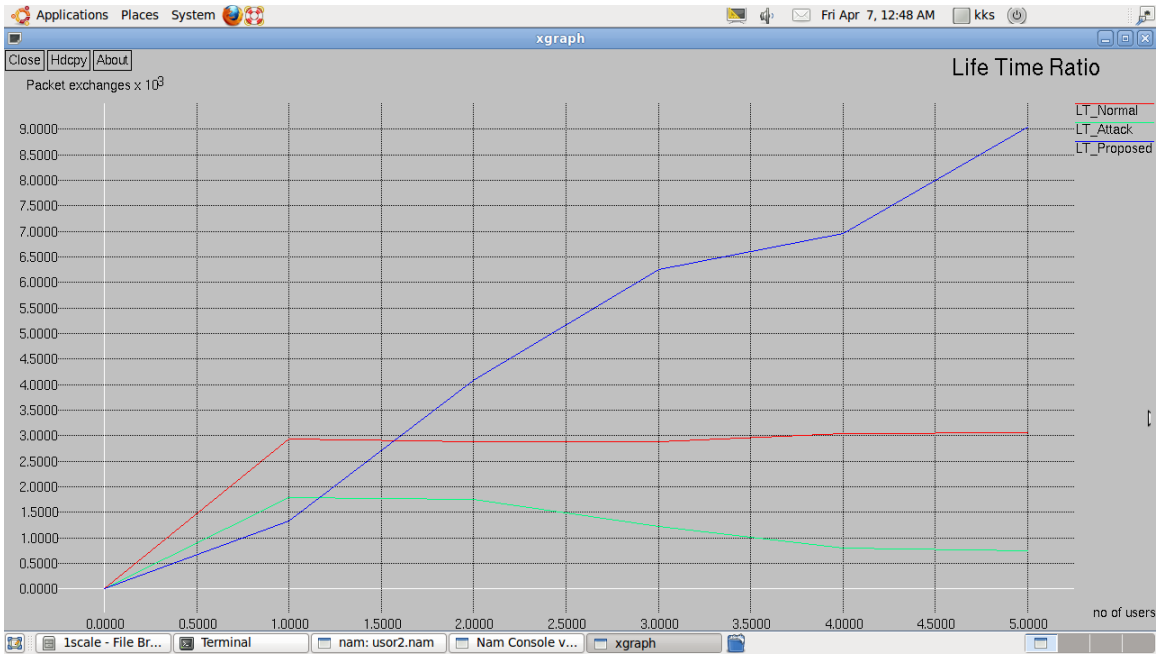

Figure 7.8 No. of users Vs Packet exchanges

The above figure 7.8 is the plot for No.of users vs packet exchanges. The red line indicates the network life time without attackers and the green line indicates the life time with attackers and the blue line indicates life time of proposed work. From the graph it is seen that the life time of proposed work is very high in scale free

7.2 SIMULATION RESULT OF RECTANGULAR

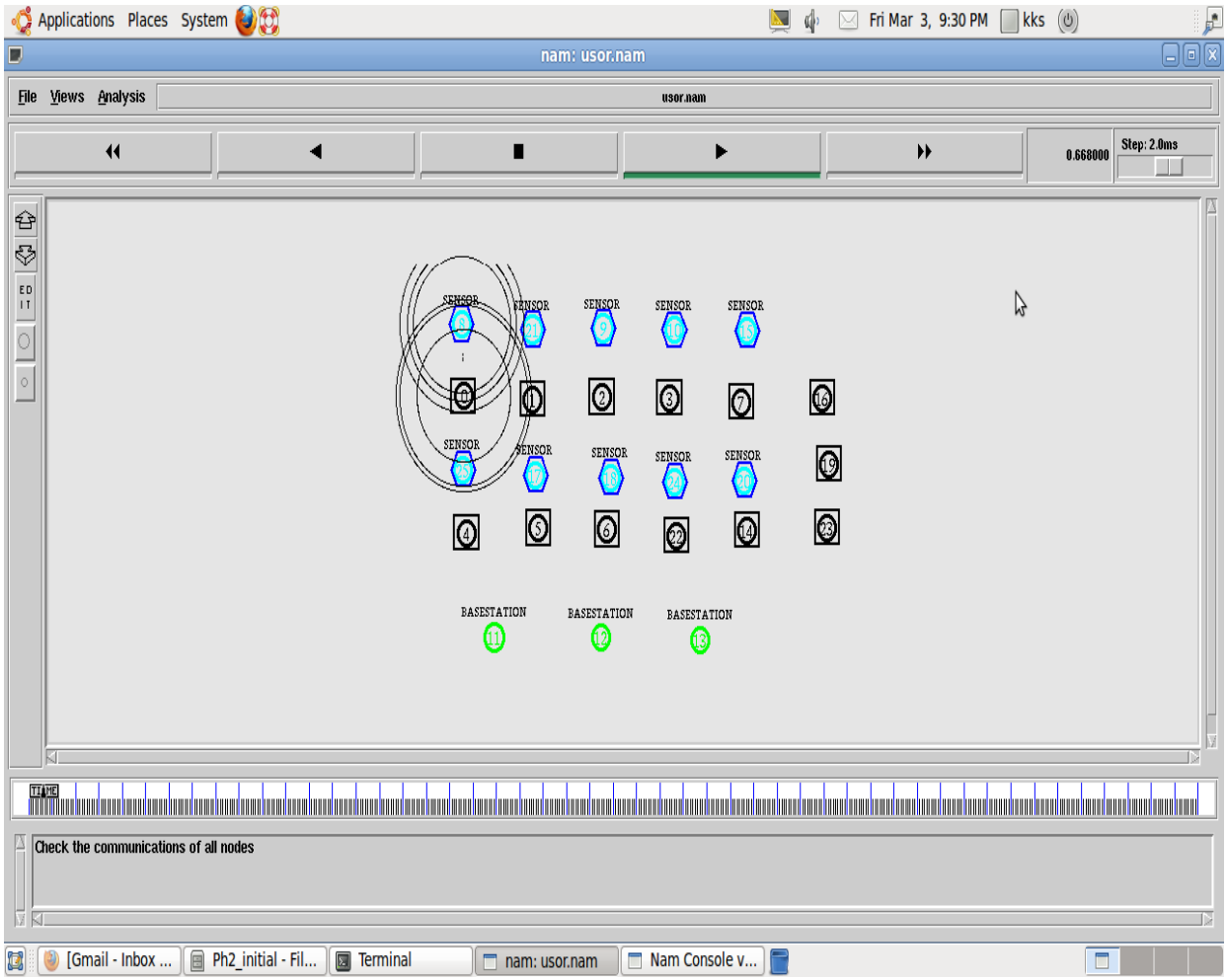

Figure7.9 Analyzing the communication between nodes

In the above Figure7.7 three colors are represented in which green indicates the base station black indicates the nodes placed on the edges and blue indicates the sensor nodes, black circle indicates the communication between nodes to analyze the best and shortest path to reach the destination.

7.2.1 LIFE TIME RATIO:

Figure7.10 No.of.users Vs Time

The above figure 7.8 is the plot for no of users Vs time . In which the life time of proposedwork is high when compared with green and red line which represents the life time without attack and with attack

7.2.2 Packet Delivery Ratio:

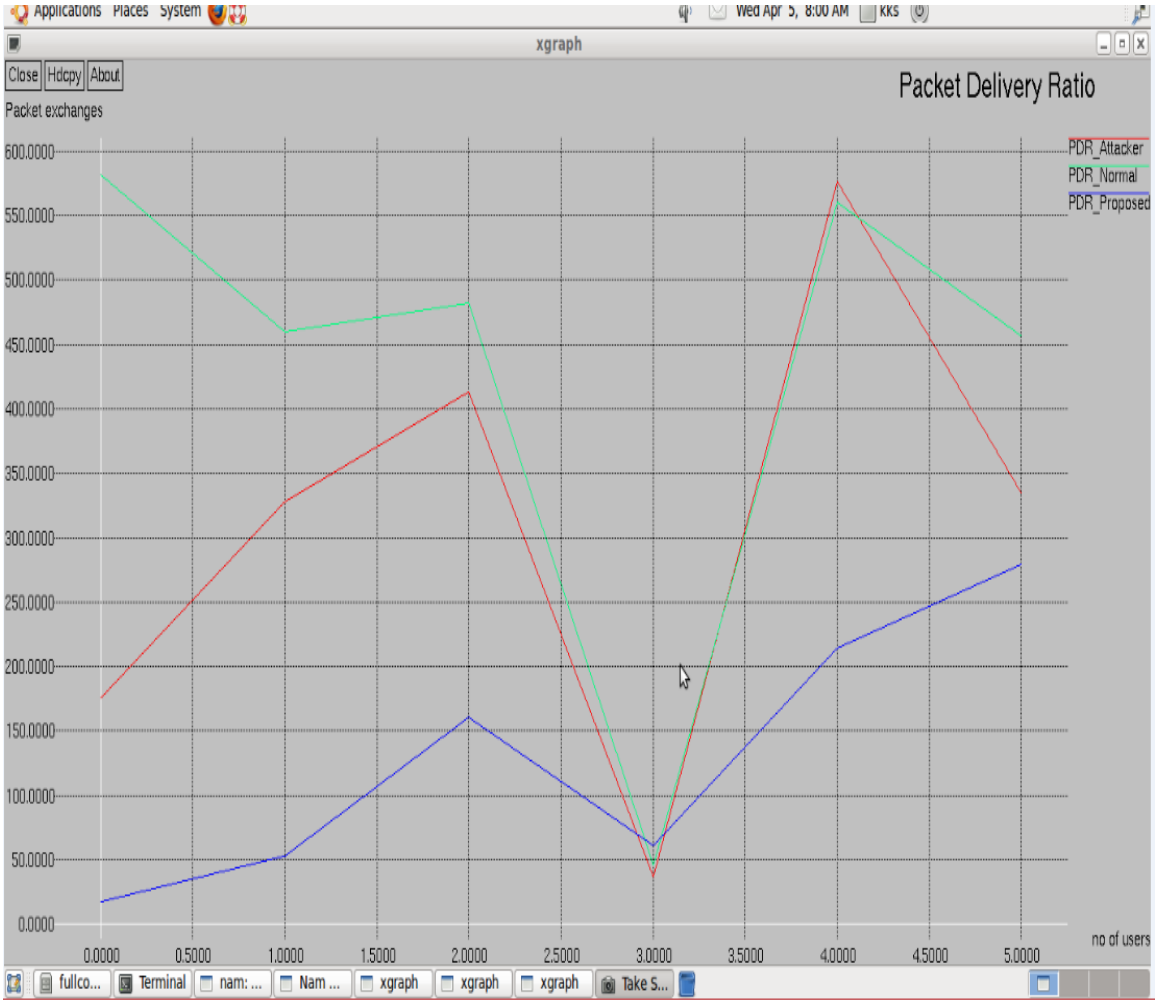

Figure 7.11 No. of users Vs packet exchanges

The above figure is the plot for no of users Vs packet exchanges in which the packet passages are less in the proposed work as represented in blue color and packet delivery are more or less same when it is without and with attack which are highlighted in red and green color

7.2.3 Energy Efficiency:

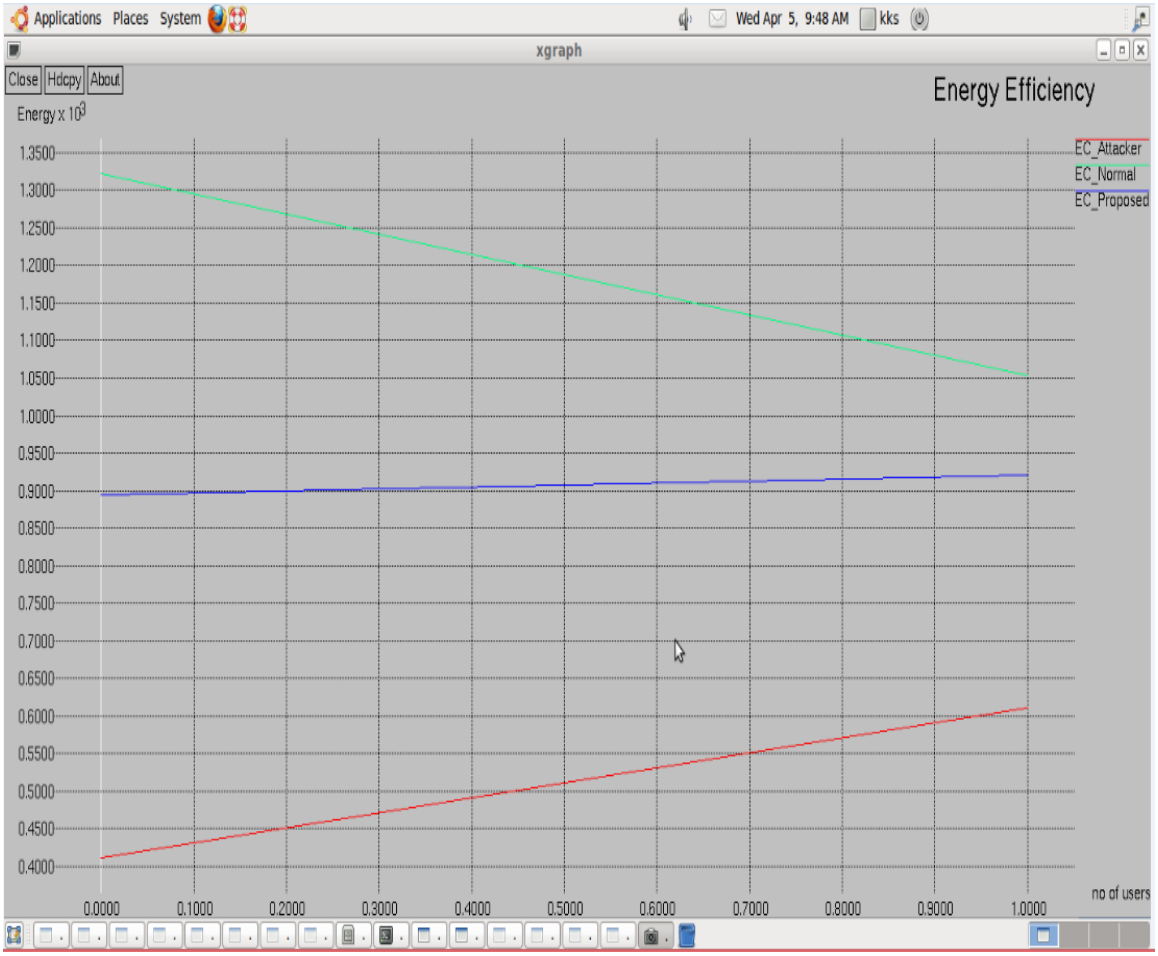

Figure 7.12 No.of.users Vs energy

The above figure 7.10 is the plot for no of users Vs energy in which the blue color indicates the proposed work in which the energy is less compared to green color in which it represent the existing work without attack and red indicates the efficiency of energy with attack

7.2.4 Throughput:

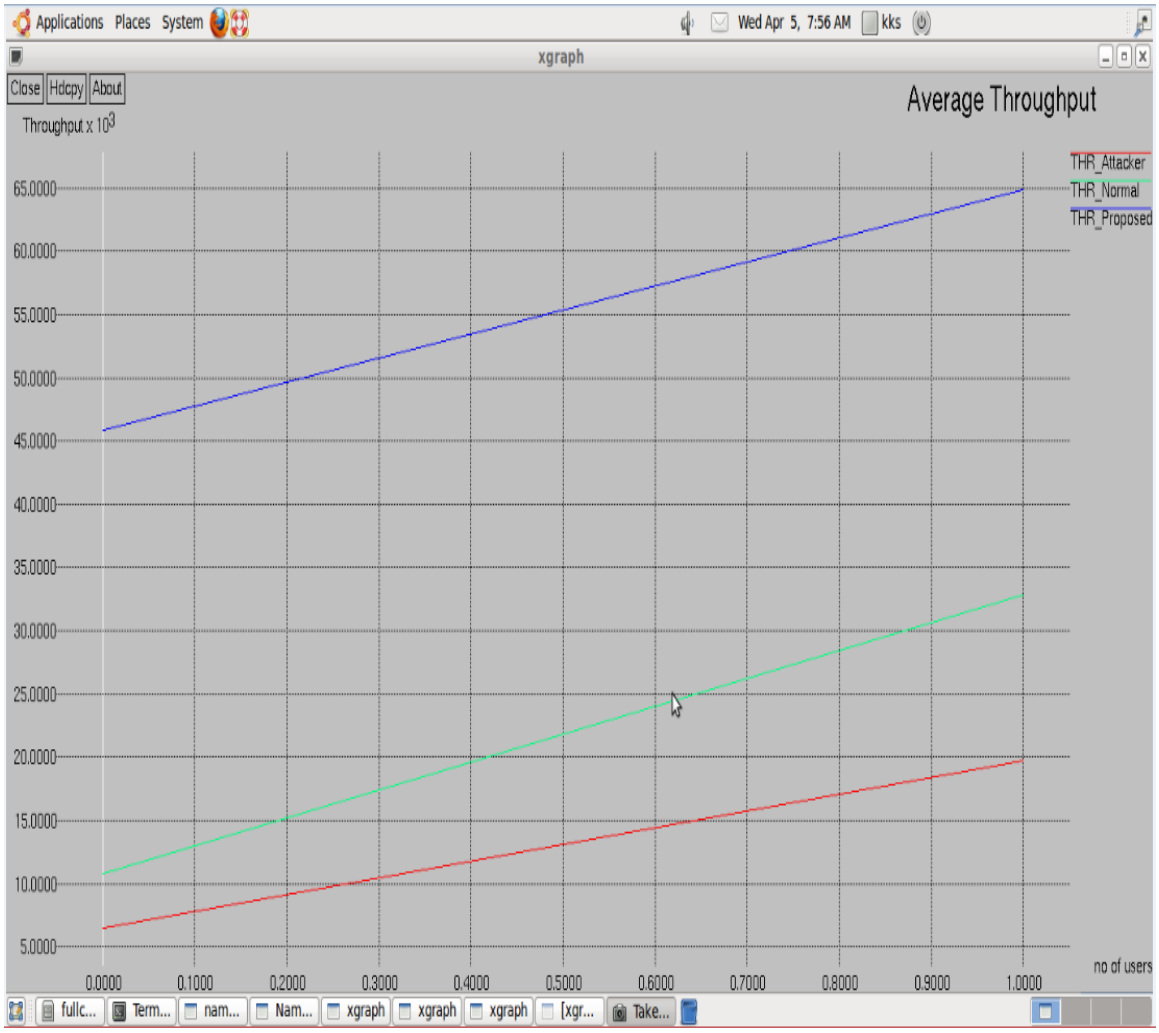

Figure 7.13 No.of.users Vs Throughput

The above figure 7.11 is the plot for no of users Vs throughput. the blue line indicates the proposed work which is higher when compared with the green line in which indicates the throughput without attack and red line indicates the throughput with attack.

7.2.5 End to End Delay:

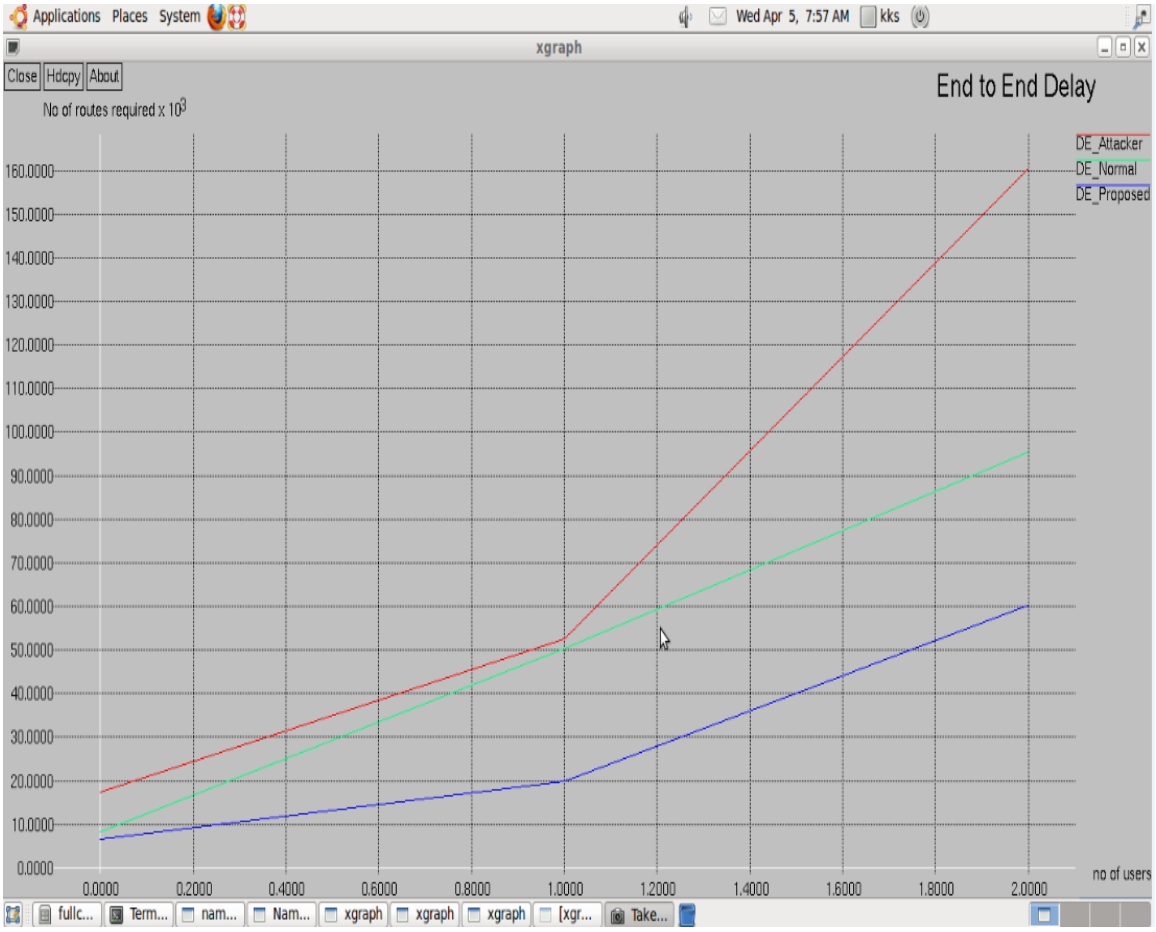

Figure 7.14 No.of.users Vs No.of.Routers

The above figure 7.12 is the plot of No.of Users Vs No.of.Routers required .The blue line indicates the proposed work in which the delay has been reduced when compared with the red line with attacker and green line without attacker.

TABLE 7.3 PARAMETERS COMPARISON TABLE WITH EXISTING TECHNIQUES

Parameters	CHMM	EAEM	MODIFIED EAEM	PROPOSED BA-E
LIFE TIME	6,445s	7,250s	7,450s	8,150s
TRANSMISSION SPEED	Light High	Light High	High	Very High
THROUGHPUT	250pkt	295pkt	300pkt	340pkt
DELAY	0.047s	0.045s	0.044s	0.042s
PDR	65	70	78	96

Table 7.4 COMPARSION OF SCALE FREE AND RECTANGULAR

PARAMETERS	RECTANGULAR	SCALE FREE
Life Time	6,125s	8,150s
Energy Consumption	Low	Very Low
Throughput	325 packets	340 packets
End-to-End Delay	0.046s	0.042s
Packet Delivery Ratio (25 sec)	80	96

CHAPTER 8

CONCLUSION

One of the most important issues in wireless sensor network is optimum consumption of energy. If it is considered properly network lifetime would be increased. In this paper two different network topologies with man in middle attack has been examined. From the simulation results, we observe the better performance based on the metrics like throughput, packet delivery ratio ,network life time ,energy efficiency, end to end delay in scale free topology and in rectangular topology .Based on the comparison of metrics it is analyzed that the packet delivery ratio and energy efficiency which are the important parameters in WSNs which are less in rectangular topology compared to the scale free topology which it provides promising results when compared to rectangular topology in presence of Man In The Middle Attack.

REFERENCES

[1] Younis M, Senturk I, Akkaya K, Lee S, Senel F. Topology management techniques for tolerating node failures in wireless sensor networks: a survey. Comput Netw 2014;58:254–83.

[2] Albert R, Jeong H, Barabasi AL. Error and attack tolerance of complex network. Nature 2000;406:378–82.

[3] Yang LX, Yang XF. The spread of computer viruses over a reduced scale-free network. Physica A 2014;396:173–84.

[4] Momhammad ASM, Mahdi J, Zohreh A. Topology and vulnerability of the Iranian power grid. Physica A 2014;406:24–33.

[5] Peng GS, Wu J. Optimal network topology for structural robustness based on natural connectivity. Physica A 2016;443:212–20.

[6] Bari A, Jaekel A, Jiang J, Xu YF. Design of fault tolerant wireless sensor networks satisfying survivability and lifetime requirements. Comput Commun 2012;35:320–33.

[7] Barabasi AL, Ravasz E, Vicsek T. Deterministic scale-free networks. Physica A 2001;3-4:559–64.

[8] Zhu HL, Luo H, Peng HP, Li LX, Luo Q. Complex networks-based energy-efficient evolution model for wireless sensor networks. Chaos Solitons Fractals 2009;41:1828–35.

[9] Qi XG, Ma SQ, Zheng GZ. Topology evolution of wireless sensor networks based on adaptive free-scale networks. J Iran Chem Soc 2011;8:467–75.

[10] Chen LJ, Liu M, Chen DX, Xie L. Topology evolution of wireless sensor networks among cluster heads by random walkers. Chin J Comput 2009;32:69– 76.

[11] Saffre F, Jovanovic H, Hoile C, Nicolas S. Scale-free topology for pervasive networks. BT Technol J 2004;22:200–8.

[12] Liu LF, Qi XG, Xue JL, Xie M. A topology construct and control model with small-world and scale-free concepts for heterogeneous sensor networks. Int J Distrib Sens Netw 2014;1:1–8.

[13] Holme P, kim BJ. Growing scale-free networks with tunable clustering. Phys Rev E 2002;65:026107.

[14] Zheng GZ, Liu SY, Qi XG. Scale-free topology evolution for wireless sensor networks with reconstruction mechanism. Comput Electr Eng 2012;38:643–51.

[15] Yin RR, Liu B, Liu HR, Li YQ. The critical load of scale-free fault-tolerant topology in wireless sensor networks for cascading failures. Physica A 2014;409:8–16.
[16] Y.Wu,X.L.Li,Y.Liu,W.Lou,Energy-efficient wake-upschedulingfordata collection andaggregation,IEEETransac.ParallelDistrib.Syst.21(2010) 275–287

[17] J.A.Fuemmeler, G.K.Atia, V.V.Veeravalli, Sleep control for tracking in sensor networks, IEEE Trans Signal Process. 59(2011)4354–4366.

[18]O.P.Kreidl, A.S.Willsky, An efficient message-passing algorithm for optimizing decentralized detection networks, IEEE Trans. Autom. Control 55(2010) 563–578

[19] S.M. George, Z.Wei, H.Chenji, W.Myounggyu, O.L.Yong., A.Pazarloglou, R. Stoleru, P.Barooah, Distress Net: a wireless adhoc and sensor network architecture for situation management in disaster response, IEEE Commun. Mag. 48 (2010)128–136

[20] N.Xiaoguang, H.Xi, Z.Ze, Z.Yuhe, H.Changcheng, C.Li, TheDesign and Evaluation of a Wireless Sensor Network for Mine Safety Monitoring, in: Proceedings of the IEEE Global Telecommunications Conference, GLOBECOM 07, 2007, pp.1291–1295