ACKNOWLEDGEMENTS

We take this opportunity to thank our project guide **Prof. M.M Chandane** for providing us the opportunity to work in an exciting and challenging field of WSN. Our interactions with him have been of immense help in defining our project goals and in identifying ways to achieve them.

We would like to thank **Prof. G. Bhole**, Head of Department and all other faculty members of Information Technology Department for providing all the facilities to complete the project.

List of Figures

List of Tables

Table of Contents

Chapter 1

Introduction

In 1999 it was called one of "21 ideas for the 21st century" [1] and in 2003 it was heralded as one of "10 emerging technologies that will change the world" [2]. This revolutionary technology is known as Wireless Sensor Networks (WSNs).

A sensor network is an infrastructure comprised of sensing (measuring), computing, and communication elements that gives an administrator the ability to instrument, observe, and react to events and phenomena in a specified environment. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance. Today networks are administered applications such as area monitoring, industrial process monitoring and control, structural monitoring, passive localization and monitoring, machine health monitoring, and many more applications ranging beyond human fancy.

There are four basic components in a sensor network: (1) an assembly of distributed or localized sensors; (2) an interconnecting network (usually, but not always, wireless-based);

(3) a central point of information clustering; and (4) a set of computing resources at the central point (or beyond) to handle data correlation, event trending, status querying, and data mining.

The communication between sensor nodes starts with data being forwarded via multiple hops, to a sink (sometimes denoted as controller or monitor) that can use it locally or is connected to other networks (e.g., the Internet) through a gateway. The design issues for network set up and communication include cost, energy efficiency, energy sufficiency, ability to cope with node failures, nature of node i.e. homogenous or heterogeneous, communication failures, scalability to large scale of deployment, environment accessibility, ease of use and many more.

To exemplify, consider a large number of nodes deployed in a hazardous environment where once configured their batteries cannot be replaced. Here, the failure of single node could set apart the WSN from rest of the connected networks. The reason could be emphasis on energy efficient paths leading to compromise with lifetime of a network. Hence achieving the balance between energy efficiency and energy sufficiency must be the catch of future algorithms.

Thus, as a step forward in this direction, our research focusses on network layer to develop an energy efficient routing protocol.

1.1 Scope

The scope of this research is development of efficient distributed energy adaptive routing (DEAR) protocol for WSN. Even though there are numerous proposals for WSN routing protocols the scope of developing ones to balance energy efficient and energy sufficient routing methodologies is wide.

1.2 Motivation

Wireless Sensor Networks are an emerging technology used currently in more than 200 distinct categories with its future scope to be laid in applications as the state of the art in communication, sensing and energy technologies. Due to the hostile nature of location of sensor nodes in the environment leading to inaccessibility, the major design issue remains to be conserving energy throughout the network and on every layer of protocol stack. With reference to [3] battery of node is depleted by (i) computational processing and (ii) transmission and reception of data. Optimization of transmissions and computational processes could be achieved through design of energy efficient network layer which will help in increasing lifetime of network.

With the very first attempt to develop a routing protocol lays back in 1990, we aim to contribute in this regard. Routing protocols are classified on the basis of network structure into flat or hierarchical. In flat networks all of the nodes are equal and can participate equally in the routing task. Hierarchical networks on the other hand, require some nodes to control the communication of other nodes. Flat protocols are more efficient for use in WSNs than hierarchical protocols due to the fact that they are more scalable, generally require fewer messages to be sent and are simpler in computational requirements.

Routing protocols are classified on the basis of path establishment as either proactive or reactive. Proactive protocol maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. The main disadvantages of such algorithms are (i) Respective amount of data for maintenance and (ii) Slow reaction on restructuring and failures. Reactive protocol finds a route on demand by flooding the network with Route Request packets. The main disadvantages of such algorithms are (i) High latency time in route finding and (ii) Excessive flooding can lead to network clogging.

Routing protocols can be further subdivided into source initiated and destination initiated protocols. Nodes employing source initiated protocols send data either periodically, or in response to certain events in their environment. In destination initiated routing, nodes only send data in response to a request for data. The drawback of destination initiated protocols is

the fact that requests are usually flooded through the network, draining the energy sources of nodes. Therefore, source initiated operation can achieve higher energy efficiency.

Our literature review includes protocols requiring excessive number of messages for data transfer ([4], [5], [6], [7], [8]), are computationally complex [9], require sensor node to have capabilities ([10], [11], [12]) or require certain network structure ([10], [11], [12]) to function.

The proposed algorithm addresses above problem by designing proactive routing algorithm which is source initiated and is analysed to be energy efficient, computationally efficient with no additional hardware requirements

1.3 Objective

The objective of this research is to develop a DEAR protocol with the following features:

1. The protocol must increase lifetime of the network (energy sufficiency) and use optimum path for transmission (energy efficiency)
2. The protocol must function irrespective of topology and remove limitations of existing protocols if any.
3. The protocol has to minimize the number of transmissions made by a WSN node.
4. The protocol must be simple to implement.
5. The protocol must not depend on hardware capabilities of nodes.

The objectives for the routing protocol to be developed can be summarized as: energy sufficiency, energy efficiency, simplicity, scalability and practicality.

1.4 Research Methodology

A significant constituent to the proposal of any routing protocol is in depth knowledge and understanding of the factors that influence the specific network for which the routing protocol is intended. Hence fair amount of literature review was done to identify parameters of concern in current applications of WSN. The further step was necessity to study pros and cons of existing protocols. Subsequently, acquaintance with the simulator QUALNET 4.5 was gained by implementing case studies on Design and Integration of Protocol. Gradually, over a period

of time, an improved DEAR protocol was researched upon which was simulated and analysed to overcome limitations of existing one and this achieve the penultimate goal.

1.5 Overview

Chapter 2 provides an introduction to wireless sensor networks. It discusses the evolution of WSNs, the differences between WSNs and traditional ad hoc wireless networks, possible WSN applications, factors that influence the design of WSNs and concludes with a discussion of emerging standards in WSNs.

WSN routing protocols are investigated in Chapter 3. The challenges and design issues related to WSN routing are discussed and a classification of WSN protocols follows. A thorough overview of some of the available protocols is then given and the chapter ends with a comparison of these.

Chapter 4 emphasizes on design motives and working of existing DEAR protocol.

In Chapter 5, the protocol designed during this research (DEAR2 and DEAR3) in stages is described. The chapter starts off with a discussion of the design goals of the protocol and how the goals were achieved. The chapter then gives an explanation of the operation of the protocol.

Comprehensive simulation results and an analysis of each set of results are presented in Chapter 6.

Future scope is highlighted in Chapter 7

This research is concluded in Chapter 8.

Chapter 2

Introduction to Wireless Sensor Network

2.1 History of Wireless Sensor Networks

2.1.1 Early Research on Military Sensor Networks

As with many technologies, defence applications have been a push for research and development in sensor networks. During the Cold War, the Sound Surveillance System (SOSUS), a system of acoustic sensors (hydrophones) on the ocean bottom, was deployed at strategic locations to detect and track quiet Soviet submarines ([13, 14]). Subsequently, during the Cold War, networks of air defence radars were developed and deployed to defend the continental United States and Canada.

These sensor networks generally adopt a hierarchical processing structure where processing occurs at consecutive levels until the information about events of interest reaches the user. Even though research was focused on satisfying mission needs, e.g., acoustic signal processing and interpretation, tracking, and fusion, it provided some key processing technologies for modern sensor networks. Both of these sensor networks were wired networks that did not have the energy or bandwidth constraints of wireless systems are two of the main design issues related to WSN routing protocols.

2.1.2 Distributed Sensor Networks Program at the Defense Advanced Research Projects Agency

Modern research on sensor networks started around 1980 with the Distributed Sensor Networks (DSN) program at the Defense Advanced Research Projects Agency (DARPA). By this time, the Arpanet (predecessor of the Internet) had been operational for a number of years, with about 200 hosts at universities and research institutes. The Distributed Sensor Networks (DSN) program, as it was known, assumed a network with many independent, low-cost sensing nodes that were spatially distributed but able to collaborate ([15], [16]). Information was routed to the node that could use it best.

Researchers at Carnegie Mellon University (CMU), Pittsburgh, PA, focused on providing a network operating system that allows flexible, transparent access to distributed resources needed for a fault-tolerant DSN ([17], [18]).

Researchers at the Massachusetts Institute of Technology (MIT), Cambridge, focused on knowledge-based signal processing techniques [19] for tracking helicopters using a distributed array of acoustic microphones by means of signal abstractions and matching techniques. Microphones, arranged in arrays of six, were used for the acoustic sensing. The mobile vehicle nodes consisted of one computer and three processors, with 256kB memory and 512kB shared memory, processing the acoustic signals [U16-20]. Energy was supplied by an acoustically quiet generator, mounted on the back of the vehicle node. The nodes communicated with microwave radio and Ethernet was used for fixed line communication. One of the mobile vehicle nodes and the equipment rack of the node are shown in Figure 2.1

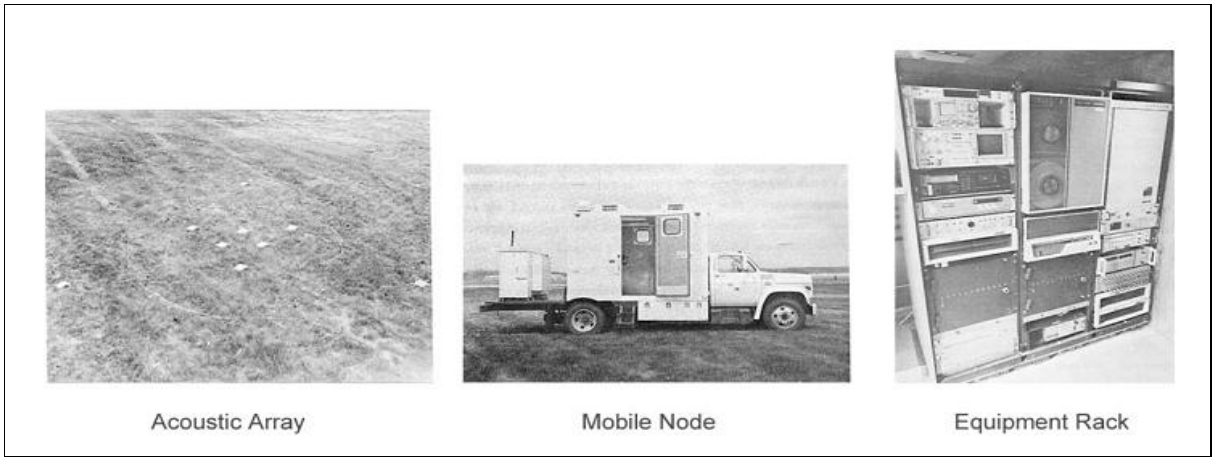


Figure 2.1 Components in DSN test node in 1985

2.1.3 Sensor Network in 21st Century

Recent advances in computing and communication have caused a significant shift in sensor network research and brought it closer to achieving the original vision. Small and inexpensive sensors based upon microelectromechanical system (MEMS) [21] technology, wireless networking, and inexpensive low-power processors allow the deployment of wireless ad hoc networks for various applications.

The recently concluded DARPA Sensor Information Technology (SensIT) program [22] pursued two key re-search and development thrusts. First, it developed new networking techniques. In the battlefield context, these sensor devices or nodes should be ready for rapid deployment, in an ad hoc fashion, and in highly dynamic environments. The second thrust was networked information processing, i.e., how to extract useful, reliable, and timely information from the deployed sensor network. This implies leveraging the distributed computing environment created by these sensors for signal and information processing in the network, and for dynamic and interactive querying and tasking the sensor network.

SensIT networks have developed new capabilities [23]. The networks are interactive and programmable with dynamic tasking and querying. A multitasking feature in the system allows multiple simultaneous users.

2.2 Trends in Technology

Current sensor networks can exploit technologies not available 20 years ago and perform functions that were not even dreamed of at that time. Sensors, processors, and communication devices are all getting much smaller and cheaper.

Wireless networks based upon IEEE 802.11 standards can now provide bandwidth approaching those of wired networks. At the same time, the IEEE has noticed the low expense and high capabilities that sensor networks offer.

	(1980's - 1990's)	(2000 – 2003)	(2010)
Manufacturer	Custom contractors, eg for TRSS	Commercial: Crossbow Technology, Inc. Sensoria Corp., Ember Corp.	Dust, Inc. and others to be formed
Size	Large shoe box and up	Pack of cards to small shoe box	Dust particle
Weight	Kilograms	Grams	Negligible
Node architecture	Separate sensing processing and communication	Integrated sensing, processing and communication	Integrated sensing, processing and communication
Topology	Point-to-point, star	Client server, peer to peer	Peer to peer
Power supply lifetime	Large batteries, hours, days and longer	AA batteries, days to weeks	Solar, months to year
Deployment	Vehicle-placed or air-drop single sensors	Hand-emplaced	Embedded, "sprinkled" left-behind

Table 2.1: Three Generation of Sensor Networks

Looking into the future, we predict that advances in MEMS technology will produce sensors that are even more capable and versatile [24].

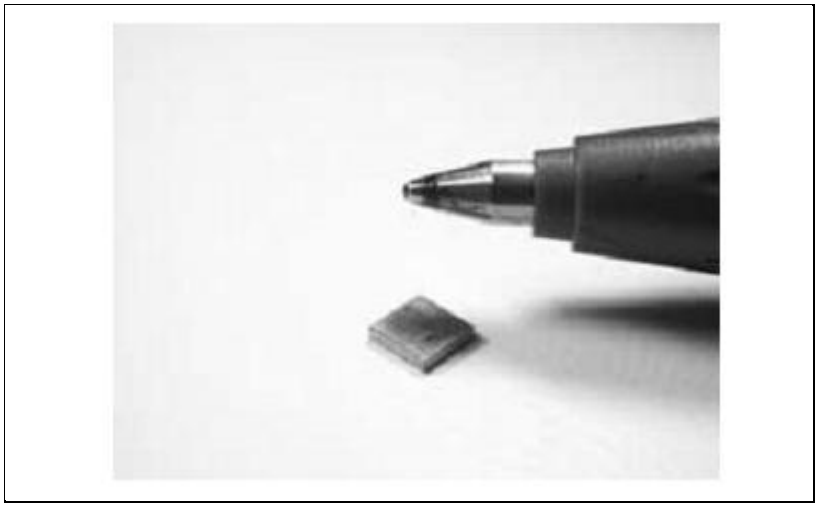


Figure 2.2: Wireless Sensor Node in near Future

2.3 New Applications

The availability of low-cost sensors and communication networks has resulted in the development of many other potential applications apart from defence which include the following

2.3.1 Infrastructure Security

Critical buildings and facilities such as power plants and communication centers have to be protected from potential terrorists. Networks of video, acoustic, and other sensors can be deployed around these facilities. These sensors provide early detection of possible threats. Improved coverage and detection and a reduced false alarm rate can be achieved by fusing the data from multiple sensors. Examples of such networks can be found in [25], which also describes other uses of sensor networks.

2.3.2 Environment and Habitat Monitoring

Environment and habitat monitoring [26] is a natural candidate for applying sensor networks, since the variables to be monitored, e.g., temperature, are usually distributed over a large region. The recently started Center for Embedded Network Sensing (CENS) [27], Los Angeles, CA, has a focus on environmental and habitat monitoring.

2.3.3 Industrial Sensing

Commercial industry has long been interested in sensing as a means of lowering cost and improving machine (and perhaps user) performance and maintainability. Monitoring machine "health" through determination of vibration or wear and lubrication levels, and the insertion of sensors into regions inaccessible by humans, are just two examples of industrial applications of sensors [28].

2.3.4 Traffic Control

Sensor networks have been used for vehicle traffic monitoring and control for quite a while. Most traffic intersections have either overhead or buried sensors to detect vehicles and control traffic lights. Furthermore, video cameras are frequently used to monitor road segments with heavy traffic, with the video sent to human operators at central locations.

However, these sensors and the communication network that connect them are costly; thus, traffic monitoring is generally limited to a few critical points [28].

2.4 Technical Challenges

2.4.1 Ad Hoc Network Discovery

Knowledge of the network is essential for a sensor in the network to operate properly. Each node needs to know the identity and location of its neighbours to support processing and collaboration. In planned networks, the topology of the network is usually known a priori. For ad hoc networks, the network topology has to be constructed in real time, and up-dated periodically as sensors fail or new sensors are deployed [29]. In the case of a mobile network, since the topology is always evolving, mechanisms should be provided for the different fixed and mobile sensors to discover each other [30].

2.4.2 Network Control and Routing

The network must deal with resources—energy, band-width, and the processing power—that are dynamically changing, and the system should operate autonomously, changing its configuration as required. Since there is no planned connectivity in ad hoc networks, connectivity must emerge as needed from the algorithms and software. Since communication links are unreliable and shadow fading may eliminate links, the software and system design should generate the required reliability. This requires research into issues such as network size or the number of links and nodes needed to provide adequate redundancy.

One of the benefits of not requiring IP addresses at each node is that one can deploy network devices in very large numbers. Also, in contrast to the case of IP, routes are built up from geo-information, on an as-needed basis, and optimized for survivability and energy. This is a way to form connections on demand, for data-specific or application-specific purposes. IP is not

likely to be a viable candidate in this context, since it needs to maintain routing tables for the global topology, and because updates in a dynamic sensor network environment incur heavy overhead in terms of time, memory, and energy.

Survivability and adaptation to the environment are ensured through deploying an adequate number of nodes to provide redundancy in paths, and algorithms to find the right paths. Diffusion routing methods, which rely only upon information at neighbouring nodes, are a way to address this [31], although such methods may not achieve the information-theoretic capacity of a spatially distributed wireless network [32].

2.4.3 Collaborative Signal and Information Processing

The nodes in an ad hoc sensor network collaborate to collect and process data to generate useful information. Collaborative signal and information processing over a network is a new area of research and is related to distributed information fusion. Important technical issues include the degree of information sharing between nodes and how nodes fuse the information from other nodes.

2.4.4 Tasking and Querying

A sensor field is like a database with many unique features. It is important that users have a simple interface to interactively task and query the sensor network. An example of a human-network interface is a handheld unit that accepts speech input. The users should be able to command access to information, e.g., operational priority and type of target, while hiding details about individual sensors.

It is important that users have a simple interface to interactively task and query the sensor network. An example of a human-network interface is a handheld unit that accepts speech input. The users should be able to command access to information, e.g., operational priority and type of target, while hiding details about individual sensors [33].

2.4.5 Security

Since the sensor network may operate in a hostile environment, security should be built into the design and not as an afterthought. Network techniques are needed to provide low-latency, survivable, and secure networks. Low probability of detection communication is needed for networks because sensors are being envisioned for use behind enemy lines. For the same reasons, the network should be protected again intrusion and spoofing.

2.5 Diff between WSN and other Ad-hoc networks

A wireless ad hoc network (WANET) is a temporary network that is set up between peer nodes to satisfy an immediate need [34]. Many protocols exist for wireless ad hoc networks, but are unsuitable for WSNs due to the unique requirements of WSNs. According to Akyildiz et al. [35], WSNs differ from other WANETs in seven areas, namely: network size, node density , node proneness to failure, frequency of topology changes , communication paradigm employed , resource limitations of nodes and node identification . Each of these areas is discussed in the following paragraphs.

The network size of a WSN can be anything from a few nodes up to many thousands of nodes. Other WANETs on the other hand usually consist of less than a hundred nodes. A Bluetooth piconet, which can consist of up to a maximum of eight nodes, is an example of a WANET. A wireless local area network (WLAN) is another example of a WANET. WLAN is based on the IEEE 802.11b standard, which was developed by the Institute of Electrical and Electronic Engineers (IEEE). The size of a WLAN is limited to 32 nodes per access point [R18-36].

Node density in a WSN is usually high, with a large number of nodes in a relatively small area, while other WANETs mostly consist of only a few nodes in close proximity of each other. This is due to the size of nodes. A WSN node can be as small as a one Euro coin, while nodes of other WANETs are mostly notebook computers, palmtops or cellular telephones.
A WSN might be deployed in a remote or inaccessible area, such as a jungle or a disaster area. In such circumstances the node proneness to failure is high due to the possibility of nodes being damaged and failing. Some nodes might also drain their energy resources quicker than other nodes due to being on a routing path that is utilized more than other paths. Nodes in

other WANETs have rechargeable energy supplies and are not subjected to adverse environmental conditions that could damage them to the extent of not being able to function any longer.

The frequency of topology changes in a WSN is high, due to factors such as node failures, node additions, nodes moving and environmental interference. The network has to be able to adapt to these changes in node position and number. Topology changes can happen as frequently as every few milliseconds. In other WANETs, nodes usually request to join the network and leave the network after a certain period of time, which is rarely less than a couple of minutes.

The communication paradigm employed in WSNs includes a large number of broadcasts that are sent through the network. These broadcasts are used for network set up and maintenance, discovery of neighbours and sending of data. Other WANETs usually use point to point communications, since the source knows how to reach the destination.

The resource limitations of nodes in WSNs include limited energy and bandwidth resources, compared to other WANETs. The energy resources of WSN nodes cannot be replenished, while other WANETs' nodes have rechargeable batteries. The limited data rate of up to a few kilobits per second in WSNs is small compared to data rates of between one and a few hundred megabits per second in other WANETs. The memory of WSN nodes is limited to a few kilobytes, while other WANETs' nodes can have gigabytes of memory. The processors employed in WSN nodes are limited. The TUV WSSN nodes, for example, use 4MHz processors. This is very limited, compared to the GHz processors of notebook computers.

Node identification by means of globally unique identifiers are not always possible in WSNs, due to the possibly very large number of nodes in the network and the overhead caused by having a unique identifier for each node. In other WANETs, the nodes have unique identifiers such as internet protocol (IP) addresses.

The WSN is a new and unique class of WANET that differs considerably from other WANETs. The unique nature of WSNs implies that protocols designed for other WANETs cannot be implemented in WSNs and, therefore, new protocols have to be developed

2.6 Wireless networking standards

In March 1999, the IEEE established the 802.15 working group as part of the IEEE computer Society's 802 Local and Metropolitan Area Network Standards Committee. The 802.15 working group was established with the specific purpose of developing standards for short distance wireless networks, otherwise known as wireless personal area networks (WPANs). There exist four task groups within the 802.15 working group. Task group one (802.15.1) defined a standard for WPANs based on the physical (PHY) and MAC layers of the Bluetooth specification version 1.1 [37]. Task group two (802.15.2) is developing a model for the coexistence of WLAN (802.11) and WPAN (802.15). The goal of task group three (802.15.3) is to develop standards for high data rate WPANs (20Mbps and greater). Task group four (802.15.4) is responsible for developing PHY an d MAC layer standards for low data rate, low complexity solutions that will achieve battery lifetime of months to years.

2.6.1 IEEE 802.15.1 and Bluetooth

Bluetooth was designed to be a short range (less than 10m), low cost (less than $5), and low power (1 to 100mW) wireless cable replacement technology to provide communication between portable devices and desktop machines and peripherals. The Bluetooth radio transceivers operate in the globally available, unlicensed 2.4 GHz ISM radio band. Bluetooth uses frequency-hopping spread spectrum (FHSS) and hops at a rate of 1600 hops/s [37].

The basic unit of a Bluetooth network is a piconet. A piconet consists of between two and eight nodes. One node is the master and up to seven active slave nodes may be connected to it. The limit of seven slaves is due to the three bit address used for active slaves in a piconet. Three bits allows eight addresses but the all zeros address is reserved for broadcasts, thus seven addresses are available for slaves. The master's clock is used to synchronize communication within a piconet. All communication within a piconet is routed via the master. When a node participates in more than one piconet, the piconets become linked and a

scatternet is formed. A node participating in more than one piconet is called a gateway and uses Time Division Duplex (TDD) in order to be active in only one piconet at a time.

The IEEE 802.15.1 specification defines a standard for the PHY and MAC layers of WPANs, based on the Bluetooth specification. In particular, the logical link control and adaptation protocol (L2CAP), link manager protocol (LMP), and Baseband layers of the Bluetooth protocol stack form the 802.15.1 MAC layer and the Radio layer of the Bluetooth protocol stack forms the PHY layer of 802.15.1. The MAC layer is responsible for the time synchronisation of the FHSS communication and the PHY layer specifies the communication band (2.4GHz)

2.6.2 IEEE 802.15.3a and Ultrawideband

The United States (US) military developed Ultrawideband (UWB) in the 1970s for various uses including low-power communications cap able of evading mainstream eavesdropping techniques. UWB is an impulse radio as opposed to carrier-based radio which transmits data continuously [38]. UWB typically transmits signals via sub-nanosecond pulses of energy operating at about 100nW per MHz of transmission bandwidth. The IEEE's proposed UWB standard would increase the pulse duration to 4 nanoseconds.

UWB sends the various pulses of a single transmission over a relatively large part of the radio spectrum, not just at a specific frequency or narrow frequency range, as is the case with cellular-phone and other radio-based technologies. The US Federal Communications Commission (FCC) has allocated UWB the spectrum 3.1-10.6GHz, currently used by satellite based telecommunications providers. This was done to avoid potential interference with radio-based technologies that use other parts of the spectrum. UWB's data rate is typically 200-400Mbps. The proposed IEEE standards would le t UWB run anywhere from 110Mbps over 10 metres to 480Mbps over 1 metre [38].

The end result of UWB is a technology that provides simplicity, very low transmit power, multipath and interference immunity, and the capability to deliver data rates in excess of

100Mbps; all the while consuming very little battery power and relatively small amounts of silicon area, translating to low cost.

2.6.3 IEEE 802.15.4 and ZigBee

In 2002 the non-profit ZigBee Alliance was formed by an association of companies. The goal of the ZigBee Alliance is to develop monitoring and control products that are reliable, low cost, low power and can be wirelessly networked using an open global standard. Task group four of the IEEE 802.15 working group started working on a standard for low data rate WPANs shortly thereafter. The IEEE and the ZigBee Alliance joined forces and decided that ZigBee would be the commercial name of the technology.

Potential applications of the 802.15.4 standard include sensors, home automation, smart badges, remote controls, and interactive toys [39], amongst others. The standard specifies two direct sequence spread spectrum (DSSS) PHY layers and the use of three license free frequency bands. One PHY layer is at 868/915MHz and uses the 868-870MHz band with one channel and the 902-928MHz band with ten channels. This PHY achieves a data rate of 20kbps in the 868-870MHz band and 40kbps in the 902-928MHz band. The other PHY is at 2.4GHz and uses the 2.4-2.4835GHz frequency band with sixteen channels. It achieves a data rate of 250kbps. Table 2.2 summarises the frequency band and data rates of the 802.15.4 standard.

PHY	BAND	Channel Numbering	Chip Rate	Modulation	Bit Rate
868/915 MHz	868-870MHz 902-928MHz	0 1 to 20	300 Kchip/s 600 Kchip/s	BPSK BPSK	20kbps 40kbps
2.4GHz	2.4-2.4835GHz	11 to 26	2 Mchip/s	O-QPSK	250 kbps

Table 2.2: 802.15.4 frequency bands

The 802.15.4 standard supports two addressing modes, namely 16 bit short and 64 bit IEEE addressing. The PHY layer also has features for link quality indication, receiver energy detection and clear channel assessment. A maximum packet size of 128 bytes, with a payload of up to 104 bytes, is supported along with bot h contention-based and contention-free

channel access. The MAC layer uses full handshaking for reliability and carrier sense multiple access with collision avoidance (CSMA-CA) for channel access.

Zigbee defines three software layers [40] (network, security and application) on top of the PHY and MAC 802.15.4 layers. The network layer supports three network topologies, namely star, mesh or peer-to-peer, and cluster tree as shown in Figure 2.6. The 802.15.4 standard specifies two types of nodes: a full function device (FFD) and a reduced function device (RFD). A FFD is able to route data, while a RFD is not. The standard also specifies that the network be coordinated by at least one FFD. A star topology promotes long battery lifetime since every RFD is connected directly to the coordinator. A mesh or peer-to-peer topology provides reliability and scalability since all the nodes are FFDs and therefore can be interconnected. This introduces multiple routing paths. The cluster tree topology combines aspects of both the star and mesh topologies and tries to provide long battery lifetime as well as reliability and scalability.

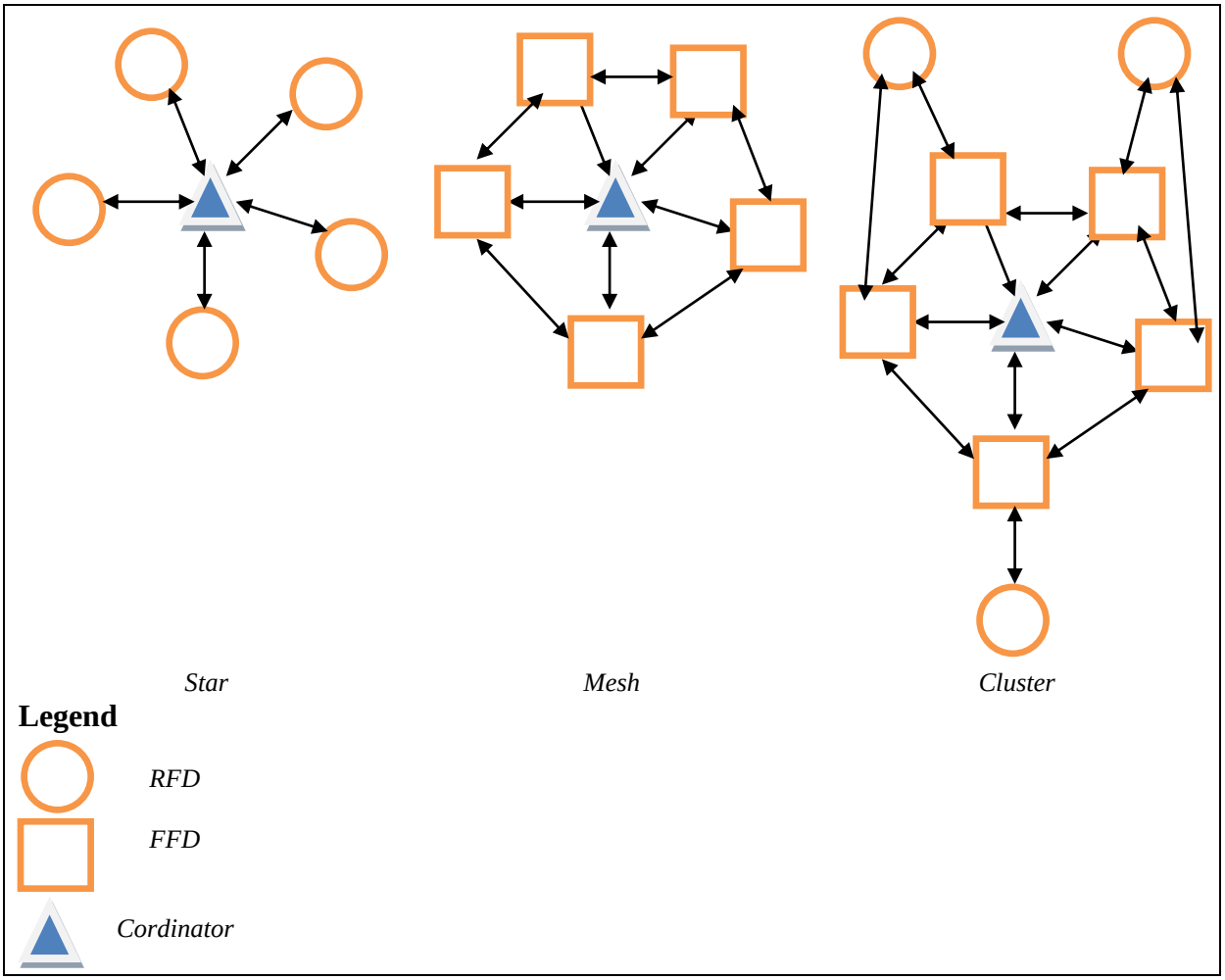


Figure 2.3: Node structure of 802.15.4

The routing protocol used in ZigBee is based on the ad hoc on demand distance vector (AODV) routing protocol, Motorola's Cluster-Tree protocol and some ideas from Ember Corporation's GRAD. It is a hierarchical routing protocol with some table-driven optimisations. AODV is a well-known reactive ad hoc network routing protocol. The AODV protocol works on a query-reply route discovery exchange, where a routing query is flooded through the network until it reaches its destination [41]. Each node along the path to the destination keeps track of which of its neighbours originated the specific route query. The destination then unicasts the reply back to the source along a path constructed during the query. This path is calculated from the next hop information stored at each node along the path.

The security layer adds the ability to encrypt the MAC layer frames with 32, 64 or 128 bit Advanced Encryption Standard (AES) encryption. The application layer defines profiles that aim to enable interoperability. It also enables nodes to determine which other devices are within their vicinity and makes it possible to match devices based on their services

2.6.4 Comparison of networking standards

There are many different standards for wireless networks. These standards divide wireless networks into categories based on factors such as network size, data rate, and transmission range and battery lifetime. Table 2.3 shows a comparison of three important wireless network standards.

Market Name	**Wi-Fi**	**Bluetooth**	**ZigBee**
Standard	**IEEE 802.11b**	**IEEE 802.15.1**	**IEEE 802.15.4**
Type of Network	WLAN	WPAN	WPAN
Application Focus	Web, Email, Video	Cable Replacement	Monitoring and Control
System Resources	1MB+	250KB+	4KB – 32KB
Battery Life (days)	0.5-5	1-7	100-1000+
Network Size	32	7	255/65000
Data rate (kbps)	11000+	720	20-250
Transmission Range (meters)	1-100	1-10+	1-100+
Success Metrics	Speed, Flexibility	Cost, Convenience	Reliability, Power, Cost

Table 2.3: Comparison of Networking Standards

Chapter 3

WSN Routing Protocols

3.1 Factors influencing Routing Protocols

The main design challenge in WSNs is to prolong network lifetime while keeping communication integrity. This is complicated by the fact that nodes in a WSN are constrained in energy supply, processing capability and available bandwidth. There are many factors related to the inherent characteristics of WSNs that have to be considered in order to design an efficient WSN routing protocol. These factors include: node deployment, data reporting method, node and link heterogeneity, reliability, energy consumption, scalability, network dynamics, transmission media, connectivity, coverage, data aggregation and quality of service [42].

Node deployment can be either manual or random. If nodes are manually deployed, the routing in the network can be done using predetermined paths. Random deployment, on the other hand, requires routing paths to be established in an ad hoc fashion. Due to the limited transmission range of nodes, the routing path will most likely be multi-hop. The density of node deployment also plays a role in network survivability. It is preferable that the density be higher close to the sink, since all of the data from all the nodes in the network are routed through the nodes surrounding the sink.

Data reporting in WSNs depends on the time criticality of data and on the WSN application. Data reporting can be time-driven, query-driven, event-driven or some mixture of these methods. Time-driven reporting occurs when sensor nodes periodically switch on their sensors and transmitters, to transmit sensed environmental data that is of interest. Event-driven reporting occurs when nodes react to drastic changes sensed in their environment. Query-driven reporting occurs when nodes respond to queries for data. Event-driven and query-driven methods can be used for situations where data delivery is time critical. The data reporting method has a big influence on the routing protocol in terms of route calculation and energy consumption.

Node heterogeneity has to do with the fact that sensor nodes might have different capabilities or different roles within the network. This is mostly the case in hierarchical or cluster networks. Some nodes in the network are assigned the role of cluster head. Cluster head nodes might be nodes with different capabilities in terms of energy resources, processing capability and bandwidth, compared to other nodes in the network. If they have enhanced capabilities, they remain cluster heads throughout the lifetime of the network. In the case where all the nodes in the network have the same capabilities, the cluster heads are assigned at periodic intervals. These assigned cluster heads have to be rotated to prevent energy hotspots from forming. Link heterogeneity has to do with the fact that some nodes might be required to send data more frequently than other nodes in the network and that more than one data reporting method might be used in the same network. The routing protocol employed has to consider the capabilities of the different nodes in the network and has to be able to route data at different rates, if necessary.

Reliability is an important issue in sensor networks since the nodes are pr one to failure. Node failures may be due to nodes depleting their energy sources or physical damage or environmental interference. The overall network functionality should not be compromised when some of the nodes fail. Node failures lead to areas losing sensor coverage and might cause data to be lost if a node has received data and fails before it can transmit the data. The routing protocol has to route packets through regions of the network where there are higher levels of available energy if failures occur.

Energy consumption in sensor nodes occurs mainly due to computational processing and communication. WSNs are usually multi -hop networks. If a node fails in such a network, the topology changes and rerouting of da ta and network reorganisation might have to occur. Therefore, it is essential to apply energy conserving techniques in computation and communication. Communication energy conservation can be achieved by limiting the packet sizes of the data to be sent and by limiting the number of packets that are routed through the network. Computational energy efficiency can be achieved by limiting the number of computational tasks to be done by a node, in other word s: making the routing protocol as simple as possible.

Scalability is needed in sensor networks due to the fact that the number of nodes in the network could be anything from a few nodes to a few thousand nodes or more. A routing protocol used in a WSN has to be able to function efficiently with any number of nodes. Network dynamics has to do with the mobility of nodes. In some networks the nodes are fixed while in others, the nodes are mobile. If sensor nodes or the sink node are mobile, routing becomes more difficult since static routes cannot be used. The events to be monitored might also be of a mobile nature, for instance if the network is used for vehicle tracking. In such a scenario the routing is reactive (routes are established as needed). Routing in a network where the events are static might use a table-driven approach (each node keeps a routing table).

Transmission media in WSNs can be any wireless communication link. WSNs also face the problems associated with wireless channels, such as fading, noise and interference. Efficient use of the transmission media is related more to the MAC layer. The MAC layer might use a time division multiple access (TDMA) channel access method or a contention based channel access method such as CSMA. The TDMA method generally consumes less energy than the CSMA method [43]. The data rate of the wireless communication media in a WSN is usually in the order of 1-100kbps, which is low compared to other wireless networks. This is an important consideration for the design of the routing protocol since large network layer packets will result in more than one packet being transmitted every time the sensor node needs to send data. The network layer packets have to be kept small in order to limit the number of required transmissions for new sensed data.

Connectivity in WSNs is assumed to be high due to the high node density. The large number of nodes in a WSN makes it unlikely that nodes will be isolated. The connectivity will however decrease as nodes fail. As the connectivity changes due to topology changes, the routing paths also change.

Coverage in WSNs deals with the range and accuracy of the sensing that a sensor node can achieve. This limited area coverage of sensor nodes makes it important to have densely deployed nodes; otherwise there might be some areas that are not covered by the WSN. If node density is low, it also causes nodes to be cut off from the network more easily since there are fewer paths to the sink. Therefor e network partition occurs sooner.

Data aggregation is very important in WSNs since the density of nodes results in a great deal of redundant data being sent through the network. A node in a WSN might receive the same sensed data from more than one neighbour. Transmitting the data more than once would result in energy wastage. Data aggregation can be done using duplicate suppression, maxima, minima or average [42]. Duplicate suppression occurs when a node discards messages that it has already received. This is the simplest form of data aggregation. Data aggregation using maxima, minima and average can also be called data fusion. In the case of data fusion, the data that a node receives from its neighbours is combined and only the maximum, minimum or average of all the received messages is transmitted in a single message. Data aggregation can reduce the number of messages that are routed through the network but can introduce latency if data fusion is used, since nodes have to wait to receive data from all of their neighbours before transmitting the combined data. Timing has to be considered since a node cannot simply wait until it has received data from all of its neighbours as one neighbour might have failed. A time limit has to be set for each round of data transmissions and after that time has elapsed, the data is sent even if the node has not received data from all of its neighbours.

Quality of service in WSNs mostly deals with latency and reliability. Some WSN applications require that sensed data reach the sink within a certain amount of time in order to be useful. An example of a time critical application might be vehicle tracking. If the latency in the network is high, the vehicle might be far from the reported position by the time the data arrives at the sink. In other applications the da ta from nodes might not be critical in terms of

latency but critical in terms of being delivered. Such critical data might have adverse effects on the network if undelivered. An example of an application with data that is critical but not time critical might be a WSN that monitors the number of working lights in a shopping centre. If a light fails, it is important that it be replaced but it does not have to be replaced within seconds.

3.2 Classification of Routing Protocols

WSN routing protocols can be classified in three ways: according to the way routing paths are established [44], according to the network structure [42] and according to the initiator of communications. The classification of WSN routing protocols is shown in Figure 3.1.

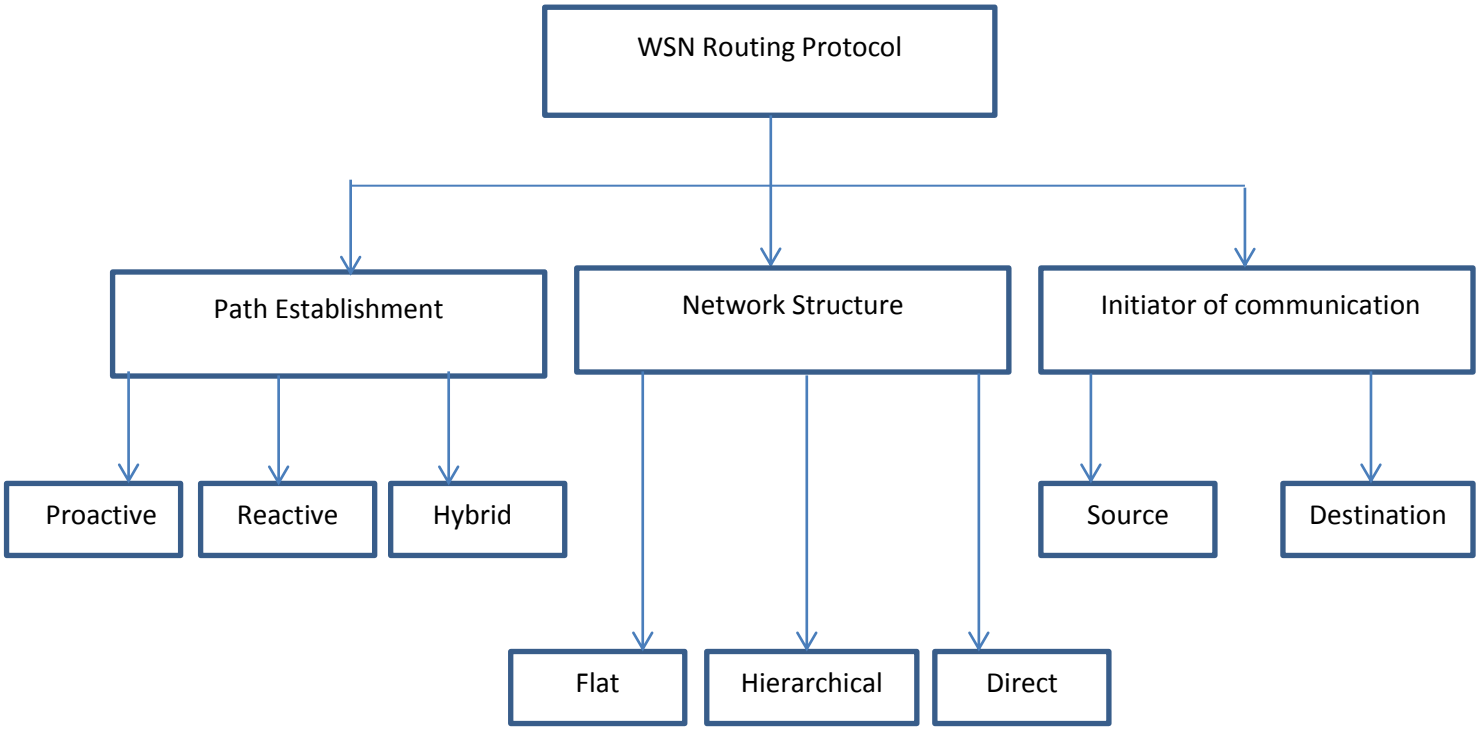


Figure 3.1: Classification of WSN Routing Protocols

Routing paths can be established in one of three ways, namely proactive, reactive or hybrid. Proactive protocols compute all the routes before they are really needed and then store these routes in a routing table in each node. When a route changes, the change has to be propagated throughout the network. Since a WSN could consist of thousands of nodes, the routing table that each node would have to keep could be huge and therefore proactive protocols are not suited to WSNs. Reactive protocols compute routes only when they are needed. Hybrid protocols use a combination of these two ideas.

There are basically three possible network structures for WSNs. They are: flat, hierarchical and direct. Direct communication is impractical in WSNs since it requires that all of the nodes be one hop away from the sink. In flat protocol s, all the nodes in the network are equal and can participate equally in the routing task. Nodes close to the sink participate more than nodes further away since all of the messages destined for the sink pass through the nodes around it.

In hierarchical or clustering protocols, the network is subdivided into clusters of nodes and each cluster has a cluster head. The nodes within a cluster send messages only to the cluster head. The cluster head then in turn forwards all messages of its cluster towards the sink. Communication within a WSN can be initiated either by the source of data or by the destination of the data. In source initiated protocols, nodes send data to the sink when they have data of interest. Source initiated protocols use time-driven or event-driven data reporting.

This means that data is sent either at certain intervals or when nodes sense certain events. Destination originated protocols use query-driven reporting and nodes respond with data to queries that are sent by the sink or another node. Destination-initiated protocols incur a large amount of overhead since requests are usually flooded through the network. This means that every request for data will result in a flooding of the network.

Most routing protocols can be divided into either flat or hierarchical protocols at the highest level and can then be further divided into source initiated or destination initiated protocols. Routing path establishment in WSNs is generally reactive.

A discussion of some of the available routing protocols is given in the following sections.

3.3 Proactive Routing Protocols

3.3.1 Minimum Cost Forwarding Algorithm

The minimum cost forwarding algorithm (MCFA) assumes that the direction of routing is always known. MCFA is a source initiated protocol that uses a flat network structure and

proactive routing. Nodes need not have unique IDs and instead of maintaining routing tables nodes maintain the least cost estimate from them to the sink. The sink node sets its minimum cost to zero while all the nodes in the network set their initial costs to infinity. The sink then broadcasts a message with its cost. A node receiving the broadcast updates its cost if the cost in the message plus the cost of the link is lower than the current cost. The metric used in the link cost could be hop count, delay, etc. If the new cost is lower, the node rebroadcasts the message, otherwise it discards it and thus, establishes a minimum cost at each node in the network. A node broadcasts the message to be sent to all its neighbours. A node that receives such a message checks whether it is on the least cost path to the sink. If it is on the least cost path, it rebroadcasts the message to all of its neighbours. This is repeated until the message reaches the sink. One problem of MCFA is that nodes will deplete energy along certain paths if the minimum cost is not update d regularly. Another problem is that if hop count is used as the cost or if nodes are uniformly distributed and energy expenditure is used as the cost, multiple nodes will consider themselves on the minimum cost path and the protocol is reduced to flooding.

3.3.2 Energy Aware Routing

Energy aware routing is similar to directed diffusion but maintains multiple paths at each node instead of just one. It is a destination initiated protocol that uses a flat network structure and proactive routing. Based on the energy metric, each path is assigned a probability of being chosen among the multiple paths between source and destination. When data is to be sent, a path is chosen based on its probabilities. Diffusion sends data along all paths at regular intervals, while energy aware routing sends data only along one path at all times. The protocol has three phases. In the first phase which is the setup phase, localized flooding is used to build routing tables. During the data communication (second) phase, data is delivered from source to destination. The final phase is the route maintenance phase which uses periodic localized flooding to maintain routes. Assumptions such as that all the nodes are location aware and that interests are sent only to nodes that are closer to the source and further away from the destination, in the direction of the source pose some serious problems for the protocol to work. Another problem is that protocol requires nodes to have two transceivers. The route setup is also very complicated since the nodes have to be addressed according to location and the node type.

3.3.3 DSDV

The destination sequenced distance vector routing protocol is a proactive routing protocol which is a modification of conventional Bellman-Ford routing algorithm. This protocol adds a new attribute, sequence number, to each route table entry at each node. Routing table is maintained at each node and with this table, node transmits the packets to other nodes in the network. This protocol was motivated for the use of data exchange along changing and arbitrary paths of interconnection which may not be close to any base station.

Each node in the network maintains routing table for the transmission of the packets and also for the connectivity to different stations in the network. These stations list for all the available destinations, and the number of hops required to reach each destination in the routing table. The routing entry is tagged with a sequence number which is originated by the destination station. In order to maintain the consistency, each station transmits and updates its routing table periodically. The packets being broadcasted between stations indicate which stations are accessible and how many hops are required to reach that particular station. The packets may be transmitted containing the layer 2 or layer 3 address.

Routing information is advertised by broadcasting or multicasting the packets which are transmitted periodically as when the nodes move within the network. The DSDV protocol requires that each mobile station in the network must constantly; advertise to each of its neighbors, its own routing table. Since, the entries in the table my change very quickly, the advertisement should be made frequently to ensure that every node can locate its neighbours in the network. This agreement is placed, to ensure the shortest number of hops for a route to a destination; in this way the node can exchange its data even if there is no direct communication link. The data broadcast by each node will contain its new sequence number and the following information for each new route:

–The destination address

–The number of hops required to reach the destination and

–The new sequence number, originally stamped by the destination

3.4 Reactive Routing Protocols

3.4.1 AODV

AODV is a very simple, efficient, and effective routing protocol for Mobile Ad-hoc Networks which do not have fixed topology. This algorithm was motivated by the limited bandwidth that is available in the media that are used for wireless communications. It borrows most of the advantageous concepts from DSR and DSDV algorithms. The on demand route discovery and route maintenance from DSR and hop-by-hop routing, usage of node sequence numbers from DSDV make the algorithm cope up with topology and routing information. Obtaining the routes purely on-demand makes AODV a very useful and desired algorithm for MANETs.

Each mobile host in the network acts as a specialized router and routes are obtained as needed, thus making the network self-starting. Each node in the network maintains a routing table with the routing information entries to it's neighbouring nodes, and two separate counters: a node sequence number and a broadcast-id. When a node (say, source node 'S') has to communicate with another (say, destination node 'D'), it increments its broadcast-id and initiates path discovery by broadcasting a route request packet RREQ to its neighbors. The RREQ contains the following fields:

– Source - address
– Source - sequence # -to maintain freshness info about the route to the source.
– Destination - address
– Destination - sequence # - specifies how fresh a route to the destination must be before it is accepted by the source.
– Hop - count

The (source-address, broadcast-id) pair is used to identify the RREQ uniquely. Then the dynamic route table entry establishment begins at all the nodes in the network that are on the path from Source to Destination.

3.4.2 Flooding and gossiping

The foremost two algorithms to be applied to WSNs were Flooding and gossiping. But flooding has some disadvantages:

- Implosion : Duplicate messages are sent to the same node

- Overlap : Two nodes present in the same region send similar messages to the same neighbour
- Resource Blindness : the nodes do not take energy constraints into consideration

Gossiping avoids implosion by randomly selecting one or a subset of neighbours and then sending the message only to those neighbours which results in propagation delay. Since the two protocols were not designed for energy constrained networks, they do not provide energy efficiency.

3.4.3 Sensor Protocols for Information via Negotiation

Sensor protocol for information via negotiation (SPIN) is a source initiated protocol that uses a flat network structure and reactive routing. SPIN assumes that each node its range possess the same data and hence transmits only those data. The data available at each node gets distributed via the whole network resulting in each node having all the relevant data. Significance of SPIN is that the sensor nodes maintain only the routing information about their immediate neighbours which makes it scalable.

Nodes make use of smaller sized meta-data to describe the available data which helps in eliminating the sending of redundant data through the network. The format of the meta-data is application specific. The main idea behind the protocol is to address the deficiencies of flooding by eliminating the possibility of sending duplicate data by using time-driven reporting.

Data is sent through the network by advertisement and requests that takes place in three stages. In first stage, a node having the relevant data sends an advertisement message (ADV) containing meta-data to its peers. During the second stage, the neighbours interested in the advertised data respond with a request (REQ) for the data. In the final stage, the originating node sends the data (DATA) to all its neighbours that requested the data. This process is then repeated by all of the nodes that have received the data. Figure 3.2 shows the three stages of the SPIN data negotiation process.

SPIN produces a large number of messages if all the data produced at each node in the network is requested by each of its neighbours. The fact that data reporting is time-driven instead of event-driven causes node s to send advertisements even if no new data is available. Another problem with SPIN is the fact that if some nodes between the source and the sink do not request advertised data, the data never reaches the sink. The protocol is valid only if the network is small and only a few peers request for the advertised data.

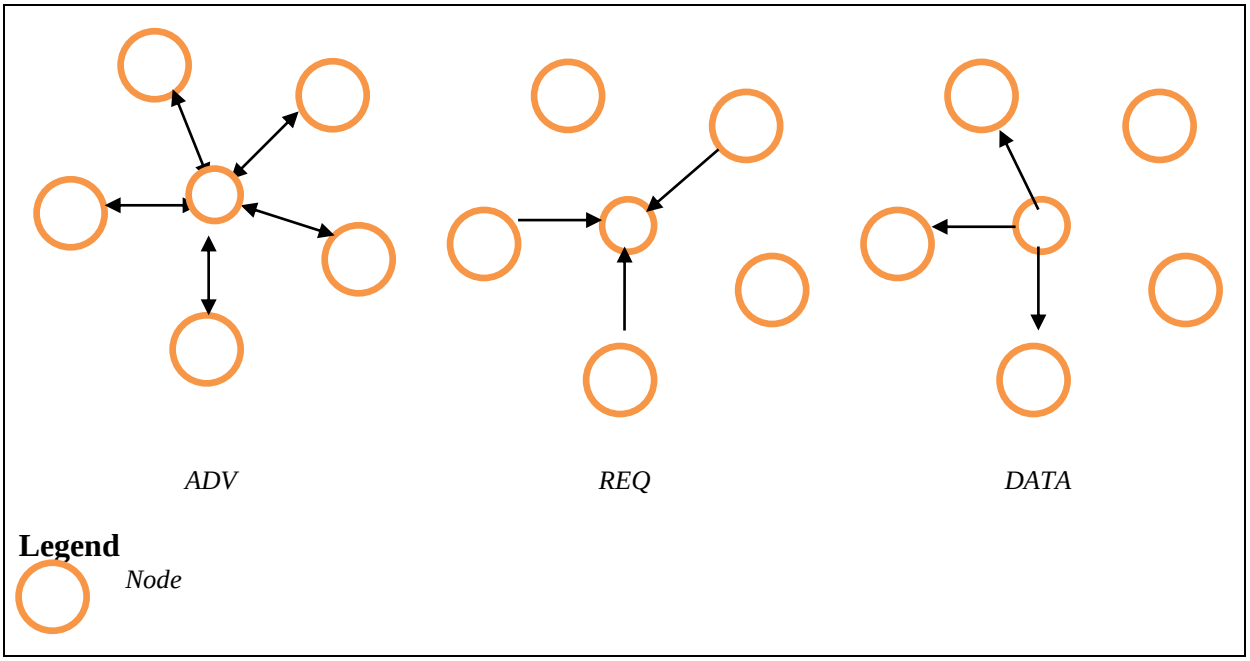


Figure 3.2: Three stages of SPIN data negotiation process

3.4.4 Directed Diffusion

Directed diffusion is probably the best known WSN routing protocol. Many other routing protocols have been derived from it. Directed diffusion is a destination initiated protocol that uses a flat network structure and reactive routing. The protocol uses data-centric routing, where queries are directed at certain areas in the network and not the whole network. Directed diffusion consists of three stages, namely interest diffusion, gradient set up and data delivery.

During the first stage, the sink node floods an interest for named data via the network where named data consists of attribute and value pairs. For e.g. An attribute might be “temperature” and the value might be “33”. A request for the named data might be for the nodes having their temperature greater than 33 should respond with their data. This is one of the efficient ways to

eliminate the possibility of receiving irrelevant data. The initial interest also indicates the initial rate at which the nodes have to send data to the sink, which might be every ten seconds, and includes a timestamp that specifies when nodes can stop sending data, for example after ten minutes. Nodes add the interest to an interest cache which contains an entry for each received interest. The interest entry contains the ID of each neighbour from which the interest was received and the data rate towards that neighbour.

During the second stage of directed diffusion, the nodes match their attribute-value pairs with the interest and start sending data to all the neighbours in the interest cache according to certain data rate. Gradients, which are simply the data rate at which data is sent to a specific interest to a specific neighbour, are also set up for the interest. Directed diffusion also incorporates data aggregation. Nodes receiving data directed at the sink add the data to a data cache. Nodes will check the data cache each time a data message is received to see if the data is new. If the data has already been seen the node will disregard the message. When data reaches the sink, it reinforces one or more paths by sending another interest. This interest is for the same named data but it is sent to a specific destination node along one path and specifies a higher data rate and a longer time before transmission should be stopped. This path might be calculated by sending data only to the node from which the interest response was first received at each hop.

During the final stage of the protocol, a node that has been reinforced sends data towards the sink at the data rate specified in the reinforcement message. Data is sent along the single path that was established. Directed diffusion involves the problem of overhead. The initial replies and interests are flooded which consumes a lot of energy leading to wastage as well. Another problem is of the large memory requirements since each node stores a table containing all the interests that it has received which also contains a sub-entry for each node from which it received that interest. In a large sensor network, there might be many interests and thus tables can grow exponentially. Therefore, directed diffusion cannot be used for applications where data is needed from all of the nodes at frequent intervals.

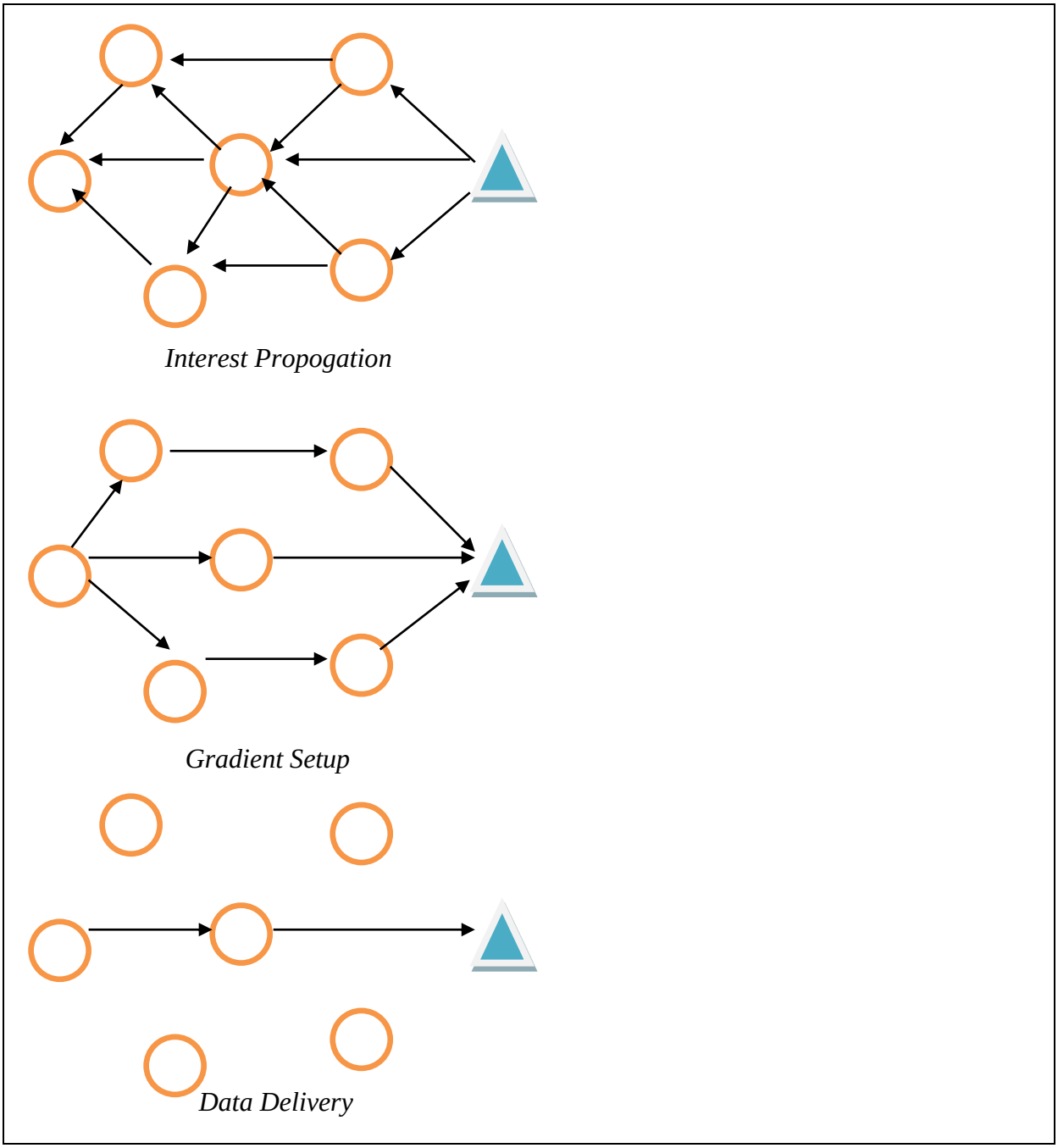


Figure 3.3 Three Stages of Directed Diffusion

3.4.5 Gradient-Based Routing

Based on directed diffusion, gradient-based routing (GBR) is a destination initiated protocol that uses a flat network structure and reactive routing. In this routing, hop count is added to the interest when it is diffused through the network which helps to calculate the height of the node which is the minimum number of hops required to reach the sink. The protocol uses one of the three methods to choose one of the multiple neighbours with same height. First method chooses one of the neighbours at random. Second method is for the nodes to increase their

height if their energy drops below a threshold. The third method is for nodes not to route new message streams through neighbours that are already on a different message stream. Since interests are still flooded through the network, GBR faces the same overhead problem.

3.4.6 Routing protocol with random walks

Routing based on random walks achieve load balancing by multi-path routing. It is a source initiated protocol that uses a flat network structure and reactive routing designed specifically for large networks with static nodes. Each node in the network has a unique ID, but the topology of the network is not practical. Each node in the network is arranged such that it falls on exactly one crossing point of a grid on a plane. In order to find a route it uses a distributed asynchronous version of the Bellman-Ford algorithm to calculate the distance between nodes which is the general case of Djikstra's algorithm. Dijkstra's algorithm is used to calculate single-source shortest paths in a weighted graph, where the weights of the edges of the graph are positive. The Bellman-Ford algorithm does exactly the same except that it is able to work with negative weights. Intermediate nodes in this network will choose the nearest neighbour to the destination according to certain probability. Load balancing is achieved by manipulating this probability. The drawback of this protocol is the impractical required network topology.

3.4.7 Minimum Energy Communication Network

Minimum energy communication network (MECN), proposed by Rodoplu et al. is a location-based protocol that tries to achieve energy efficiency by minimizing the transmission power used by nodes. It is a source initiated protocol that uses a flat network structure and reactive routing. The protocol creates a relay region for nodes which consists of other nodes through which a node can transmit data towards the sink in an energy saving manner. The transmission power needed to reach a node at distance d in any wireless network using radio communication, is proportional to α d. Based on this, the protocol chooses a path from the source to the sink that has more hops with shorter transmission distances, assuming that nodes have variable transmission power. The protocol also assumes that every node in the network is within transmission distance of every other node in the network. The nodes in the network need to be location aware and are assumed to have GPS receivers. This requirement causes the nodes to use excessive amounts of energy. Also the requirement that every node is within

communication distance of every other node is impractical for WSNs. Small minimum energy communication network (SMECN) was derived from MECN and has all of the problems that MECN has. The only differences are that SMECN considers the possibility that there might be obstacles between two nodes, hampering communication and the relay region is smaller.

3.4.8 Comparison of WSN protocols

From the discussion in the previous sections it is apparent that a flat network structure is better for WSNs than a hierarchical structure. A flat network structure can be simple and is scalable. The simplicity that flat network structures can achieve, has to do with the fact that fewer messages are sent through the network and that nodes do not need to perform complex computations to elect cluster heads or to decide which cluster to join. Flat routing protocols can however also be inefficient if they are not designed with the limitations of WSNs in mind. Table 3.1 gives a comparison of the discussed flat routing protocols.

Protocol	**Path Establishment**	**Initiator of Communication**	**Main Problem**
SPIN	Reactive	Source	Large number of messages
Rumour routing	Hybrid	Destination	Large number of messages
Directed diffusion	Reactive	Destination	Large number of messages
MCFA	Proactive	Source	Regular updates needed to prevent node failure
GBR	Reactive	Destination	Large number of messages
Energy aware routing	Proactive	Destination	Requires nodes to have two transceivers
Random walks	Reactive	Source	Irregular network structure required
MECN	Proactive	Source	All nodes have to be within transmission distance of the sink Nodes are required to have GPS

Table 3.1: Comparison of Flat Network Routing Protocols

Chapter 4

Literature Review of DEAR

4.1 Introduction

A fundamental objective of sensor networks is to report events of a predetermined nature or transmit sensed data to sink nodes or the base station for further analysis [45-47]. To achieve this objective, a proper routing algorithm that determines the paths of the data flow should be present.

While considering above basic requirements, the protocol must emphasize on following design issues. (i) The design must allow selection of path which consumes minimum power. (ii) In addition to above, the distribution of data must spread throughout the network in order to increase its lifetime. (iii) Further, the routing algorithm should be robust to diverse event generation methods [48-50] in contrast to most existing algorithms which assume uniform event generation.

The literature review is focussed to study above design factors being addressed in existing DEAR protocols.

4.2 Design Issues

The design of existing DEAR protocol is discussed in this chapter. The goals of DEAR are: scalability, energy efficiency, energy sufficiency, simplicity and practicality. The following sections describe how each of these goals was achieved.

4.2.1 Scalability

WSNs can consist of anything from a few nodes to a few thousand nodes. Therefore a WSN routing protocol has to be scalable. An important factor that influences the scalability of a routing protocol is the network structure. A flat network structure was chosen for DEAR due to the fact that it scales better than a hierarchical network structure. The use of flat network structure implies that every node in the network will be able to participate equally in the routing task.

4.2.2 Energy Sufficiency

Energy sufficiency in a WSN concerns prolonging the lifetime of the network as a whole, by prolonging the lifetime of each individual node. The goal is to have the energy of all of the nodes in the network decrease at more or less the same rate. If some nodes deplete their energy sources sooner than other nodes, the network might become partitioned. As discussed in Section, communication and computational processing are the two factors that consume the most of a WSN node's energy. Therefore, to ensure that nodes survive for as long as possible, DEAR implements some design strategies:

(i) The protocol uses event driven reporting. Here, nodes exchange their battery information. Further, uniform distribution of data throughout the network is observed by selecting paths on the basis of nodes battery information.

4.2.3 Energy Efficiency

Energy efficiency aims to follow the path for transmission which consumes minimum power. The goal is to optimize transmissions and complement the very aspect of Energy Efficiency in prolonging life of network. Therefore, DEAR compute the best path with the aim to aid Energy efficiency using following design strategy.

(i) The protocol is source initiated. This eliminates the need for the sink to flood an interest for data through the network and therefore reduces the number of messages that are transmitted by individual nodes.

4.2.4 Simplicity

The goal of simplicity has two aspects, namely computational simplicity and implementation simplicity. Computational simplicity is achieved by not requiring nodes to do any complex computations during any part of the protocol operation. Implementation simplicity is achieved by making the operation of the protocol easy to understand, so that it can be applied to nodes without difficulty.

4.2.5 Practicality

The goal of practicality sets DEAR apart from most protocols in the literature. Practicality is achieved by designing the protocol such that it functions without dependencies on node capabilities or network layout. DEAR does not require nodes to have specific capabilities, such as GPS positioning, dual transceivers or variable transmit power in order to function. The protocol also functions regardless of the network layout.

4.3 Sensor Network Model

With n homogenous sensors randomly and uniformly distributed over a target area, all sensed data must be sent to the base station. Each sensor has limited battery power. Sensors can control their respective transmission power for minimal consumption to transmit to a destination [53, 54] and they have discrete adjustable transmission power levels [55-58]. This ability is necessary to allow the routing algorithm to maximize sensor networks' operational times. Therefore, sensors can send data to either a neighbour or the base station directly, according to their routing policies [49, 53 -54]. The details of the problem are

4.3.1 Energy Consumption

Each sensor uses a fixed transmission power for communicating with its neighbouring sensors while each sensor transmits data to the base station. The neighbouring distance is defined as

the maximal reachable distance with the fixed transmission power for neighbouring sensors. For a given sensor the sensors within its neighbouring distance are its "neighbouring sensors" or "neighbours". Also, each node can be aware of the current energy level of its neighbours or energy required to transmit from its neighbouring nodes to the base station by anticipating and/or eavesdropping data from the neighbours. Generally, sensors consume energy when they sense, receive and transmit data. However, the amount of energy consumption for sensing is unaffected by the routing algorithm and only a small difference exists between the power consumption for idle and receiving modes [59]. Therefore, in this work, we consider only the energy consumed while transmitting messages. According to the radio model [53], energy consumption (E) for transmitting data is proportional to the transmission distance as well as the square of the amount of data. By normalization of the amount of sensed data, the energy consumption model is simplified to $E=d^2$, where E and d are the required energy and the transmission distance respectively [49].

4.3.2 Lifetime of a Sensor Network

We validate the effectiveness of the proposed DEAR routing algorithm using a sensor network's lifetime as the performance measure. The definition of sensor network lifetime is the time until the first node or a portion of nodes become incapable, due to energy depletion, of sending data to its neighbours [49, 53, 55, 58]. The portion (number of depleted nodes) can vary depending on the context of the sensor networks. With reference to Figure 4.4, we infer the lifetime of a sensor network is the number of rounds until the first (L1), 10% (L10), or 20% (L20) of node(s) expend all their energy [55, 58]. We say that L1 denotes the full functioning period of the sensor network.

4.3.3 Event Generation Functions

For evaluation purposes, many previous studies of routing algorithms assumed that all sensors have uniform data or event generation rates [49, 53, 54]. In infrastructure monitoring applications, each sensor performs a sensing task for every fixed time and has a homogeneous event generation function or the same event generation rate. However, in many sensor network applications, this assumption becomes unrealistic. In a monitoring the migration of a herd of animals, the animals might move along a path in the target area repeatedly [50]. In the case of forest fire detection, events occur rarely and randomly over the target area [48].

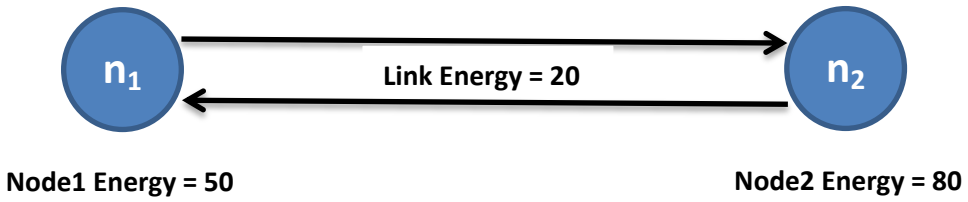
Furthermore, some event generation functions can be a combination of uniform, random, and repeated types. Therefore, one must consider several event types for the evaluation of routing algorithms.

4.4 DEAR Protocol

The routing algorithm uses a path with energy sufficiency as well as energy efficiency to pursue energy balance for the sensor network. Energy sufficiency depends upon the available energy, and energy efficiency depends upon the required transmission energy. By using a composite of both quantities, a good path that achieves energy balance can be found. Only one of them, by itself cannot indicate the goodness of a path because of the dual objectives of (i) not depleting the energy reserves of popular paths and of (ii) sending messages through energy efficient paths to ensure the total energy needed to route the messages are kept to a minimum. The definition of the composite measure, Energy Cost ($\mathbf{EC_{ij}}$) for a transmission from node *i* to *j* is:

$$\mathbf{EC_{ij}} = \frac{\text{Required energy from node i to j}}{\text{Available energy at node i}} \qquad \textbf{(4.1)}$$

The computation of EC_{ij} is exemplified below



EC_{12} and EC_{21} for above network are calculated as follows:

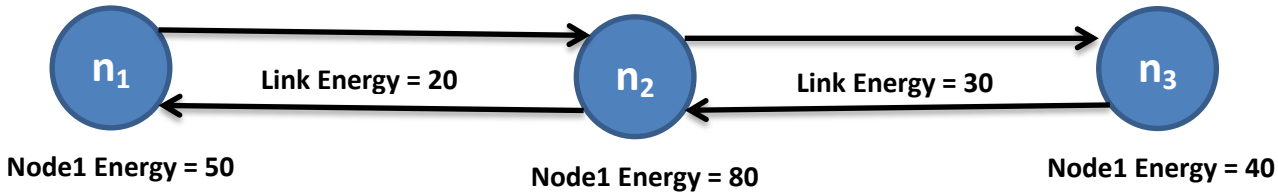
$$\mathbf{EC_{12}} = \frac{\textbf{Required energy from node 1 to 2}}{\textbf{Available energy at node 1}} = \frac{20}{50} = 0.4$$

$$\mathbf{EC_{21}} = \frac{\textbf{Required energy from node 2 to 1}}{\textbf{Available energy at node 2}} = \frac{20}{80} = 0.25$$

The Total Energy Cost ($\mathbf{TEC}_{ik}$) of a path k at sender *i* is the composite quantity that indicates the goodness of a path. This measure is simply the sum of the energy costs in the path:

$$TEC_{ik} = \sum_{ij \in k} EC_{ij} \quad \textbf{(4.2)}$$

For example,



$$TEC_{13} = \sum EC_{ij} = EC_{12} + EC_{23} = \frac{20}{50} + \frac{30}{80} = 0.4 + 0.375 = 0.775$$

Similarly,

$$TEC_{31} = \sum EC_{ij} = EC_{32} + EC_{21} = \frac{30}{40} + \frac{20}{80} = 0.75 + 0.25 = 1$$

When a sensor, or node, needs to send data to the base station, the node checks its routing table and chooses a node among its neighbouring nodes based on the energy cost. In evaluating the neighbours, the node computes the energy costs as if the neighbours will send the data directly to the base station. However, the best candidate may not send data directly to the base station if an indirect path with less energy cost exits. If the best candidate node is the node itself, it sends data to the base station and completes the routing process for the data. Otherwise, it forwards the data to the best candidate among its neighbouring nodes and that node then repeats the same routing process. This process continues until a node selects itself as the best candidate and sends directly to the base station.

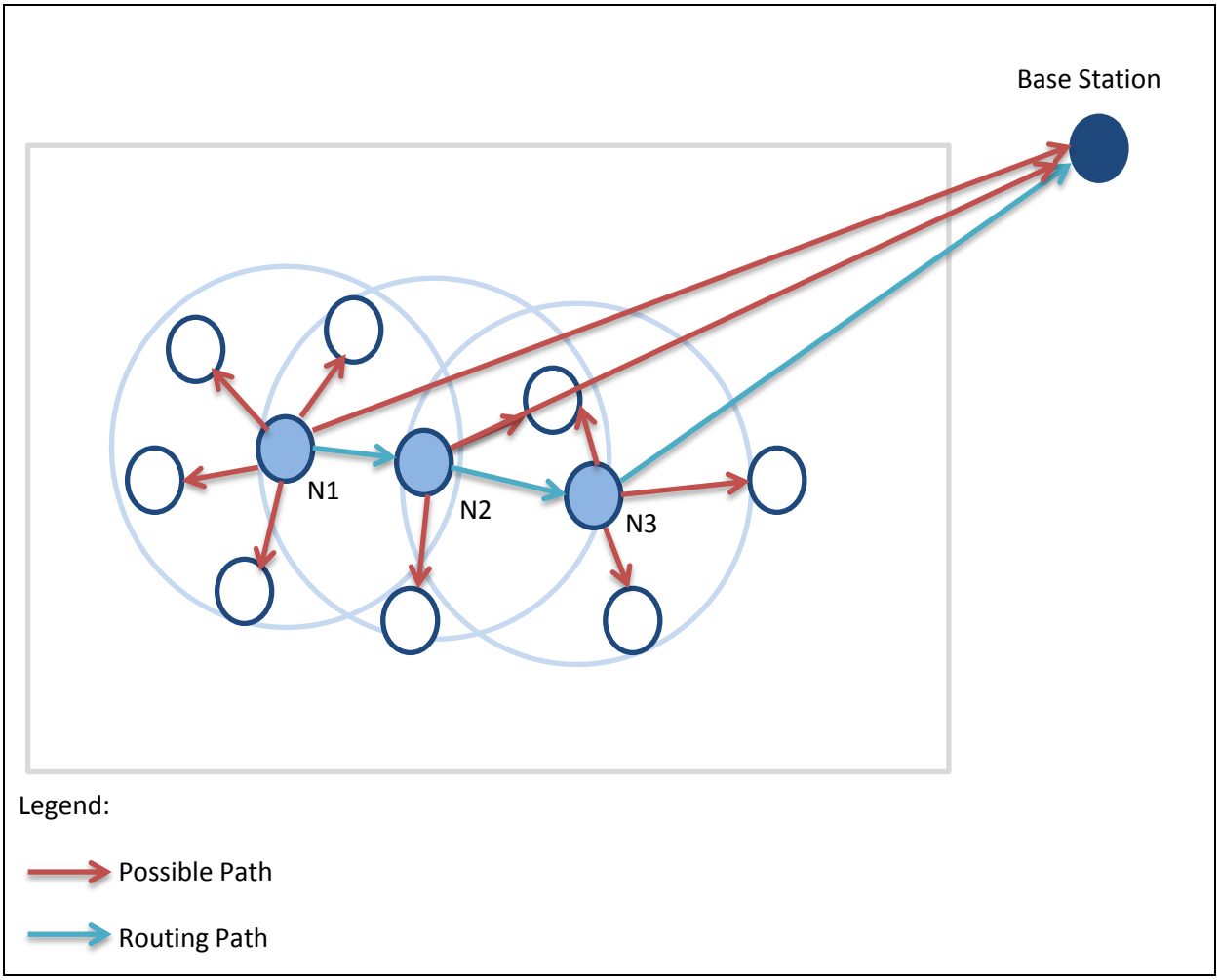


Figure 4.1: An Example routing path: N1 sends to N2 and further to N3 which sends the data to base station

This localized decision-making process results in a monotonic decrease of energy cost over time because the best candidate can have an indirect path that is better than direct transmission. Each sensor makes its decision with the assumption that one of its neighbouring nodes sends data to the base station directly. Sensors do not care if the receiving node sends data to the base station or passes data to one of its neighbouring nodes. This characteristic makes the proposed algorithm different from that proposed by Dijkstra and the Distance vector algorithm, which consider the best path from the next node. Through this local decision making process, a sensor network can achieve energy balance and prolong the lifetime of the sensor network.

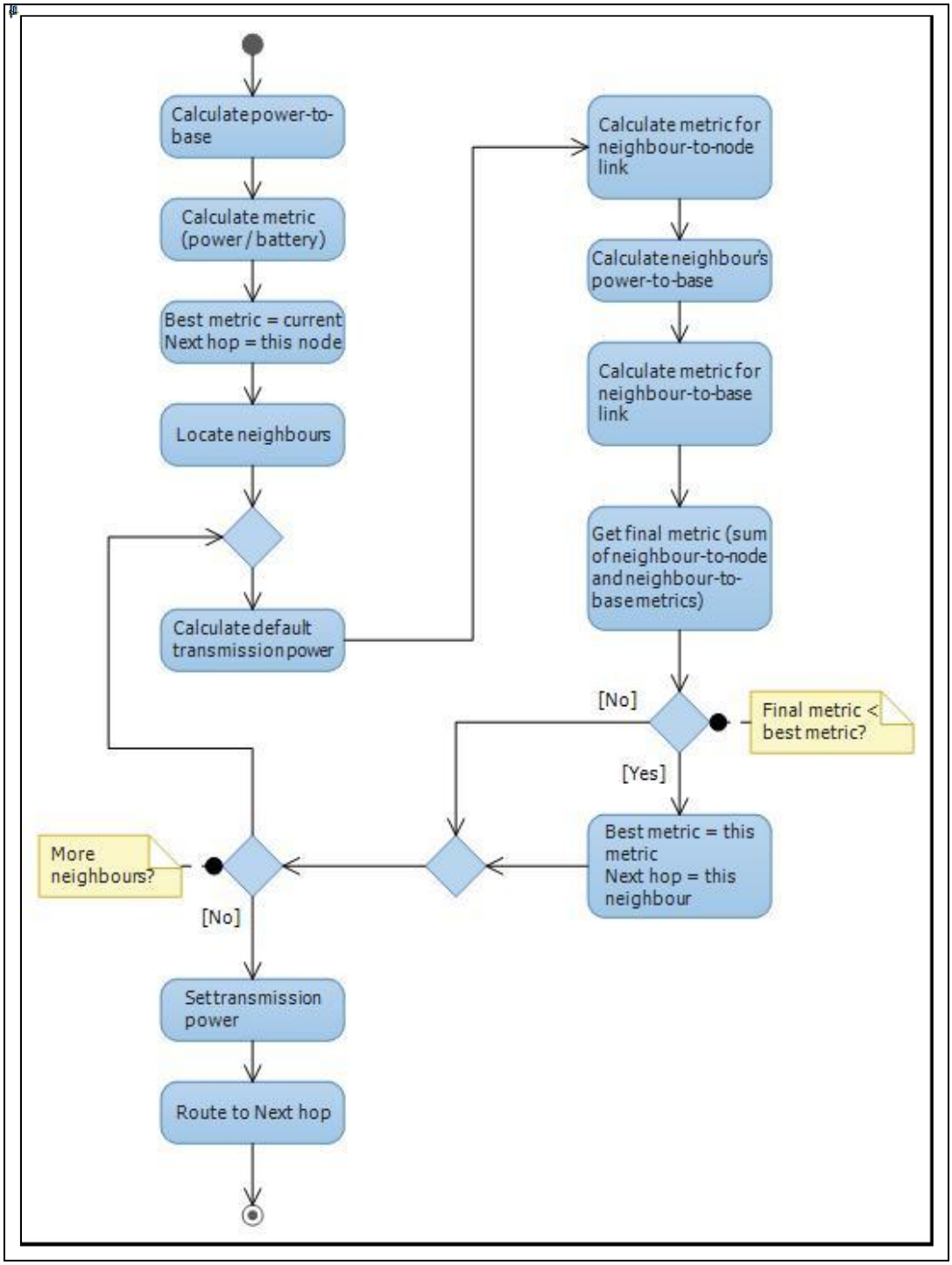


Figure 4.2: Original Dear activity diagram

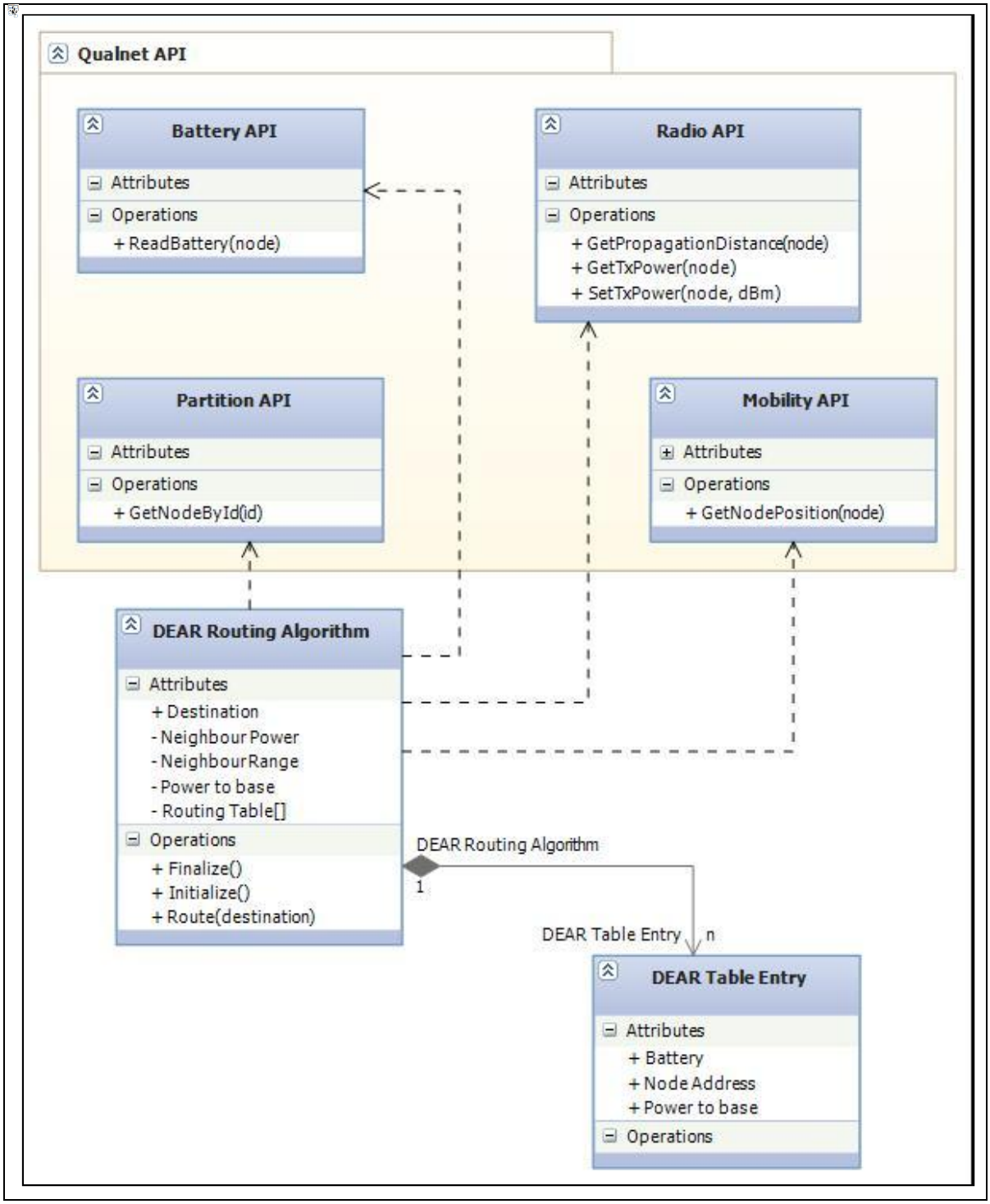


Figure 4.3: Original Dear class diagram

4.5 Example and Working

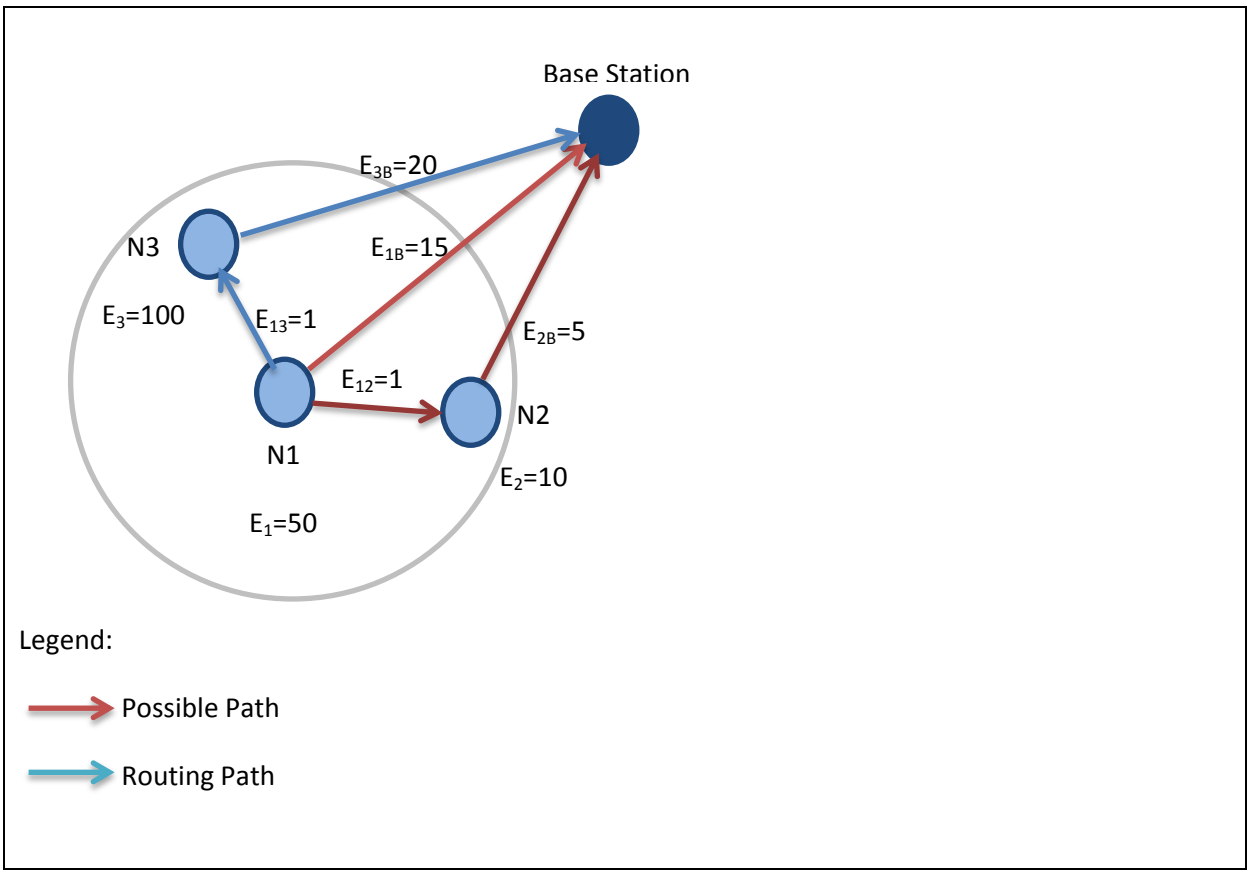


Figure 4.4: An Example Scenario

Consider the scenario as shown in figure containing one Base station where data or packet is to be routed suppose node n1 wants to send the data to base station then following steps are followed:

4.5.1 Initializing EC table:

First step is initialising EC table where all neighbour nodes are identified for (i) its Energy and (ii) Direct transmission energy to Base Station.

Example: Considering node N1 as a transmitter in Figure 4.4 then EC table of node N1 will be:

Fields of EC Table: Node Id, Node Energy, Direct Transmission Energy to Base Station.

\

Node Id	Node Energy (dB)	Direct Transmission Energy to Base Station (dB)
2	10	5
3	100	20

As shown above EC table for a given node contains only the entry for neighbour node.

4.5.2 Decentralized Routing:

Node N1 will determine the total indirect transmission power through neighbour node and then compares with its direct transmission power. The path with minimum energy cost required is chosen. Once packet is transmitted to the neighbour node it will iteratively follow previous step until the base station is the neighbourhood range.

Example: Considering Figure 4.4 for transmission from Node N1 to Base Station computation of paths is shown in Table.

Fields of Interest: Route, EC(node , neighbour), EC(node, base station), TEC(node, base station)

Route 1	Details	$EC_{(Node\ ,\ Neighbor)}$	$EC_{(Node\ ,\ BS)}$	$TEC_{(Node,\ BS)}$
Route 1	**N1- > BS (Direct)**	-	$EC_{1\ BS} = \frac{15}{50} = 0.3$	**0.3**
Route 2	**N1->N2->BS**	$EC_{12} = \frac{1}{50} = 0.02$	$EC_{2\ BS} = \frac{5}{10} = 0.5$	**0.52**
Route 3	**N1->N3->BS**	$EC_{13} = \frac{1}{50} = 0.02$	$EC_{3\ BS} = \frac{20}{100} = 0.2$	**0.22**

Table: all possible paths from node N1

Thus Node1 will transmit through Route 3 as TEC along that path is minimum.

4.5.3 Update EC table:

Whenever node receives any update packet from neighbour it updates EC table because energy of node changes after every transmission.

Example: Suppose in above example the node N1 wants to transmits a packet through Route 3 then it first of sends packet to neighbour node N3 with fixed power and then node N3 will transmit to base station with required power depends on the distance of the base station as if base station is in the neighbourhood range of node N3 then it will transmit with fixed power else will transmit with power actually required.

Considering one packet is routed through route N3 the energy of node N1 suppose depletes by 1.5 and energy of node N3 depletes by 20 then EC table for node N1 will be,

Fields of EC Table: Node id, Updated Node Energy, Direct Transmission Energy to Base Station.

Node Id	Node Energy (dB)	Direct Transmission Energy to Base Station (dB)
2	**10**	**5**
3	**80**	**20**

Note that original DEAR transmits to the neighbour with the fixed power without considering the distance of neighbour; this limitation is overcome by DEAR2.

4.6 Limitations

4.6.1 Default transmission power

Since the source node communicates with its neighbour nodes with default transmission power, the loss due to inaccurate estimation of power for each node separately is considerable.

Example: With reference to figure 4.4, if the distance between N1 and N2 is 100m and distance between N1 and N3 is 150m then DEAR protocol fails to identify this difference and act accordingly by selecting optimum transmission power.

4.6.2 Single hop path discovery mechanism

Since DEAR peeps only the table of neighbour nodes and computes path accordingly we term this as single hop discovery mechanism which fails to choose optimum path when network scales.

4.6.3 Topology dependent output

The adverse effect of Single hop path discovery mechanism is topology dependent output. Example: For random topology the DEAR protocol may utilize entire network but for grid topology it transmits only in diagonal direction as shown in Figure 4.5.

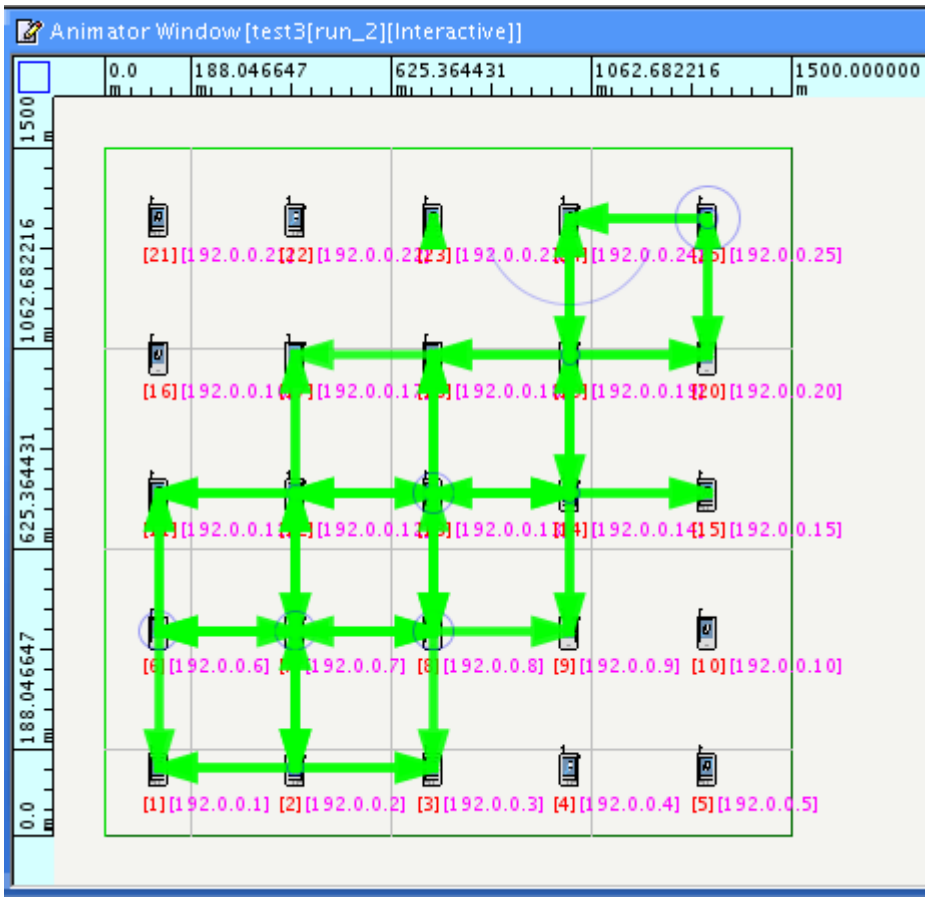


Figure 4.5 Diagonal forwarding of packets

Chapter 5

Proposed Algorithm DEAR 2, DEAR 3

5.1 Limitations addressed by DEAR 2

DEAR 2 include use of variable transmission power for node to neighbour node communication.

Example: With reference to figure the transmission power between node N1 to node N3 and node N1 to N2 is computed to be distinct because of their distinct distances.

5.2 Proposed algorithm

As an improvement of DEAR support for variable transmission power is an additional functionality in DEAR 2 whereas the working of rest of DEAR remains intact. As mentioned earlier the benefit of DEAR 2 is preventing wastage of energy caused by DEAR where default power used to reduce the life time of the network.

Consider the static scenario where each node has fixed but distinct distance from the other nodes. Here we can determine the minimum power needed for transmission using this fixed distance and a pair of predefined power and range. In QUALNET 4.5 the API called radio range gives range for a given power. Thus using approximation method one can determine the

required minimum power for given distance with desired accuracy. In real time application the minimum power for transmission is provided by feedback from receiver node.

Calculation of EC_{ij} and TEC_{ik} remains the same. Formula is reinstated below for reference below.

$$\mathbf{EC_{ij}} = \frac{\text{Required energy from node i to j}}{\text{Available energy at node i}} \quad \textbf{(5.1)}$$

$$\boldsymbol{TEC_{ik}} = \sum_{ij \in k} \boldsymbol{EC_{ij}} \quad \textbf{(5.2)}$$

The difference lays in total energy invested while communicating from source to destination. To exemplify, consider the following figure

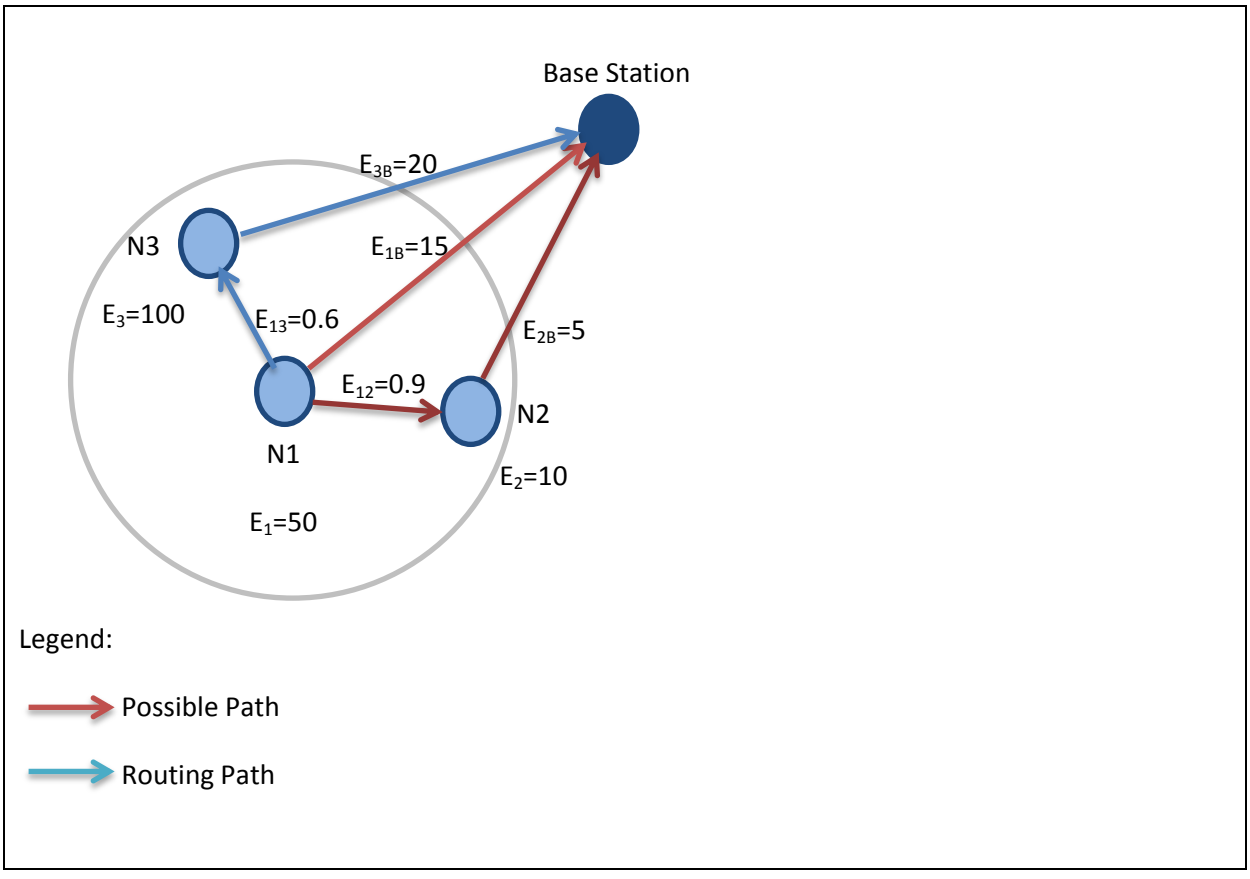


Figure 5.1 Example Scenario

Route	DEAR : Split of Transmission Energy (dB)	DEAR : Total Transmission Energy (dB)	DEAR 2 : Split of Transmission Energy (dB)	Total Transmission Energy (dB)	Energy Saved (DEAR – DEAR2) (dB)
N1 - > N3 - > Base Station	1 + 20	21	0.6 + 20	20.6	0.4
N1 - > N2 - > Base Station	1 + 5	6	0.9 + 6	6.9	0.9
N1 - > Base Station	15	15	15	15	0

We also provided option for the power boost which helps in reducing the retransmission as we are determining the minimum power which can cause the low accuracy as some time bad weather condition requires some little extra power and hence power boost option as 1db or 2db as per the user requirement and importance of the data.

As every node has table containing energy required to transmit to every other node as in case of original DEAR, it transmits to only neighbour node but here all node are neighbour as no predefined power is used to define neighbourhood hence can discover better path then original DEAR.

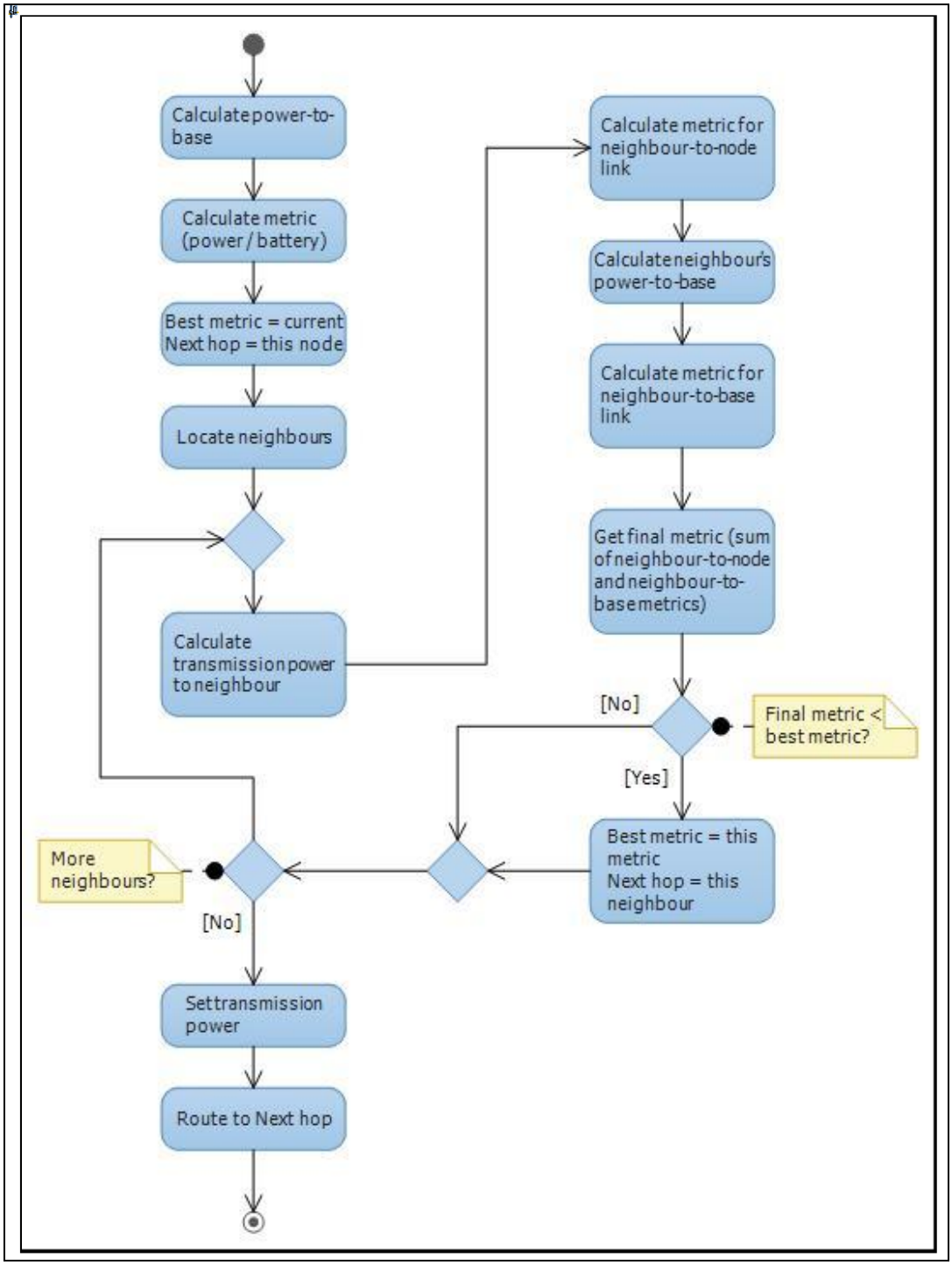


Figure 5.2: Dear 2 activity diagram

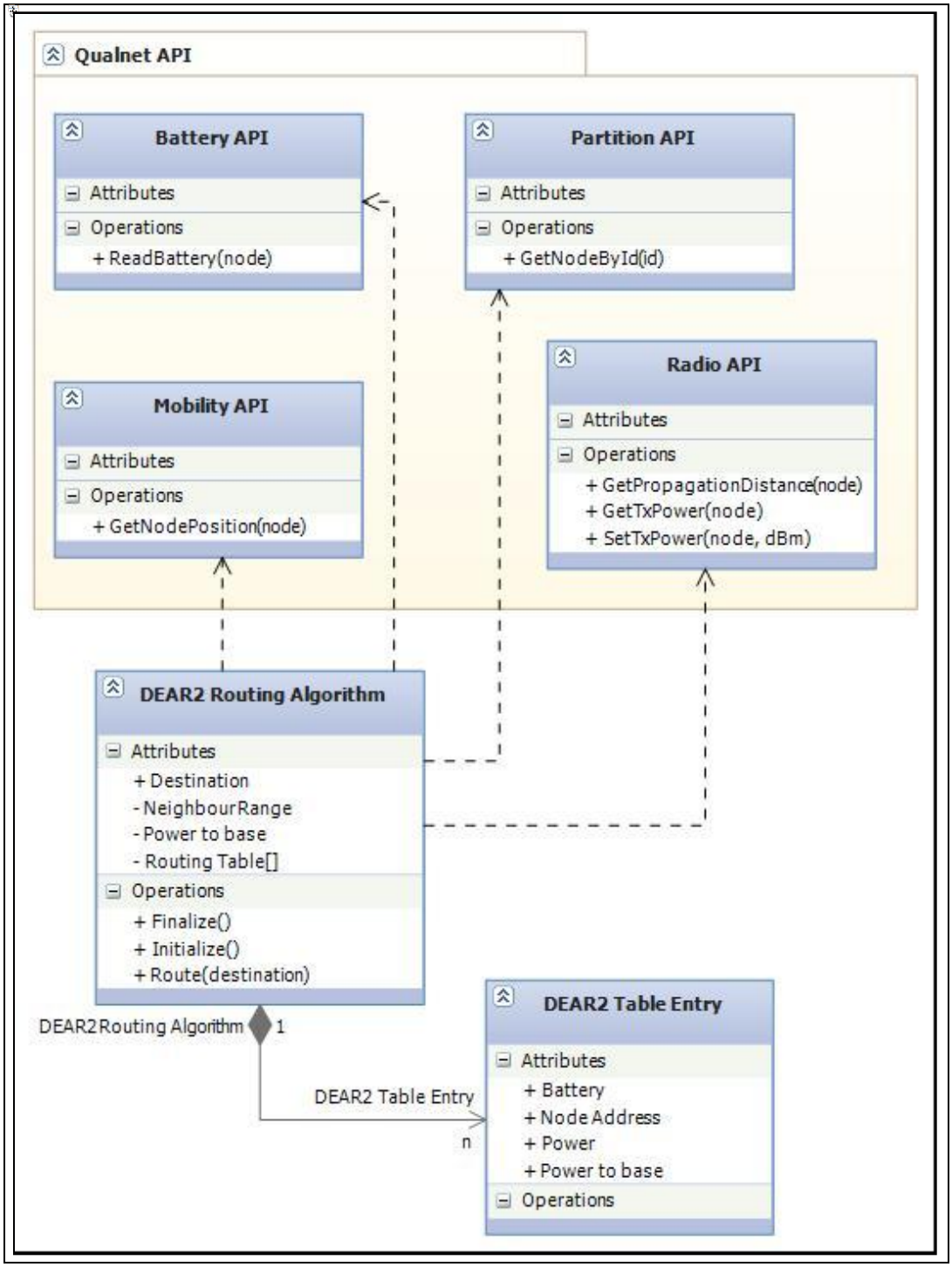


Figure 5.3: Dear 2 Class diagram

\

5.3 Example and Working

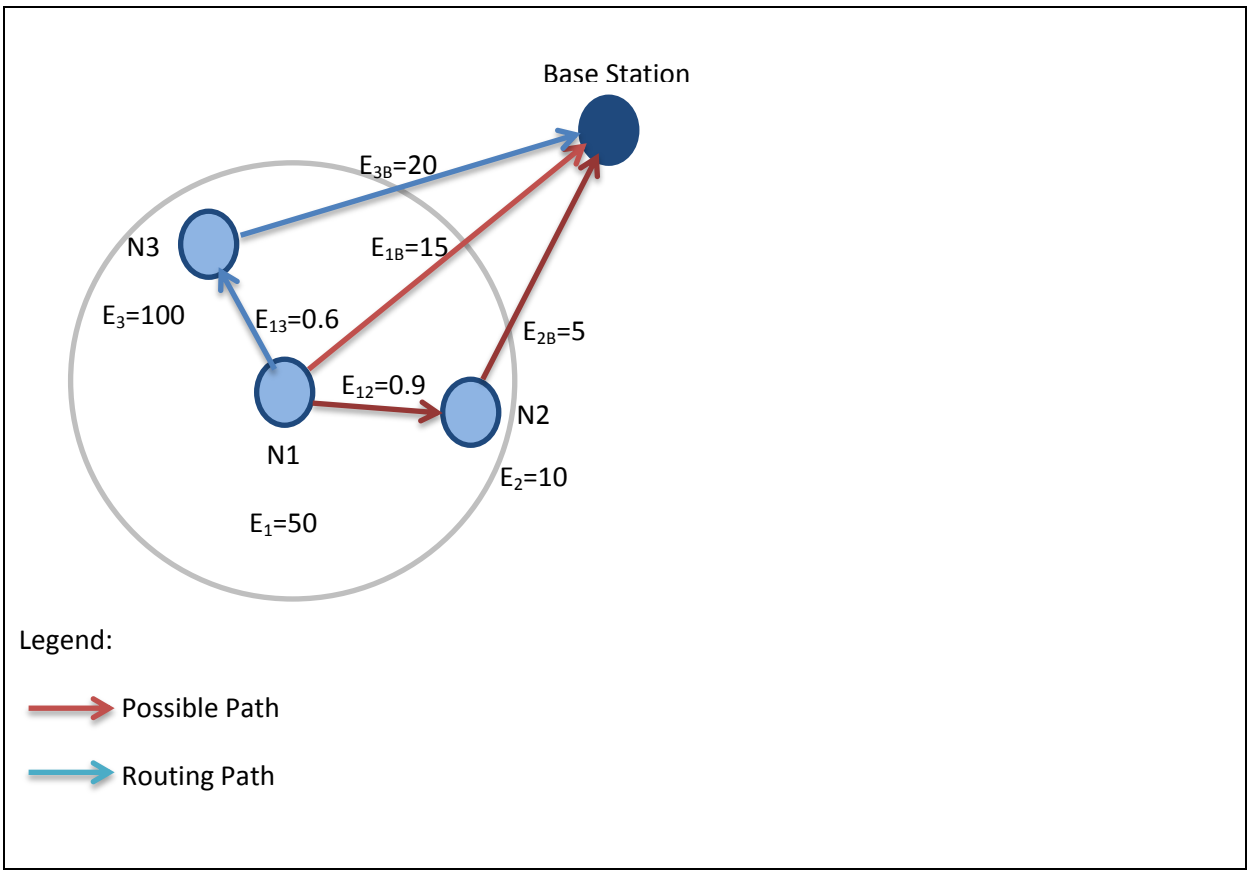


Figure 5.4 Example Scenario

Consider the same scenario as shown in figure containing one Base station where data or packet is to be routed suppose node N1 wants to send the data to base station then following steps are followed:

5.3.1 Initializing EC table:

First step is initialising EC table where all neighbour nodes are identified for (i) its Energy, (ii) Direct transmission energy to Base Station and (iii) Link Energy

Example: Considering node N1 as a transmitter in Figure 5.4 then EC table of node1 will be:
Fields of EC Table: Node Id, Node Energy, Direct Transmission, Link Energy

Node Id	Node Energy (dB)	Direct Transmission Energy(Neighbour to Base Station) (dB)	Link Energy (Node to Neighbour) (dB)
2	10	5	0.9
3	100	20	0.6

As shown above EC table for a given node contains only the entry for neighbour node.

5.3.2 Decentralized Routing:

Node 1 will determine the total indirect transmission power through neighbour node and then compares with its direct transmission power. The path with minimum energy cost required is chosen. Once packet is transmitted to the neighbour node it will iteratively follow previous step until the base station is the neighbourhood range.

Example: Considering Figure 5.4 for transmission from Node N1 to Base Station computation of paths is shown in Table.

Fields of Interest: Route, EC (node, neighbour), EC (node, base station), TEC (node, base station)

Route 1	Details	$EC_{(Node\ ,\ Neighbor)}$	$EC_{(Node\ ,\ BS)}$	$TEC_{(Node,\ BS)}$
Route 1	**N1- > BS (Direct)**	-	$EC_{1\ BS} = \frac{15}{50} = 0.3$	**0.3**
Route 2	**N1->N2->BS**	$EC_{12} = \frac{0.9}{50} = 0.018$	$EC_{2\ BS} = \frac{5}{10} = 0.5$	**0.518**
Route 3	**N1->N3->BS**	$EC_{13} = \frac{0.6}{50} = 0.012$	$EC_{3\ BS} = \frac{20}{100} = 0.2$	**0.22**

Table: all possible paths from node N1

Thus Node1 will transmit through Route 3 as TEC along that path is minimum.

5.3.3 Update EC table:

Whenever node receives any update packet from neighbour it updates EC table because energy of node changes after every transmission.

Example: Suppose in above example the node N1 wants to transmits a packet through Route 3 then it first of sends packet to neighbour node N3 with fixed power and then node N3 will transmit to base station with required power depends on the distance of the base station as if base station is in the neighbourhood range of node N3 then it will transmit with fixed power else will transmit with power actually required.

Considering one packet is routed through route N3 the energy of node N1 suppose depletes by 1.5 and energy of node N3 depletes by 20 then EC table for node N1 will be:

Fields of EC Table: Node Id, Updated Node Energy, Direct Transmission, Link Energy

Node Id	Node Energy	Direct Transmission Energy(Neighbour to Base Station)	Link Energy (Node to Beighbour)
2	**10**	**5**	**0.9**
3	**80**	**20**	**0.6**

Note that original DEAR transmits to the neighbour with the fixed power without considering the distance of neighbour; this limitation is overcome by DEAR2.

5.4 Limitations addressed by DEAR 3

DEAR 3 is the final improvement of this research which overcomes limitation of DEAR like (i) default transmission power, (ii) one-hop discovery and (iii) diagonal path utilization. The implementation includes variable power support as suggested by DEAR 2 and Dijkstra's algorithm to find out energy efficient path.

5.5 Proposed Algorithm

When original DEAR and DEAR2 is implemented in grid arrangement of node they both follows the diagonal path instead the alternative available path with the same energy coefficient because transmitter looks up path up to next one hop not to the complete path.

In this protocol we assume a fully connected graph of nodes. We implement the dijkstra algorithm which finds all possible paths to the destination node without any hop limitation

and also calculates the total energy cost (**TEC**) for every path. Further it selects that path which has minimum energy cost.

To exemplify, consider the transmitter is node i and receiver is node k. The energy cost is formulated using

$$\mathbf{EC_{ij}} = \frac{\textbf{Required energy from node i to j}}{\textbf{Percentage of battery remain at node i}} \qquad \textbf{(5.3)}$$

Note: one more parameter is added to store initial energy of every node which helps in determining the how much percentage of battery is there according to the initial energy hence battery percentage is calculated by

$$\textbf{Percentage of Battery remaining} = \frac{\textbf{Current Battery Amount}}{\textbf{Battery at the start}} * \mathbf{100} \qquad \textbf{(5.4)}$$

This helps us to switch to that path which might have same or slightly difference total energy cost (**TEC**) but having higher percentage of battery, using percentage of battery we can avoid node which is depleted most so as to increase the network life. Hence final formula for path selection is

The energy cost is calculated for each path associated with node *i* to *k* using

$$\boldsymbol{TEC_{ik}} = \sum_{\boldsymbol{ij} \in \boldsymbol{k}} \boldsymbol{EC_{ij}} \qquad \textbf{(5.5)}$$

The optimum path is selected using

$$\textbf{Final Path} = \textbf{Min}\left[\sum \left\{ \mathbf{EC_{ij}} = \frac{\textbf{Required energy from node i to j}}{\textbf{Percentage of battery remain at node i}} \right\} \right] \qquad \textbf{(5.6)}$$

$$= \textbf{min}\ (\mathbf{TEC_{ik}})$$

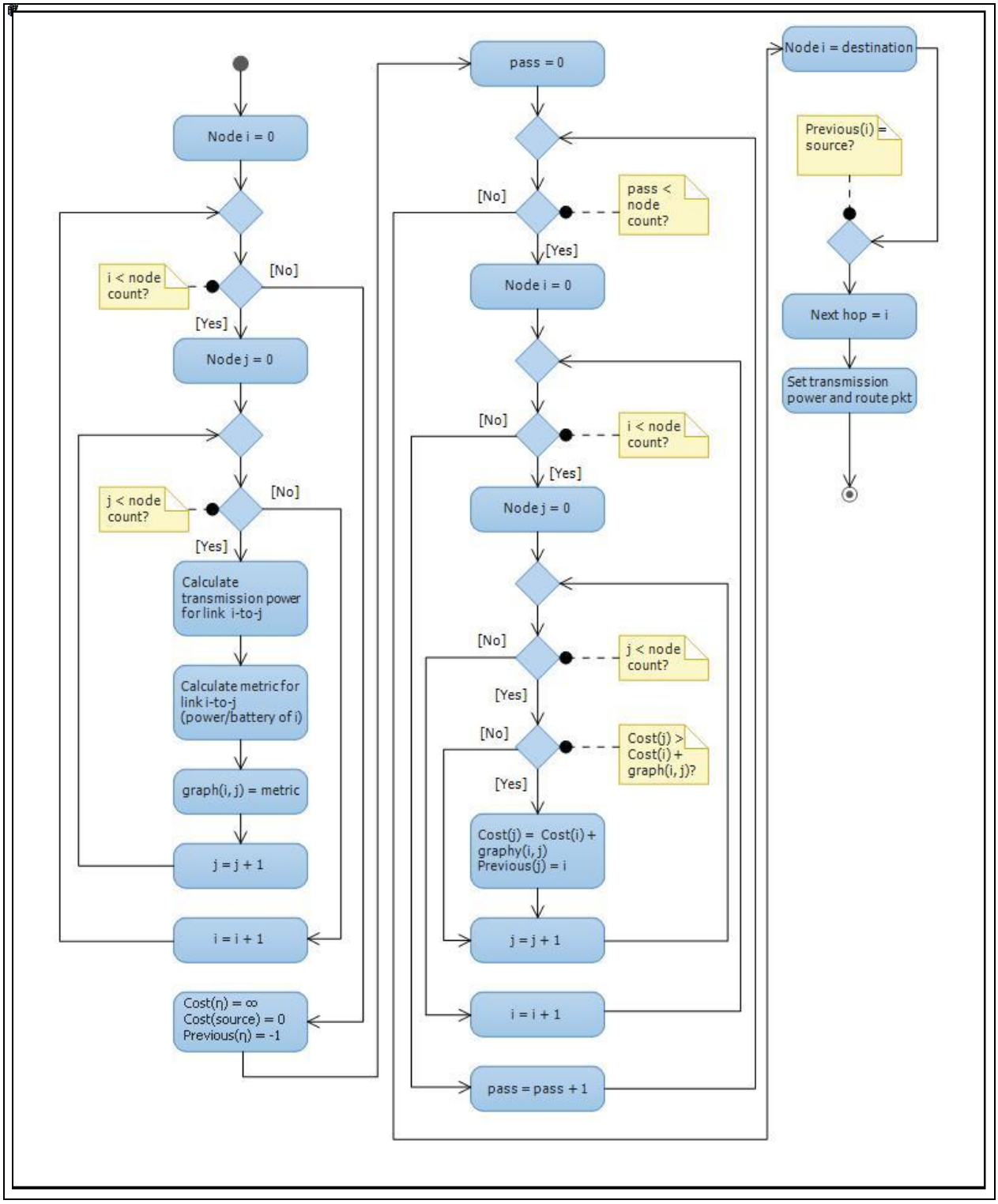


Figure 5.5: Dear 3 Activity diagram

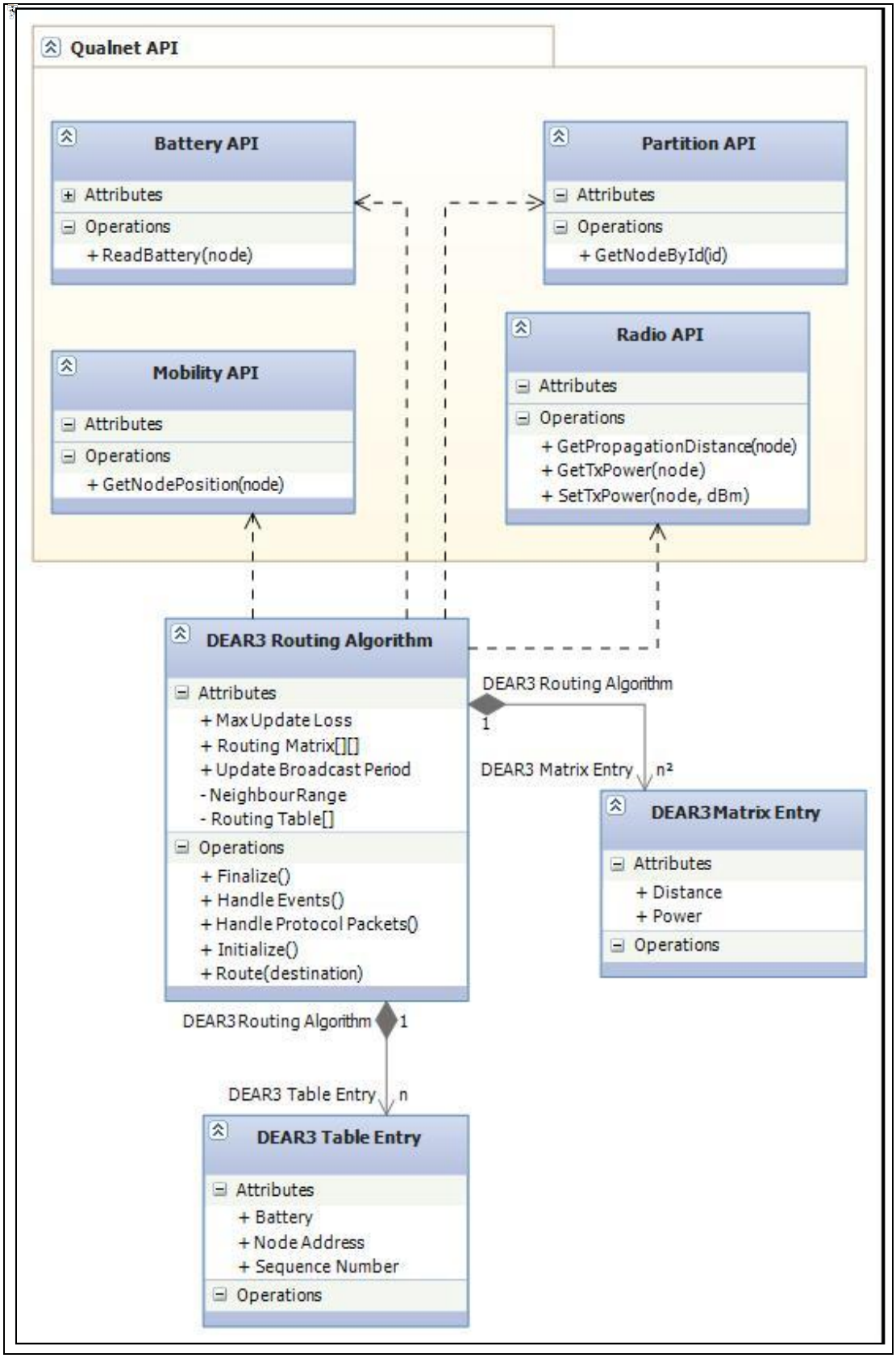


Figure 5.6: Dear 3 class diagram

5.6 Example and Working

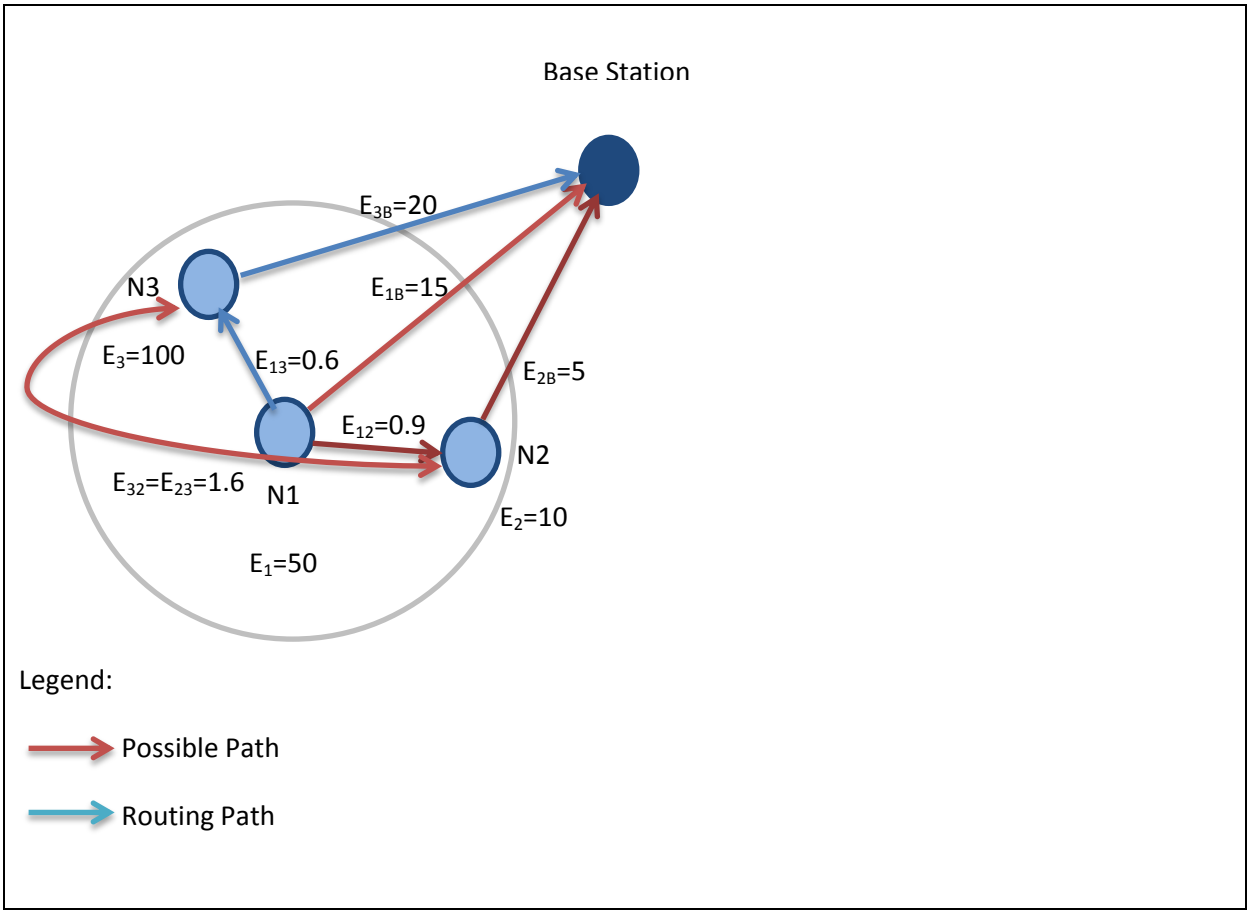


Figure 5.7 Example Scenario

Considering the same scenario as node N1 wants to transmit the data to the base station.

5.6.1 Initializing EC table and Power table:

It not only determines the neighbour nodes but also stores the distance of node with the minimum power required to transmit. It also initializes the power table which contains the sequence number and current percentage energy of node.

While determining the transmission cost it uses the link power divided by the percentage battery which means the transmission cost on the both direction will not be same.

Example: Refer Figure 5.7.

Fields of EC Table: (distance, link energy) between pair on nodes.

	Node 1	Node 2	Node 3	Base Station
Node 1	-	$Dist_{12}$, 0.9	$Dist_{13}$, 0.6	$Dist_{1B}$, 15
Node 2	$Dist_{21}$, 0.9	-	$Dist_{23}$, 1.6	$Dist_{2B}$, 5
Node 3	$Dist_{31}$, 0.6	$Dist_{32}$, 1.6	-	$Dist_{3B,}$ 20
Base Station	$Dist_{B1,\ 15}$	$Dist_{B2,}$ 5	$Dist_{B3}$, 20	-

Table: EC Table

Fields of Power Table: Sequence Number, Battery Percentage

Node	Sequence No	Battery Percentage
Node 1	1	100
Node 2	1	100
Node 3	1	100

Table: Power Table

5.6.2 Decentralized Routing:

Node 1 will determine the total indirect transmission power through neighbour node in this case it will determine from node 2 and node 3 and then compares with its direct transmission power whichever is minimum it will follow that path. Once packet is transmitted to the neighbour node it will iteratively follow previous step until the base station is the neighbourhood range. One thing is to note here is communication between neighbour node is using minimum power required and not by predefined power so as to reduce usage and increase the network life. Even using the percentage of the battery will allow us to determine the path which is least used with least power required for total transmission.

Example: With reference to Figure 5.7 assume all nodes have 100% energy initially.

Fields of Interest: Route, EC (node, neighbour), EC (node, base station), TEC (node, base station)

	Node 1	Node 2	Node 3	Base Station
Node 1	-	0.009	0.006	0.15
Node 2	0.009	-	0.016	0.05
Node 3	0.006	0.016	-	0.20
Base Station	0.15	0.05	0.20	-

EC Table

Route 1	Details	$EC_{(Node\ ,\ Neighbor)}$	$EC_{(Node\ ,\ BS)}$	$TEC_{(Node,\ BS)}$
Route 1	**N1- > BS (Direct)**	-	$EC_{1\ BS} = \frac{15}{100} = 0.15$	**0.15**
Route 2	**N1->N2->BS**	$EC_{12} = \frac{0.9}{100} = 0.009$	$EC_{2\ BS} = \frac{5}{100} = 0.05$	**0.059**
Route 3	**N1->N3->BS**	$EC_{13} = \frac{0.6}{100} = 0.006$	$EC_{3\ BS} = \frac{20}{100} = 0.02$	**0.026**
Route 4	**N1- >N2->N3 >BS**	$EC_{12} = \frac{0.9}{100} = 0.009$ $EC_{23} = \frac{1.6}{100} = 0.016$	$EC_{3\ BS} = \frac{20}{100} = 0.02$	**0.045**
Route 5	**N1->N3->N2->BS**	$EC_{13} = \frac{0.6}{100} = 0.006$ $EC_{32} = \frac{1.6}{100} = 0.016$	$EC_{2\ BS} = \frac{5}{100} = 0.05$	**0.072**

The Best Route is computed to be Route 3.

5.6.3 Update EC table and Power table:

Whenever node receives Power update packet from neighbour it updates table because each time energy of node changes, if it does not receive any energy update from particular node it is assumed to be dead and very high value is stored in EC table so it will be avoided during path selection. According to the current power status the EC table is updated.

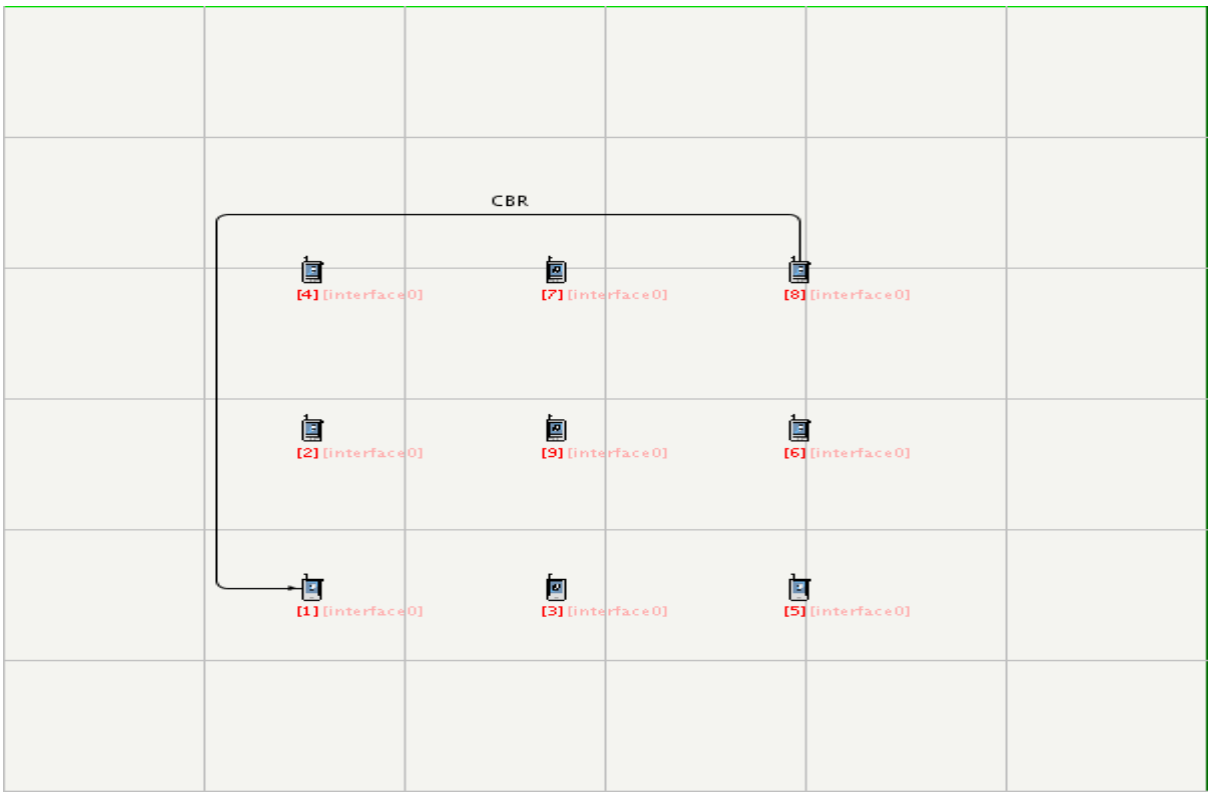
Consider update packet after two packets are transmitted through N1->N3->BS. Hence the Power Table would modify to the following:

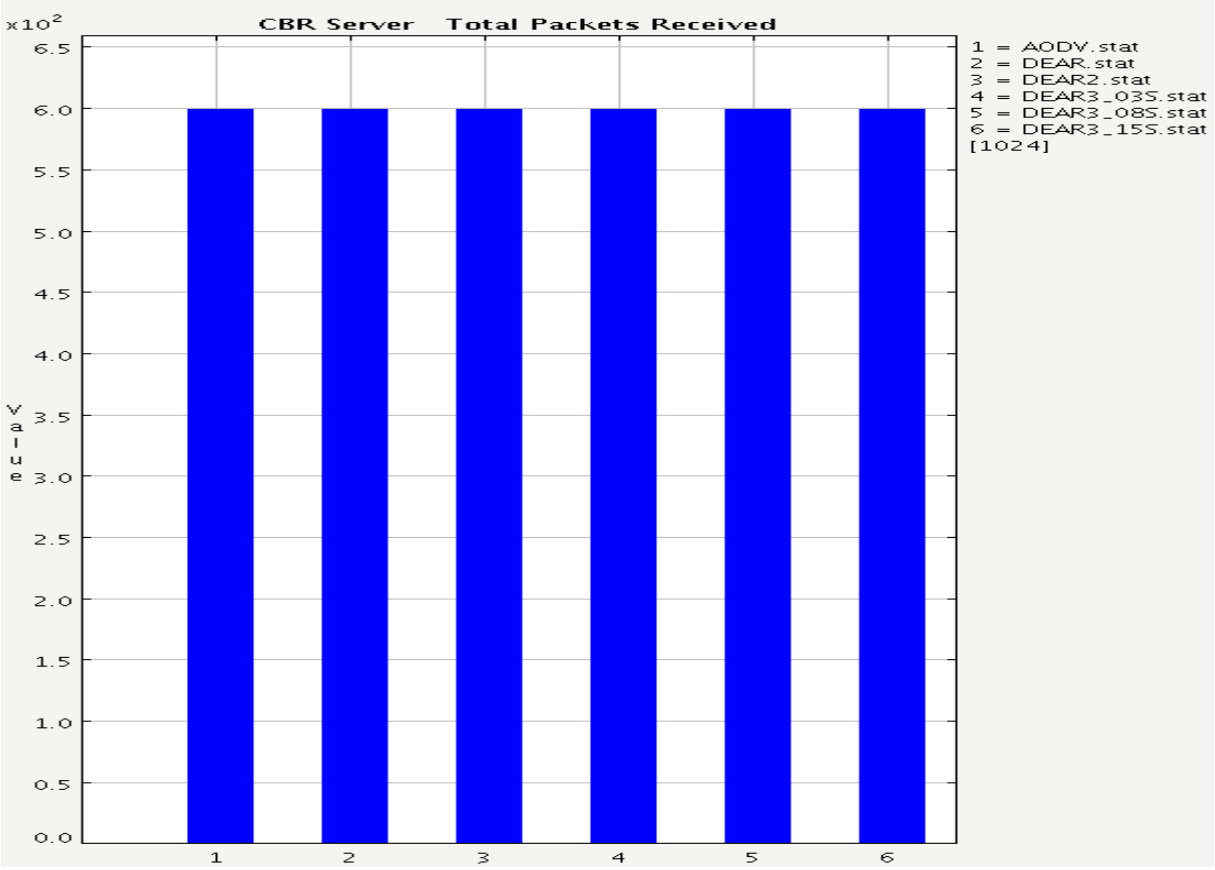
Node	Sequence No	Battery
Node 1	2	97.8
Node 2	2	60
Node 3	2	100

Chapter 6

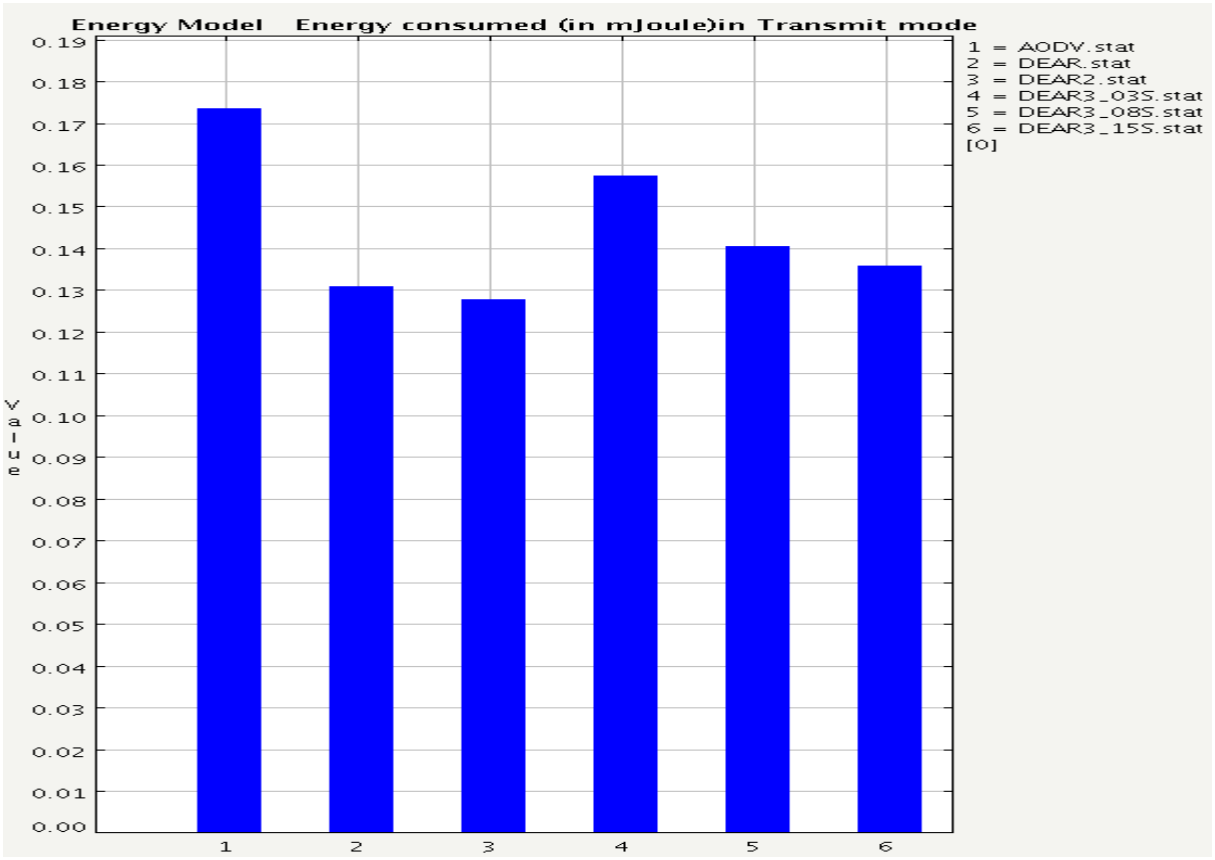
Results and Discussion

6.1 Scenario 1

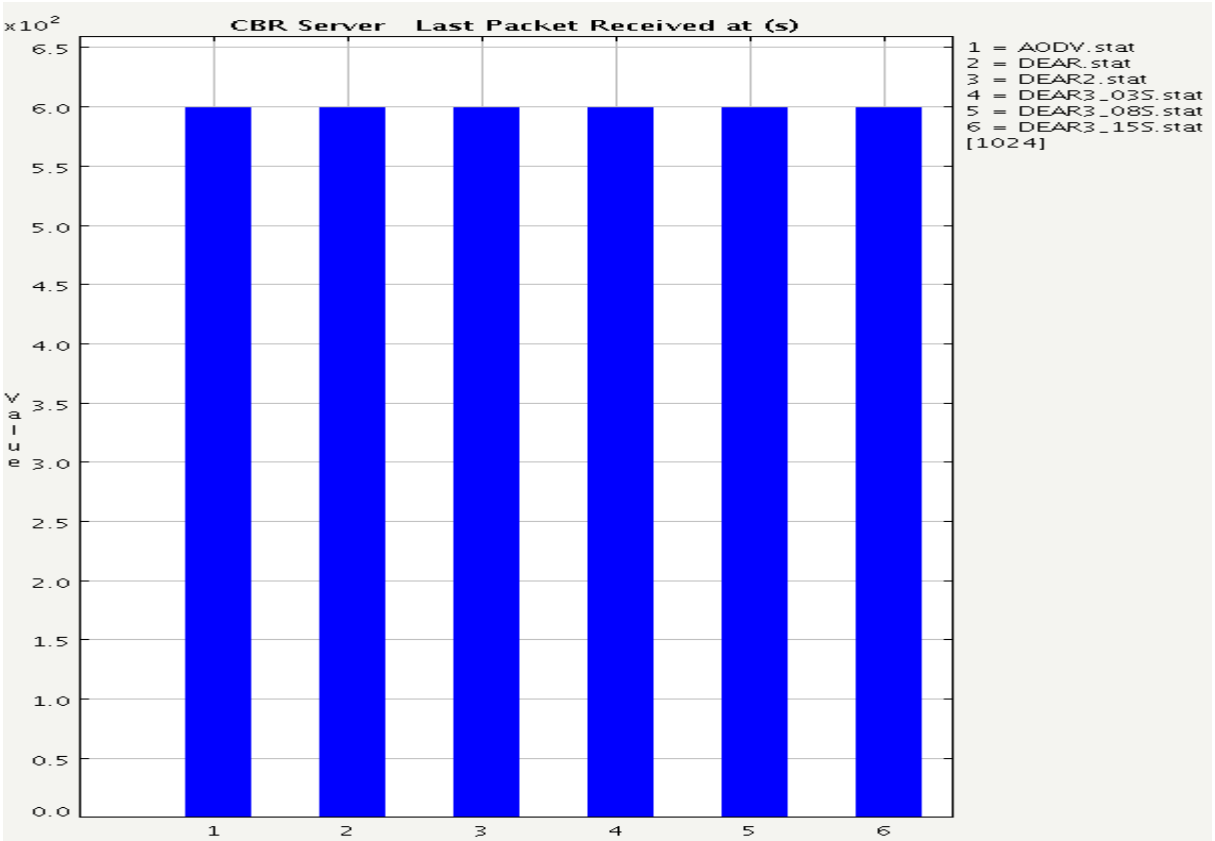




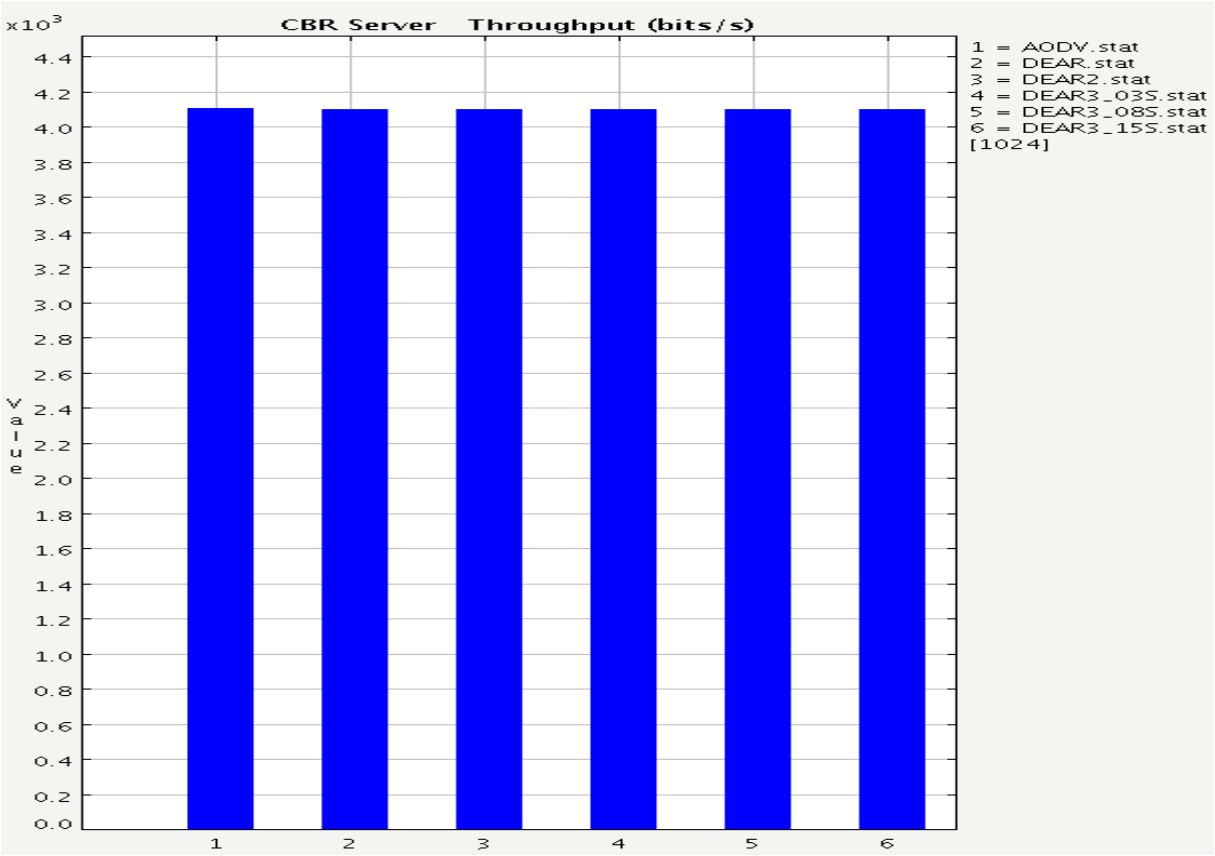
Total Packets Received



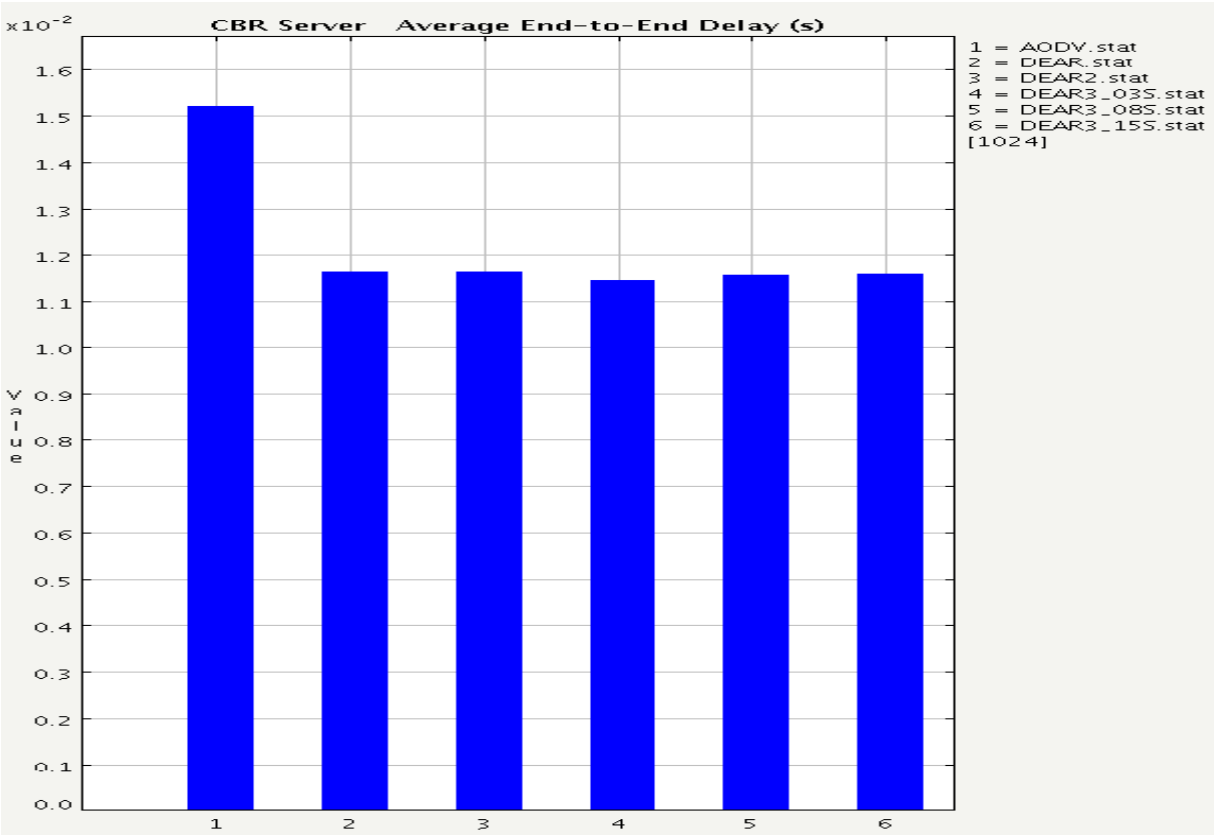
Energy Consumed



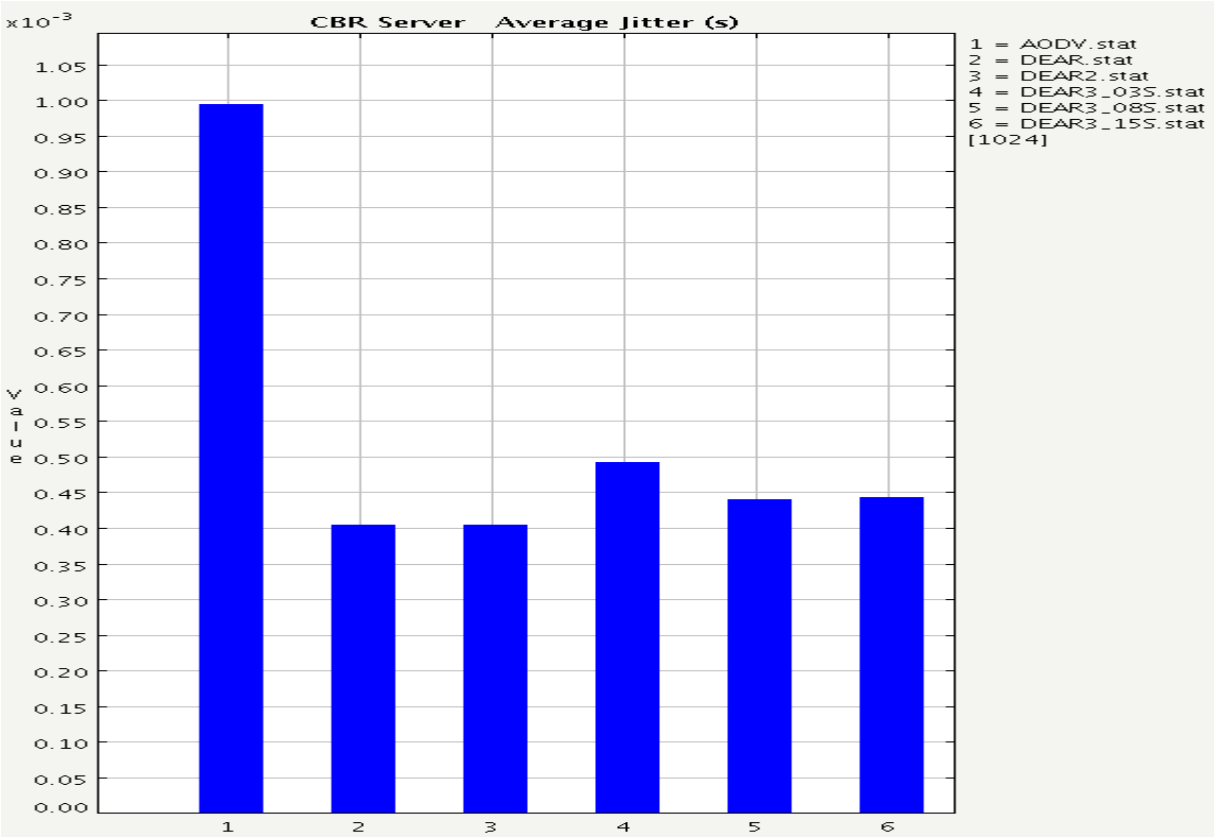
Last Packet Received



Throughput

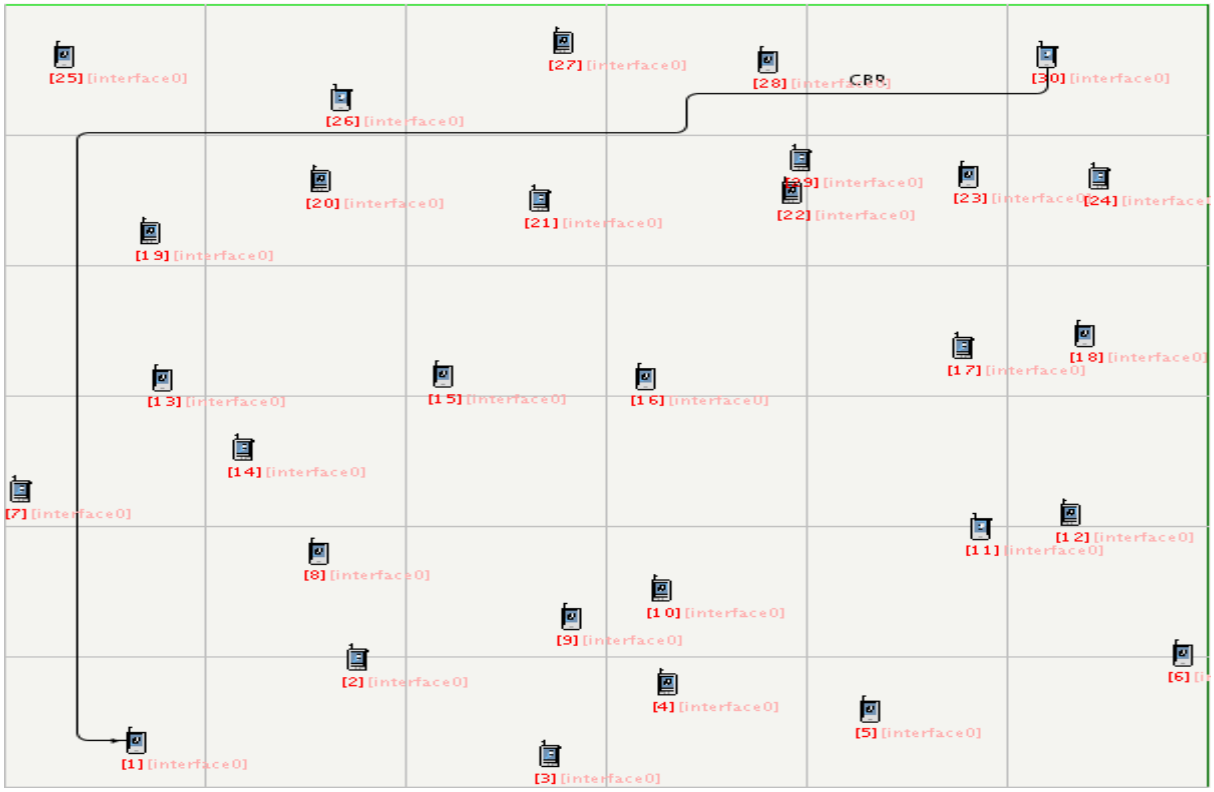


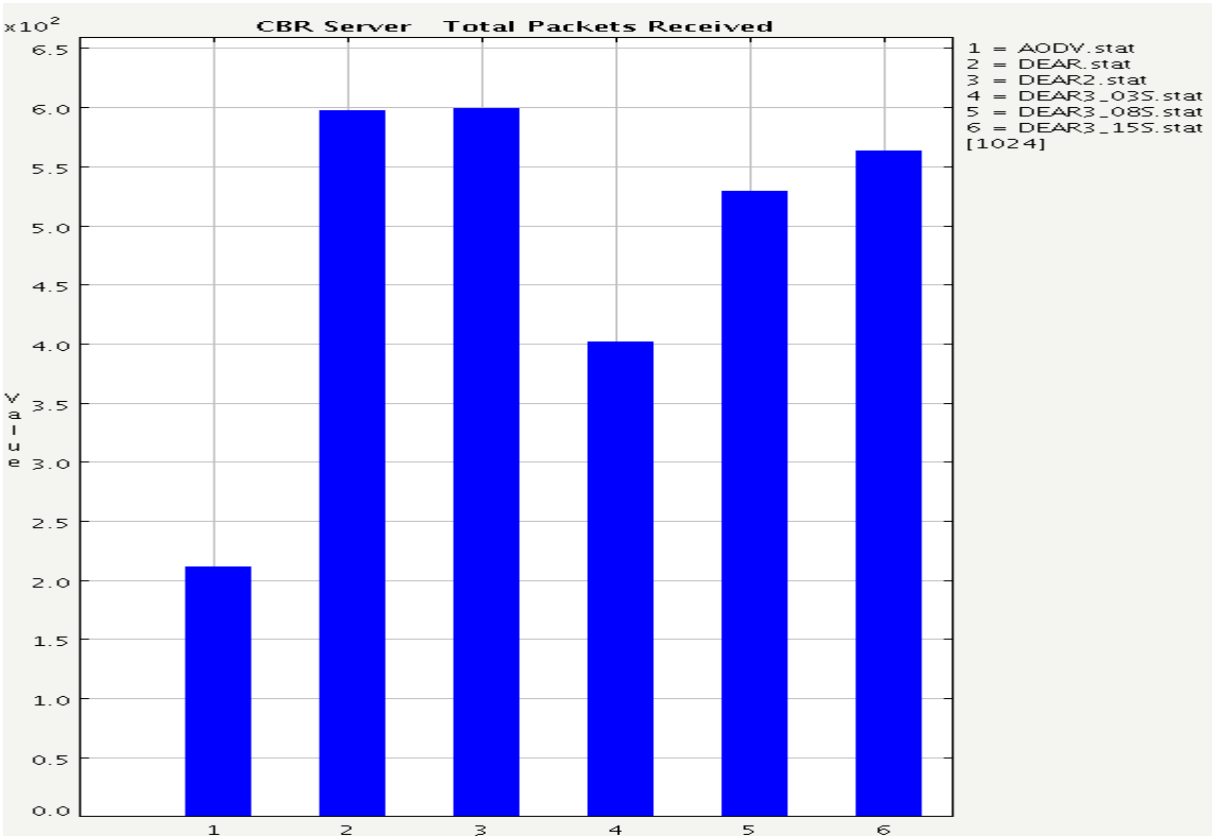
End to End Delay



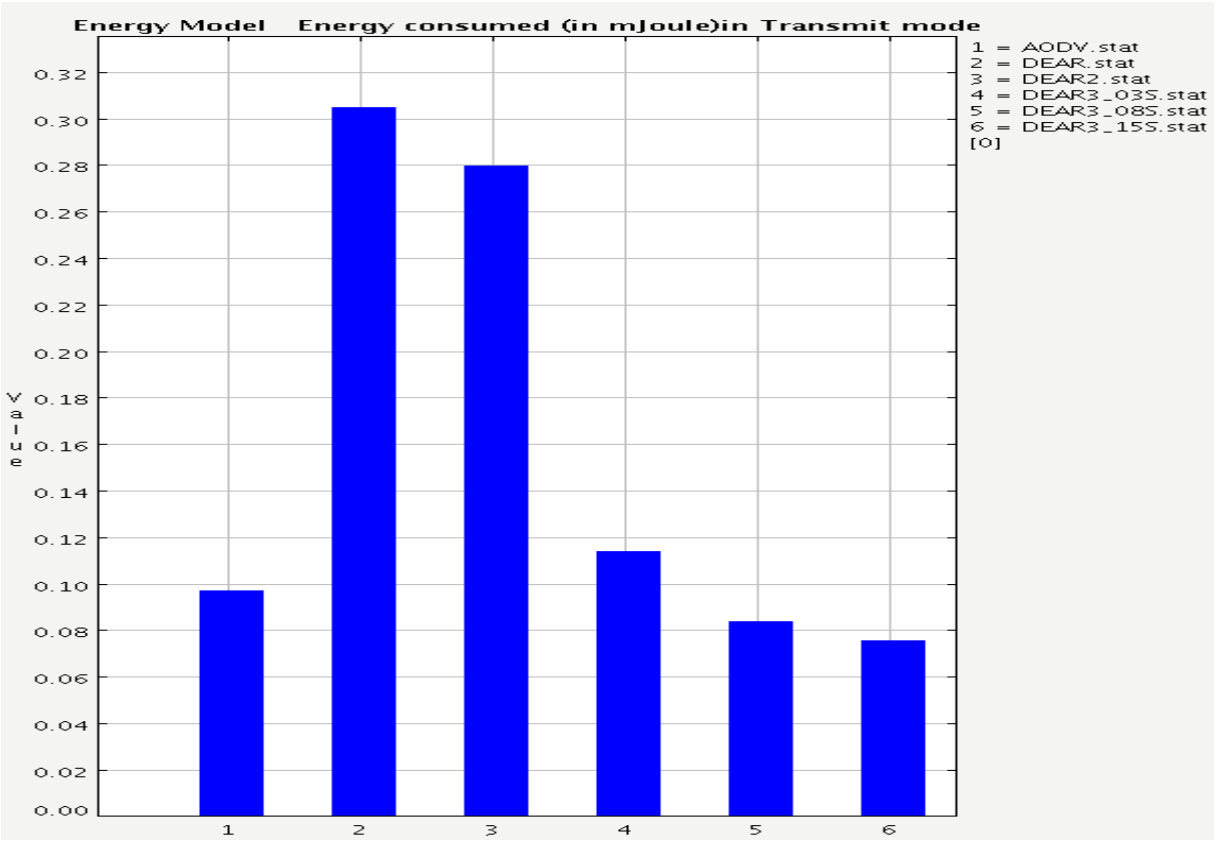
Jitter

6.2 Scenario 2

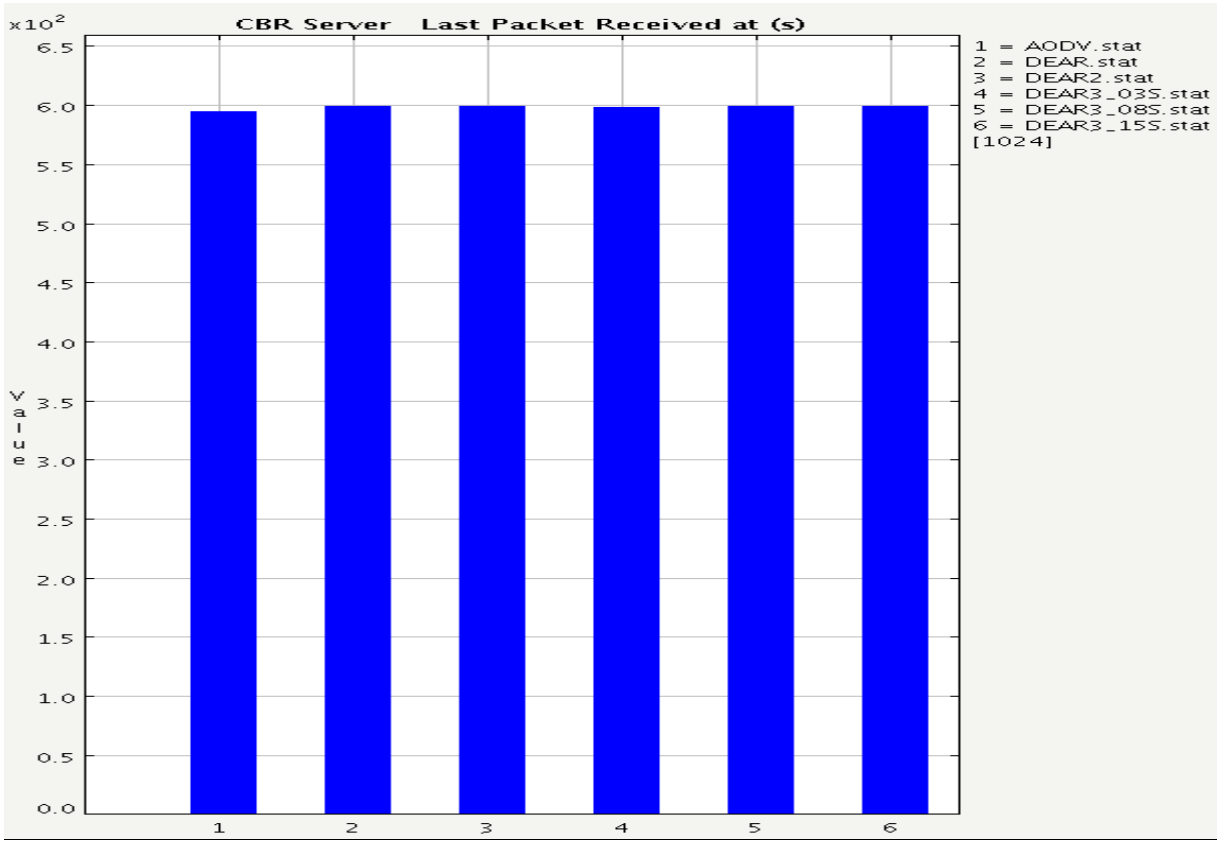




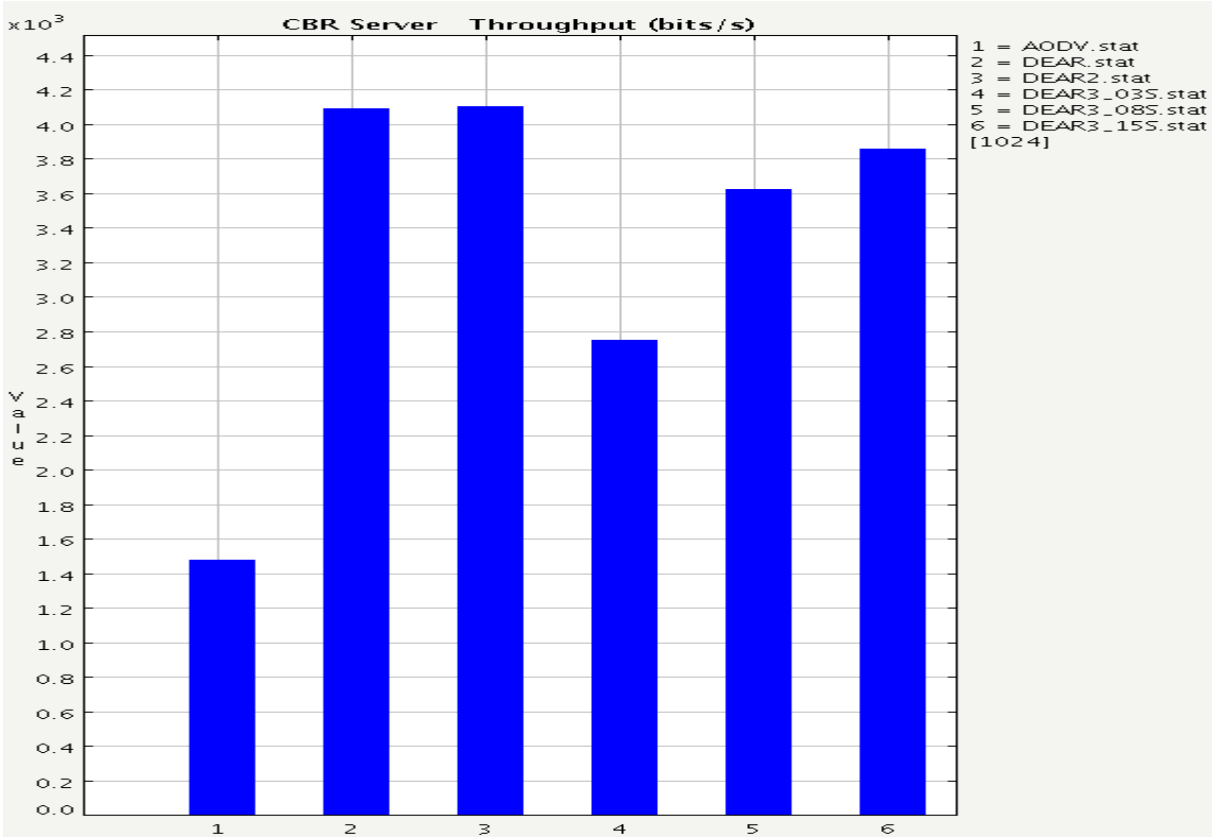
Total Packets Received



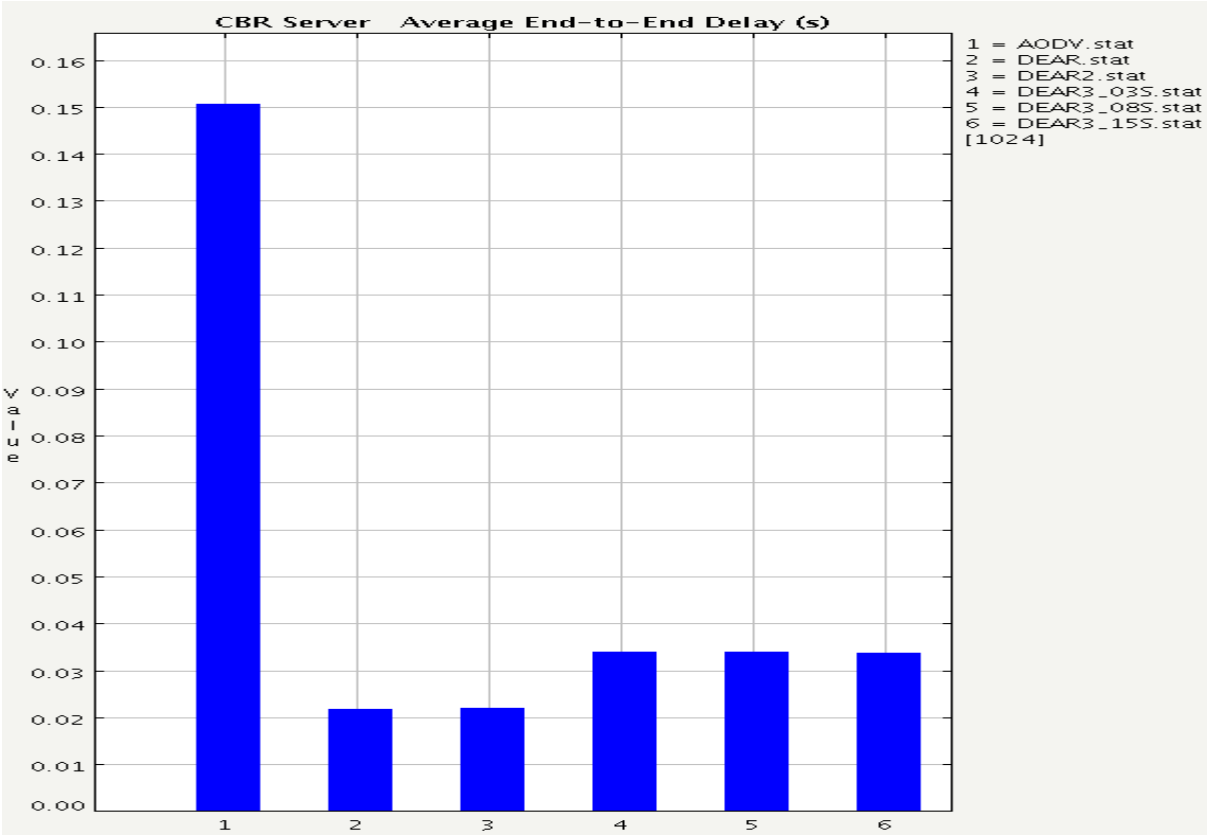
Energy Consumed



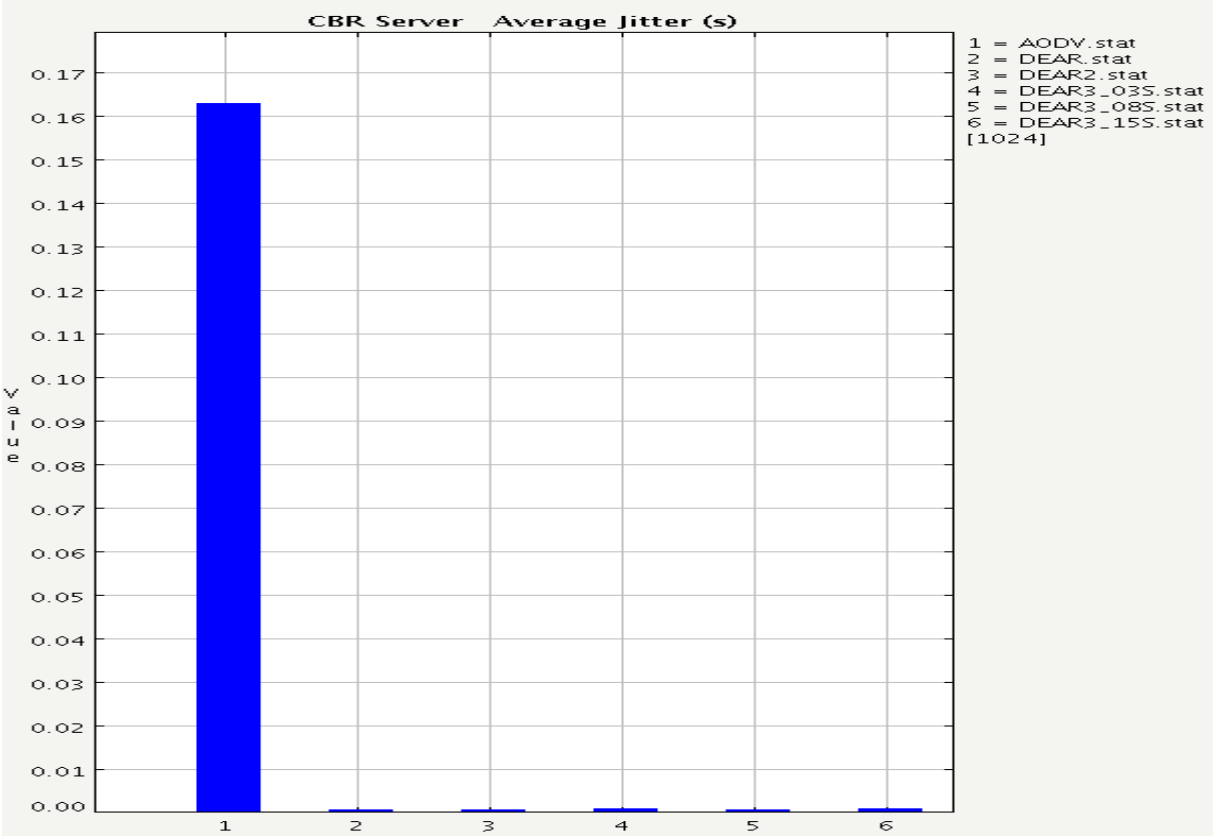
Last Packet Received



Throughput

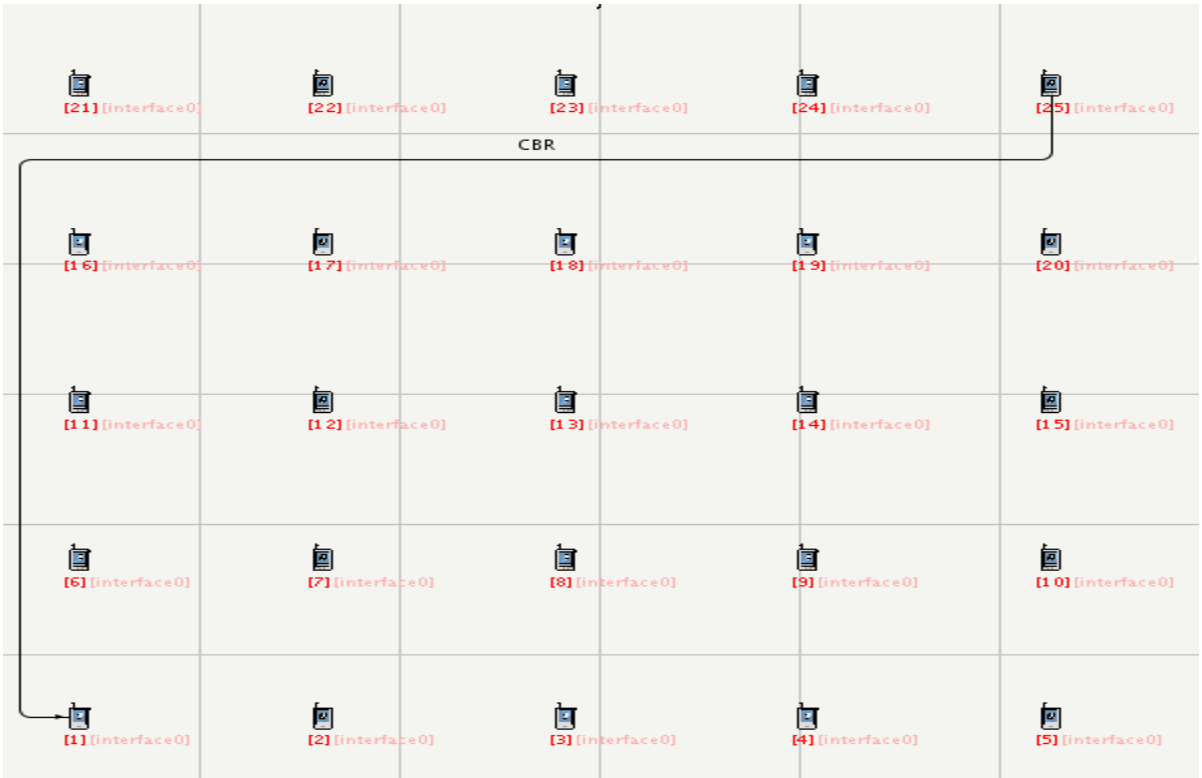


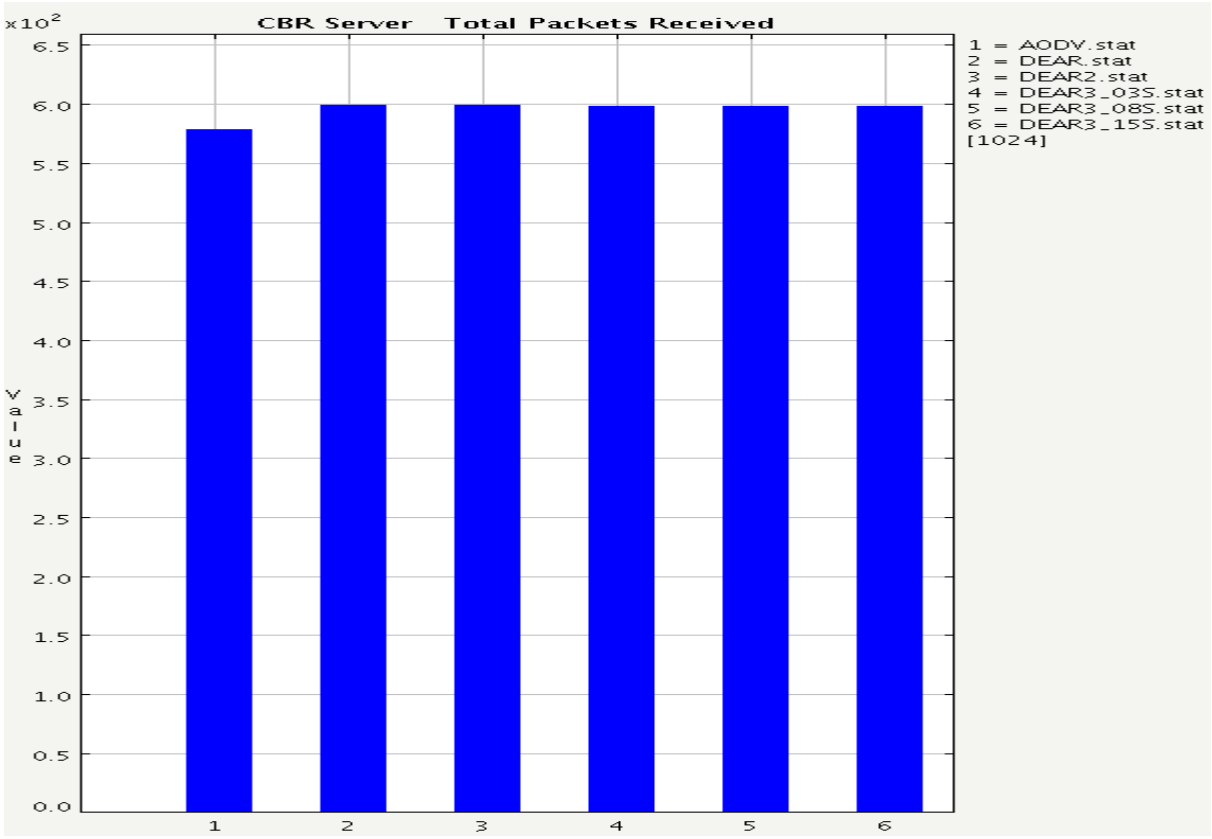
End to End Delay



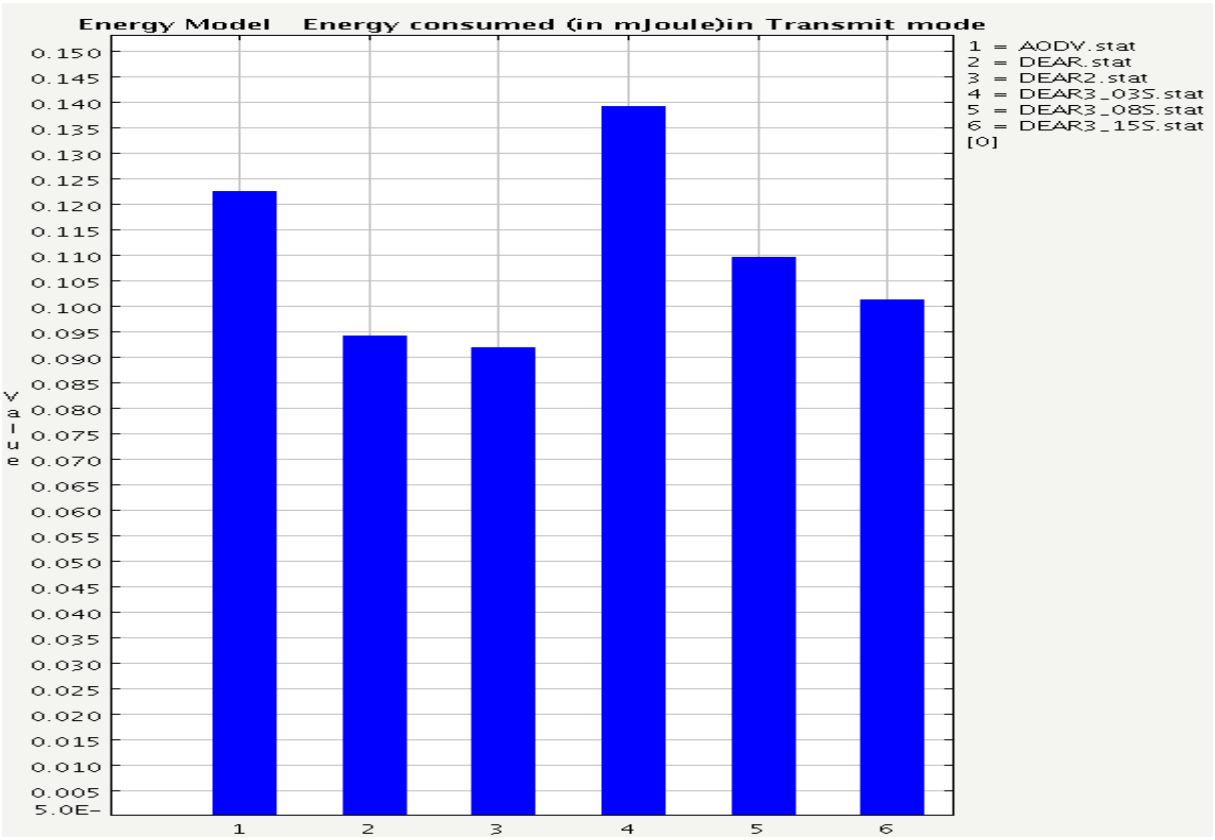
Jitter

6.3 Scenario 3

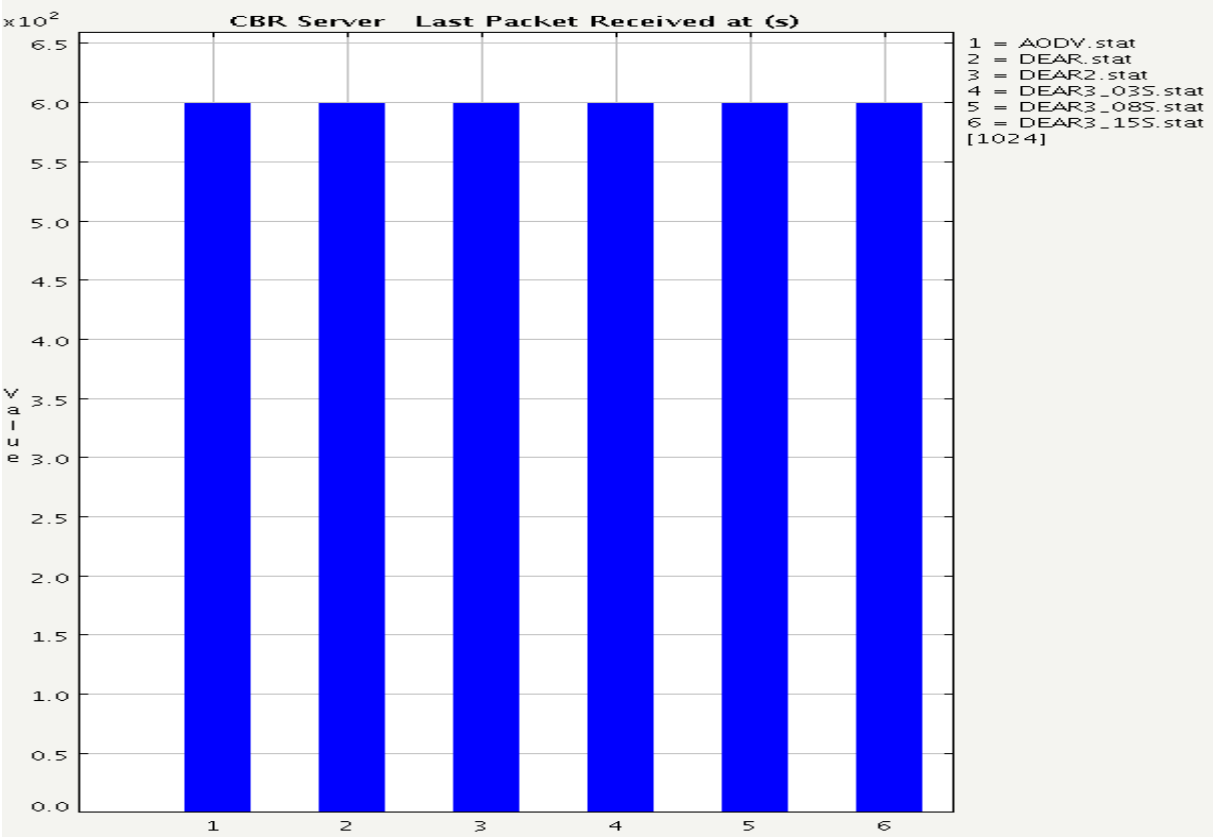




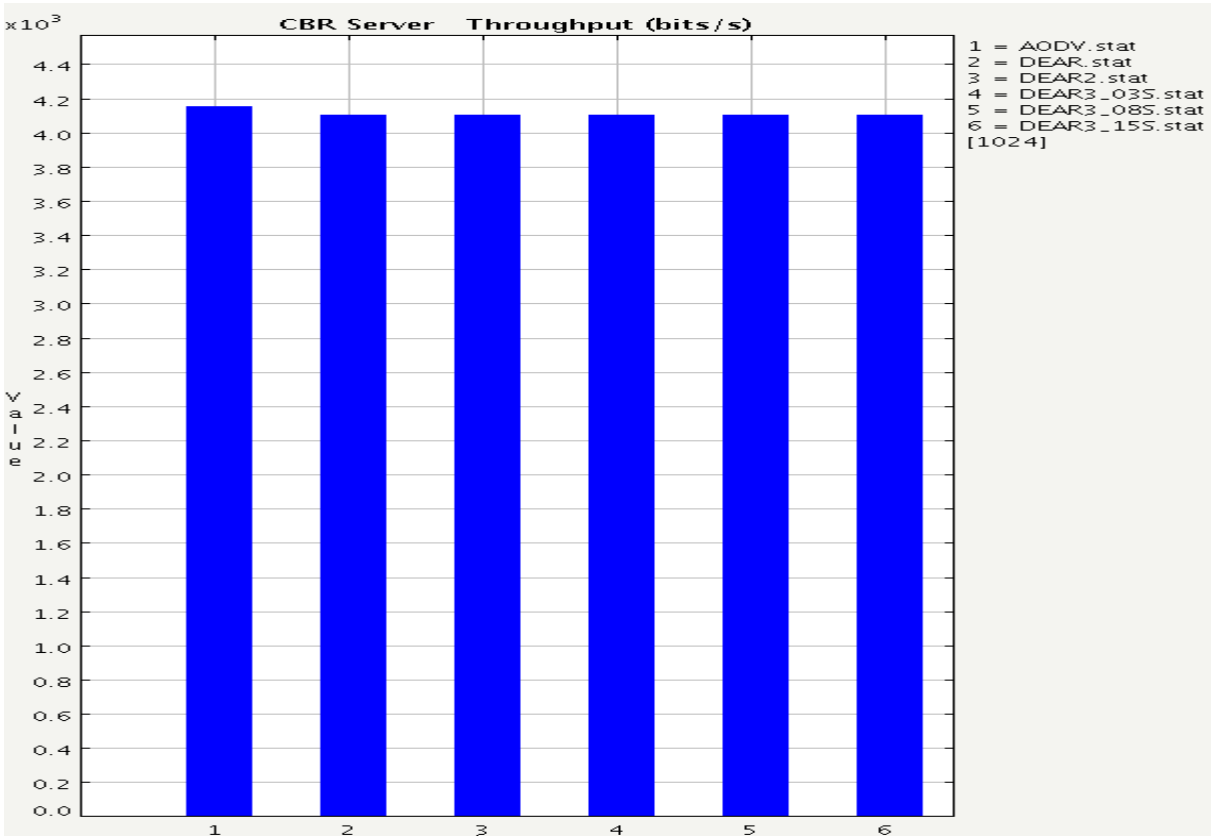
Total Packets Received



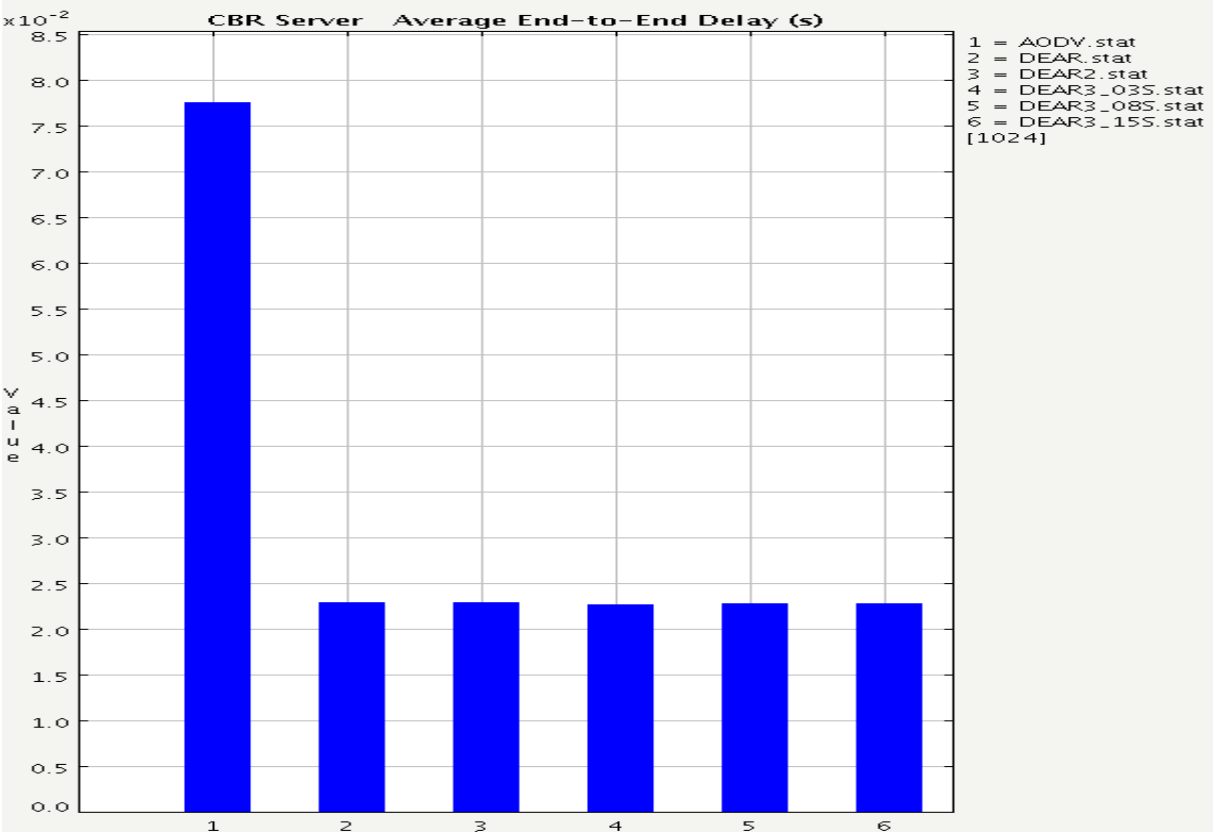
Energy Consumed



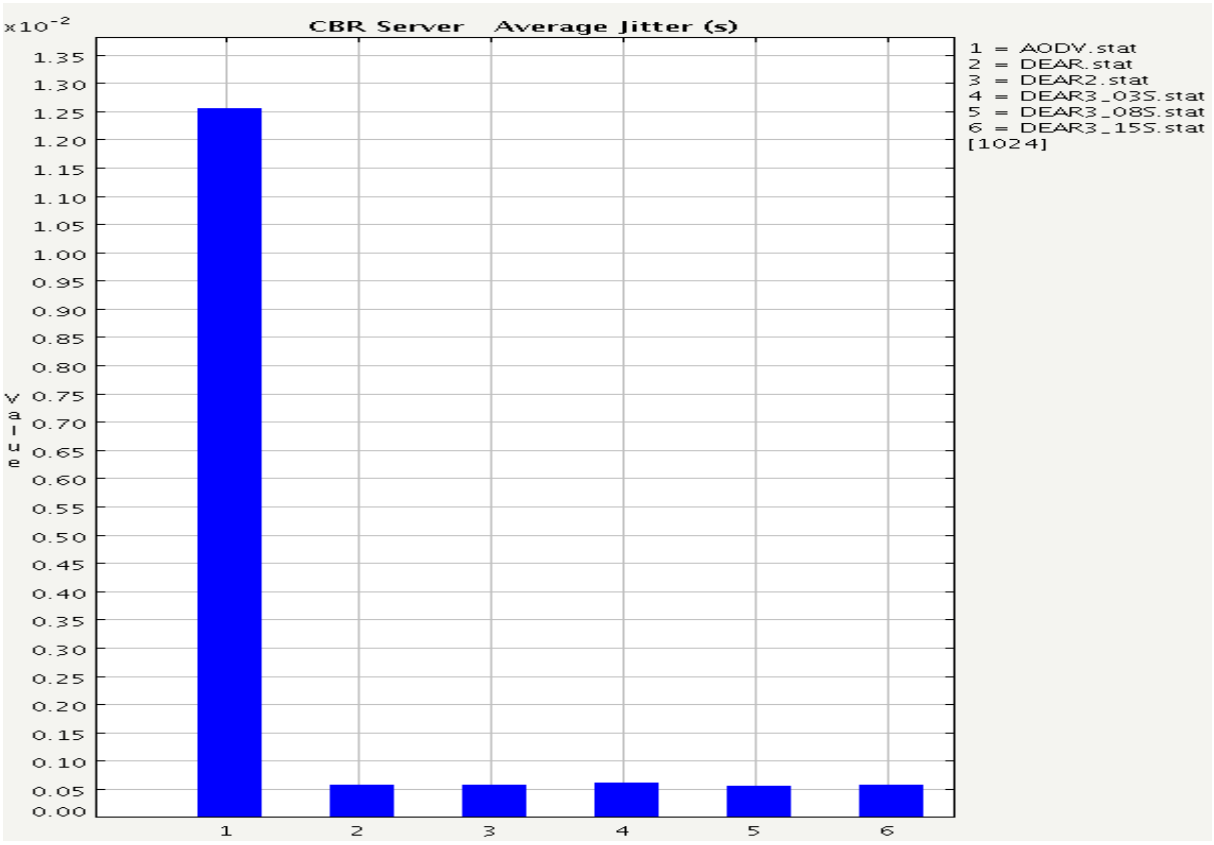
Last Packet Received



Throughput

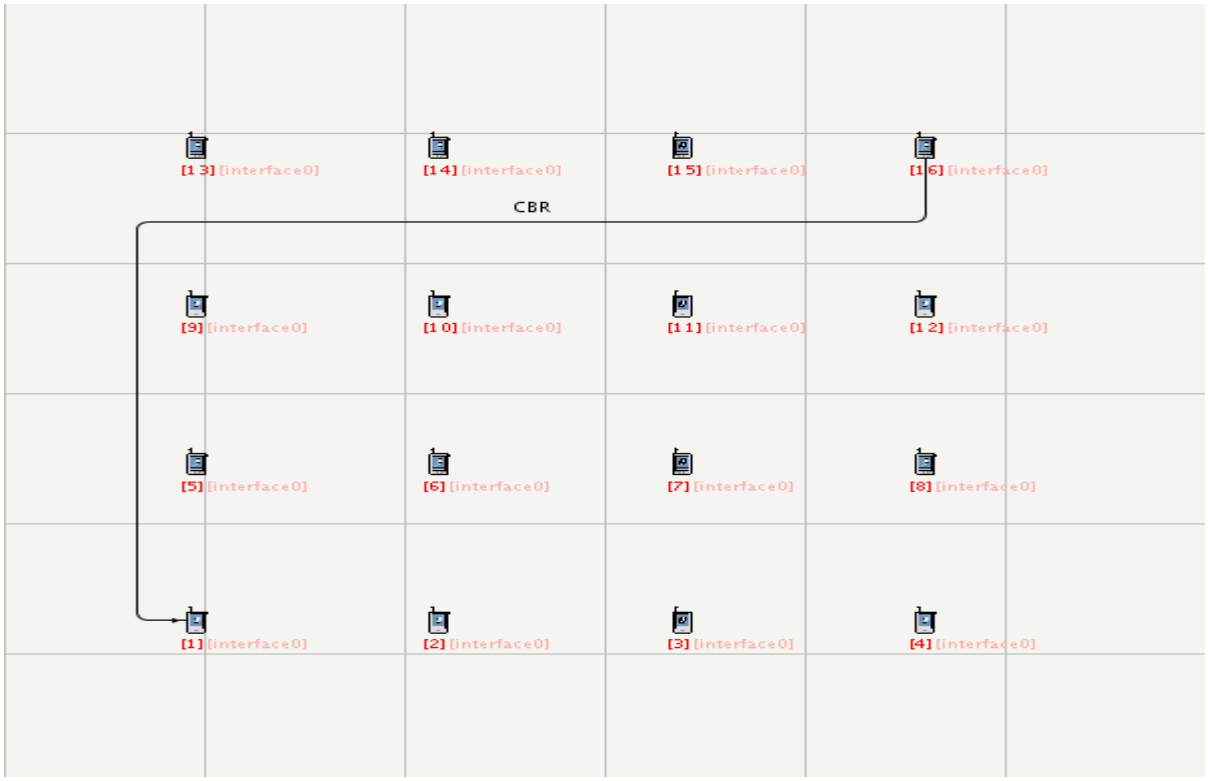


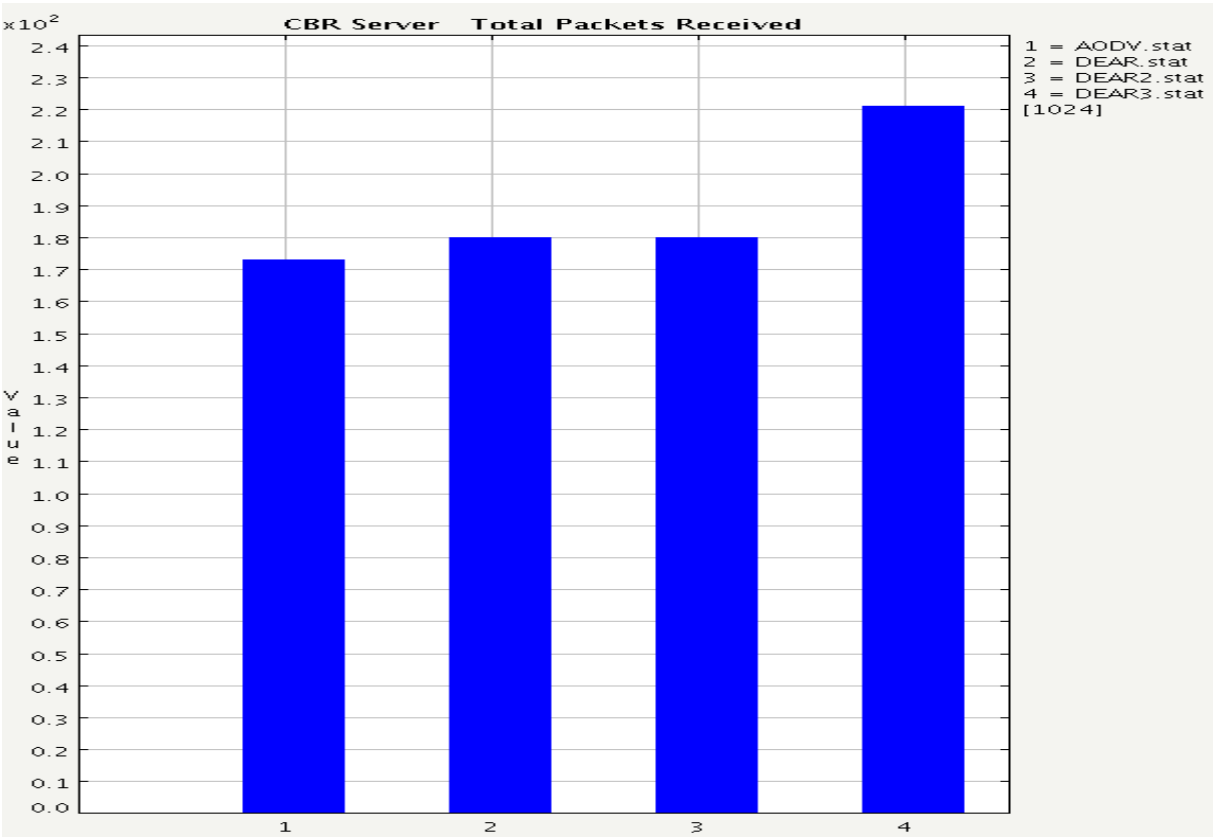
End to End Delay



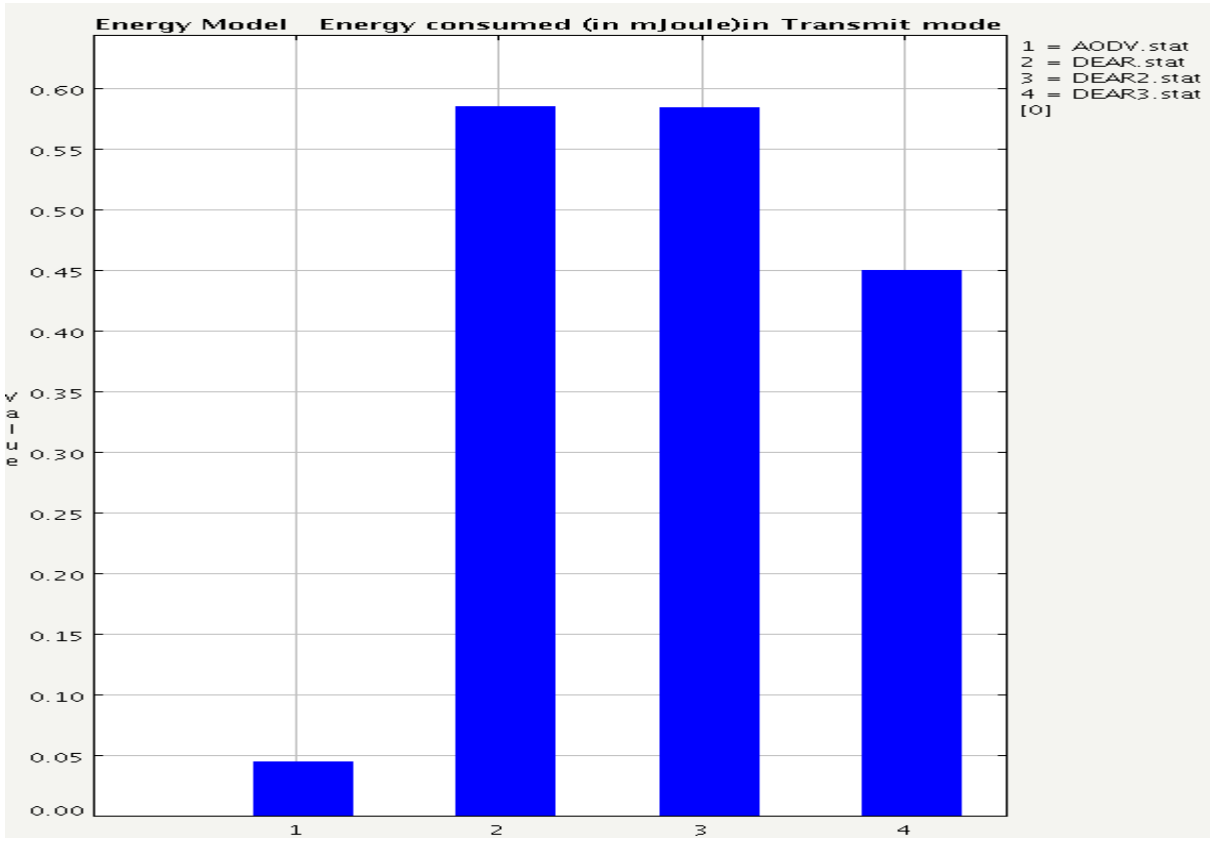
Jitter

6.4 Scenario 4

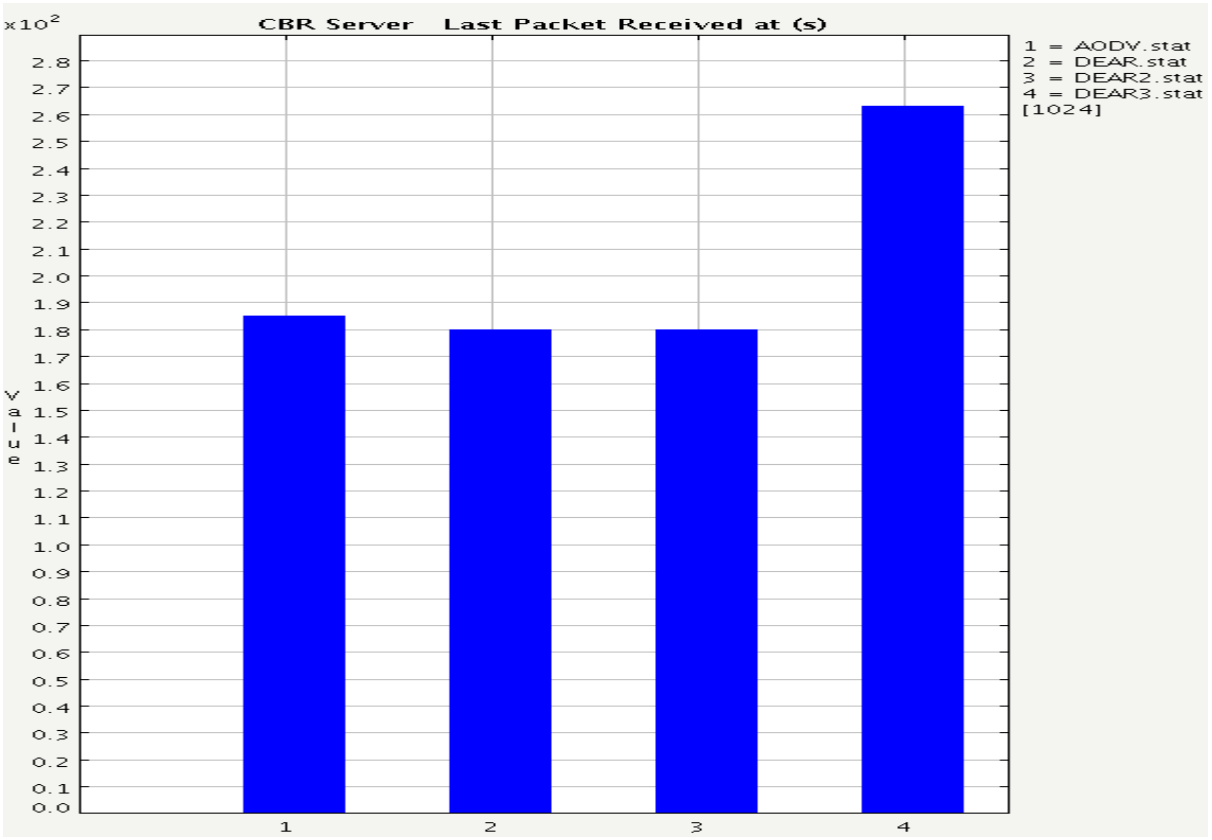




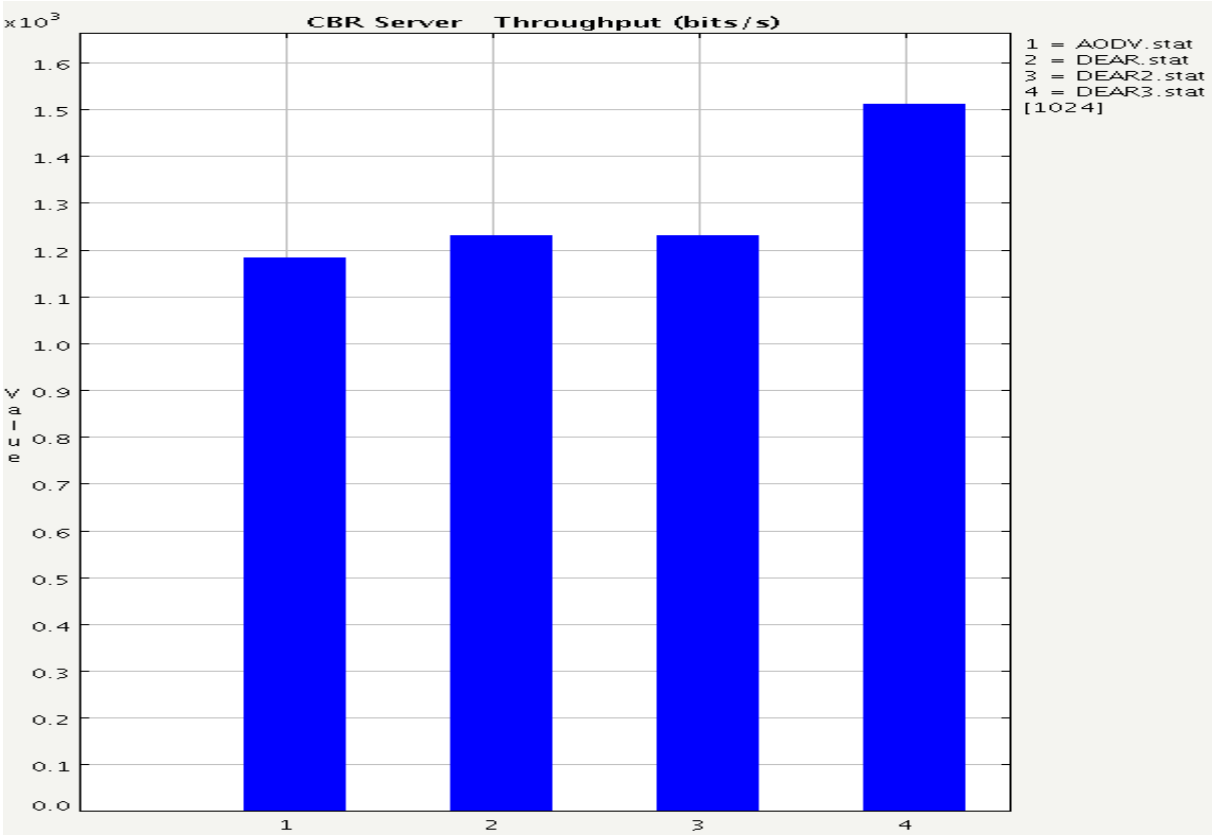
Total Packets Received



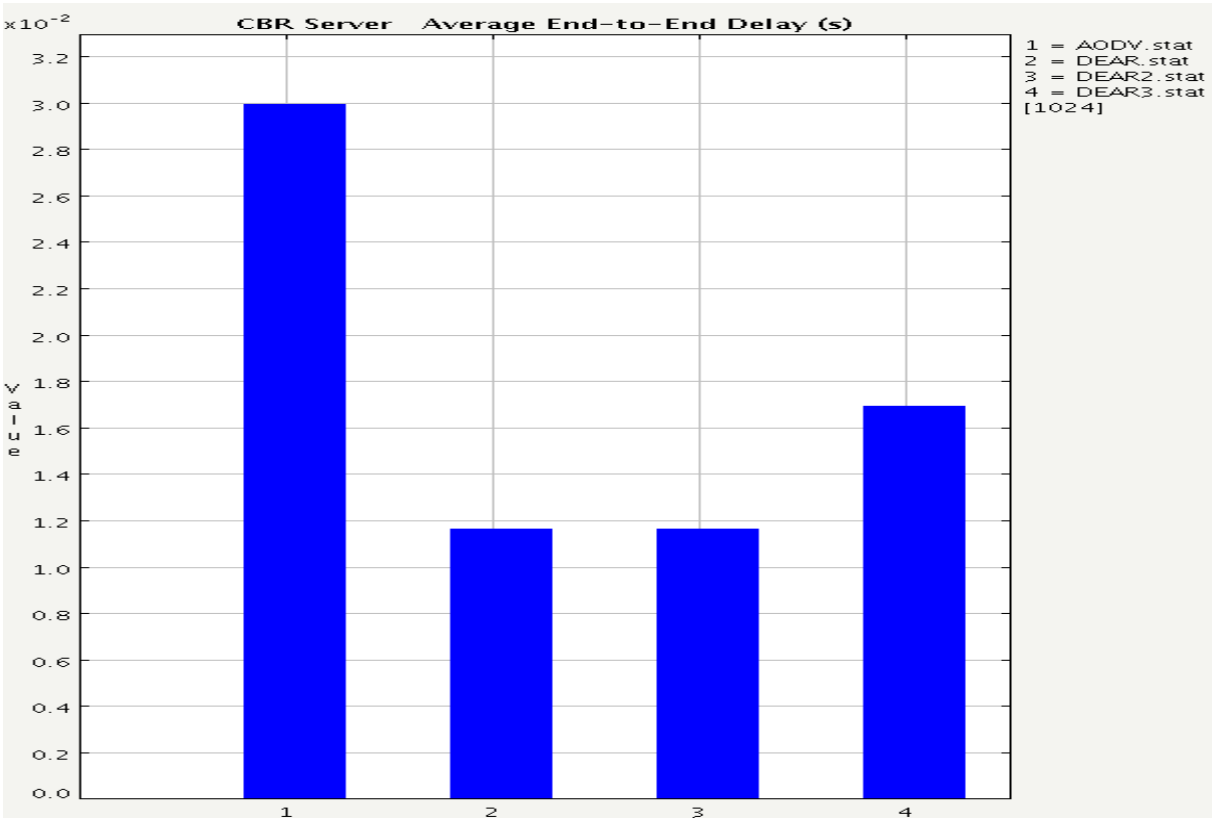
Energy Consumed



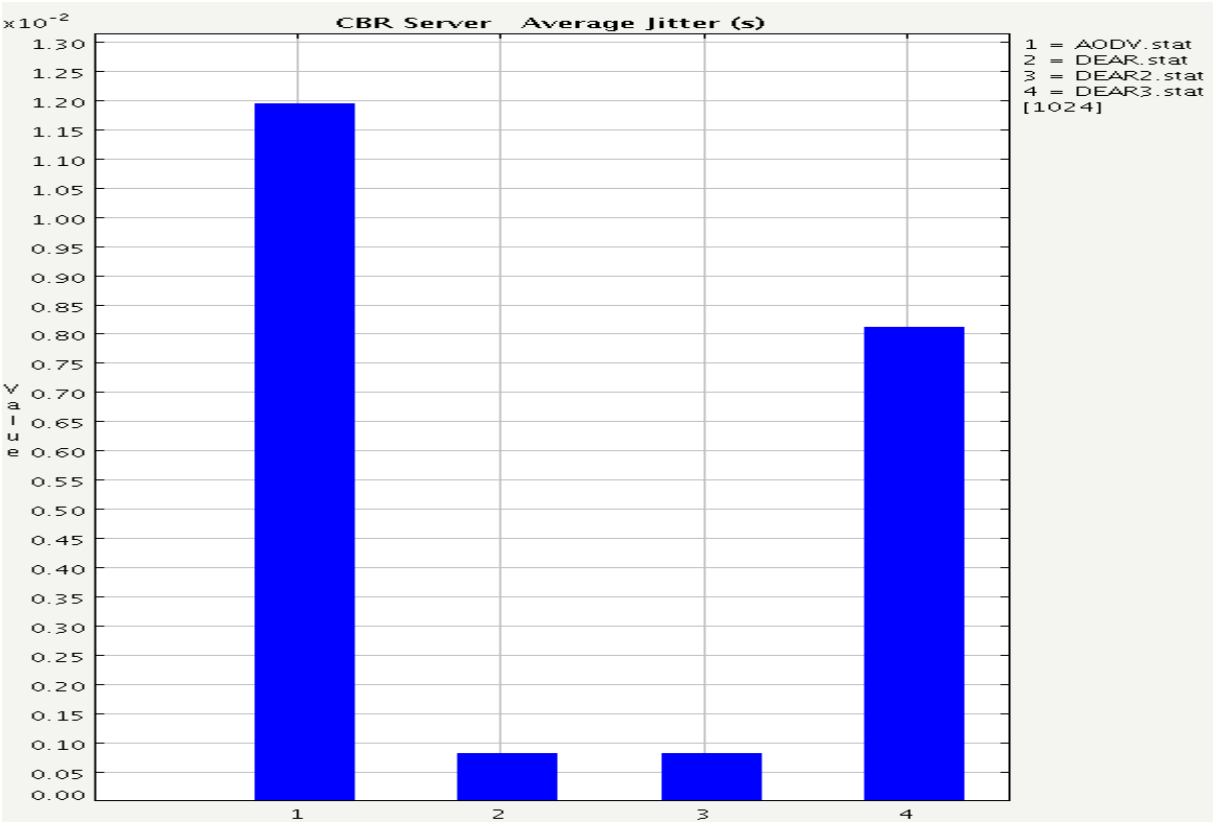
Last Packet Received



Throughput



End to End Delay



Jitter

Chapter 7

Future Scope

Future scope includes the Support for following:

- Mobility – DEAR 2 is implemented only for static scenario which can be further extended to support Mobility.
- Link quality – transmission power can be associated with reliability of the link which is expected to be studied in future [61, 62, 63].
- Multitasking – Since many networks in WSN are used for specific task, major research can be directed towards Multitasking without compromising basic usage of low power devices in WSN.
- Voice Interface – Easy interfacing calls for support for Voice which can be thought of as need of time in near future.

Chapter 8

Conclusion

Sensor networks should be able to achieve energy balance as well as energy efficiency to prolong their lifetimes and prepare for the uncertainties of event generation. Most energy aware routing algorithms are only concerned about energy efficiency. This paper presents a heuristic criterion, called Energy Cost, to consider energy balance and efficiency simultaneously. Using this metric, we have designed and improved the Distributed Energy Adaptive Routing (DEAR) algorithm to produce DEAR 2 and DEAR 3 which overcome limitations of DEAR such as default transmission power, one hop discovery and topology dependence.

References

[1] "21 ideas for the 21st century," Business Week , pp. 78–167, Aug. 30, 1999.

[2] "10 emerging technologies that will change the world," Technology Review , vol. 106, no. 1, pp. 33–49, Feb. 2003.

[3] K. Intae and R. Poovendran, "Maximizing static network lifetime of wireless broadcast ad hoc networks ", in Proceedings of the IEEE International Conference on Communications, 11-15 May 2003, Anchorage, USA, vol. 3, 2003, pp. 2256 – 2261.

[4] W. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks," in Proceedings of the 5th International Conference on Mobile Computing and Ne tworking (Mobicom), 15-19 Aug. 1999, Seattle, USA, 1999, pp. 174–185.

[5] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks," in Proceedings of the 6th International Conference on Mobile Computing and Networking (Mobicom), 6-11 Aug. 2000, Boston, USA , 2000, pp. 56–67.

[6] D. Braginsky and D. Estrin, "Rumor Routing Algorithm for Sensor Networks," in Proceedings of the first Workshop on Sensor Networks and Applications, 28 Sept. 2002, Atlanta, USA , 2002, pp. 22–31.

[7] F. Ye , A. Chen, S. Lu and L. Zhang "A Scalable Solution to Minimum Cost Forwarding in Large Sensor Networks," in Proceedings of the IEEE International Conference on Computer Communication and Networks (ICCCN), 15-17 Oct. 2001, Phoenix, USA, 2001, pp. 304–309.

[8] C. Schurgers and M.B. Srivastava, "Energy efficient routing in wireless sensor networks", in Proceedings of the IEEE Military Communications Conference (MILCOM), 28-31 Oct. 2001, Washington, USA, vol. 1, 2001, pp. 357–361 .

[9] R. C. Shah and J. Rabaey, "Energy Aware Routing for Low Energy Ad Hoc Sensor Networks," in Proceedings of the IEEE Wireless Communications and Networking Conference, 17-21 Mar. 2002, Orlando, USA, vol. 1, 2002, pp. 350–355.

[10] V. Rodoplu and T. H. Meng, "Minimum Energy Mobile Wireless Networks," IEEE Journal on Selected Areas in Communications , vol. 17, no. 8, pp. 1333–1344, Aug. 1999.

[11] S. Servetto and G. Barrenechea, "Constrained Random Walks on Random Graphs: Routing Algorithms for Large Scal e Wireless Sensor Networks," in Proceedings of the first International Workshop on Wireless Se nsor Networks and Applications, 28 Sept. 2002, Atlanta, USA , 2002, pp. 12–21.

[12] L. Li, and J. Y. Halpern, "Minimum-Ener gy Mobile Wireless Networks Revisited," in Proceedings of the IEEE International Conference on Communications (ICC), 11-15 Jun. 2001, Helsinki, Finland, 2001, vol. 1, pp. 278–283.

[13] Sensor Networks: Evolution, Opportunities,and Challenges, chee-yee chong , member, ieee andsrikanta p. kumar , senior member, IEEE

[14] C. Y. Chong, S. Mori, and K. C. Chang, "Distributed multitarget mul-tisensor tracking," in Multitarget Multisensor Tracking: Advanced Applications, Y. Bar-Shalom, Ed. Norwood, MA: Artech House,1990, pp. 247–295.

[15] Proceedings of the Distributed Sensor Nets Workshop. Pittsburgh, PA: Dept. Comput. Sci., Carnegie Mellon Univ., 1978.

[16] R. F. Sproull and D. Cohen, "High-level protocols,"Proc. IEEE, vol.66, pp. 1371–1386, Nov. 1978

[17] R. Rashid and G. Robertson, "Accent: A communication oriented network operating system kernel," in Proc. 8th Symp. Operating System Principles, 1981, pp. 64–75

[18] R. Rashid, D. Julin, D. Orr, R. Sanzi, R. Baron, A. Forin, D. Golub, and M. Jones, "Mach: A system software kernel," in 34th Computer Society Int. Conf. (COMPCON) , San Francisco, CA, 1989.

[19] C. Myers, A. Oppenheim, R. Davis, and W. Dove, "Knowledge-based speech analysis and enhancement," presented at the Int. Conf. Acoustics, Speech and Signal Processing, San Diego, CA, 1984.

[20] "Distributed sensor networks," MIT Lincoln Laboratory, Lexington, MA, Rep. No. ESD-TR-88-175, 1986.

[21] J. W. Gardner, V. K Varadan, and O. O. Awadelkarim, Microsensors, MEMS and Smart Devices. New York: Wiley, 2001.

[22] S. Kumar and D. Shepherd, "SensIT: Sensor information technologyfor the warfighter," in Proc. 4th Int. Conf. on Information Fusion, 2001, pp. TuC1-3–TuC1-9.

[23] J. Corella, "Tactical automated security system (TASS): Air force expeditionary security," presented at the SPIE Conf. Unattended Ground Sensor Technologies and Applications, Orlando, FL, 2003.

[24] J. M. Kahn, R. H. Katz, and K. S. J. Pister, "Mobile networking for smart dust," in Proc. ACM/IEEE Int. Conf. Mobile Computing and Networking (MobiCom), 1999, pp. 271–278.

[25] R. Hills. (2001, July/Aug.) Sensing for danger . Sci. Technol. Rep.[Online] Available: http://www.llnl.gov/str/JulAug01/Hills.html

[27] D. Steere, A. Baptista, D. McNamee, C. Pu, and J. Walpole, "Re-search challenges in environmental observation and forecasting sys-tems," in Proc. 6th Int. Conf. Mobile Computing and Networking (MOBICOMM), 2000, pp. 292–299.

[28] B. Charny. (2002, Dec.) Wireless research senses the future. DNet News[Online] Available: http://zdnet.com.com/2100-1105-976377.html

[29] B. Deb, S. Bhatnagar, and B. Nath, "A topology discovery algorithm for sensor networks with applications to network management," Dept. Comput. Sci., Rutgers Univ., Tech. Rep. DCS-TR-441, 2001.

[30] J. Hightower and G. Borriello, "Location systems for ubiquitous computing," IEEE Computer , vol. 34, pp. 57–66, Aug. 2001

[31] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: Scalable coordination in sensor networks," in Proc. Int. Conf. Mobile Computing and Networking (MOBICOM), 1999, pp. 263–270

[32] P. Gupta and P. R. Kumar, "The capacity of wireless networks," IEEE Trans. Inform. Theory , vol. 46, pp. 388–404, Mar. 2000

[33] Y. Yao and J. E. Gehrke, “Query processing in sensors networks,” in Proc. 1st Biennial Conf. Innovative Data Systems Research (CIDR 2003), Asilomar, CA, 2003.

[34] W. Stallings, Data & Computer Communications, 6th ed., Prentice Hall, New Jersey, p. 453, 2000

[35] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey,” Computer Networks (Elsevier), vol. 38, pp. 393-422, 2002.

[36] Charl Jaco Leuschner, “The design of a simple energy efficient routing protocol to improve wireless sensor network lifetime” April 2005

[37] Bluetooth SIG, “Bluetooth Specification v1. 1,” 2001, http://www.bluetooth.org/spec/.Last accessed on 20 April 2005

[38] L. D. Paulson, “Will ultrawideband technology connect in the marketplace?,” Computer, vol. 36, issue 12, Dec. 2003, pp. 15–17.

[39] IEEE 802.15 WPAN Task Group 4, “IEEE 802.15.4 Standard 2003,” 2003, http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf. Last accessed on 20 April 2005

[40] G. Karayannis, “Emerging Wireless Standards: Understanding the Role of IEEE 802.15.4 & ZigBee in AMR & Submetering,” 2003, http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=820. Last accessed on 21 April 2005.

[41] M. Ilyas, The Handbook of Ad Hoc Wireless Networks , CRC Press, Boca Raton, USA, pp. 14-2 to 14-3, 2003.

[42] J. N. Al-Karaki and A. E. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey,” IEEE Wireless Communications , vol. 11, no. 6, pp. 6–28, Dec. 2004.

[43] A. El-Hoiydi, “Spatial TDMA and CSMA with Preamble Sampling for Low Power Ad Hoc Wireless Sensor Networks”, in Proceedings of the IEEE Symposium on Computers and Communications (ISCC), 1-4 July 2002, Taormina/Giardini Naxos, Italy , 2002, pp. 685–692.

[44] Q. Jiang and D. Manivannan, “Routing protocols for sensor networks”, in Proceedings of the 1st IEEE Consumer Communications and Networking Conference, 5-8 Jan. 2004, Las Vegas, USA , 2004, pp. 93–98.

[45] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: scalable coordination in sensor networks," in Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking. Seattle, Washington, United States: ACM Press, 1999, pp. 263-270.

[46] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," IEEE Communications Magazine , vol. 38, pp. 393-422, 2002.

[47] M. Tubaishat and S. Madria, "Sensor networks: an overview," Potentials, IEEE, vol. 22, pp. 20-23, 2003.

[48] D. Braginsky and D. Estin, "Rumor Routing Algorithm for Sensor Networks," presented at the proceedi ngs of the first Workshop on Sensor Networks and Applications (WSNA), 2002.

[49] A. Rogers, E. David, and N. R. Jennings, "Self-organized routing for wireless microsensor networks," IEEE Transactions on Systems, Man and Cybernetics, Part A , vol. 35, pp. 349-359, 2005.

[50] Z. Butler and D. Rus, "Event-based motion control for mobile-sensor networks," IEEE Pervasive Computing, vol. 2, pp. 34-42, 2003.

[51] E. W. Dijkstra, "A note on two problems in connexion with graphs," Numerische Mathematik , pp. 269-271, 1959.

[52] C. Hedrick, "Routing Information Protocol," in RFC 1058, 1988.

[53] S. Lindsey, C. Raghavendra, and K. M. Sivalingam, "Data Gathering Algorithms in Sensor Networks Using Energy Metrics," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, vol. 13, pp. 924-935, 2002.

[54] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," presented at Proceedings of the 33rd Hawaii International Conference on System Sciences - 2000, 2000

[55] J. Wanger and R. Cristescu, "Power Control for Target Tracking in Sensor Networks," presented at 2005 Conference on Information Sciences and Systems, The Johns Hopkins University, 2005.

[56] R. RWattenhofer, L. Li, P. Bahl, and Y. Wang, "Disributed topology control for power fefficient opera tion in multihop wireless ad hoc networks," presented at INFORCOM 2001, Anchorage, AK, USA, 2001.

[57] R. Ramanathan and R. Rosale s-Hain, "Topology Control of Multihop Wireless Networks using Transmit Power Adjustment," presented at NFOCOM 2000, 2000.

[58] H. Zhang and J. C. Hou, "Maximizing α -Lifetime for Wireless Sensor Networks," presented at SenMetrics 2005, 2005.

[59] M. Stemm and R. H. Katz, "Measuring and reducing energy consumption of network interface in hand-held devices," IEICE Transactions on Communications, vol. E80-B, pp. 1125-1131, 1997.

[60] Shi Bhai, Weiyi Zang, Guoliang Zue, Jian Tang, Chonggang Wang ”DEAR: Delay-bounded Energy-constrained Adaptive Routing in Wireless Sensor Networks”, 2012 Proceedings IEEE INFOCOM, pp 1593- 1601

[61] Himanshu Sharma, Vibhav Kumar Sachan, Syed Akhtar Imam and Monika, "Optimisation of Energy Efficiency in Wireless Sensor Networks using Error Control Codes", 2012 Students Conference on Engineering and Systems (SCES), pp 1-6.

[62] Jin Wang, Imanishimwe Jean de Dieu, Asturias De Leon Diego Jose, Sungyoung Lee, Young-Koo Lee . "Prolonging the Lifetime of Wireless Sensor Networks via Hotspot Analysis", 2010 10th Annual International Symposium on Applications and the Internet, pp 383 – 386.