Performance Analysis of ZigBee Protocol in Smart Dust Communication Network

Thesis submitted in partial fulfillment of the requirements
for the award of degree of

Master of Engineering
in
Computer Science and Engineering

Submitted By
Sandeep Kumar
(Roll No. 801032021)

Under the supervision of:
Dr. V. P. Singh
Assistant Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA – 147004

June 2012

Certificate

I hereby certify that the work which is being presented in the thesis entitled, "**Performance Analysis of ZigBee Protocol in Smart Dust Communication Network**", in partial fulfillment of the requirements for the award of degree of Master of Engineering in Computer Science and Engineering submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Dr. V. P. Singh and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

(Sandeep Kumar)

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

(Dr. V. P. Singh)

Assistant Professor,

Computer Science and Engineering Department

Countersigned by

03/Jul/2011

(Dr. Maninder Singh)
Head
Computer Science and Engineering Department
Thapar University
Patiala

(Dr. S. K. Mohapatra)
Dean (Academic Affairs)
Thapar University
Patiala

Acknowledgement

First of all, I am thankful to God for his blessings and showing me the right direction. With His mercy, it has been made possible for me to reach so far.

It gives me great pleasure to express my gratitude towards the guidance and help I have received from **Dr. V. P. Singh**. I am thankful for his continual support, encouragement, and invaluable suggestion. He, not only provided me help whenever needed, but also the resources required to complete this thesis report on time.

I am also thankful to **Dr. Maninder Singh**, Head, Computer Science and Engineering Department and **Mr. Karun Verma** PG coordinator for their kind help and cooperation. I express my gratitude to all the staff members of Computer Science and Engineering Department for providing me all the facilities required for the completion of my thesis work.

I would like to say thanks to all my friends especially Parth, Jaspreet and Maninder for their support. I want to express my appreciation to every person who contributed with either inspirational or actual work to this thesis.

Last but not the least I am highly grateful to all my family members for their inspiration and ever encouraging moral support, which enables me to purse my studies.

Sandeep Kumar

Abstract

Smart Dust is comprised of a vast number of ultra-small fully autonomous computing, communication and sensing devices. It has very restricted energy and computing capabilities that co-operate to accomplish a large sensing task. Smart Dust sensing devices are capable of gathering many types of information from the environment including temperature, light, humidity and vibrations. Such devices exchange information with either to other nodes or to the outside world without being physically connected to another device**.** These sensor networks are very different from traditional networks since sensor nodes (SNs) are very small devices with many electronic components such as memory, CPU, radio and sensor and each of these components consumes power. SNs have a battery and can work only as long as the battery lasts. In other words, it is very important to optimize every computation in order to increase the sensor's lifetime.

The present research work is the performance analysis of Smart Dust Network in terms of number of nodes, number of nodes/cluster and distance from the PAN coordinator. The work is implemented using energy-efficient ZigBee Protocol and simulated using NS2 Simulator.

This thesis comprises of 5 Chapters, Chapter 1 describes Smart Dust Network, its applications, Network topologies and ZigBee protocol. Chapter 2 describes Literature Survey. Chapter 3 specifies the problem statement, objective defined for this thesis and methodology to achieve these objectives. Chapter 4 describes Simulation Environment and Results of analysis. Chapter 5 concludes the overall thesis with overall observations and future work is highlighted.

Keywords: Smart Dust, ZigBee Protocol, Random topology, Clustered topology, Ring topology.

Table of Contents

Certificate	ii
Acknowledgement	iii
Abstract	iv
Table of Contents	v
List of Figures	viii
List of Tables	x
Chapter 1 Introduction	**1**
1.1 Smart Dust Networks	1
1.2 Smart Dust Node Components	2
1.2.1 Sensing	2
1.2.2 Processing	2
1.2.3 Communication	3
1.2.4 Power	3
1.3 Smart Dust applications	3
1.3.1 Defense-related Applications	4
1.3.2 Environmental applications	4
1.3.3 Home applications	4
1.4 Network Design Parameters	5
1.4.1 Small node size	5
1.4.2 Low node cost	5
1.4.3 Low power consumption	5
1.4.4 Scalability	5
1.4.5 Reliability	5
1.4.6 Self-configurability	6
1.4.7 Adaptability	6
1.4.8 Channel utilization	6
1.4.9 Fault tolerance	6
1.4.10 Security	6
1.5 Factors Influencing Smart Dust Network Design	6
1.5.1 Fault Tolerance	6

1.5.2 Scalability 7
1.5.3 Hardware Constraints 7
1.5.4 Transmission media 7
1.5.5 Power Consumption 7
1.6 Routing Protocols in Smart Dust Network 7
1.6.1 The Sleep-Awake Protocol (SWP) 7
1.6.2 The Density Adaptive Sleep-Awake Protocol (DA-SWP) 8
1.6.3 The Energy Adaptive Sleep-Awake Protocol (EA-SWP) 8
1.6.4 The Sleep-Awake Probabilistic Forwarding Protocol (SW-PFR) 9
1.6.5 Hierarchical Threshold-sensitive Energy Efficient Network Protocol 11
1.6.6 Variable Transmission Range Protocol (VTRP) 12
1.6.7 The Local Target Protocol (LTP) 12
1.6.8 Secure Network Encryption Protocol (SNEP) 12
1.7 Network Design Challenges and Routing Issues 13
1.7.1 Limited energy capacity 14
1.7.2 Sensor locations 14
1.7.3 Limited hardware resources 14
1.7.4 Massive and random node deployment 14
1.7.5 Network characteristics and unreliable environment 14
1.7.6 Data Aggregation 15
1.7.7 Diverse sensing application requirements 15
1.8 ZigBee Protocol 15
1.8.1 ZigBee Architecture 16
1.8.2 ZigBee Features 18
1.9 Network Topologies 18
1.9.1 Ring 18
1.9.2 Bus 19
1.9.3 Star 20
1.9.4 Tree 21
1.9.5 Mesh 21
1.10 Network Simulator – NS-2 21

Chapter 2 Literature Survey **23**
Chapter 3 Problem Statement & Objectives **27**
3.1 Problem Definition 27
3.2 Objectives 27
3.3 Methodology used to achieve Objectives 28
Chapter 4 Simulation Environment and Results **30**
4.1 Simulation Environment I 30
4.1.1 Scenario 1 (Random Topology) 30
4.1.2 Scenario 2 (Random Topology) 31
4.1.3 Scenario 3(Random Topology) 33
4.1.4 Scenario 4 (Random Topology) 34
4.1.5 Performance Analysis of Random topology 35
4.2 Simulation Environment II 39
4.2.1 Scenario 1(Ring Topology) 39
4.2.2 Scenario 2(Ring Topology) 41
4.2.3 Performance Analysis of Ring Topology 42
4.3 Simulation Environment III 45
4.3.1 Scenario 1 (Clustered Topology) 45
4.3.2 Scenario 2 (Clustered Topology) 46
4.3.3 Performance Analysis of Clustered Topology 47
Chapter 5 Conclusion and Future Scope **51**
References **52**
List of Publications **55**

List of Figures

Figure 1.1 Particles communication from event E to sink S.……10

Figure 1.2 Angle Φ and closeness to optimal line ……10

Figure 1.3 Communication between sensor nodes in HTEEN……...……11

Figure 1.4 ZigBee Architecture……..17

Figure 1.5 Ring network layout……..19

Figure 1.6 Bus network layout……19

Figure 1.7 Star network layout……20

Figure 1.8 Tree Network layout……..21

Figure 4.1 Network of 10 nodes (Random Topology)…….……..31

Figure 4.2 Communication between Nodes (Random Topology/10 Nodes)…….…….31

Figure 4.3 Network of 25 Nodes (Random Topology)…….……..32

Figure 4.4 Communication between Nodes (Random Topology/25 Nodes)…….…….32

Figure 4.5 Network of 50 Nodes (Random Topology)…….……..33

Figure 4.6 Communication between Nodes (Random Topology/50 Nodes)…….……34

Figure 4.7 Network of 75 Nodes (Random Topology)……...……34

Figure 4.8 Communication between Nodes (Random Topology/75 Nodes)…….……35

Figure 4.9 Number of packets Transmitted (Random Topology)……...36

Figure 4.10 Number of packets loss (Random Topology)…….……...36

Figure 4.11 Bit Rate (Random Topology)……37

Figure 4.12 Packet Loss Rate (Random Topology)…….……38

Figure 4.13 Network of 7 Nodes (Ring Topology)…….…….……40

Figure 4.14 Communication between Nodes (Ring Topology/7 Nodes).……....40

Figure 4.15 Network of 13 nodes (Ring Topology)……..……41

Figure 4.16 Communication between Nodes (Ring Topology/13 Nodes).……...41

Figure 4.17 Number of Packets Transmitted (Ring Topology)……....42

Figure 4.18 Number of Packets Lost (Ring Topology)……43

Figure 4.19 Bit Rate (Ring Topology)……..43

Figure 4.20 Packet loss rate (Ring Topology)……..44

Figure 4.21 Network of 30 Nodes (Clustered Topology)…….……46
Figure 4.22 Network of 50 Nodes (Clustered Topology)……..……...46
Figure 4.23 Communication between Nodes (Clustered Topology/50 Nodes)…...…47
Figure 4.24 Number of Packets Transmitted (Clustered Topology)……...……..48
Figure 4.25 Numbers of Packets Lost (Clustered Topology).……..48
Figure 4.26 Bit rate (Clustered Topology)……49
Figure 4.27 Packet Loss Rate (Clustered Topology)……49

List of Tables

Table 4.1 Random Topology Network Configuration……...30

Table 4.2 Analysis of Smart Dust Network using Random Topology…….38

Table 4.3 Ring Topology Network Configuration……..…….39

Table 4.4 Analysis of Smart Dust Network using Ring Topology……...44

Table 4.5 Clustered Topology Network Configuration……45

Table 4.6 Analysis of Smart Dust Network using Clustered Topology……...46

Chapter 1
Introduction

1.1 Smart Dust Networks

During the last decade, communication technology and computer technology have increased significantly due to improvements in miniaturization [1]. Advances in these technologies have enabled to build small electronic components that are able to sense, process and communicate information to other nodes. Sensor Nodes (SNs) are capable of gathering many types of information from the environment including temperature, light, humidity and vibrations. Such nodes exchange information with either to other nodes or to the outside world without being physically connected to another device. Communication Network created by these small sensor nodes with each other is called Smart Dust Network or Smart Dust. Smart Dust offer economically viable monitoring solutions for a wide variety of applications and have become popular since data gathering is becoming an important component for the success of several mission critical applications. A typical of application of Smart Dust is in the battlefield where the nodes gather information in the enemy territory. Sensor Nodes (SNs) are very small in size and dropped off from an airplane. Then SNs use self-configuration and self-organization techniques to establish a Smart Dust and send the data to a base station. In other applications such as environment monitoring, Smart Dust Networks are used to detect bushfires or tsunamis. It is easy to see the potential benefits by using Smart Dust Networks.

Smart Dust Networks offers a cheap, viable and efficient option. Additionally, using a large number of small sensors instead of using one big sensor for sensing data in a certain area is more accurate since errors in the devices or communication can be detected easily. Smart Dust is a relatively new and immature technology. Building Smart Dust poses challenges of secure routing, energy efficient, sensor node authentication, data integrity, data confidentiality and access control that are faced in conventional wireless and wired networks as well. Smart Dust is very different from traditional networks since SNs are only small devices with many electronic components such as memory, CPU, radio and sensor and each of those components consumes power. SNs have a battery and can work only as long as the battery lasts. In other words, it is very important to optimize every computation in order to increase the sensor's lifetime. These constraints make it impossible to ensure efficient use of

data propagation mechanism that is used in traditional networks. Thus, designing and implementing new efficient protocols with low power and resource consumption is a significant part in Smart Dust. Features of Smart Dust that makes it different from traditional or other wireless networks are:

- Size: Number of nodes in Smart Dust is generally start from thousands and goes up to millions.
- Node failure: Nodes may be deployed in harsh environmental conditions; unexpected node failure may be common.
- Communication: Communication in sensor networks typically takes place in the form of very short packets, meaning that the relative overhead imposed at the different network layers becomes much more important.
- Shorter lifetime, less computational power, and less memory.

1.2 Smart Dust Node Components

The concept of sensor networks is based on a simple equation:

Sensing + CPU + Radio = Thousands of potential applications

Conceptually, a sensor node consists of a power unit, sensing unit, processing unit and radio unit that is able to both transmit and receive data. Sometimes the sensor node also has a mobility unit as well as a localization unit e.g. a global positioning system (GPS).

1.2.1 Sensing

The sensing unit consists of two subunits, one or a group of sensors and an analog to digital converter (ADC). The ADC converts analog signals from the sensors to digital signals, used by the processing unit. The sensors are devices that respond to changes in the surroundings. The type of sensors being used on a sensor node depends on the application. The sensors can monitor speed, temperature, pressure, movement, humidity or vibrations to name a few.

1.2.2 Processing

The processing unit, usually a low speed CPU with small storage capabilities, performs tasks like routing and processing of sensed data etc. The choice of processing unit also determines, to a great deal, both the energy consumption as well as the computational capability of a sensor node.

1.2.3 Communication

The transmission between sensor nodes is wireless and can be implemented by radio, infrared, optical media etc. Much of the current hardware for sensor nodes is based on radio link communication.

1.2.4 Power

The power unit provides power to the other units and is typically a battery. Since the battery limits the amount of energy available to the node, this affects the lifetime of the node, thus in the end it also affects the lifetime of the sensor network. In many application scenarios, replacement or recharging (by e.g. solar cells or vibrations) of power resources is costly or even impossible. The most power-consuming activity of a sensor node is typically communication. Hence, communication must be kept to an absolute minimum in order to maximize the lifetime of the sensor nodes. All activities involving communication (sending, receiving and listening for data) are power-consuming and one important way to save power is to have the communicating device turned off as much as possible[2].

1.3 Smart Dust applications

Smart Dust networks consist of many different types of sensors such as seismic, low sampling rate magnetic, thermal, visual, infrared, and acoustic and radar, which are able to monitor a wide variety of ambient conditions that include the following:

- Temperature
- Humidity
- Vehicular movement
- Lightning condition
- Pressure
- Soil makeup
- Noise levels
- The presence or absence of certain kinds of objects
- Mechanical stress levels on attached objects
- The current characteristics such as speed, direction, and size of an object.

Sensor nodes can be used for continuous sensing event detection, event ID, location sensing, and local control of actuators [2]. The concept of micro-sensing and wireless connection of these nodes promises many new application areas. These applications

are classified into defense-related, environment and home applications. It is possible to expand this classification with more categories such as space exploration, chemical processing and disaster relief.

1.3.1 Defense-related Applications

Smart Dust networks are based on the dense deployment of disposable and low-cost sensor nodes. Destruction of some nodes by hostile actions does not affect a military operation as much as the destruction of traditional sensors. Some of the military applications of sensor networks are monitoring friendly forces, equipment and ammunition; battlefield surveillance; reconnaissance of opposing forces; targeting; battle damage assessment; and nuclear, biological and chemical (NBC) attack detection and reconnaissance.

1.3.2 Environmental applications

Some environmental applications of sensor networks include tracking the movements of birds, small animals, and insects; monitoring environmental conditions that affect crops and livestock; irrigation; macro instruments for large-scale earth monitoring and planetary exploration; chemical/ biological detection; precision agriculture; biological, Earth, and environmental monitoring in marine, soil, and atmospheric contexts; forest fire detection; meteorological or geophysical research; flood detection; bio-complexity mapping of the environment; and pollution study.

1.3.3 Home applications

Home automation: As technology advances, smart sensor nodes and actuators can be buried in appliances, such as vacuum cleaners, micro-wave ovens, refrigerators, and VCRs. These sensor nodes inside the domestic devices can interact with each other and with the external network via the Internet or Satellite. They allow end users to manage home devices locally and remotely more easily.

Smart environment: The design of smart environment can have two different perspectives, i.e., human-centered and technology-centered. For human-centered, a smart environment has to adapt to the needs of the end users in terms of input/ output capabilities. For technology-centered, new hardware technologies, networking solutions, and middle ware services have to be developed. The sensor nodes can be embedded into furniture and appliances, and they can communicate with each other and the room server. The room server can also communicate with other room servers to learn about the services they offered, e.g., printing, scanning, and faxing. These

room servers and sensor nodes can be integrated with existing embedded devices to become self-organizing, self-regulated, and adaptive systems based on control theory models.

1.4 Network Design Parameters

Most sensor networks are application specific and have different application requirements [30]. Some of the following main design parameters are considered in the design of sensor networks:

1.4.1 Small node size

Sensor nodes are usually deployed in a harsh or hostile environment in large numbers, reducing node size can facilitate node deployment. It will also reduce the power consumption and cost of sensor nodes.

1.4.2 Low node cost

Sensor nodes are usually deployed in an environment in large numbers and cannot be reused; reducing cost of sensor nodes is important and results into the cost reduction of whole network.

1.4.3 Low power consumption

Sensor nodes are powered by battery and it is often very difficult or even impossible to charge or recharge their batteries, it is crucial to reduce the power consumption of sensor nodes so that the lifetime of the sensor nodes, as well as the whole network is prolonged.

1.4.4 Scalability

Number of sensor nodes in sensor networks is in the order of tens, hundreds, or thousands, network protocols designed for sensor networks should be scalable to different network sizes.

1.4.5 Reliability

Network protocols designed for sensor networks must provide error control and correction mechanisms to ensure reliable data delivery over noisy, error-prone, and time-varying wireless channels.

1.4.6 Self-configurability

In sensor networks, once deployed, sensor nodes should be able to autonomously organize themselves into a communication network and reconfigure their connectivity in the event of topology changes and node failures.

1.4.7 Adaptability

In sensor networks, a node may fail, join, or move, which would result in changes in node density and network topology. Thus, network protocols designed for sensor networks should be adaptive to such density and topology changes.

1.4.8 Channel utilization

Sensor networks have limited bandwidth resources, communication protocols designed for sensor networks should efficiently make use of the bandwidth to improve channel utilization.

1.4.9 Fault tolerance

Sensor nodes are prone to failures due to harsh deployment environments and unattended operations. Thus, sensor nodes should be fault tolerant and have the abilities of self-testing, self-calibrating, self-repairing, and self-recovering.

1.4.10 Security

A sensor network should introduce effective security mechanisms to prevent the data information in the network or a sensor node from unauthorized access or malicious attacks.

1.5 Factors Influencing Smart Dust Network Design

A sensor network design is influenced by many factors, which include fault tolerance, scalability, hardware constraints, transmission media and power consumption. These factors are important because they serve as a guideline to design a protocol or an algorithm for sensor networks.

1.5.1 Fault Tolerance

Fault tolerance is the ability to sustain sensor network functionalities without any interruption due to sensor node failures. Since sensor nodes are very small in size and power, so percentage of their failure become quite high.

1.5.2 Scalability

Generally, sensor nodes deployed in the order of hundreds or thousands. Depending on the application, the number may reach an extreme value of millions. For machine diagnosis application, the node density is around 300 sensor nodes in a 5×5 m^2 region, and the density for the vehicle tracking application is around 10 sensor nodes per region.

1.5.3 Hardware Constraints

A sensor node is made up of four basic components a sensing unit, a processing unit, a transceiver unit and a power unit. These all components are very small in size and having very limited capabilities. One of the most important components of a sensor node is the power unit. Power units are supported by a power scavenging unit such as solar cells. There are also other subunits, which are application dependent.

1.5.4 Transmission media

In a multi-hop sensor network, communicating nodes are linked by a wireless medium. These links can be formed by radio, infrared or optical media. But these sensors have very less energy and transmission range, so optical medium is preferred.

1.5.5 Power Consumption

The wireless sensor node, being a micro-electronic device, can only be equipped with a limited power source. Sensor node lifetime shows a strong dependence on battery lifetime. So network needs to be designed in such a way that it consumes very less amount of energy.

1.6 Routing Protocols in Smart Dust Network

Wireless communications and digital electronics have already led to the development of small in size, low-power, low-cost sensor devices. Such extremely small devices integrate sensing, data processing and communication capabilities. It becomes very important to develop and implement energy efficient protocols for Smart Dust. Some of the protocols are explained below:

1.6.1 The Sleep-Awake Protocol (SWP)

According to the SWP protocol, each particle goes though alternating periods of “sleeping” and “awake”. During a sleeping period, the particles cease any communication with the environment, thus the power consumption is assumed to be

minimal and practically insignificant, whereas when a particle is awake, it consumes the regular amount of energy [4].

Let T_s and T_w are the sleep and awake time periods respectively

The sleep-awake scheme is basically achieved by setting a global ratio, which defines the proportion between the durations of the sleep and awake periods.

$$Y = T_s/T_w ,$$

i.e. Y represents the energy saving specifications of the smart dust particles

Energy saving specification is : $en = T_s/(T_s + T_w) = 1 - 1/(1+Y)$

1.6.2 The Density Adaptive Sleep-Awake Protocol (DA-SWP)

Assuming that the particles are random uniformly distributed on the smart dust plane, the particle density can be calculated according to

$$\mu(R) = (n\pi R^2) /A$$

Where n is the total number of particles deployed in the area A and radius R. Basically, $\mu(R)$ gives the number of particles within the transmission radius of each particle in region A. However, since SWP forces each particle to alternate between periods of "sleeping" and "awake", $\mu(R)$ is in fact an upper bound for the number of particles that are "awake". Let $\mu_a(R)$ be the number of active particles in the area A. Then, since the length of each "sleep" and "awake" period is adjusted by the energy saving specification en, it is $\mu_a(R)/ \mu(R) \propto en$.

Clearly if the parameters that affect the performance of propagation protocols are (more or less) known in advance, the energy saving specification can be adjusted by the network operator to maximize the energy-efficiency and keep the network functional for as long as possible.

1.6.3 The Energy Adaptive Sleep-Awake Protocol (EA-SWP)

An adaptive way to adjust the sleep interval of each node by explicitly taking into account the energy available at the sensor devices is proposed in [25]. The density adaptive protocol only implicitly considers the energy by monitoring the active number of neighbors; as the network evolves, some nodes will exhaust their power and disconnect, affecting in this way the number of active neighbors. In contrast to this approach, the Energy Adaptive Sleep-Awake Protocol (EA-SWP) attempts to evenly distribute energy consumption among particles by adjusting the sleep interval of strained particles. Balancing the energy dissipation among the sensors in the

network avoids the early energy depletion of certain sensors and thus increases the lifetime of the system by preventing from early network disconnection.

Initially, all particles select a random sleep-awake schedule with the duration of T_s and T_w fixed by the network operator. Then, as the network evolves in time, each particle before switching to the sleep state computes a new value for T_s and T_w by using the average energy E_{avg} estimated by P_{energy} where P_{energy} includes in the header of the message ,an estimation of the particle's remaining energy $E(i)$

$$dSW = T_s * (E_{avg}\ (t)/E_{(i)}) - T_s$$

$$T_s = T_s - dSW$$

$$T_w = T_w + dSW$$

By using this, these particles are allowed to sleep more when their energy supplies are less than average in their neighbourhood or forces particles to awake in the opposite case

1.6.4 The Sleep-Awake Probabilistic Forwarding Protocol (SW-PFR)

The basic idea of the protocol lies in probabilistically favoring transmissions towards the sink within a thin zone of particles around the line connecting the particle sensing the event *E* and the sink *S*. Although data propagation along this line is optimal with respect to energy and time cost, such propagation is not always feasible [5]. This is true because, even if initially this direct line was appropriately occupied by sensors, certain sensors on this line might become inactive, either permanently (because their energy has been exhausted) or temporarily (because these sensors might enter a sleeping mode to save energy). The protocol evolves in two phases:

Phase 1: The Front Creation Phase. In this phase, the header of each message includes a counter called β. This counter is set to a predefined value by the source particle. Following this initialization, each particle, upon receiving a message containing a positive β counter, reduces its value by 1 and deterministically forwards the message towards the sink. In order to do so, each particle uses directed "angle" transmission to broadcast data to all of its neighbours that lie in the direction of the sink. When the β counter becomes zero, the particle proceeds to the second phase of the SW-PFR protocol. Ultimately, the beta counter determines the length of the first phase of the SW-PFR protocol.

Phase 2: The Probabilistic Forwarding Phase. In this second phase, data propagation is done in a probabilistic manner. Each particle calculates a probability of

participation in the propagation process. The closer a particle is to the optimal transmission line, connecting the source node *E* detecting an event and the sink *S* as shown in figure 1.1, the higher its probability to forward data pertinent to that particular sense event.

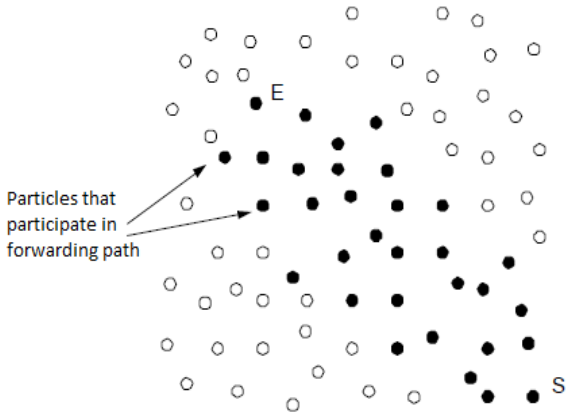


Figure 1.1: Particles communication from event *E* to sink *S*

The "forwarding probability" P_{fwd} is chosen to be $P_{fwd} = \Phi/\pi$ where Φ is the angle defined by (a)the line connecting the particle performing the random choice and the sensor that initially sensed the event and (b) the line connecting this node to the sink. Remark that indeed a bigger angle Φ suggests a sensor position closer to the direct line between *E* and *S*, figure 1.2 displays this graphically. Clearly, when $\Phi = \pi$, then the sensor lies on this line. Thus, $\Phi 1 > \Phi 2$ implies that for the corresponding particles *p1*, *p2*, *p1* is closer to the *E*-*S* line than *p2*, thus

$$P_{fwd}(p1) = \Phi 1/\pi > \Phi 2/\pi = P_{fwd}(p2)$$

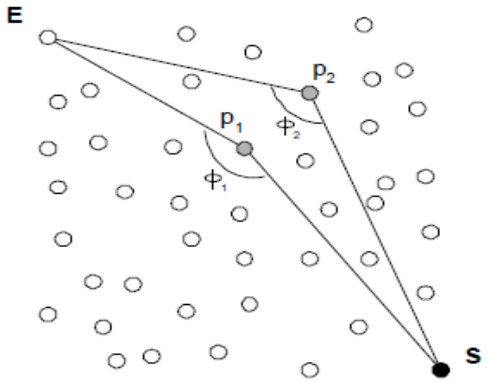


Figure 1.2: Angle Φ and closeness to optimal line

1.6.5 Hierarchical Threshold-sensitive Energy Efficient Network Protocol (HTEEN)

HTEEN is modified version of TEEN protocol. The basic concept in TEEN is the clustering of particles and the use of thresholds in order to decide whether a particle should transmit data to the sink. TEEN uses particle self-organization into clusters in order to reduce transmissions. A tree of transmissions is built, where each particle transmits data only to its parent (cluster-head) in this tree. To be more specific, TEEN's operation is divided into two phases:

Phase 1: Setup Phase. In this phase, each particle decides on whether it becomes a cluster-head or not. This decision is based on a fixed probability P_c and on whether it has been a cluster head in the last $1/P_c$ rounds. a particle n picks a random number from 0 to 1 and compares it to a threshold $T(n)$, which is calculated in every round as

$$T(n) = \quad P_c/(1 - P_c(r \bmod 1/P_c)) \qquad if\ n\ \varepsilon\ G$$

Here r is current round and G is the set of particles that have not been elected as cluster-heads in the last $1/P_c$ rounds. As threshold value increases in every round, there is surety for every particle to become a cluster head once in $1/P_c$ Steps. After a particle decides to become a cluster-head, it broadcasts the message to the entire network. In HTEEN, further these Cluster Head repeat this process and select their cluster heads[26].

Phase 2: Steady phase. After all the levels of clustering have been set up, the actual data transmission from particles begins. Cluster head collects the data from its child nodes and send to Base station as shown in Figure 1.3.

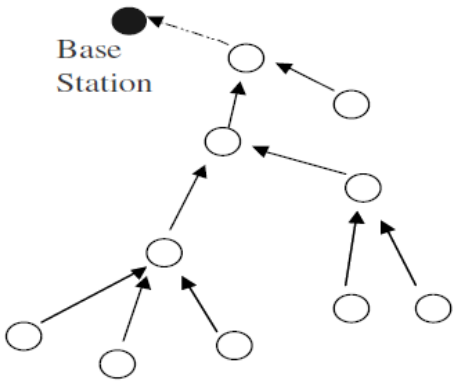


Figure 1.3: Communication between sensor nodes in HTEEN

1.6.6 Variable Transmission Range Protocol (VTRP)

The basic idea of data propagation in VTRP is the varying range of data transmissions, i.e. Allow the transmission range to increase in various ways. Thus data propagation in our protocol exhibits high fault-tolerance (by bypassing obstacles or faulty sensors) and increases network lifetime (since critical sensors, i.e. close to the control center are not overused). It is the first time varying transmission range is used.

Implementation of this protocol is divided into three phases:

Let each particle p^1 received *info(E)* from p ,

Phase 1: The Search Phase. It uses a periodic low energy broadcast of a beacon in order to discover a particle nearer to *S* than itself. Among the particles returned, p^1 selects a unique particle p^{11} that is "best" with respect to progress towards the sink.

Phase 2: The Direct Transmission Phase. Then, p^1 sends *info(E)* to p^{11} and sends a success message to p (i.e. to the particle that it originally received the information from).

Phase 3: The Transmission Range Variation Phase. If the search phase fails to discover a particle nearer to *S*, p^1 enters the transmission range variation phase. More specifically,

Each particle maintains a local counter τ, with initial value $\tau = 0$. Every time the search phase fails, this counter is increased by 1. Thus τ is an indication of the number of failures to locate an active particle. Based on τ, the particle modifies its transmission range *R*.

1.6.7 The Local Target Protocol (LTP)

LTP, is similar to VTRP except Phase 3, where backtrack mechanism is implemented, instead of modifying the particle's transmission range in the case when no particles towards the sink are found.

Phase 3 in LTP: Backtrack Phase**.** If Phase 1 fails several a certain (appropriately chosen) number of times, i.e. an awake neighbour particle p^{11} is not found in the particle's search area, then p^1 will send a failure notice and *info(E)* back to p. If p is the source of *info(E)*, then it will decide that propagation of this information towards the control centre is impossible and erases *info(E)* from its memory.

1.6.8 Secure Network Encryption Protocol (SNEP)

SNEP provides a number of unique advantages [9]. Some of which are following:

- It has low communication overhead since it only adds 8 bytes per message
- Like many cryptographic protocols it uses a counter, but we avoid transmitting the counter value by keeping state at both end points
- SNEP achieves even semantic security, a strong security property which prevents eavesdroppers from inferring the message content from the encrypted message
- This protocol also gives us data authentication, replay protection, and weak message freshness.

A simple form of confidentiality can be achieved through encryption, but pure encryption is not sufficient. Another important security property is semantic security, which ensures that an eavesdropper has no information about the plaintext, even if it sees multiple encryptions of the same plaintext. To provide semantic security, concept of randomization is used. According to which, Sender precedes the message with a random bit string before encrypting the message with a chaining encryption function. This prevents the attacker from inferring the plaintext of encrypted messages if it knows plaintext-ciphertext pairs encrypted with the same key. To achieve two-party authentication and data integrity, Message authentication code (MAC) can be used.

The combination of these mechanisms forms Sensor Network Encryption Protocol (SNEP). The encrypted data has the following format:

$E = \{D\}_{(Ken,C)}$ where D is the data, the encryption key is K_{en}, and the counter is C

The MAC is

$$M = MAC(K_{mac}, C/E)$$

The complete message that A sends to B is

$$A \rightarrow B : \{D\}_{(Ken,C)}, MAC(K_{mac}, C|\{D\}_{(Ken,C)})$$

If the MAC verifies correctly, node A knows that node B generated the response after it sent the request. The first message can also use plain SNEP if confidentiality and data authentication are needed.

1.7 Network Design Challenges and Routing Issues

The design of routing protocols for Smart Dust is challenging because of several network constraints. Smart Dust suffers from the limitations of several network resources. For example: energy, bandwidth, central processing unit, and storage. The design challenges in sensor networks involve the following main aspects:

1.7.1 Limited energy capacity

Sensor nodes are battery powered, they have limited energy capacity. Energy poses a big challenge for network designers in hostile environments, for example, a battlefield, where it is impossible to access the sensors and recharge their batteries. Furthermore, when the energy of a sensor reaches a certain threshold, the sensor will become faulty and will not be able to function properly, which will have a major impact on the network performance. Thus, routing protocols designed for sensors should be as energy efficient as possible to extend their lifetime, and hence prolong the network lifetime while guaranteeing good performance overall.

1.7.2 Sensor locations

Another challenge that faces the design of routing protocols is to manage the locations of the sensors. Most of the proposed protocols assume that the sensors either are equipped with global positioning system (GPS) receivers or use some localization technique to learn about their locations.

1.7.3 Limited hardware resources

In addition to limited energy capacity, sensor nodes have also limited processing and storage capacities, and thus can only perform limited computational functionalities. These hardware constraints present many challenges in software development and network protocol design for sensor networks, which must consider not only the energy constraint in sensor nodes, but also the processing and storage capacities of sensor nodes.

1.7.4 Massive and random node deployment

Sensor node deployment in sensor network is application dependent and can be either manual or random which finally affects the performance of the routing protocol. In most applications, sensor nodes can be scattered randomly in an intended area or dropped massively over an inaccessible or hostile region. If the resultant distribution of nodes is not uniform, optimal clustering becomes necessary to allow connectivity and enable energy efficient network operation.

1.7.5 Network characteristics and unreliable environment

A sensor network usually operates in a dynamic and unreliable environment. The topology of a network, which is defined by the sensors and the communication links between the sensors, changes frequently due to sensor addition, deletion, node failures, damages, or energy depletion. Also, the sensor nodes are linked by a wireless

medium, which is noisy, error prone, and time varying. Therefore, routing paths should consider network topology dynamics due to limited energy and sensor mobility as well as increasing the size of the network to maintain specific application requirements in terms of coverage and connectivity.

1.7.6 Data Aggregation

Sensor nodes generate significant redundant data; similar packets from multiple nodes can be aggregated so that the number of transmissions is reduced. Data aggregation technique has been used to achieve energy efficiency and data transfer optimization in a number of routing protocols.

1.7.7 Diverse sensing application requirements

Sensor networks have a wide range of diverse applications. No network protocol can meet the requirements of all applications. Therefore, routing protocols should guarantee data delivery and its accuracy so that the sink can gather the required knowledge about the physical phenomenon on time.

1.8 ZigBee Protocol

ZigBee technology is a low data rate, low power consumption, low-cost, wireless networking protocol targeted towards automation and remote control applications[28]. ZigBee provides low cost and low power connectivity for equipment that needs battery life as long as several months to several years but does not require data transfer rates as high as those enabled by Bluetooth. ZigBee is implemented in mesh networks, clustered and ring networks. ZigBee wireless devices are expected to transmit 10-75 meters, depending on the RF environment and the power output consumption required for a given application.

The network supported by the ZigBee protocol is basically a Personal Area Network (PAN) or the Home area network. It is basically the small area network represented by some campus, medical area, research center or the home area. ZigBee protocol is also used in a wireless sensor network with some constraint specification in terms of size, distance etc. Each sub network in the PAN area is identified by a PAN id. The PAN id is a 16 bit id which identifies the network. A network can have number of sub-networks that are controlled by separate coordinators. When the network coordinator chooses the PAN id it should not be used by any other sub network.

ZigBee protocol uses the network of smart sensors that area having their own processing unit, memory unit and the control unit. Because of this, these kinds of networks are very much dependent on the devices to perform the smart decision and the communication. The use of ZigBee protocol is also growing in some other areas such as body area network with wearable components.

Most of the ZigBee protocols work on static routing or the fixed network topologies to reduce the evaluation time and to provide higher degree of accuracy. To detect the data loss over the network CSMA, approach is being implemented along with ZigBee. When a packet is about to send but the CSMA/CA mechanism is stopping it for a longer period then the lower layer drops the packet and indicates channel access failure to the network layer. This test was conducted to an indication on how often this occurs and if it is dependent on the packet size [33].

1.8.1 ZigBee Architecture

ZigBee builds upon the Physical layer and Medium access control as defined in IEEE standard 802.15.4. This specification goes on to complete the standard by adding four main components: network layer, application layer, ZigBee device objects (ZDOs) and manufacturer-defined application objects which allow for customization and favor total integration. Architecture of ZigBee as shown in figure 1.4 is defined below.

- **Application (APL) Layer**

The top layer in the ZigBee protocol stack consists of the Application Framework, ZigBee Device Object (ZDO), and Application Support (APS) Sub layer.

- **Application Framework**

It provides a description of how to build a profile onto the ZigBee stack (to help ensure that profiles can be generated in a consistent manner). It also specifies a range of standard data types for profiles, descriptors to assist in service discovery, frame formats for transporting data, and a key value pair constructs to rapidly develop simple attribute-based profiles.

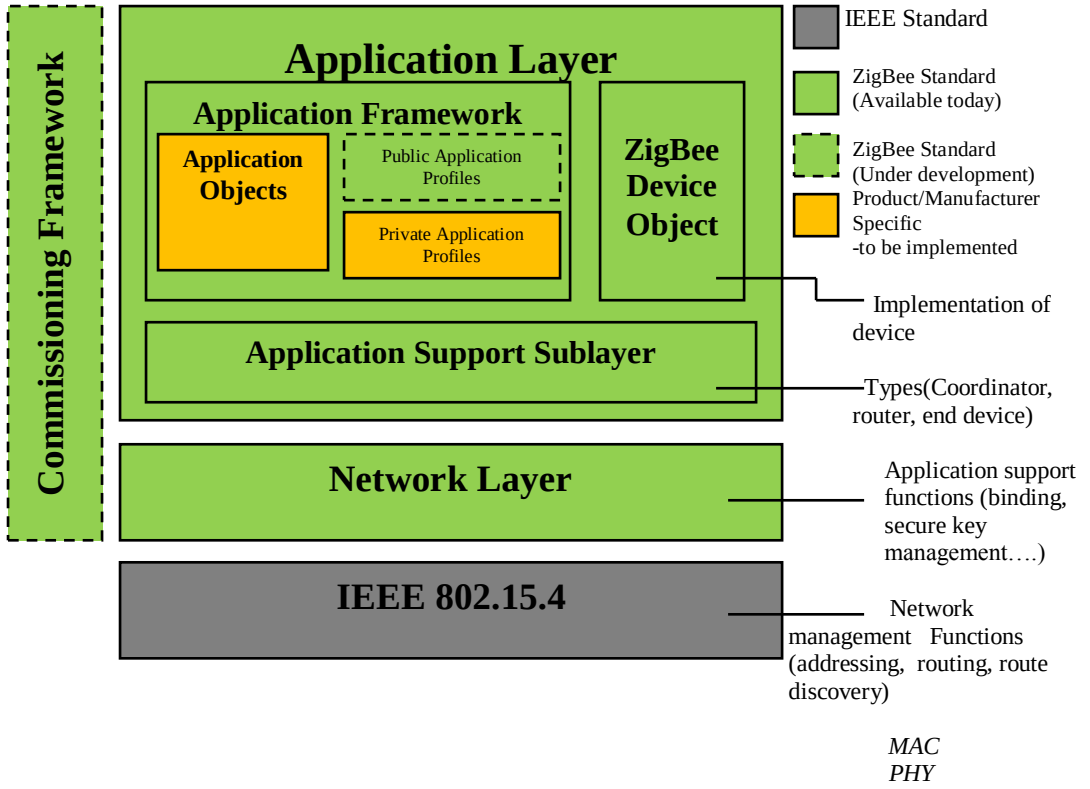


Figure 1.4: ZigBee Architecture

- **Application Objects**

Application object is software at an endpoint that controls the ZigBee device. A single ZigBee node supports up to 240 application objects. Each application object supports endpoints numbered between 1 and 240 (with endpoint 0 reserved for the ZigBee Device Object (ZDO)).

- **ZigBee Device Object (ZDO)**

Defines the role of a device within the network (coordinator, router or end device), initiates and/or responds to binding and discovery requests, and establishes a secure relationship between network devices. It also provides a rich set of management commands defined in the ZigBee Device Profile (used in ZigBee commissioning). The ZDO is always endpoint zero.

- **ZDO Management Plane**

Facilitates communication between the Application Support and Network layers with the ZDO and allows the ZDO to deal with requests from applications for network access and security using ZDP (ZigBee Device Profile) messages.

- **Application Support (APS) Sublayer**

Responsible for providing a data service to the application and ZigBee device profiles. It also provides a management service to maintain binding links and the storage of the binding table itself.

- **Security Service Provider (SSP)**

Provides security mechanisms for layers that use encryption (NWK and APS). Initialized and configured through the ZDO.

- **Network (NWK) Layer**

Handles network address and routing by invoking actions in the MAC layer. Its tasks include starting the network (coordinator), assigning network addresses, adding and removing network devices, routing messages, applying security, and implementing route discovery.

1.8.2 ZigBee Features

- Low cost
- Secure
- Reliable and self healing
- Global with use of unlicensed Radio bands
- Flexible and extendable
- Low power consumption
- Easy and inexpensive to deploy
- Integrated intelligence for network set-up and message routing

1.9 Network Topologies

A network topology is the pattern of links connecting pairs of nodes of a network. So it is a physical layout of the network's computers, terminals, and links. In both wired and wireless networks, the network layer is responsible for topology construction and maintenance. The different network topologies are as follows:

1.9.1 Ring

A ring network is a topology of computer networks where each node is connected to two other nodes, so as to create a ring as shown in figure 1.5.

Advantages:

- Easy to implement.
- Easy to install new nodes within existing network.

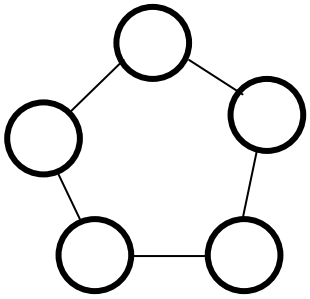


Figure 1.5: Ring network layout

Disadvantage:

- If one of the nodes in the network breaks down then the entire network will break down with it as it requires a full circle in order to function.
- Inefficient when compared to Star networks because data must travel through more points before reaching its destination.
- Communication delay is the directly proportional to number of node.

1.9.2 Bus

A bus network is a network architecture in which a set of clients are connected via a shared communications line, called a bus as shown in figure 1.6.

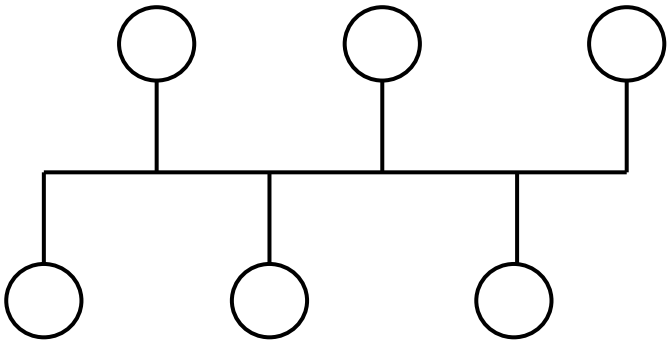


Figure 1.6: Bus network layout

Bus networks are the simplest way to connect multiple clients, but often have problems when two clients want to transmit at the same time on the same bus.

Advantages:

- Easy to implement and extend.
- Well suited for temporary networks (quick setup).
- Typically the cheapest topology to implement.

Disadvantages:

- Difficult to administer/troubleshoot.
- Limited cable length and number of stations.
- A cable break can disable the entire network.
- Maintenance costs may be higher in the long run.
- Low security.

1.9.3 Star

Star networks are one of the most common computer network topologies. In its simplest form, a star network (as shown in figure 1.7) consists of one central switch, or hub computer which acts as a router to transmit messages.

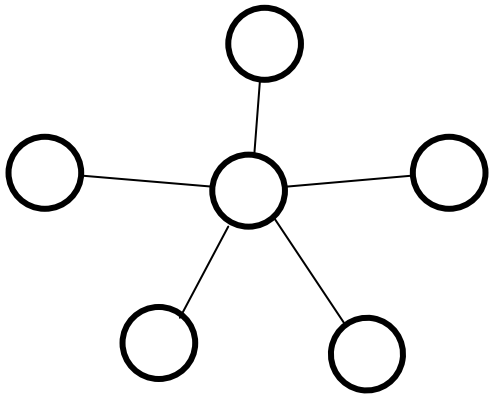


Figure 1.7: Star network layout

Advantages:

- Easy to implement and extend, even in large networks.
- Well suited for temporary networks (quick setup).
- The failure of a non-central node will not have major effects on the functionality of the network.
- No problems with collisions of Data.
- Security can be implemented in the hub/switch.

Disadvantages:

- Failure of the central node can disable the entire network.
- Limited cable length and number of stations.
- Maintenance costs may be higher in the long run.

1.9.4 Tree

It is the modification of bus topology. Coaxial cable is often used to connect computers in a bus topology. T- Connectors are used to branch off in a third direction to enable a new computer to be connected to the network as shown in figure 1.8.

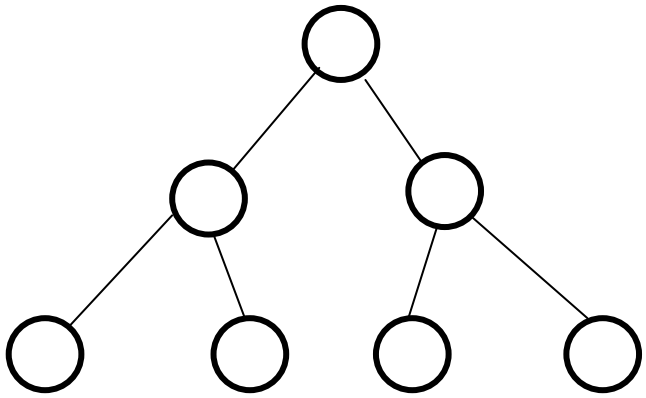


Figure 1.8: Tree Network layout

Special hardware has to be used to terminate both ends of coaxial cable such that a signal travelling to the end of the bus would come back as repeat data transmission.

1.9.5 Mesh

All computers are connected to each other so it is sometimes called completely connected networks. The number of links on networks are determined by: n(n-1)/2.

Advantages:

- Reliable: any line breakdown will affect only communication between the connected computers.
- Each node of the network need not have individual routing capacity.
- Communication is very fast between any two nodes.

1.10 Network Simulator – NS-2

Ns-2 is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. It consists of two simulation tools. The network simulator (NS) contains all commonly used IP protocols. The network animator (NAM) is use to visualize the simulations. Ns-2 fully simulates a layered network from the physical radio transmission channel to high-level applications.

Version 2 is the most recent version of NS (NS-2). The simulator was originally developed by the University of California at Berkeley and VINT project. The simulator was recently extended to provide simulation support for ad hoc network by Carnegie Mellon University (CMU Monarch Project homepage, 1999). The NS-2 simulator has several features that make it suitable for our simulations.

- A network environment for ad-hoc networks,
- Wireless channel modules (e.g.802.11),
- Routing along multiple paths,
- Mobile hosts for wireless cellular networks.

Ns-2 is an object-oriented simulator written in C++ and OTcl. The simulator supports a 28 class hierarchy in C++ and a similar class hierarchy within the OTcl interpreter. There is a one-to-one correspondence between a class in the interpreted hierarchy and one in the compile hierarchy. The reason to use two different programming languages is that OTcl is suitable for the programs and configurations that demand frequent and fast change while C++ is suitable for the programs that have high demand in speed. NS-2 is highly extensible. It not only supports most commonly used IP protocols but also allows the users to extend or implement their own protocols. It also provides powerful trace functionalities, which are very important in our project since various information need to be logged for analysis. The full source code of NS-2 can be downloaded and compiled for multiple platforms such as UNIX, Windows and Cygwin.

Chapter 2
Literature Survey

K. Selvarajah described the use of smart sensor in the field of transportation system. The main approach used by the selevarajah is the type of network. The presented work in this paper is about the use of smart sensor in a heterogeneous network. Here an intelligent transported system is defined, discussed using the smart sensors. These devices include the vehicles, road side devices, traffic lights etc. It includes the concept of Vehicle to Vehicle communication as well the communication between the vehicle and road side units and lights. The results driven from the research shows that the presented concept is very much feasible in real environment [11].

K. Selvarajah presented another application of smart dust as the middleware in mobile application. The presented result shows the favorable outcome of the smart sensor in embedded projects. The embedded project here is defined with mobility factor. It can be used in Mobile Network or in VANET as the middle ware component [12].

S.S.Riaz Ahamed described the use of ZigBee protocol in the advanced communication system. The better use of ZigBee protocol with its capabilities and the relative applications is defined. It is presented that ZigBee as the low cost technologies with low establishment cost, the communication cost and less power requirement and introduced some applications where the power requirement is minimum and that can use the ZigBee protocol effectively. The main concentration is on small area network like PAN, Home Automation. The ZigBee architecture is defined with channel specifications and the protocol strength in the paper. The complete review of paper describes the applications of ZigBee in small area networks [13].

Yao-Jung Wen presented that the use of smart sensor is growing in the commercial application very fast. But when such an intelligent system is implemented in any network there is also the requirement of control mechanism to perform the accurate decision making. Yao-Jung Wen, presented a fuzzy based decision making approach regarding the sensor validation, fusion and the Actuation. It is that the day-lighting control system that can detect the confliction of light sources and provide the maximum energy utilization. The presented work has been implemented in a real

application and shows that that about 40% of energy is being saved by the used of smart sensors. Smart sensor is used as the middle ware components [14].

Su-Chu Hsu discussed that the emerging technology of Wireless Sensor Networks (WSNs) can make a unique contribution to make in creativity on a mass scale. In this position paper, four artworks/installations are reviewed, built in Taiwan that use WSNs, show how WSNs can support new forms of creative interaction and learning on a large scale, and discuss future applications [15].

Meng-Shiuan Pan presented the use of ZigBee protocol in wireless sensor network. The presented work is about to use smart sensors and ZigBee protocol in Long Thin sensor network. The paper basically address to the topological representation of sensor network where ZigBee can be implemented. ZigBee is low power consumption protocol with limited requirements. The protocol can be implemented in wireless sensor network (WSN) in special cases. Here these cases are described in the form of topologies. Long thin WSN is also a topology type. Many supportive topologies respective to WSN in case of ZigBee protocols and routing schemes are defined to get the better utilization of ZigBee protocol. But the limitation is that the work gives the successful results only in case of some specific topology [16].

Ben W. Cook presented the smart dust as the automated network with intelligent devices where the device itself is capable in power distribution, route identification etc. The presented work is the low cost solution of the devices as the middleware devices. The work is integrated with CMOS and MEMS processing units. In this work an architecture approach to define the component network in which on chip components can be connected so that the maximum benefit can be driven from the sensors is defined. The results obtained shows that the smart sensors are very much capable with the embedded components as they provide low cost communication with low power requirements [17].

Lubomír Smutný presented that the integration of smart sensor with a local area network (LAN). The main problem with this integration is to the intercommunication between two different protocol sets. The wireless LAN works on its defined protocol and the smart sensor works on the ZigBee protocol. The benefit driven from the integration is the low power consumption over the network. The proposed system

allows communicating with ZigBee protocol in full duplex mode, so that maximum utilization of bandwidth and the power will be driven from the system. It provides the integration with personal system by using the USB devices or the ZigBee nodes. The system gives the concept of home or office automation at low cost architecture and the communication model [18].

Meng-Shiuan Pan presented the use of ZigBee protocol in a wireless sensor network with a topology specific architecture. The work here presented is based on the tree based topology. The paper considered the concept of partial aggregation to resolve the traffic over the network. The work here is about to derive the results in effective time constraint. Some algorithmic approaches to design the routing scheme specific to the tree architecture under the ZigBee capabilities are defined. The work is to minimize the communication delay and to improve the network throughput effectively [19].

Steffen Peter presented a cryptography based security mechanism. The system is implemented on smart sensor. The smart sensors are having their own processing unit, memory unit and the control system. As the cryptographic system is implemented, it gives the new authentication area that can be implemented on any home, office network to control the user access. The sensors are now capable to communicate in a encoded format where only the authenticated sensor can decode the message and process on it accordingly. The cryptographic work is implemented as integrated hardware system it means as the hardware is implemented the authentication will be activated at the same time. The system does not required any extra hardware [20].

Li-Chien Huang presented that the electrical safety is one of most concerned challenge for any protocol. ZigBee as the communication control protocol to handle the building electrical safety is used. As the ZigBee is low power requirement based protocol, it can provide the reliable communication to intimate the fire situation and the cause. The ZigBee will use the smart sensors to detect the chances of fire cause and the fire chances in the building as some chances detected the protocol will broadcast the message effectively to all the related units. In this system, smart transceivers are being implemented to get the effective results from the system [21].

Mark Hempstead proposed an extensive approach to define the sensor devices that can control and recognize the nature of load in a power system is defined in this work.

The system is not only do the work of recognition, it can also perform the load distribution in such a way so that the overall power consumption of network will be reduced [22].

Chapter 3
Problem Statement & Objectives

3.1 Problem Definition

In Smart Dust Networks, the nodes are used to sense the environment and to transmit the data. These nodes are very small in size i.e. of some cubic millimeters. These sensor networks must works for a long time. But, because of their small size it is difficult to have these nodes with larger battery size. So to increase the life time of nodes scientists are researching for different protocols. They are researching for the high productive batteries with small size to be fit in a cubic nodes, antennas of such type that are small in size but provide high range of coverage area. So, there is need to find energy efficient protocol that consumes very less amount of energy while communication with other sensor nodes and check the scalability of network i.e. to find maximum number of nodes in the network in which this protocol gives best results. The present research work is to analyze scalability of Smart Dust Network in terms of number of nodes using Random topology, number of nodes/cluster using Clustered topology and distance from PAN coordinator using Ring topology. This work is implemented using energy-efficient ZigBee Protocol and simulated using NS2 Simulator.

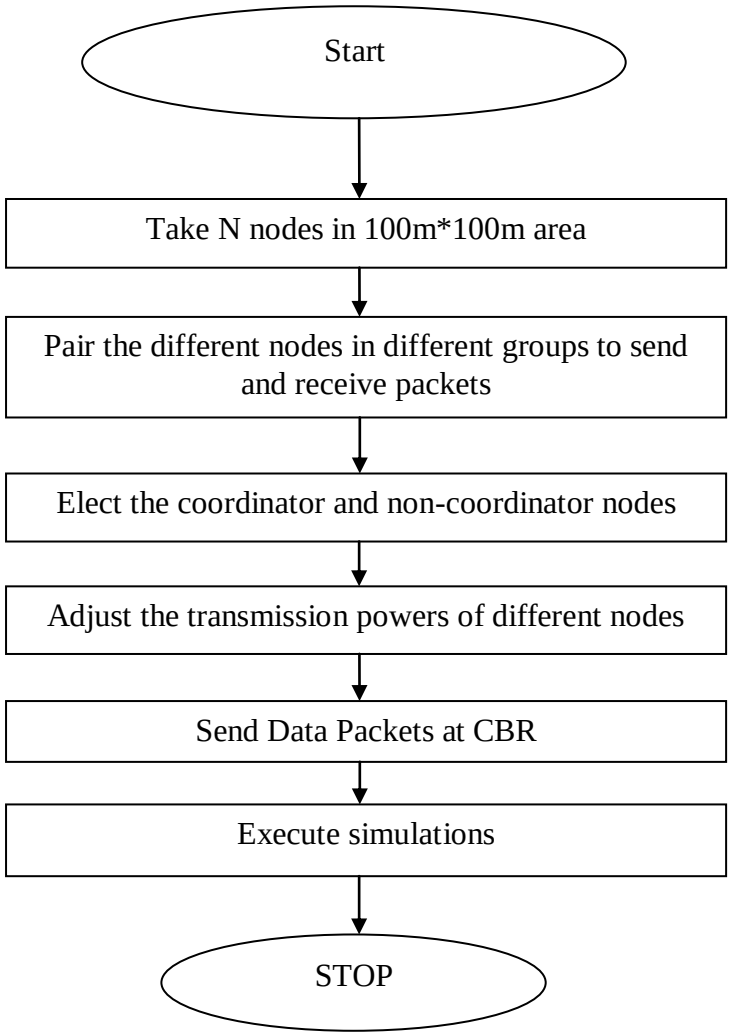
3.2 Objectives

Objectives of proposed work are to:

- Analyze the scalability of network in terms of nodes using Random topology. It shows that the network with same communication node is affected by number of nodes. It helps to take the decision regarding minimum and maximum number of node distribution in smart dust network.
- Analyze distance from PAN coordinator using Star topology. Distance from PAN coordinator affects the throughput rate over the network.
- Analyzing the scalability of network in terms of number of clusters using Clustered topology. It helps in defining number of clusters required in the network. Number of clusters in the network can also affect the efficiency of a network.

3.3 Methodology used to achieve Objectives

In all topologies, some common steps are used to perform the analysis. These steps are presented in the form of Flow chart presented here.



- Nodes are uniformly deployed in the rectangular area.
- A network over a 100m*100m area consisting of N nodes is taken
- Nodes in different groups are paired to send and receive packets.
- Elect the coordinator (active) nodes and non- coordinator nodes (in power saving mode)

- Adjust the transmission powers of different nodes accordingly
- Send the data packets at constant bit rate(CBR)
- Execute the simulations in networks with different node densities

Chapter 4
Simulation Environment and Results

4.1 Simulation Environment I

In Simulation environment I, analysis of ZigBee protocol in Smart Dust Network is done using Random Topology. Analysis is performed on scalability of network in terms of number of nodes. The system is implemented on Ubuntu Environment with NS2 simulator and XGraph is used as the tool for graph analysis. Analysis is divided into 4 scenarios as defined below. Configuration of network is shown in Table 4.1.

Table 4.1: Random Topology Network Configuration

Parameter	Value
Number of Nodes	10, 25, 50, 75
Topography Dimension	670 m x 670 m
Traffic Type	Constant Bit Rate(CBR)
Radio Propagation Model	Two-Ray Ground Model
MAC Type	802.15.4 Mac Layer
Packet Size	512 bytes
Mobility Model	Random Way Point
Antenna Type	Omni directional
Protocol	ZigBee
Topology	Random
Number of Clusters	Single

4.1.1 Scenario 1 (Random Topology)

In scenario 1, Network of 10 nodes is designed using random topology as shown in figure 4.1. Communication starts between the same colored nodes i.e. node 5 is communicating with node 6 and node 1 is communicating with node 4 as shown in figure 4.2

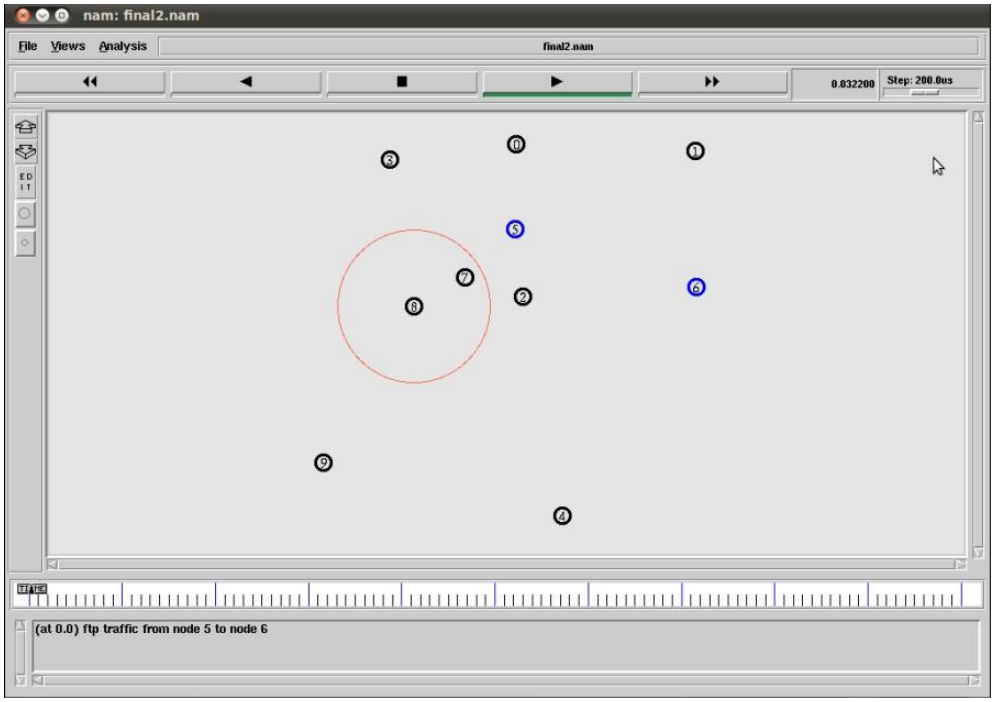


Figure 4.1: Network of 10 nodes (Random Topology)

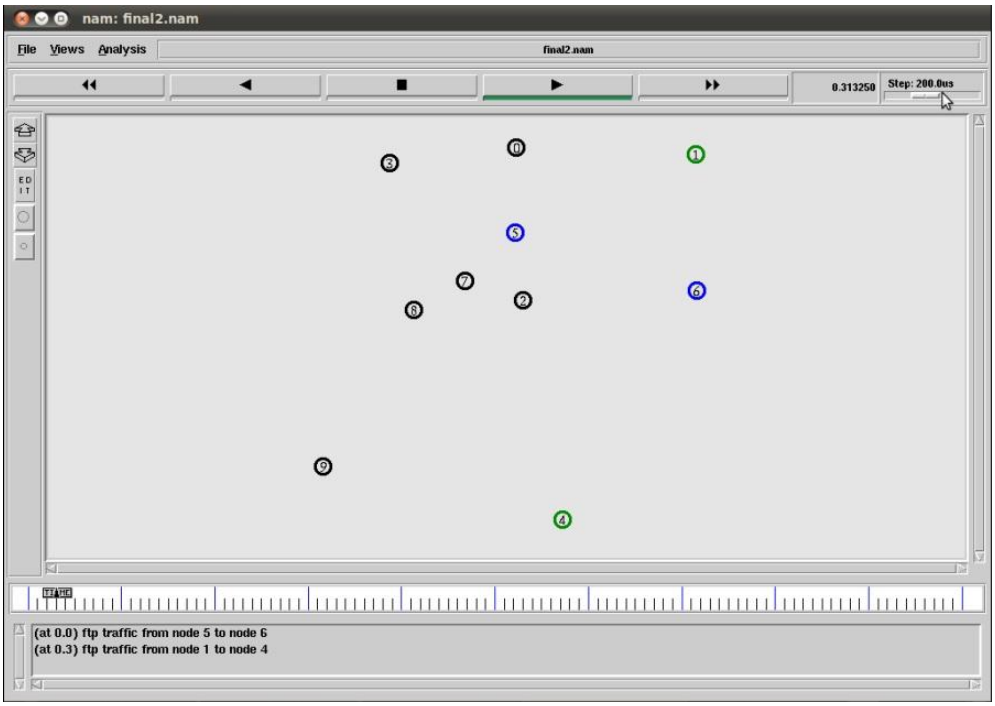


Figure 4.2: Communication between Nodes (Random Topology/10 Nodes)

4.1.2 Scenario 2 (Random Topology)

In scenario 2, Random topology is used taking 25 numbers of nodes and rest of configuration is same as in Table 4.1.

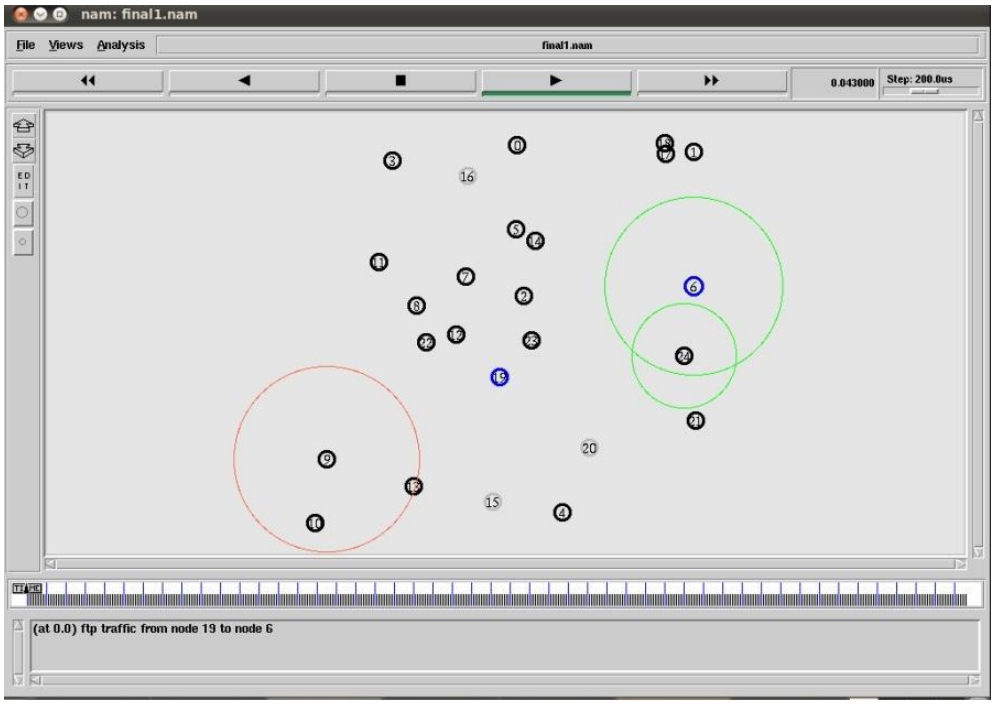


Figure 4.3: Network of 25 nodes (Random Topology)

Network of 25 nodes is shown in figure 4.1. In the network, grey colored nodes represent that they are in sleep mode. The circles represent the coverage area. In initialization, every node broadcast the message to find its neighbors. So that it becomes easy for the nodes to transmit the packet efficiently.

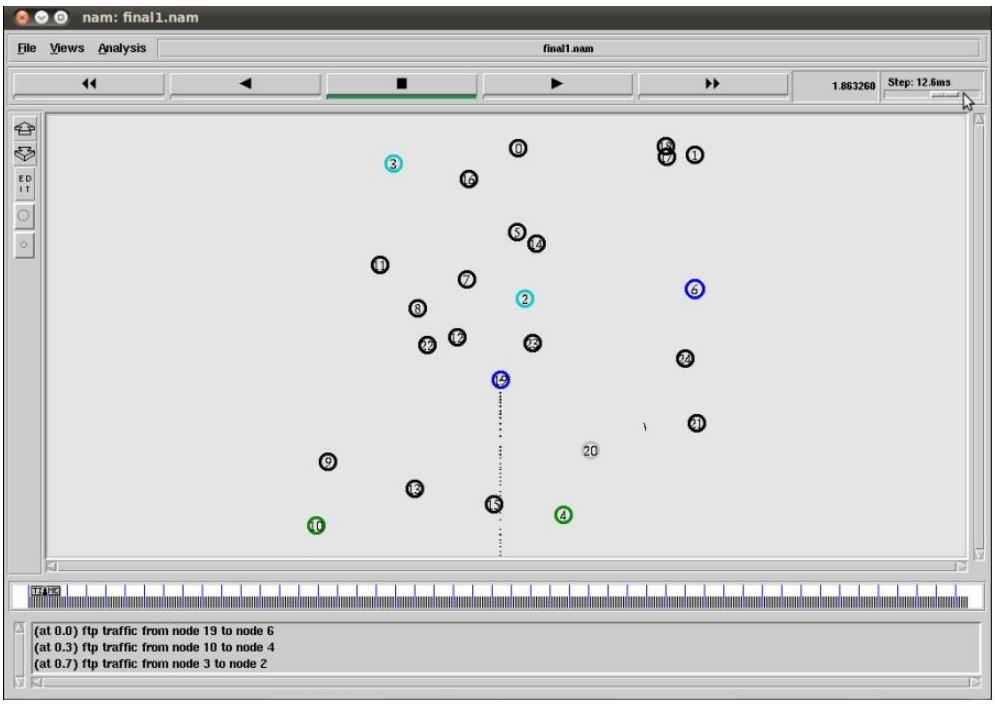


Figure 4.4: Communication between Nodes (Random Topology/25 Nodes)

Communication is being performed in three different node pair's i.e. green, blue and sky blue node pairs. Node 19 is transferring data to node 6(blue nodes), node 10 is transferring data to node 4(green nodes) and node 3 is transferring data to node 2(sky blue). The dark-line coming downward is showing the packet loss during the communication over the network.

4.1.3 Scenario 3(Random Topology)

In scenario 3, number of nodes in the network are 50 and topology used is Random. Rest of the configuration is same as in Table 4.1.

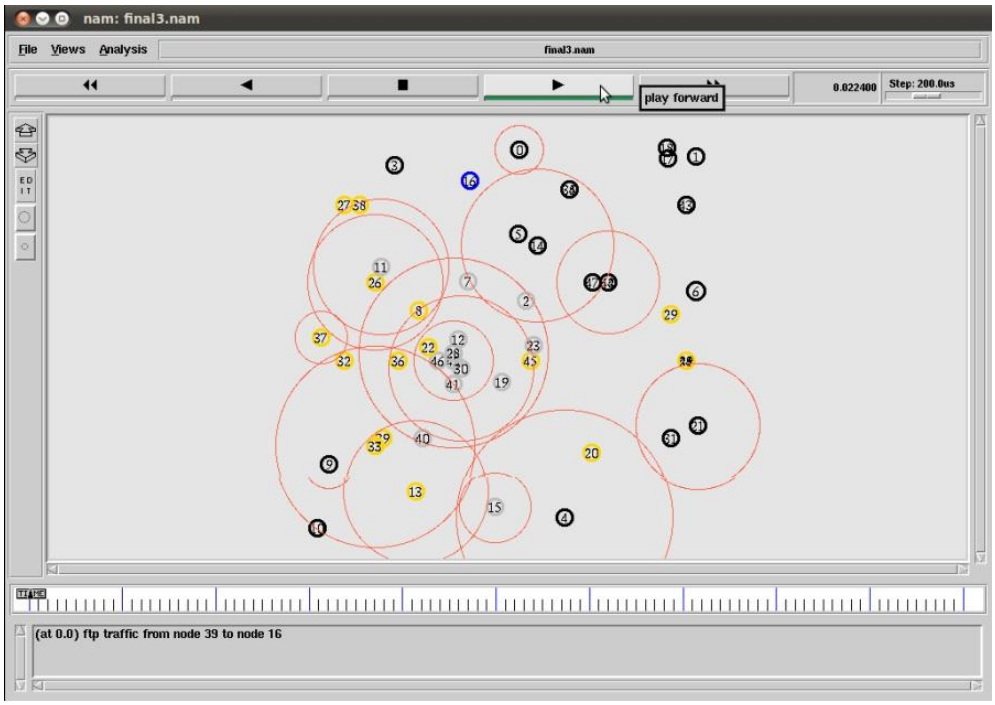


Figure 4.5: Network of 50 Nodes (Random Topology)

The communication begins at 0 seconds. The circles represent the coverage area and the blue nodes are the source and destination nodes as shown in figure 4.5.

Communication is being performed in three different node pairs as shown in figure 4.6. Blue nodes are communicating with each other, sky blue nodes are communicating with each other and green nodes are communicating with each other. The dark-line coming downward is showing the packet loss during the communication over the network.

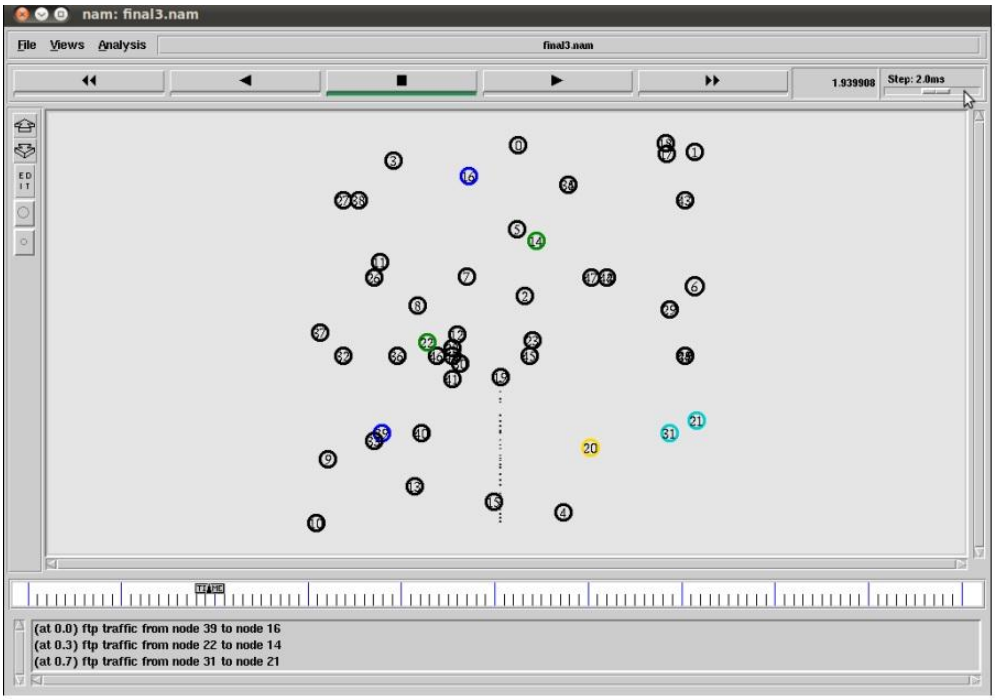


Figure 4.6: Communication between Nodes (Random Topology/50 Nodes)

4.1.4 Scenario 4 (Random Topology)

In scenario 4, Number of nodes in the network used are 75. Network of 75 nodes is shown in figure 4.7. Circles representing the coverage area. Initially, all nodes are broadcasting the dummy message to get information about the neighbors. This helps in finding shortest path between source and destination.

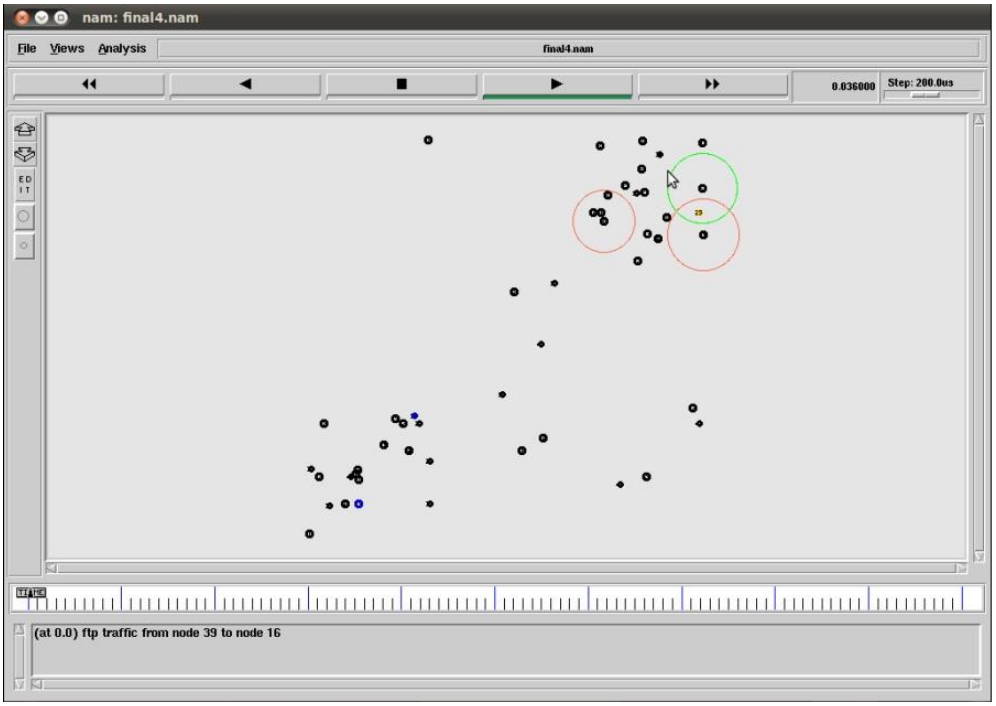


Figure 4.7: Network of 75 Nodes (Random Topology)

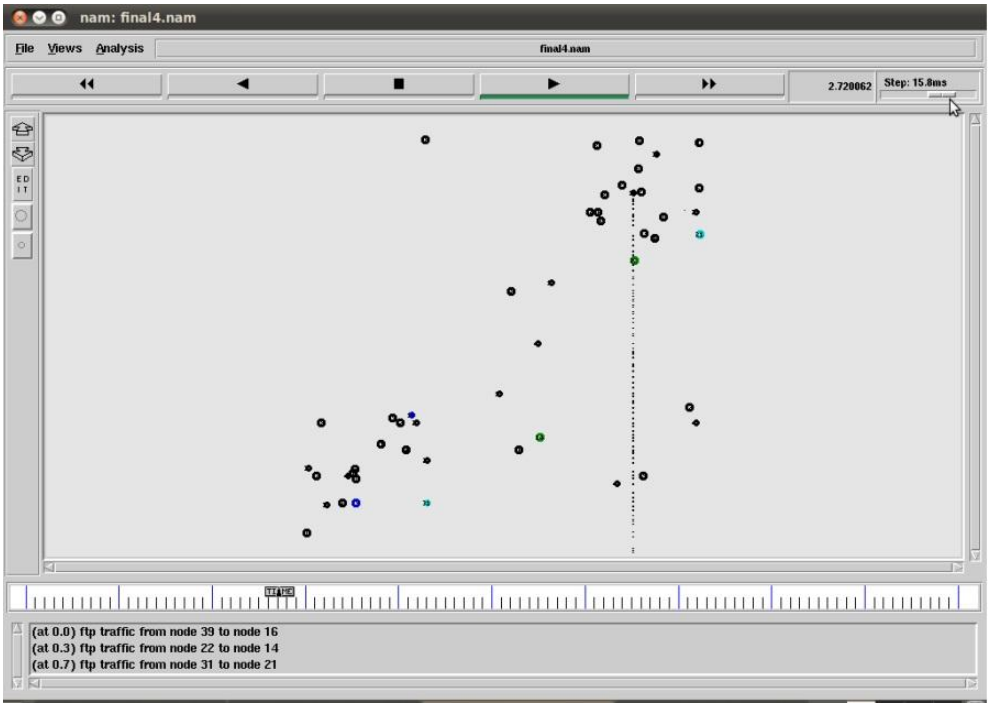


Figure 4.8: Communication between Nodes (Random Topology/75 Nodes)

In figure 4.8, actual communication starts. Same colored nodes are sending messages to each other by using in between nodes. There is dark line that is coming downward, showing the data loss in the network.

4.1.5 Performance Analysis of Random topology

To analyze the effect of scalability, Xgraph of NS-2 is used. The parameters taken for the comparison are

- Number of Packet Transmitted
- Number of Packets Lost
- Bit Rate
- Packet Loss Rate

In all graphs of random topology, 4 scenarios are taken which are different in number of nodes and rest of parameters is same in all scenarios.

- Yellow line represents Network of 75 nodes.
- Red line represents Network of 50 nodes.
- Blue line represents network of 25 nodes.
- Green line represents network of 10 nodes.
- X-axis represents time and Y-axis represents parameter written in every figure.

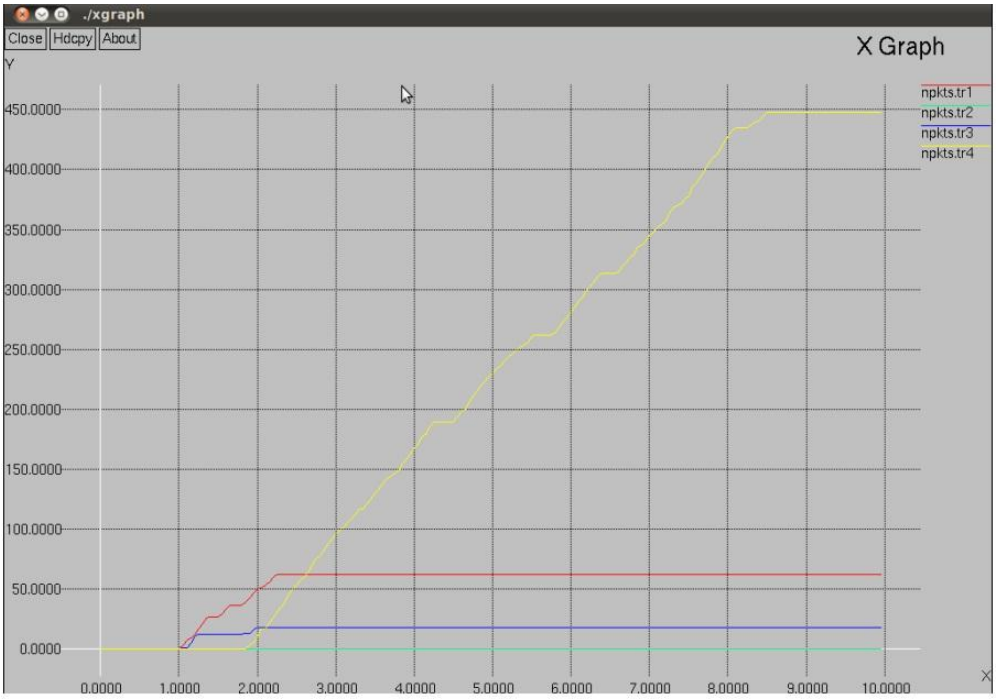


Figure 4.9: Number of packets Transmitted (Random Topology)

The yellow line (as shown in figure 4.9) represents network of 75 nodes and the green line represents the network of 10 nodes. As the number of nodes in the network increases, the distance between the nodes decreases. As the distance between nodes in a network decreases, number of packet transmitted increases.

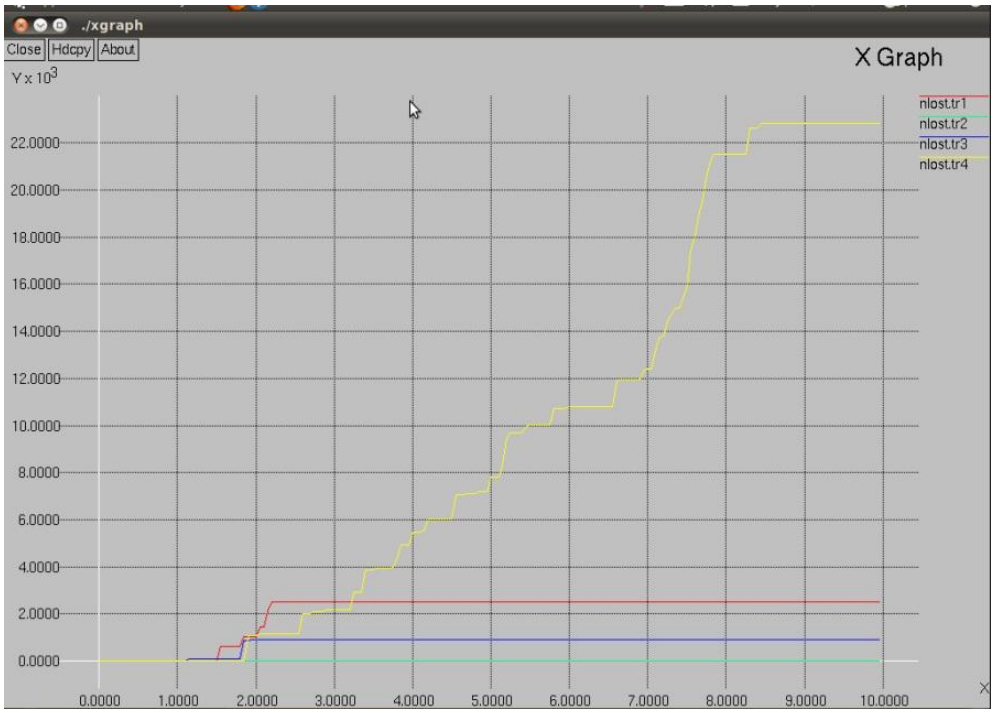


Figure 4.10: Number of packets loss (Random Topology)

The x-axis here represents the time and y axis represents the number of packets loss over the network as shown in figure 4.10. As the number of nodes in the network increases, the distance between the nodes decreases. Because of this there are more chances of collision. As the collision rate increased the data loss is also increased. So we can conclude as the collision rate between nodes in a network increases the loss rate will also increase over the network. Yellow line in graph represents maximum number of nodes i.e. 75 nodes and shows maximum packets loss.

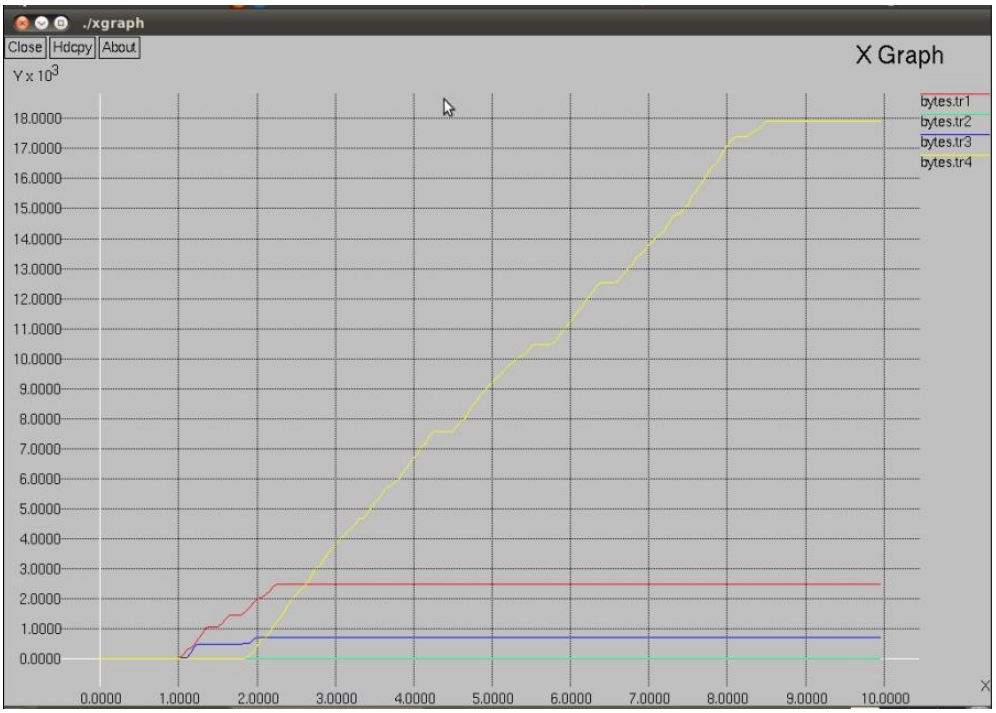


Figure 4.11: Bit Rate (Random Topology)

The x-axis here represents the time and y axis represents the Bit Rate over the network as shown in figure 4.11. As the number of nodes in the network increases, the distance between the nodes decreases. Because of this, there are more chances of collision. So, the rate of data transmission i.e. bit rate is increased. So, it can be concluded that as the distance between nodes decreases, Communication rate get increases.

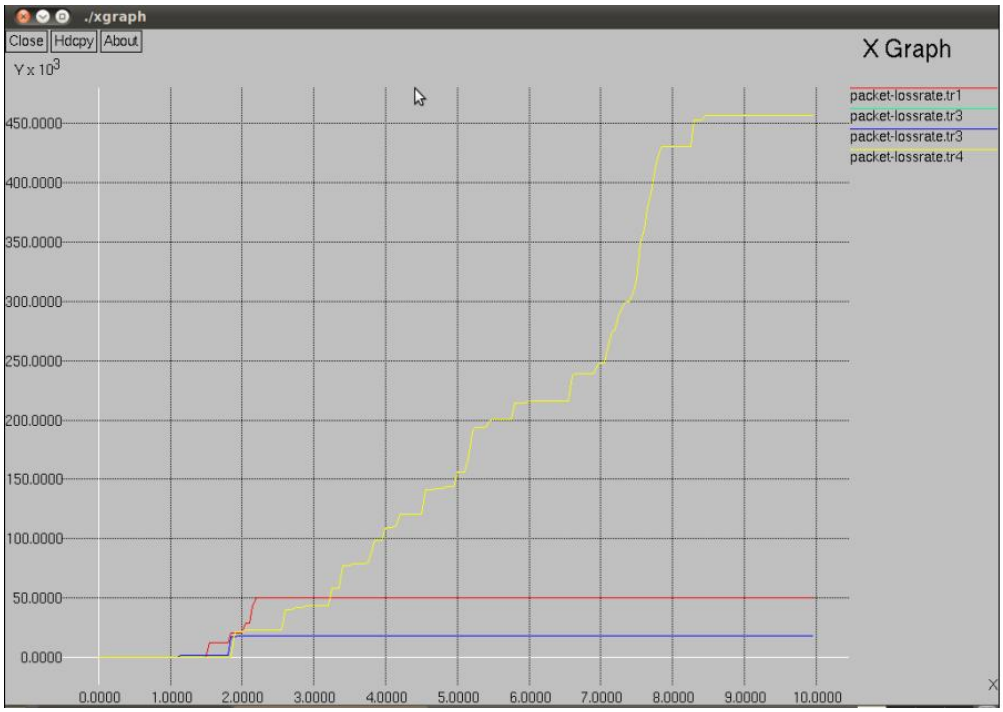


Figure 4.12: Packet Loss Rate (Random Topology)

The x-axis here represents the time and y axis represents Packet Loss Rate over the network. As the collision rate between nodes in a network increases the Packet loss rate will also increase over the network. Yellow line in graph represents maximum number of nodes i.e. 75 nodes and shows maximum packets loss rate. Performance analysis results of ZigBee protocol using random topology is shown in Table 4.2.

Table 4.2: Analysis of Smart Dust Network using Random Topology

	No. of nodes (10)	**No. of nodes (25)**	**No. of nodes (50)**	**No. of nodes (75)**	**Description**
Number of Packet Transmitted	Less	Medium	High	Very High	Low Distance between nodes increase the communicate rate and improve the packet transmitted
Number of Packet Lost	Low	Low	Medium	High	As the communication rate increases, the chances of collision increased, so, it increase the packet loss

Packet Loss Rate	Low	Low	High	High	Distance decreases between nodes, improve the packet loss over the network.
Bit Rate	Less	Medium	High	Very High	Number of nodes increases distance between nodes decreases, so it increases bit rate.

4.2 Simulation Environment II

In Simulation environment II, analysis of ZigBee protocol in Smart Dust Network is done using Ring Topology. Analysis is performed on scalability of network in terms of number of nodes. The system is implemented on Ubuntu Environment with NS2 simulator and XGraph is used as the tool for graph analysis. Analysis is divided into 2 scenarios as defined below. Configuration of network is shown in Table 4.3.

Table 4.3: Ring Topology Network Configuration

Parameter	Value
Number of Nodes	7, 13
Topography Dimension	670 m x 670 m
Traffic Type	Constant Bit Rate(CBR)
Radio Propagation Model	Two-Ray Ground Model
MAC Type	802.15.4 Mac Layer
Packet Size	512 bytes
Mobility Model	Random Way Point
Antenna Type	Omni directional
Protocol	ZigBee
Topology	Ring
Number of Clusters	Single

4.2.1 Scenario 1(Ring Topology)

In scenario 1, analysis of Smart Dust Network is done using Ring topology. Network consists of 7 numbers of nodes and there is one node at the centre which acts as coordinator as shown in 4.13 and rest of the configuration is same as in Table 4.3.

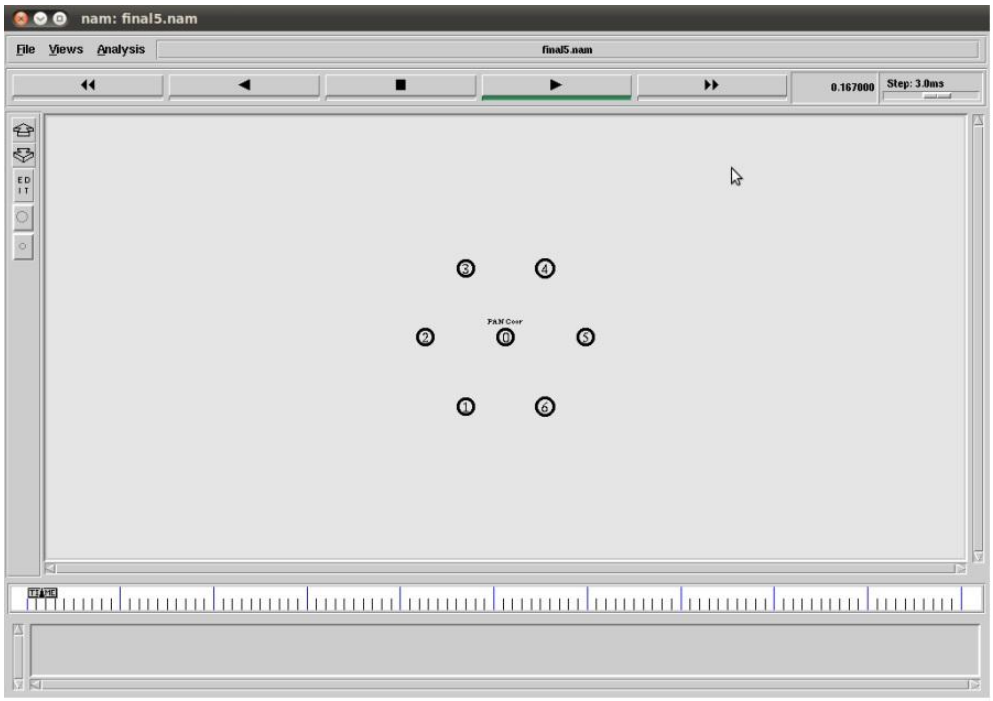


Figure 4.13: Network of 7 Nodes (Ring Topology)

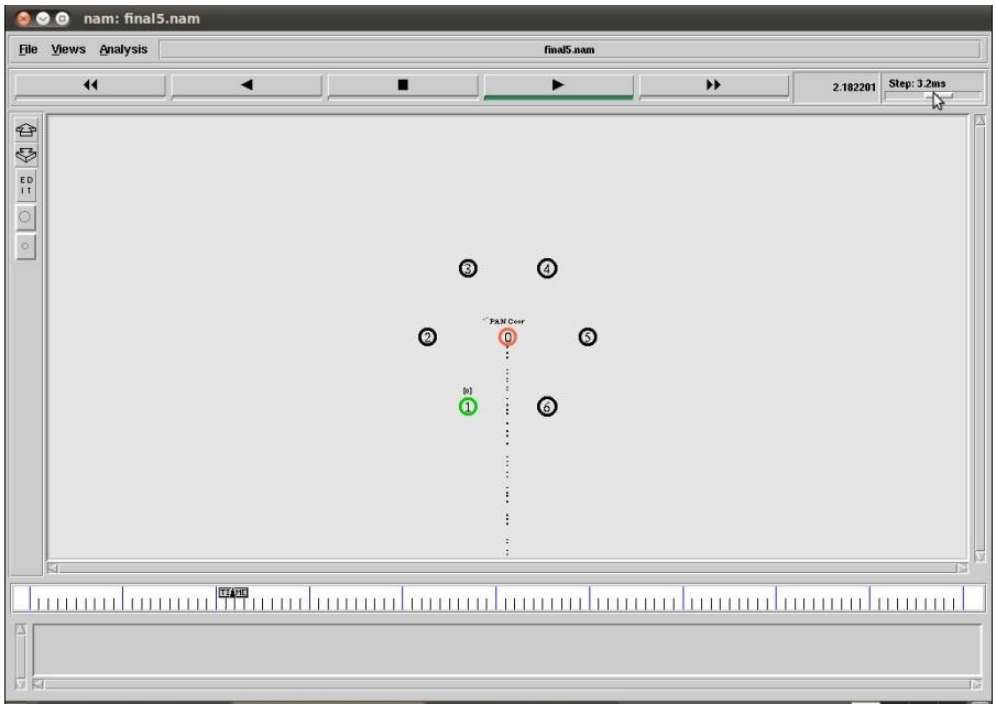


Figure 4.14: Communication between Nodes (Ring Topology/7 Nodes)

Communication is being performed in three different node pairs as shown in figure 4.14. The darkline coming downward is showing the packet loss during the communication over the network.

4.2.2 Scenario 2(Ring Topology)

In scenario 2, number of nodes in the network are 13 as shown in figure 4.15 and rest of the configuration is same as in Table 4.3.

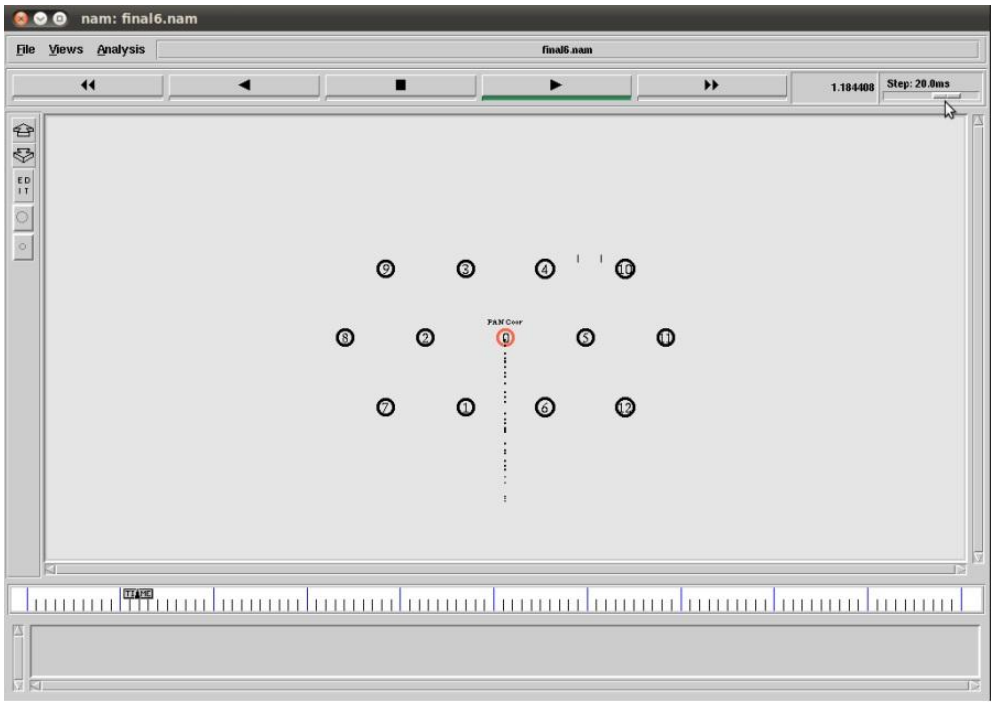


Figure 4.15: Network of 13 Nodes (Ring Topology)

In figure 4.15, Number of nodes from 1 to 6 are near PAN coordinator i.e. node 0. Numbers of nodes from 7 to 12 are farthest from PAN coordinator.

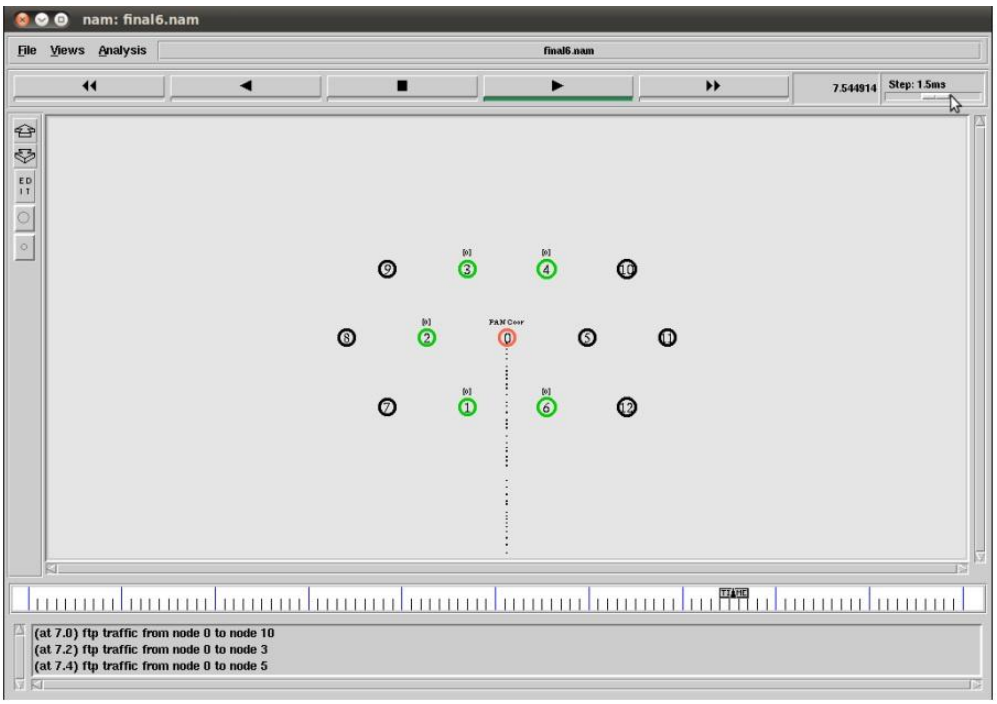


Figure 4.16: Communication between Nodes (Ring Topology/13 Nodes)

In figure 4.16, Communication is being performed in three different node pairs. The darkline coming downward is showing the packet loss during the communication over the network

4.2.3 Performance Analysis of Ring Topology

In this analysis, two different Scenarios are taken in terms of number of nodes in ring topology, all other parameters are identical. The particular work is showing the difference in terms of scalability. Basically, distance of nodes from a centralized PAN Coordinator is increasing. The particular scenario will analyze the security as well as role of centralized PAN coordinator. As the PAN is small area network because of this more number of nodes reduces the gap between nodes. The parameters taken for the comparisons are

- Number of Packet Transmitted
- Number of Packets Lost
- Bit Rate
- Packet Loss Rate

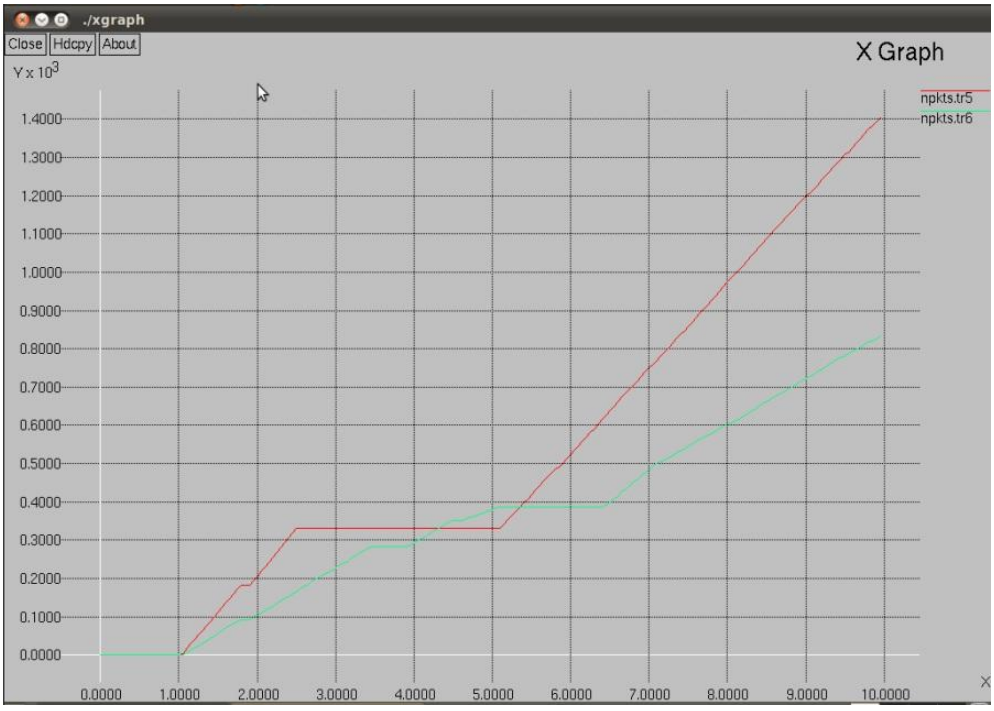


Figure 4.17: Number of Packets Transmitted (Ring Topology)

The x-axis here represents the time and y axis represents the number of packet transmitted over the network as shown in figure 4.17. As the distance from the PAN coordinator increases the throughput over the network decreases. The red line

represents the network of 7 nodes and the green line represents the network of 13 nodes.

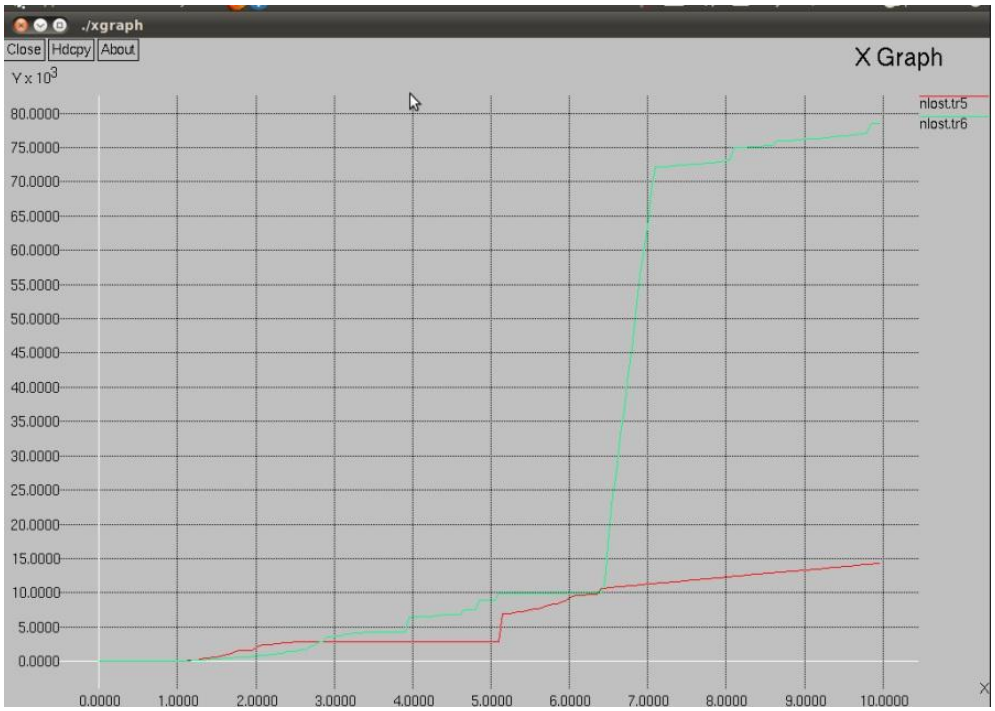


Figure 4.18: Number of Packets Lost (Ring Topology)

As the distance from the PAN coordinator increases, the data loss over the network increases as shown in figure 4.18.

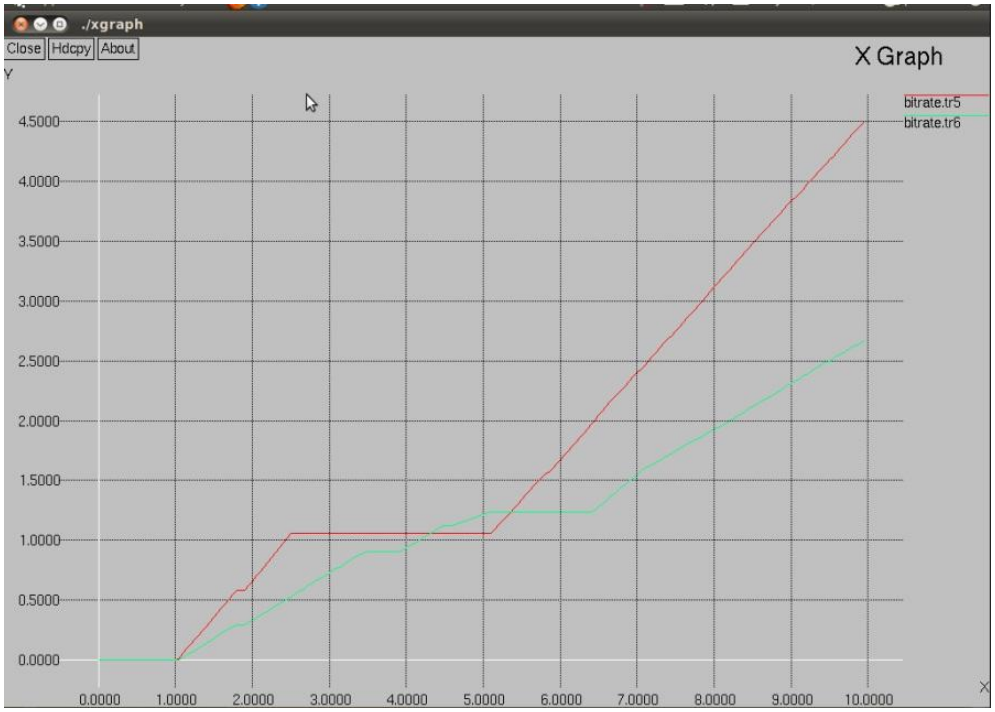


Figure 4.19: Bit Rate (Ring Topology)

The red line represents network of 13 nodes and green line represents network of 7 nodes as shown in figure 4.19. Distance from coordinator affects the Bit Rate, Higher the distance lower the bit rate. Packet Loss Rate also increases as number of nodes in network increases as shown in figure 4.20.

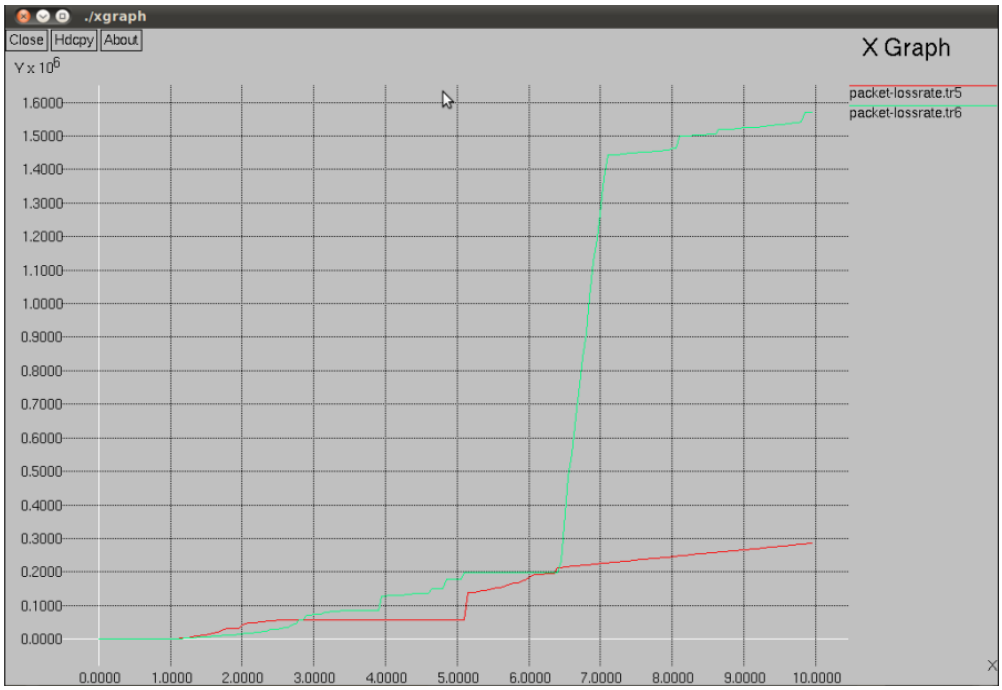


Figure 4.20: Packet loss rate (Ring Topology)

Performance analysis results of ZigBee protocol using ring topology is shown below in Table 4.4.

Table 4.4: Analysis of Smart Dust Network using Ring Topology

	No of Nodes(7)	**No of nodes(13)**	**Description**
Total Packet Transmitted	High	Low	As the distance from the coordinator is less, the total packet transmission will be improved.
Packet Lost	Low	High	As the distance of nodes from the coordinator is increased the packet loss will be increased.
Bit Rate	High	Low	The distance from the coordinator will affect the bit rate, higher the distance lower the bit rate

Packet Loss Rate	Low	High	The packet loss rate is increased as the number of nodes increased.

4.3 Simulation Environment III

In Simulation environment III, analysis of ZigBee protocol in Smart Dust Network is done using Clustered Topology. Analysis is performed on scalability of network in terms of number of nodes/cluster. The system is implemented on Ubuntu Environment with NS2 simulator and XGraph is used as the tool for graph analysis. Analysis is divided into 2 scenarios as defined below. Configuration of network is shown in Table 4.5.

Table 4.5: Clustered Topology Network Configuration

Parameter	Value
Number of Nodes	30, 50
Topography Dimension	670 m x 670 m
Traffic Type	Constant Bit Rate(CBR)
Radio Propagation Model	Two-Ray Ground Model
MAC Type	802.15.4 Mac Layer
Packet Size	512 bytes
Mobility Model	Random Way Point
Antenna Type	Omni directional
Protocol	ZigBee
Topology	Clustered
Number of Clusters	5

4.3.1 Scenario 1 (Clustered Topology)

In scenario 1, Network consists of 30 nodes and Topology used is Clustered Topology. Numbers of Nodes per Cluster are 6 as shown in figure 4.21. Rest of configuration is shown in Table 4.5. Blue nodes represent PAN coordinator.

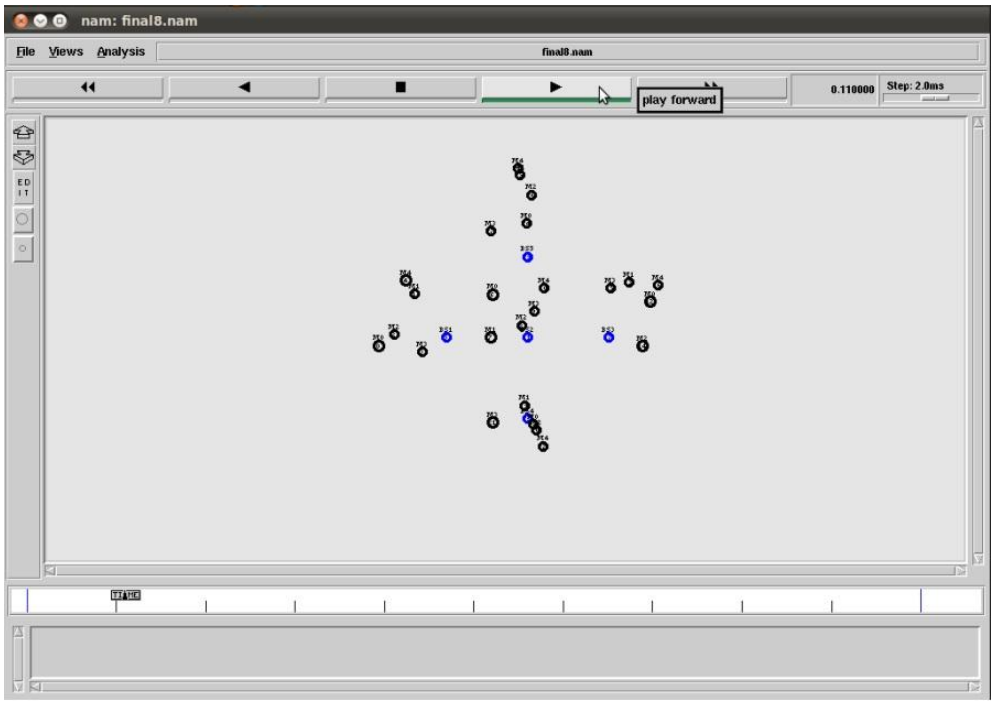


Figure 4.21: Network of 30 Nodes (Clustered Topology)

4.3.2 Scenario 2 (Clustered Topology)

In scenario 2, Network consists of 50 nodes and rest of the configuration is same as in Table 4.5. Blue nodes represented PAN coordinator. With each PAN coordinator 10 nodes are attached i.e. 5 clusters are there as shown in figure 4.22.

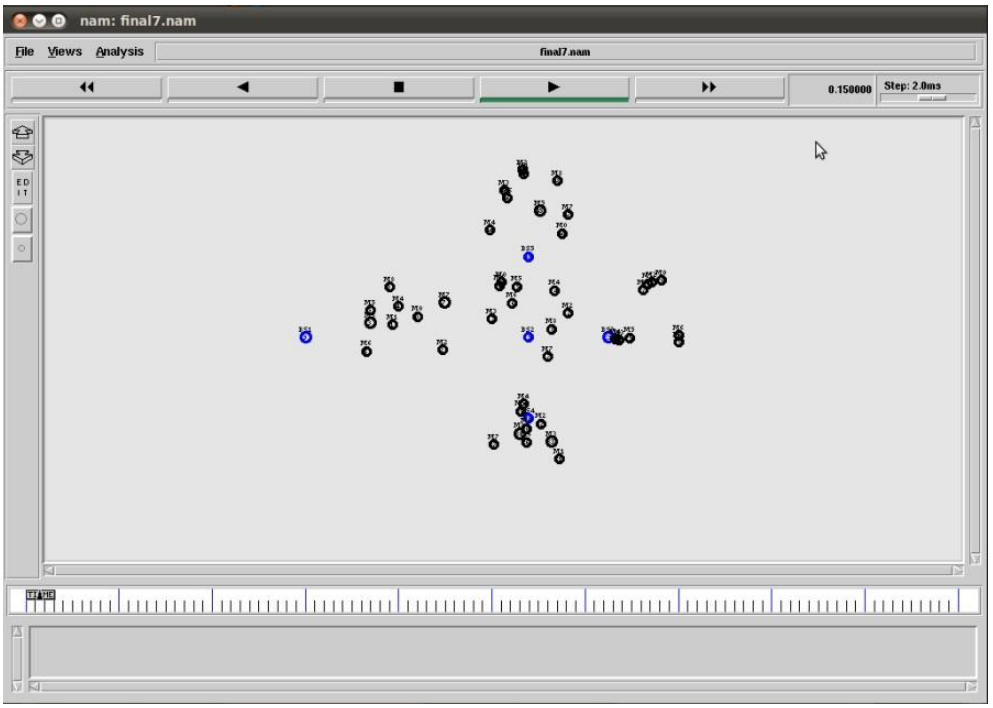


Figure 4.22: Network of 50 Nodes (Clustered Topology)

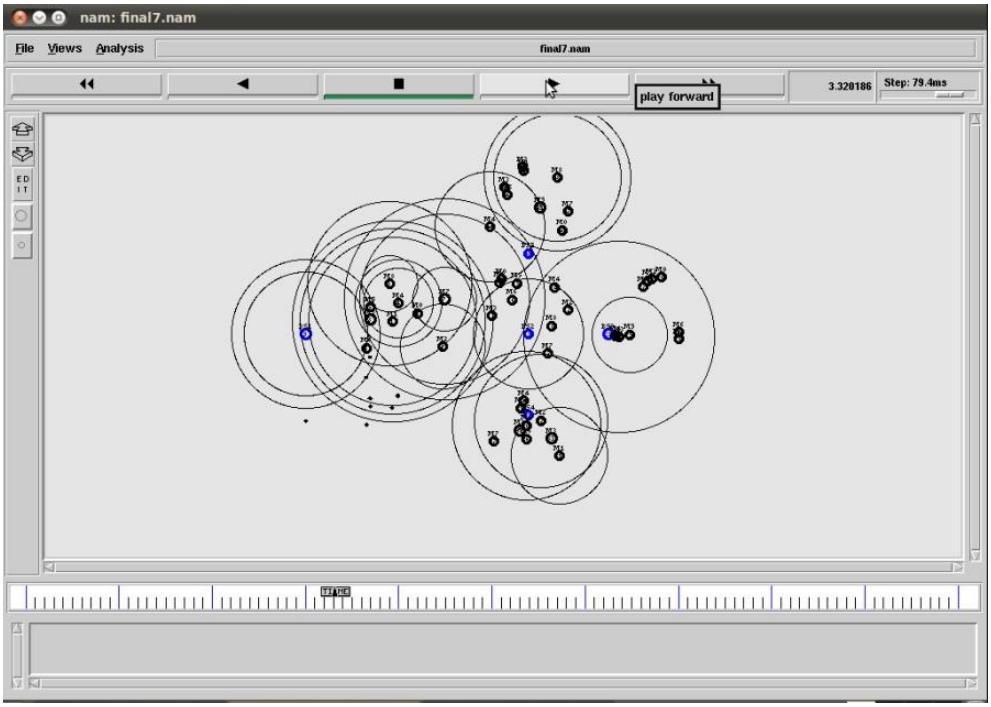


Figure 4.23: Communication between Nodes (Clustered Topology/50 Nodes)

Nodes are communicating as shown in figure 4.23. Every node is broadcasting data to its neighbors, they further sends data to another nodes. Process continues till packet reaches its destination. Darkline coming downwards is showing packet loss occurs.

4.3.3 Performance Analysis of Clustered Topology

In this analysis, 2 different Scenarios are taken in terms of Number of nodes/cluster using Clustered network. Each cluster is defined with a PAN coordinator. The particular work is showing the difference in terms of scalability. The parameters taken for the comparison are

- Number of Packet Transmitted
- Number of Packets Lost
- Bit Rate
- Packet Loss Rate

In figure 4.24, x-axis represents the time and y axis represents the packet transmitted over the network. The red line represents the minimum number of nodes in network i.e. 30 nodes and 6 nodes/cluster. And the green line shows the maximum number of nodes in the network i.e. 50 nodes and 10 nodes/cluster.

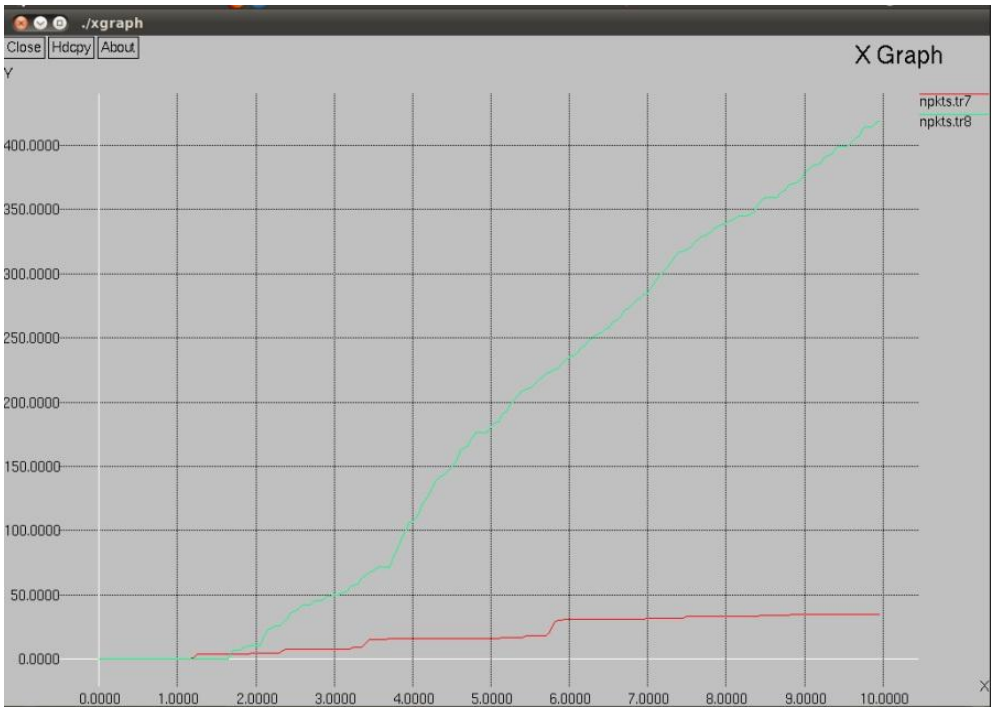


Figure 4.24: Number of Packets Transmitted (Clustered Topology)

It can be observed that in a PAN network number of nodes/cluster affects the network efficiency and reliability. It can be concluded that less the number of nodes/cluster, more efficient and reliable the network is. Numbers of packets loss is more in 50 nodes as compared to 30 nodes as shown in figure 4.25.

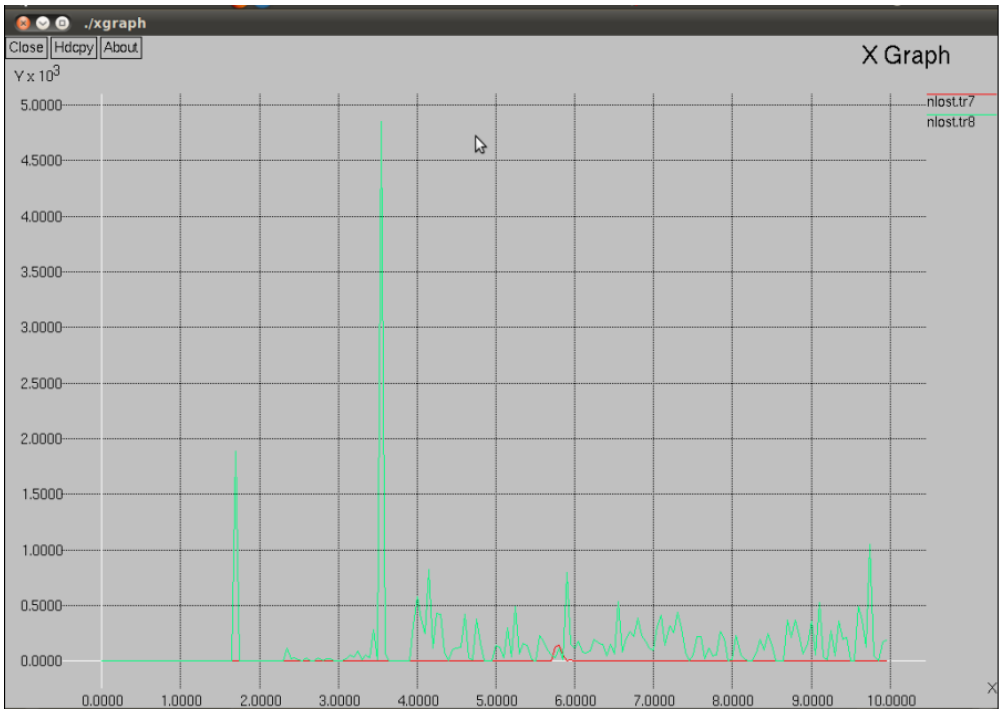


Figure 4.25: Numbers of Packets Lost (Clustered Topology)

As the number of nodes/cluster increases, distance between the nodes decreases. Because of this, there are more chances of collision, so need to resend the data again and again this indirectly increases rate of data transmission i.e. bit rate as shown in figure 4.26.

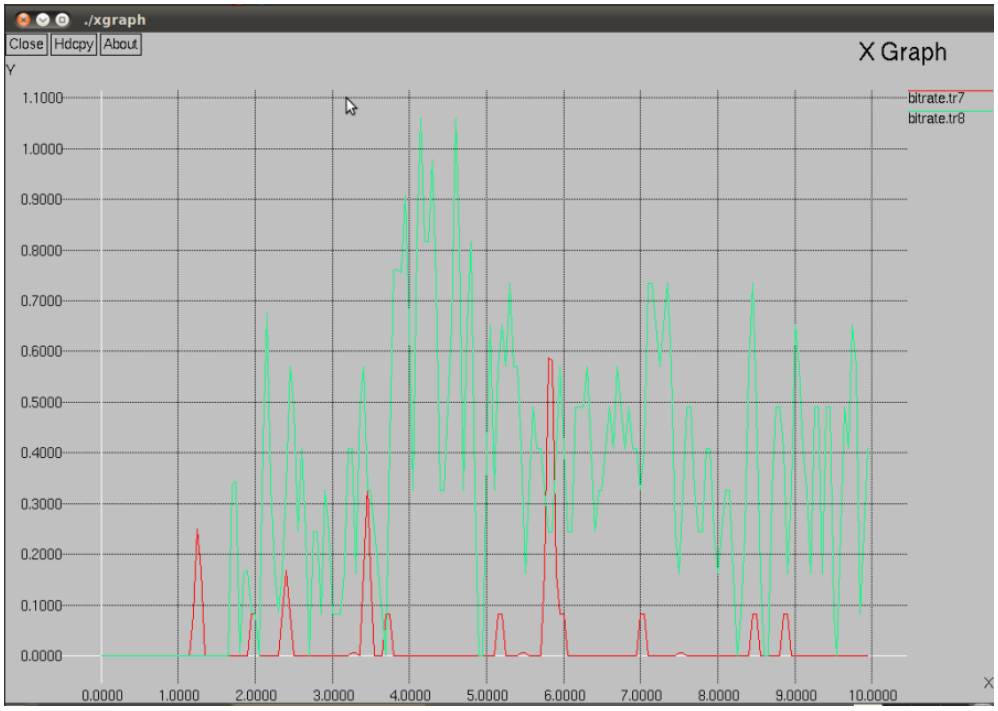


Figure 4.26: Bit rate (Clustered Topology)

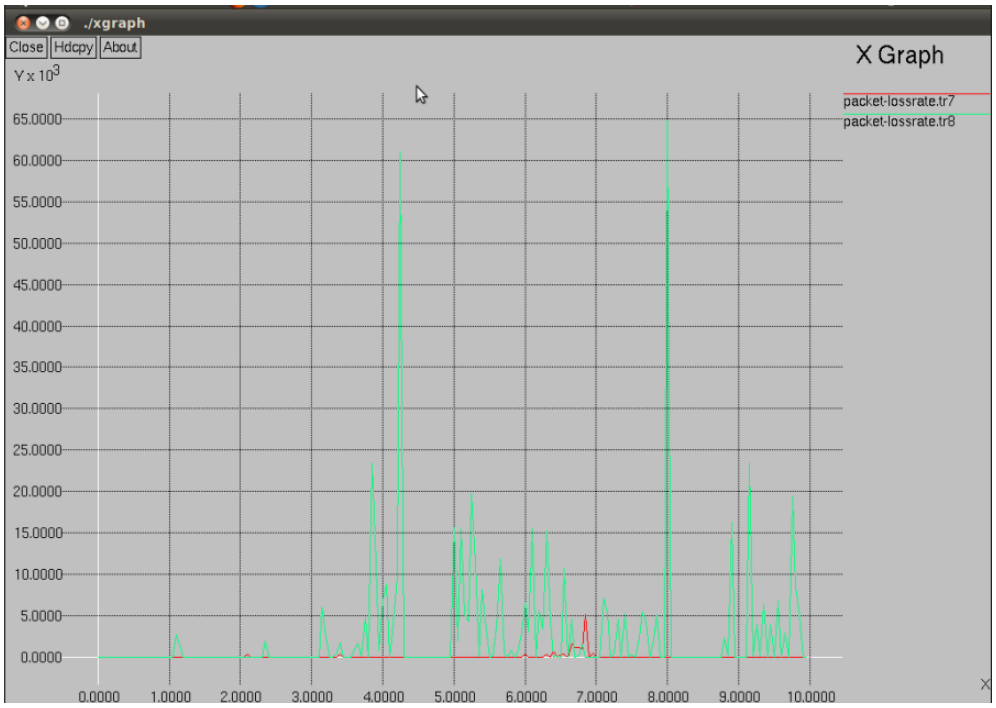


Figure 4.27: Packet Loss Rate (Clustered Topology)

The x-axis represents the time and y axis represents Packet Loss Rate over the network in figure 4.27. Green line represents scenario 2 i.e. network of 50 nodes and red line represents scenario 1 i.e. network of 30 nodes. Packet Loss rate in scenario 2 is more. Because as network size increases, collision rate also increases which significantly increases Packet Loss Rate. Performance analysis results of ZigBee protocol using clustered topology is shown in Table 4.6.

Table 4.6: Analysis of Smart Dust Network using Clustered Topology

	Number of Nodes(30)	**Number of Nodes(50)**	**Description**
Number of Packets Transmitted	Low	High	In dense clustered network, more communication is performed between nodes and it increases the total packets transmitted over the network.
Number of Packets Lost	Low	High	In a clustered network as the inter cluster communication is increased the load on coordinator node increase, it results more packet loss.
Bit Rate	Low	High	As the communication over the network increases, the rate of data transmission is also increased.
Packet Loss Rate	Low	High	More the communication between inter cluster nodes, more the congestion on centralized nodes. It increases the loss rate over the network.

Chapter 5
Conclusion and Future Scope

5.1 Conclusion

In Smart Dust network, there are different routing protocols all of which have their own specifications and benefits. For the very small sensor network we always look for the minimum energy consumed networks. In this presented research work, Analysis of ZigBee protocol has been done in Smart Dust network using 8 different scenarios. These scenarios are different in terms of number of nodes, number of nodes/cluster and distance from the PAN coordinator. Complete work is analyzed and implemented on three different topologies. The simulation is performed in NS-2 environment. Result of analysis proves that as the number of nodes in a network increases; it increases the number of packets transmitted as well as number of packets loss over the network. In same way as the distance from the PAN coordinator increases, it decreases the total packet transmitted and significantly increases Packet Loss. In case of clustered network, Higher the number of nodes/cluster; higher number of packets transmitted as well as Packet loss rate.

5.2 Future work

In this research work, Analysis based upon different kind of network scenarios under different parameters using ZigBee protocol has been done. Limitations of ZigBee protocol in terms of scalability are also shown in results. So, in future, work can be extended to design a new protocol that can cover all or some of these drawbacks.

References

[1] I.F. Akyildiz, Weilian Su, Sankarasubramaniam, E. Cayirci, "A survey on sensor networks", IEEE Communications Magazine, Aug 2002, pp 392-422.

[2] K.S.J. Pister, J.M. Kahn and B.E. Boser, "Smart Dust: Wireless networks of milli-meter scale sensor nodes", Electronics Research Laboratory Research Summary, July, 1999.

[3] L. Doherty, B. A. Warneke, B. E. Boser, and K. S. J. Pister, "Energy and performance considerations for Smart Dust," Int. J. Parallel Distrib. Syst. Networks, vol. 4, no. 3, pp. 121–133, 2001.

[4] I. Chatzigiannakis, A. Kinalis, S. Nikoletseas, "Power Conservation Schemes for Energy Efficient Data Propagation in Heterogeneous Wireless Sensor Networks", Sept. 2004.

[5] A. Boukerche, I. Chatzigiannakis, S. Nikoletseas, "Power-Efficient Data Propagation Protocols for Wireless Sensor Networks", February 28, 2005.

[6] T. Antoniou, A. Boukerche, I. Chatzigiannakis, G. Mylonas, S. Nikoletseas, "A New Energy Efficient and Fault-tolerant Protocol for Data Propagation in Smart Dust Networks using Varying Transmission Range", 37th Annual ACM/IEEE Simulation Symposium, pp. 43–52 July 15, 2005.

[7] W.R. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energy-efficient communica-tion protocol for wireless micro-sensor networks", IEEE Hawaii International Conference on System Sciences, Aug 2000.

[8] S. Zhu, S. Setia and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks." In 10th ACM Conference on Computer and Communications Security (CCS '03), 2006.

[9] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D. Culler, "SPINS: Security protocols for sensor networks", Wireless networks 8,521-534,2002, Kluwer Academic Publications, June,2002.

[10] I. Chatzigiannakis and S. Nikoletseas, "A sleep-awake protocol for information propagation in smart dust networks",3rd International Workshop on Mobile, Ad-hoc and Sensor Networks (WMAN 2003), 2003, IPDPS Workshops, pp 225.

[11] K. Selvarajah,” HeterogeneousWireless Sensor Network for Transportation System Applications”, Inventi Impact: Vehicular Technology publication, Dec,2011.

[12] K. Selvarajah,” Integrating Smartdust Into The Embedded Middleware In Mobility Applications (Emma) Project”, Intelligent Environments, 2 008 IET 4th International Conference , 21-22 July 2008.

[13] S.S.Riaz, Ahamed,” The Role Of ZigBee Technology In Future Data Communication System”, Journal of Theoretical and Applied Information Technology © 2005 - 2009 JATIT.

[14] Yao-Jung Wen,” Smart Dust Sensor Mote Characterization, Validation, Fusion and Actuation”, National Taiwan University, Taipei, Taiwan, June, 1999.

[15] Su-Chu Hsu,” Wireless Sensor Networks: a building block for Mass Creativity and Learning”. Proceedings ACM Creativity & Cognition 2009, Understanding the Creative Conversation Workshop, October 2009.

[16] Meng-Shiuan Pan,” Address Assignment and Routing Schemes for ZigBee-Based Long-Thin Wireless Sensor Networks”. Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE 11-14 May 2008 Page(s): 173 – 177.

[17] Ben W. Cook,” SoC Issues for RF Smart Dust”. Proceedings of the IEEE June 2006 Volume: 94 , Issue: 6 Page(s): 1177 – 1196.

[18] Lubomír Smutný,” Smart Sensors with PC Connection in Wireless Networks”, Proceedings of the 13th WSEAS International Conference on Computers, ISSN: 1790-5109 ISBN: 978-960-474-099-4.

[19] Meng-Shiuan Pan,” Quick Convergecast in ZigBee Beacon-Enabled Tree-Based Wireless Sensor Networks”. Journal Computer Communications archive Volume 31 Issue 5, March, 2008 Pages 999-1011.

[20] Steffen Peter, Krzysztof Piotrowski,” Public key cryptography empowered smart dust is affordable”. International Journal of Sensor Networks, Vol. 4, No. 1/2. (2008).

[21] Li-Chien Huang,” A ZigBee-based monitoring and protection system for building electrical safety”. Energy and Buildings Volume 43, Issue 6, June 2011, Pages 1418–1426.

[22] Mark Hempstead," An Ultra Low Power System Architecture for Sensor Network Applications", IEEE,0-7695-2270-X/05 , 2005.

[23] W. Rabiner, Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks", Hawaii International Conference on System Sciences, Maui, Hawaii, Jan. 2000.

[24] V.S.Hsu, J.M.Kahn, K.S.J.Pistcr, "Wireless Communications for Smart Dust", UC Berkeley Electronics Research Laboratory Memorarzdupn, Jan. 2006.

[25] S. Nikoletseas, I. Chatzigiannakis, H. Euthimiou, A. Kinalis, T. Antoniou, and G. Mylonas, "Energy efficient protocols for sensing multiple events in smart dust networks", 37th Annual ACM/IEEE Simulation Symposium(ANSS 2004), 2004, pp. 15–24.

[26] A. Manjeshwar and D.P. Agrawal, "TEEN: A routing protocol for enhanced efficiency in wireless sensor networks", 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing (WPIM 2002),2002, IPDPS Workshops, p. 195b.

[27] Scott C. H. Huang, Maggie X. Cheng, Ding-Zhu Du, "GeoSENS: geo-based sensor network secure communication protocol", Technical report, University of Missouri, Computer Communications, pp 456–461,2005.

[28] Sinem Coleri Ergen," ZigBee/IEEE 802.15.4 Summary", September 10, 2004.

[29] A. Boukerche and S. Nikoletseas, Kluwer, "Protocols for data propagation in wireless sensor networks: A survey", Academic Publishers, June 2004.

[30] J. M. Kahn, R. H. Katz, K. S. J. Pister: "Next Century Challenges: Mobile Networking for Smart Dust", In ACM MobiCom, 1999.

[31] C. Karlof, N. Sastry and D. Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", ACM Conference, 2004.

[32] Doherty, B. A. Warneke, B. E. Boser, and K. S. J. Pister, "Energy and performance considerations for Smart Dust," Int. J. Parallel Distrib. Syst. Networks, vol. 4, no. 3, pp. 121–133, 2001

[33] Z. Alliance,"ZigBee Specifiications",1st ed. ZigBee Standard Organization, http://www.ZigBee.org. ,June 2005.

List of Publications

Sandeep Kumar, V.P. Singh, "Performance Analysis of ZigBee Protocol in Smart Dust Communication Network" communicated in International Journal of Computer Applications, (ISSN 0975-8887)**,** June 2012.