Energy Efficient Routing Algorithms for Wireless Sensor Networks and Performance Evaluation of Quality of Service for IEEE 802.15.4 Networks

A thesis submitted in partial fulfilment of the requirements for the degree of

Master of Technology (Research)
in
Electronics & Communication Engineering

By

Sanatan Mohanty
Roll No: 60609005

Under the supervision of

Dr. Sarat Kumar Patra
(Professor)

Department of Electronics & Communication Engineering
National Institute of Technology, Rourkela-769008
January 2010

Dedicated to,

WSN research community

Department of Electronics & Communication Engineering
National Institute of Technology, Rourkela
Orissa, India – 769 008

CERTIFICATE

This is to certify that the thesis titled "**Energy Efficient Routing Algorithms for Wireless Sensor Networks and Performance Evaluation of Quality of Service for IEEE 802.15.4 Networks",** submitted to the National Institute of Technology, Rourkela by **Sanatan Mohanty**, Roll No. **60609005** for the award of the degree of **Master of Technology (Research)** in Electronics & Communication Engineering, is a bona fide record of research work carried out by him under my supervision and guidance.

The candidate has fulfilled all the prescribed requirements.

The thesis, which is based on candidate's own work, has not been submitted elsewhere for a degree/diploma.

In my opinion, the thesis is of standard required for the award of a Master of Technology (Research) degree in Electronics & Communication Engineering.

To the best of my knowledge, he bears a good moral character and decent behaviour.

Prof. S. K. Patra
Professor
Email: skpatra@nitrkl.ac.in

## Acknowledgement

I would like to express my deepest gratitude to my supervisor, Prof. (Dr.) S.K. Patra. He introduced me to the field of Wireless Sensor Networks with keen interest and encouragement. I am greatly indebted to him for his valuable advice and moral support during research period.

I am grateful to Prof. G.S.Rath (Chairman), Prof. K.K. Mahapatra, Prof. A.K. Turuk members of MSC for their help and guidance. I am especially grateful to Prof. A.K. Turuk and Prof. B.D Sahoo for proof reading the thesis. I would like to thanks all faculty members for their help and guidance. I am also thankful to all the non-teaching staffs of ECE Department for their kind cooperation during the research period.

I would also like to thanks my friends Prasanta, Badri, Bijaya, Charac, Samarjit, Ayaskanta, Sudendra, Susanta, Jitendra sir and Hiremath for their help during the research period.

Last but not the least, I would like to thank my parents, my brothers and sisters for their support and patience to carry out research at NIT, Rourkela.

Sanatan Mohanty

Abstract

The popularity of Wireless Sensor Networks (WSN) have increased tremendously in recent time due to growth in Micro-Electro-Mechanical Systems (MEMS) technology. WSN has the potentiality to connect the physical world with the virtual world by forming a network of sensor nodes. Here, sensor nodes are usually battery-operated devices, and hence energy saving of sensor nodes is a major design issue. To prolong the network's lifetime, minimization of energy consumption should be implemented at all layers of the network protocol stack starting from the physical to the application layer including cross-layer optimization.

In this thesis, clustering based routing protocols for WSNs have been discussed. In cluster-based routing, special nodes called cluster heads form a wireless backbone to the sink. Each cluster heads collects data from the sensors belonging to its cluster and forwards it to the sink. In heterogeneous networks, cluster heads have powerful energy devices in contrast to homogeneous networks where all nodes have uniform and limited resource energy. So, it is essential to avoid quick depletion of cluster heads. Hence, the cluster head role rotates, i.e., each node works as a cluster head for a limited period of time. Energy saving in these approaches can be obtained by cluster formation, cluster-head election, data aggregation at the cluster-head nodes to reduce data redundancy and thus save energy. The first part of this thesis discusses methods for clustering to improve energy efficiency of homogeneous WSN. It also proposes Bacterial Foraging Optimization (BFO) as an algorithm for cluster head selection for WSN. The simulation results show improved performance of BFO based optimization in terms of total energy dissipation and no of alive nodes of the network system over LEACH, K-Means and direct methods.

IEEE 802.15.4 is the emerging next generation standard designed for low-rate wireless personal area networks (LR-WPAN). The second part of the work reported here in provides performance evaluation of quality of service parameters for WSN based on IEEE 802.15.4 star and mesh topology. The performance studies have been evaluated for varying traffic loads using MANET routing protocol in QualNet 4.5. The data packet delivery ratio, average end-to-end delay, total energy consumption, network lifetime and percentage of time in sleep mode have been used as performance metrics. Simulation results show that DSR (Dynamic Source Routing) performs better than DYMO (Dynamic MANET On-demand) and AODV (Ad–hoc On demand Distance Vector) routing protocol for varying traffic loads rates.

Contents

List of Figures

List of Tables

Acronyms and abbreviations

AODV	ad–hoc on demand distance vector
AES	advanced encryption standard
BE	back-off exponent
BI	beacon interval
BLE	battery life extension
BO	beacon order
BFO	bacteria foraging optimization
BPFK	binary phase shift keying
CAP	contention access period
CCA	clear channel assessment
CDMA	code division multiple access
CFP	contention free period
CH	cluster head
CS	carrier sense
CSMA-CA	carrier Sense multiple access with collision avoidance
CTS	clear-to-send
CW	contention window
DSSS	direct sequence spread spectrum
DSR	dynamic source routing
DYMO	dynamic MANET on-demand
EA	evolutionary algorithms
ED	energy detection
EEPROM	electrical erasable programmable read only memory
ETSI	European Telecommunications Standards Institute
FFD	full functional device
GTS	guaranteed time slot
HEED	hybrid energy efficient distributed clustering
IEEE	Institute of Electrical and Electronics Engineers
IETF	internet engineering task force
ISM	Industrial, Scientific, Medicine bands
ITU	International Telecommunication Union
LEACH	low energy adaptive clustering hierarchy

LLC	logical link control
LR-WPAN	low-rate wireless personal area networks
MAC	medium access control
MANET	mobile ad hoc networks
MEMS	micro-electro-mechanical systems
NB	number of back-off periods
PAN	personal area networks
PDR	packet delivery ratio
PEGASIS	Power-Efficient Gathering in Sensor Information Systems
PHR	phy header
PPDU	protocol packet data unit
PPS	packets per second
PSDU	protocol service data unit
QoS	quality of service
RFD	reduced functional device
RREQ	route request
RREP	route reply
RF	radio frequency
RFD	reduced functional device
RFID	radio frequency identification
RTS	request-to-send
SAPs	service access points
SD	superframe duration
SHIMMER	Sensing Health with Intelligence, Modularity, Mobility, and Experimental Reusability
SHR	synchronization header
SO	superframe order
SSCS	service specific convergence sublayer
TDMA	time division multiple access
TEEN	Threshold sensitive energy efficient sensor network protocol
WSN	wireless sensor networks

Nomenclature

b	bacteria number
c(i)	step size taken in the random direction
*C*prob	constant that limits initial cluster-head candidatures
*E*residual	the residual energy of the node
*E*max	maximum (initial) energy
G	set of nodes that have not been cluster head in the last 1/P rounds
E_{Tx} (k,d)	energy dissipated to transmit a k-bit message over distance d
E_{Tx}-elec(k)	energy dissipated by transmitter electronics
$E_{Tx\text{- amp}}$ (k,d)	energy dissipated by amplifier electronics
E_{elec}	constant energy expended to run the amp and transmitter circuitry
$E_{Rx\text{- elec}}$	energy dissipated by receiver electronics
$J_{cc}(\theta, P(j,k,l))$	cost function value to be added to the actual cost function to be minimized
J_{cc}^{i}	cell- to-cell attractant functions
N_c	chemotactic steps
N_s	swim steps
N_{re}	reproductive steps
N_{ed}	elimination and dispersal steps
P	desired percentage of cluster heads
p	dimension of the search space
P_{ed}	probability of elimination
P	number of parameters to be optimized
r	current round of advertisement phase
S	total number of bacteria
T(n)	threshold number below which node becomes cluster head
θ_m^i	m^{th} component of the i^{th} bacterium at position θ^i
$\phi(j)$	unit length in the random direction
$\theta^i(j+1,k,l)$	i^{th} bacterium at j^{th} chemotactic, k^{th} reproductive and l^{th} elimination and dispersal step

Chapter 1

Introduction

1.1 Introduction

Wireless Sensor Networks(WSN***)*** have gained world-wide attention in recent years due to the advances made in wireless communication, information technologies and electronics field [**1**,**2**,**3**,**4**,**5**].The concept of wireless sensor networks is based on a simple equation: Sensing + CPU + Radio = Thousands of potential applications [**6**] . It is an "**In situ**" sensing technology where tiny, autonomous and compact devices called sensor nodes or motes deployed in a remote area to detect phenomena, collect and process data and transmit sensed information to users. The development of low-cost, low-power, a multifunctional sensor has received increasing attention from various industries. Sensor nodes or motes in WSNs are small sized and are capable of sensing, gathering and processing data while communicating with other connected nodes in the network, via radio frequency (RF) channel.

WSN term can be broadly sensed as devices range from laptops, PDAs or mobile phones to very tiny and simple sensing devices. At present, most available wireless sensor devices are considerably constrained in terms of computational power, memory, efficiency and communication capabilities due to economic and technology reasons. That's why most of the research on WSNs has concentrated on the design of energy and computationally efficient algorithms and protocols, and the application domain has been confined to simple data-oriented monitoring and reporting applications. WSNs nodes are battery powered which are deployed to perform a specific task for a long period of time, even years. If WSNs nodes are more powerful or mains-powered devices in the vicinity, it is beneficial to utilize their computation and communication resources for complex algorithms and as gateways to other networks. New network architectures with heterogeneous devices and expected advances in technology are eliminating current limitations and expanding the spectrum of possible applications for WSNs considerably.

1.2 Wireless sensor node architecture:

The basic block diagram of a wireless sensor node is presented in Figure 1.1. It is made up four basic components: a sensing unit, a processing unit, a transceiver unit and a power unit. There can be application dependent additional components such as a location finding system, a power generator and a mobilizer. A MICAZ mote is shown in Figure 1.2.

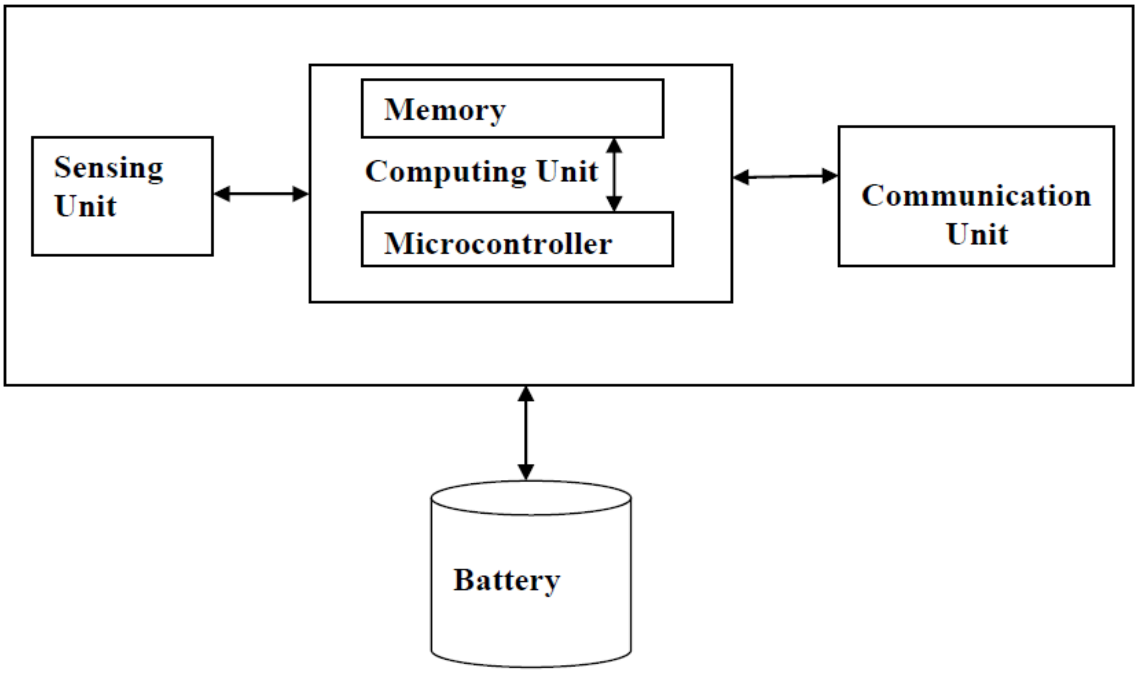


Figure 1. 1: Architecture of a Wireless Sensor Node

Figure 1. 2: MICAZ   Mote [7]

Sensing Unit: Sensing units are usually composed of two subunits: sensors and analog to digital converters (ADCs). Sensor is a device which is used to translate physical phenomena to electrical signals. Sensors can be classified as either analog or digital devices. There exists a variety of sensors that measure environmental parameters such as temperature, light intensity, sound, magnetic fields, image, etc. The analog signals produced by the sensors based on the observed phenomenon are converted to digital signals by the ADC and then fed into the processing unit.

Processing Unit: The processing unit mainly provides intelligence to the sensor node. The processing unit consists of a microprocessor, which is responsible for control of the sensors, execution of communication protocols and signal processing algorithms on the gathered sensor data. Commonly used microprocessors are Intel's Strong ARM microprocessor, Atmel's AVR microcontroller and Texas Instruments' MP430 microprocessor. For example, the processing unit of a smart dust mote prototype is a 4 MHz Atmel AVR8535 micro-controller with 8 KB instruction flash memory, 512 bytes RAM and 512 bytes EEPROM. TinyOS operating system is used on this processor, which has 3500 bytes OS code space and 4500 bytes available code space. The processing unit of µAMPS wireless sensor node prototype has a 59–206 MHz SA-1110 micro-processor. In general, four main processor states can be identified in a microprocessor*: off, sleep, idle and active*. In sleep mode, the CPU and most internal peripherals are turned on, and can only be activated by an external event (interrupt). In idle mode, the CPU is still inactive, but other peripherals are active.

Transceiver Unit: The radio enables wireless communication with neighbouring nodes and the outside world. It consists of a short range radio which usually has single channel at low data rate and operates at unlicensed bands of 868-870 MHz (Europe), 902-928 MHz (USA) or near 2.4 GHz (global ISM band). For example, the TR1000 family from RF Monolithics works in the 800–900 MHz range can dynamically change its transmission power up to 1.4 mW and transmit up to 115.2 Kbps. The Chipcon's CC2420 is included in the MICAZ mote that was built to comply with the IEEE 802.15.4 standard [**8**] for low data rate and low cost wireless personal area networks.

There are several factors that affect the power consumption characteristics of a radio, which includes the type of modulation scheme used, data rate, transmit power and the operational duty cycle. At transmitted power levels of -10dBm and below, a majority of the transmit mode power is dissipated in the circuitry and not radiated from the antenna. However, at high transmit levels (over 0dBm) the active current drown by the transmitter is high. The transmit power levels for sensor node applications are roughly in the range of -10 to +3 dBm [**9**]. Similar to microcontrollers, transceivers can operate in *Transmit, Receive, Idle and Sleep* modes. An important observation in the case of most radios is that, operating in *Idle* mode results in significantly high power consumption, almost equal to the power consumed in the *Receive* mode. Thus, it is important to completely shut down the radio rather than set it in the *idle* mode when it is not transmitting or receiving due to the high power consumed. Another influencing factor is that, as the radio's operating mode changes, the transient activity in the radio electronics causes a significant amount of power dissipation. The sleep mode is a very important energy saving feature in WSNs.

Battery - The battery supplies power to the complete sensor node. It plays a vital role in determining sensor node lifetime. The amount of power drawn from a battery should be carefully monitored. Sensor nodes are generally small, light and cheap, the size of the battery is limited. AA batteries normally store 2.2 to 2.5 Ah at 1.5 V. However, these numbers vary depending on the technology utilized. For example, Zinc–air-based batteries have higher capacity in Joules/cm3 than lithium batteries. Alkaline batteries have the smallest capacity, normally around 1200 J/cm3. Furthermore, sensors must have a lifetime of months to years, since battery replacement is not an option for networks with thousands of physically embedded nodes. This causes energy consumption to be the most important factor in determining sensor node lifetime.

1.3 Applications of Wireless Sensor Networks

According to a new report from research firm ON World "The home market for Wireless Sensor Networks (WSN) will reach US$6 billion a year by 2012". The prediction includes both products and services centred on in-home energy management and health monitoring. Meanwhile, ON World predicts the market for "Home Area Network" (HAN) energy management solutions to reach 20 million homes worldwide by 2013.

Wireless Sensor Networks may consist of many different types of sensors such as seismic, low sampling rate magnetic, thermal, visual, infrared, acoustic and radar. They are able to monitor a wide variety of ambient conditions that include temperature, humidity, vehicular movement, lightning condition, pressure, soil makeup, noise levels, the presence or absence of certain kinds of objects, mechanical stress levels on attached objects, and the current characteristics such as speed, direction and size of an object. WSN applications can be classified into two categories [3] as shown in Figure 1.3:

- Monitoring
- Tracking

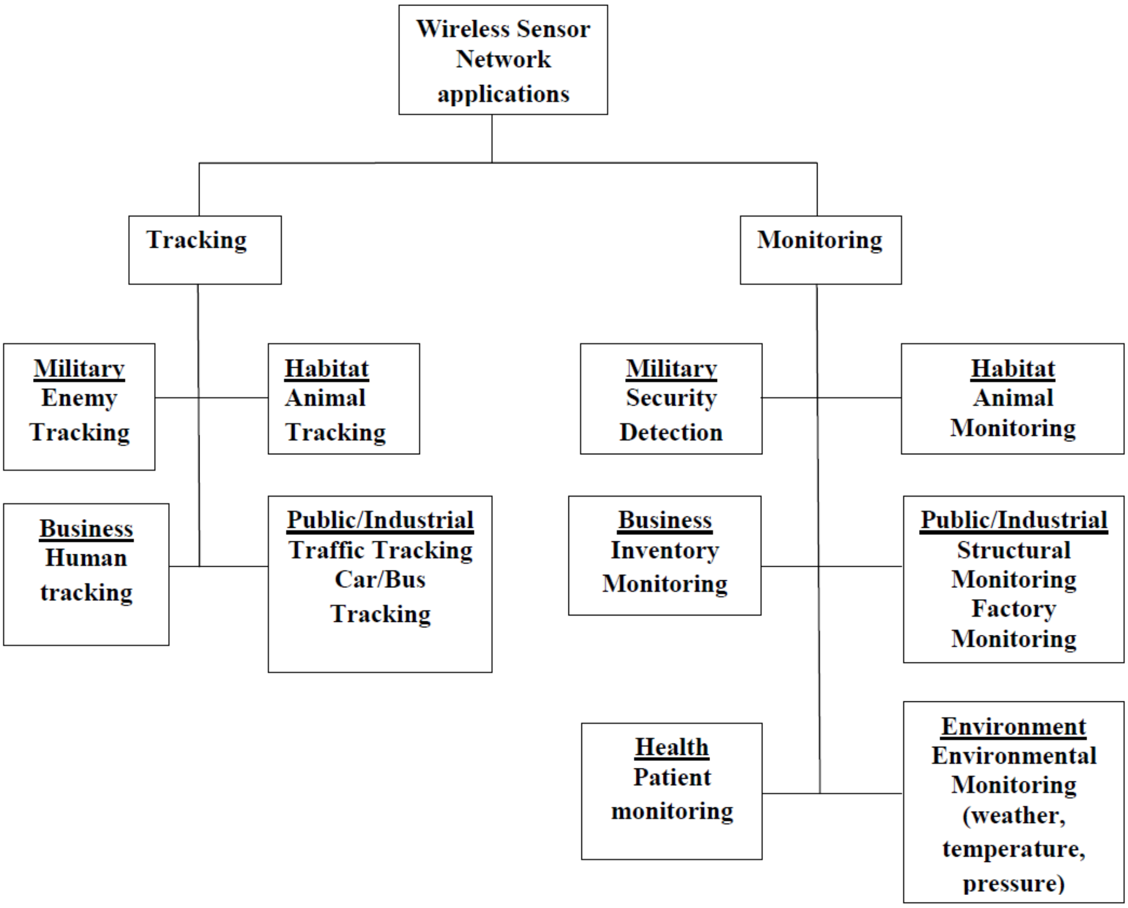


Figure 1. 3: Overview of Wireless Sensor Network applications [3]

Monitoring applications include indoor/outdoor environmental monitoring, health and wellness monitoring, power monitoring, inventory location monitoring, factory and process automation, and seismic and structural monitoring. Tracking applications include tracking objects, animals, humans, and vehicles and categorize the applications into military, environment, health, home and other commercial areas. It is possible to expand this classification with more categories such as space exploration, chemical processing and disaster relief.

Military applications: The rapid deployment, self-organization and fault tolerance characteristics of sensor networks make them a very promising sensing technique for military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting (C4ISRT) systems. Military sensor networks could be used to detect and gain as much information as possible about enemy movements, explosions, and other phenomena of interest, such as battlefield surveillance, nuclear, biological and chemical attack detection and reconnaissance. As an example, PinPtr [**10**] is an experimental counter-sniper system developed to detect and locate shooters. The system utilizes a dense deployment of sensors to detect and measure the time of arrival of muzzle blasts and shock waves from a shot. Sensors route their measurements to a base station (e.g., a laptop or PDA) to compute the shooter's location. Sensors in the PinPtr system are second-generation Mica2 motes connected to a multi-purpose acoustic sensor board. Each multi-purpose acoustic sensor board is designed with three acoustic channels and a Xilinx Spartan II FPGA. Mica2 motes run on a TinyOS [**11**] operating system platform that handles task scheduling, radio communication, time, I/O processing, etc. Middleware services developed on TinyOS that are exploited in this application include time synchronization, message routing with data aggregation, and localization.

Environmental applications: Wireless Sensor Networks have been deployed for environmental monitoring, which involves tracking the movements of small animals and monitoring environmental conditions that affect crops and livestock. In these applications, WSNs collect readings over time across a space large enough to exhibit significant internal variation. Other applications of WSNs are chemical and biological detection, precision agriculture, biological, forest fire detection, volcanic monitoring, meteorological or geophysical research, flood detection and pollution study.

Macroscope of redwood [**12**] is a case study of a WSN that monitors and records the redwood trees in Sonoma, California. Each sensor node measures air temperature, relative humidity, and photo-synthetically-active solar radiation. Sensor nodes are placed at different heights of the tree. Plant biologists track changes of spatial gradients in the microclimate around a redwood tree and validate their biological theories.

Underwater monitoring study in [**13**] developed a platform for underwater sensor networks to be used for long term monitoring of coral reefs and fisheries. The sensor network consists of static and mobile underwater sensor nodes. The nodes communicate via point-to-point links using high speed optical communications. Nodes broadcast using an acoustic protocol integrated in the TinyOS protocol stack. They have a variety of sensing devices, including temperature and pressure sensing devices and cameras. Mobile nodes can locate and move above the static nodes to collect data and perform network maintenance functions for deployment, re-location, and recovery. Similarly, ZebraNet [**14**] system is a mobile wireless sensor network used to track animal migrations.

Healthcare applications: WSN based technologies such as Ambient Assisted Living and Body Sensor Networks provide dozens of solutions to healthcare's biggest challenges such as an aging population and rising healthcare costs. Body sensor networks can be used to monitor physiological data of patients The Body sensor networks can provide interfaces for disabled, integrated patient monitoring. It can monitor and detect elderly people's behaviour, e.g., when a patient has fallen. These small sensor nodes allow patients a greater freedom of movement and allow doctors to identify pre-defined symptoms earlier on. The small installed sensor can also enable tracking and monitoring of doctors and patients inside a hospital. Each patient has small and lightweight sensor nodes attached to them, which may be detecting the heart rate and blood pressure. Doctors may also carry a sensor node, which allows other doctors to locate them within the hospital.

AT&T recently introduced a telehealth monitoring service that uses ZigBee and WiFi. Mote Track [**15**] is the patient tracking system developed by Harvard University, which tracks the location of individual patient’s devices indoors and outdoors, using radio signal information from the sensor attached to the patients. Heart@Home is a wireless blood pressure monitor and tracking system. Heart@Home uses a SHIMMER mote located inside a wrist cuff which is connected to a pressure sensor. A user’s blood pressure and heart rate is computed using the oscillometric method. The SHIMMER mote records the reading and sends it to the T-mote connected to the user’s computer. A software application processes the data and provides a graph of the user’s blood pressure and heart rate over time.

Home applications: With the advance of technology, the tiny sensor nodes can be embedded into furniture and appliances, such as vacuum cleaners, microwave ovens and refrigerators.

They are able to communicate with each other and the room server to learn about the services they offer, e.g., printing, scanning and faxing. These room servers and sensor nodes can be integrated with existing embedded devices to become self-organizing, self-regulated and adaptive systems to form a smart environment. Automated homes with Personal Area Networks such as ZigBee [**16**] can provide the ability to monitor and control mechanisms like light switches and lights, HVAC (heating, ventilating, air conditioning) controls and thermostats; computers, TVs and other electronic devices, smoke detectors and other safety equipment; alarm panels, motion sensors, and other security devices; and electricity, water and gas meters.

Traffic control: Traffic conditions can be easily monitored and controlled at peak times by WSNs. Temporary situations such as roadworks and accidents can be monitored in situ. Further, the integration of monitoring and management operations, such as signpost control, is facilitated by a common WSN infrastructure.

1.4 Background Literature Survey

In 1981, Baker and Ephremides proposed a clustering algorithms called “Linked cluster algorithm (LCA)” [**17**] for wireless networks. To enhance network manageability, channel efficiency and energy economy of MANETS, Clustering algorithms have been investigated in the past. Lin and Gerla investigated effective techniques to support multimedia applications in the general multi-hop mobile ad-hoc networks using CDMA based medium arbitration in [**18**]. Random competition based clustering (RCC) [**19**] is applicable both to mobile ad hoc networks and WSN. RCC mainly focuses at cluster stability in order to support mobile nodes. The RCC algorithm applies the First Declaration Wins rule, in which any node can ‘‘govern’’ the rest of the nodes in its radio coverage if it is the first to claim being a CH. Some of well known clustering algorithms for mobile ad hoc networks presented in the literature are Cluster Gateway Switch Routing Protocol (CGSR) [**20**], Cluster-Based Routing Protocol (CBRP) [**21**], Weighted Clustering Algorithm (WCA) [**22**]. A survey of clustering algorithms for mobile ad hoc networks has been discussed in [**23**].

In recent years, insect sensory systems have been inspirational to new communications and computing models like bio inspired routing. It is due to their ability to support features like autonomous, and self-organized adaptive communication systems for pervasive environments like WSN and mobile ad hoc networks. Biological synchronization phenomena have great potential to enable distributed and scalable synchronization algorithms for WSN [**24**]. The first MANET routing algorithm in the literature to take inspiration from ants are Ant-Colony Based Routing Algorithm (ARA) [**25**], AntNet [**26**], AntHocNet [**27**] etc. In [**28**], an energy efficient and delay-aware routing algorithm is proposed based on ant-colony-based algorithms. In [**29**], a bio-inspired scalable network synchronization protocol for large scale sensor networks is proposed, which is inspired by the simple synchronization strategies in biological phenomena such as flashing fireflies and spiking of neurons. A biologically inspired distributed synchronization algorithm introduced in [**30**] is based on a mathematical model. It explains how neurons and fireflies spontaneously synchronize. In [**31**], the principles of genetics and evolution are adopted to enable service-oriented, autonomous, and self-adaptive communication systems for pervasive environments such as WSN and mobile ad hoc networks. In [**32**], efficient bio-inspired communication paradigm for WSN is proposed based on the feedback loop mechanism developed by inspiration from the principles of cell biology. In [**33**], a clustering algorithm based on biological quorum sensing mechanism is mentioned. It helps the sensor nodes to form clusters according to spatial characteristics of the observed event signal.

QoS is the ability of a network element (e.g. an application, host or router) to have some level of assurance that its traffic and service requirements can be satisfied. QoS manages bandwidth according to application demands and network management settings. QoS has been extensively studied in wireless LANs and wired computer networks. IP and Asynchronous Transfer Mode (ATM) provide extensive QoS support ranging from best-effort service to guaranteed service.

A comprehensive overview of the state of the field of QoS in networking was provided by Chen in his thesis in 1999 [**34**]. Chakrabarti and Mishra [**35**] summarized the important QoS-related issues in MANETs and the future work that required further attention is provided in [**36**]. In 2004, Al-Karaki and Kamal [**37**] presented a detailed overview about the state of and the development trends in the field of QoS. It categorized routing into the following types of approaches: flat (all nodes play an equal role), hierarchical (some nodes are local cluster heads for example), position based (utilize location information), and power-aware (take battery usage and residual charge into consideration) QoS routing. Finally, a detailed overview of the more widely accepted MAC and routing solutions for providing better QoS was presented in [**38**,**39**].

1.4 Thesis Contributions

The work reported herein investigates two aspects of WSN.

(a) Energy efficient routing algorithm for WSN.

(b) Quality of service evaluation in IEEE 802.15.4 networks.

The first part investigates clustering techniques for cluster head selection to provide energy efficiency for WSN. Here, bacteria foraging optimization based clustering algorithm has been proposed which is seen to provide better performance than LEACH, K-Means and direct method. In the second part, QoS has been evaluated for IEEE 802.15.4 standard based star and peer to peer networks. Different performance metrics like packet delivery ratio, average end-to- end delay, throughput, network lifetime and total energy consumption have been analyzed for MANET routing algorithms AODV, DSR and DYMO.

1.5 Thesis Outline

The thesis has been organized in the following manner.

Following this chapter, Chapter 2 presents extensive literature survey on routing algorithms for WSNs. It mainly discusses energy efficient clustering routing algorithms related to WSNs. IEEE 802.15.4 standard, ZigBee and its applications have been discussed in Chapter 3. It mainly discusses physical and medium access control (MAC) protocol of IEEE 802.15.4.

In chapter 4, a novel bio-inspired clustering algorithm called **Bacteria foraging optimization (BFO)** has been proposed for increasing Network Lifetime of WSNs. To validate the algorithm, simulations have been carried out in MATLAB and compared with other protocols like LEACH, K-Means and direct method. Simulation results show better performance of BFO as compared to other protocols in terms of performance metrics like number of alive nodes and total energy dissipation in the system.

Quality of service for IEEE 802.15.4 using MANET routing protocols (AODV, DSR and DYMO) have been discussed in chapter 5. Performance evaluation of metrics like packet delivery ratio (PDR), throughput, energy per goodput bit, network lifetime of battery model, average end to end delay and energy consumption in different modes like transmission, reception, idle, sleep etc. have been presented. Performance of star and peer to peer topology based IEEE 802.15.4 networks have also been evaluated for varying traffic loads.

Chapter-6 presents the contributions of thesis. The chapter also provides the limitations of the work reported here in and lists the future research scopes from the studies undertaken.

Chapter 2

Literature Survey of routing algorithms for WSN

2.1 Introduction

Wireless sensor networks have their own unique characteristics which create new challenges for the design of routing protocols for these networks. First, sensors are very limited in transmission power, computational capacities, storage capacity and most of all, in energy. Thus, the operating and networking protocol must be kept much simpler as compared to other ad hoc networks. Second, due to the large number of application scenarios for WSN, it is unlikely that there will be a one-thing-fits-all solution for these potentially very different possibilities. The design of a sensor network routing protocol changes with application requirements. For example, the challenging problem of low-latency precision tactical surveillance is different from that required for a periodic weather-monitoring task. Thirdly, data traffic in WSN has significant redundancy since data is probably collected by many sensors based on a common phenomenon. Such redundancy needs to be exploited by the routing protocols to improve energy and bandwidth utilization. Fourth, in many of the initial application scenarios, most nodes in WSN were generally stationary after deployment. However, in recent development, sensor nodes are increasingly allowed to move and change their location to monitor mobile events, which results in unpredictable and frequent topological changes [**40**,**41**].

Due to such different characteristics, many new protocols have been proposed to solve the routing problems in WSN. These routing mechanisms have taken into consideration the inherent features of WSN, along with the application and architecture requirements. To minimize energy consumption, routing techniques proposed in the literature for WSN employ some well-known ad hoc routing tactics, as well as, tactics special to WSN, such as data aggregation and in-network processing, clustering, different node role assignment and data-centric methods. In the following sections, introduce to current research on routing protocols have been presented.

2.2 Routing Challenges and Design Issues in WSNs

Despite plethora of applications of WSN, these networks have several restrictions, e.g., limited energy supply, limited computing power, and limited bandwidth of the wireless links connecting sensor nodes. One of the main design goals of WSN is to carry out data communication while trying to prolong the lifetime of the network and prevent connectivity degradation by employing aggressive energy management techniques. In order to design an efficient routing protocol, several challenging factors should be addressed meticulously. The following factors are discussed below:

Node deployment: Node deployment in WSN is application dependent and affects the performance of the routing protocol. The deployment can be either deterministic or randomized. In deterministic deployment, the sensors are manually placed and data is routed through pre-determined paths; but in random node deployment, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner. Hence, random deployment raises several issues as coverage, optimal clustering etc. which need to be addressed.

Energy consumption without losing accuracy: sensor nodes can use up their limited supply of energy performing computations and transmitting information in a wireless environment. As such, energy conserving forms of communication and computation are essential. Sensor node lifetime shows a strong dependence on the battery lifetime. In a multihop WSN, each node plays a dual role as data sender and data router. The malfunctioning of some sensor nodes due to power failure can cause significant topological changes and might require rerouting of packets and reorganization of the network.

Node/Link Heterogeneity: Some applications of sensor networks might require a diverse mixture of sensor nodes with different types and capabilities to be deployed. Data from different sensors, can be generated at different rates, network can follow different data reporting models and can be subjected to different quality of service constraints. Such a heterogeneous environment makes routing more complex.

Fault Tolerance: Some sensor nodes may fail or be blocked due to lack of power, physical damage, or environmental interference. The failure of sensor nodes should not affect the overall task of the sensor network. If many nodes fail, MAC and routing protocols must accommodate formation of new links and routes to the data collection base stations. This may require actively adjusting transmit powers and signaling rates on the existing links to reduce energy consumption, or rerouting packets through regions of the network where more energy is available. Therefore, multiple levels of redundancy may be needed in a fault-tolerant sensor network.

Scalability: The number of sensor nodes deployed in the sensing area may be in the order of hundreds or thousands, or more. Any routing scheme must be able to work with this huge number of sensor nodes. In addition, sensor network routing protocols should be scalable enough to respond to events in the environment. Until an event occurs, most of the sensors can remain in the sleep state, with data from the few remaining sensors providing a coarse quality.

Network Dynamics: Most of the network architectures assume that sensor nodes are stationary. How-ever, mobility of both BS's and sensor nodes is sometimes necessary in many applications. Routing messages from or to moving nodes is more challenging since route stability becomes an important issue, besides energy, bandwidth etc. Moreover, the sensed phenomenon can be either dynamic or static depending on the application, e.g., it is dynamic in a target detection/tracking application, while it is static in forest monitoring for early fire prevention. Monitoring static events allows the network to work in a reactive mode, simply generating traffic when reporting. Dynamic events in most applications require periodic reporting and consequently generate significant traffic to be routed to the BS.

Transmission Media: In a multi-hop sensor network, communicating nodes are linked by a wireless medium. The traditional problems associated with a wireless channel (e.g., fading, high error rate) may also affect the operation of the sensor network. As the transmission energy varies directly with the square of distance therefore a multi-hop network is suitable for conserving energy. But a multi-hop network raises several issues regarding topology management and media access control. One approach of MAC design for sensor networks is to use CSMA-CA based protocols of IEEE 802.15.4 that conserve more energy compared to contention based protocols like CSMA (e.g. IEEE 802.11). So, Zigbee which is based upon IEEE 802.15.4 LWPAN technology is introduced to meet the challenges.

Connectivity: The connectivity of WSN depends on the radio coverage. If there continuously exists a multi-hop connection between any two nodes, the network is connected. The connectivity is *intermittent* if WSN is partitioned occasionally, and *sporadic* if the nodes are only occasionally in the communication range of other nodes.

Coverage: The coverage of a WSN node means either sensing coverage or communication coverage. Typically with radio communications, the communication coverage is significantly larger than sensing coverage. For applications, the sensing coverage defines how to reliably guarantee that an event can be detected. The coverage of a network is either sparse, if only parts of the area of interest are covered or dense when the area is almost completely covered. In case of a redundant coverage, multiple sensor nodes are in the same area.

Data Aggregation: Sensor nodes usually generate significant redundant data. So, to reduce the number of transmission, similar packets from multiple nodes can be aggregated. Data aggregation is the combination of data from different sources according to a certain aggregation function, e.g., duplicate suppression, minima, maxima and average. It is incorporated in routing protocols to reduce the amount of data coming from various sources and thus to achieve energy efficiency. But it adds to the complexity and makes the incorporation of security techniques in the protocol nearly impossible.

Data Reporting Model: Data sensing and reporting in WSNs is dependent on the application and the time criticality of the data reporting. In wireless sensor networks data reporting can be continuous, query-driven or event-driven. The data-delivery model affects the design of network layer, e.g., continuous data reporting generates a huge amount of data therefore, the routing protocol should be aware of data-aggregation

Quality of Service: In some applications, data should be delivered within a certain period of time from the moment it is sensed; otherwise the data will be useless. Therefore bounded latency for data delivery is another condition for time-constrained applications. However, in many applications, conservation of energy, which is directly related to network lifetime, is considered relatively more important than the quality of data sent. As the energy gets depleted, the network may be required to reduce the quality of the results in order to reduce the energy dissipation in the nodes and hence lengthen the total network lifetime. Hence, energy-aware routing protocols are required to capture this requirement.

2.3 Classification of Routing Protocols in WSNs

In general, routing in WSNs can be divided into flat-based routing, hierarchical-based routing, and location-based routing depending on the network structure. In flat-based routing, all nodes are typically assigned equal roles or functionality. In hierarchical-based routing, however, nodes will play different roles in the network. In location-based routing, sensor nodes' positions are exploited to route data in the network.

A routing protocol is considered adaptive if certain system parameters can be controlled in order to adapt to the current network conditions and available energy levels. Furthermore, these protocols can be classified into multipath-based, query-based, negotiation-based, QoS-based, or routing techniques depending on the protocol operation. In addition to the above, routing protocols can be classified into three categories, namely, proactive, reactive, and hybrid protocols depending on how the source sends a route to the destination. In proactive protocols, all routes are computed before they are really needed, while in reactive protocols, routes are computed on demand. Hybrid protocols use a combination of these two ideas. When sensor nodes are static, it is preferable to have table driven routing protocols rather than using reactive protocols. A significant amount of energy is used in route discovery and setup of reactive protocols. Another class of routing protocols is called the cooperative routing protocols. In cooperative routing, nodes send data to a central node where data can be aggregated and may be subject to further processing, hence reducing route cost in terms of energy usage.

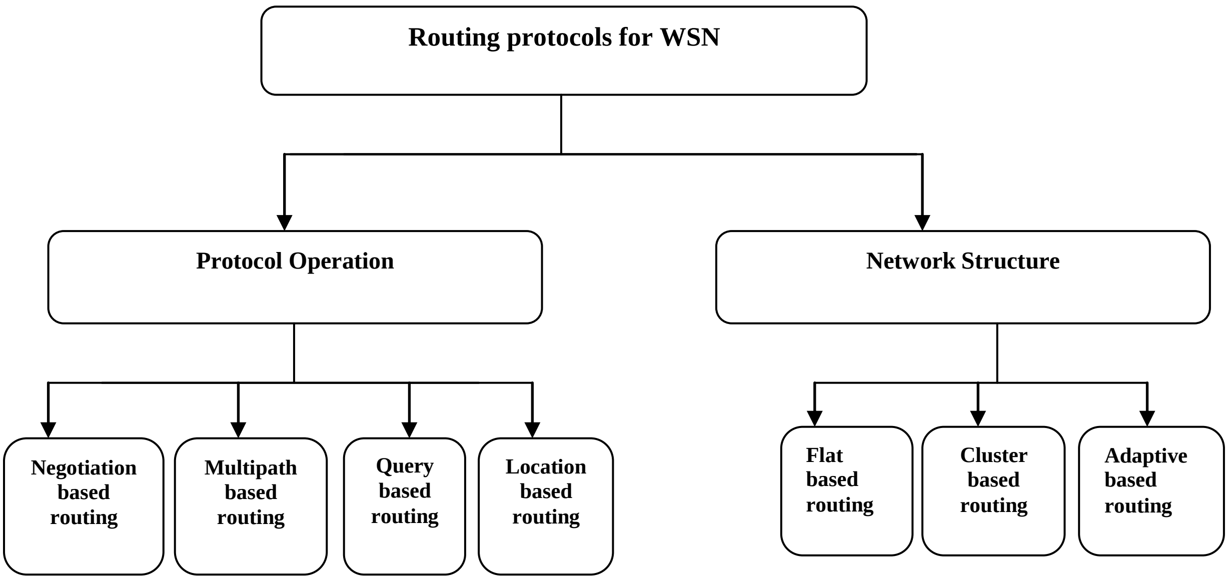


Figure 2.1: Taxonomy of routing protocols for WSN

2.3.1 The routing protocols for protocol operation

Negotiation based routing: These protocols use high-level data descriptors called "meta-data" in order to eliminate redundant data transmission through negotiations. The necessary decisions are based on available resources and local interactions.

Sensor Protocols for Information via Negotiation (SPIN) [**42**] is one of well known Negotiation based routing protocol for WSN. The SPIN protocols are designed to disseminate the data of one sensor to all other sensors assuming these sensors are potential base-stations. Hence, the main idea of negotiation based routing in WSN is to suppress duplicate information and prevent redundant data from being sent to the next sensor or the base-station by conducting a series of negotiation messages before the real data transmission begins.

Multipath based routing: These protocols offer fault tolerance by having at least one alternate path (from source to sink) and thus, increasing energy consumption and traffic generation. These paths are kept alive by sending periodic messages.

Maximum Lifetime Routing in Wireless Sensor Networks [**43**] is a protocol that routes data through a path whose nodes have the largest residual energy. The path is switched whenever a better path is discovered. The primary path will be used until its energy is below the energy of the backup path. By means of this approach, the nodes in the primary path will not deplete their energy resources through continual use of the same route, thus achieving longer lifetime. A disadvantage for applications that require mobility on the nodes, is that the protocol is oriented to solve routing problem in static wireless networks.

Hierarchical Power-aware Routing in Sensor Networks [**44**] protocol enhances the reliability of WSN by using multipath routing. It is useful for delivering data in unreliable environments. The idea is to define many paths from source to sink and send through them the same subpackets. This implies that the traffic will increase significantly (not energy aware), but increasing the reliability of the network. The idea is to split the original data packet into subpackets through each path. This can offer at the end, even with the loss of subpackets, the reconstruction of the original message.

Query based routing: In these protocols, the destination nodes propagate a query for data (sensing task or interest) from the node through the network. The nodes containing this data send it back to the node that has initiated the query.

Rumor routing protocol [**45**] is one of the routing protocol used in the context of event notification. The approach does not flood the network with information about an event occurrence but only installs few paths in the network by sending out one or several agents. The agents propagate through the network installing routing information about the event in each node that is visited. When the agents come across shorter paths or more efficient paths, they optimize the paths in the routing tables accordingly. Each node can also generate an agent in a probabilistic fashion.

Location based routing: In the protocols, the nodes are addressed by their location. Distances to next neighbouring nodes can be estimated by signal strengths or by GPS receivers.

Location based routing protocols are: .Small Minimum Energy Communication Network (SMECN) [**46**] protocol sets up and maintains a minimum energy network for wireless networks by utilizing low power GPS. Although, the protocol assumes a mobile network, it is best applicable to sensor networks, which are not mobile.

Geographic Adaptive Fidelity (GAF) [**47**] protocol is energy-aware location-based routing designed primarily for mobile ad hoc networks and can be applicable to sensor networks as well. GAF keeps energy by turning off unnecessary nodes in the network without affecting the level of routing fidelity. It forms a virtual grid for the covered area. Each node uses its GPS-indicated location to associate itself with a point in the virtual grid. Nodes associated with the same point on the grid are considered equivalent in terms of the cost of packet routing. Such equivalence is exploited in keeping some nodes located in a particular grid area in sleeping state in order to save energy. Thus, GAF can substantially increase the network lifetime as the number of nodes increase. GAF protocol has both for non-mobility (GAFbasic) and for mobility (GAF-mobility adaptation) of nodes.

Geographic and Energy Aware Routing (GEAR) [**48**] is the protocol which uses geographic information while disseminating the queries to the areas of interest since data queries often includes geographic attributes. The protocol uses energy aware and geographically informed neighbour selection to route a packet towards the target area. GEAR can complement directed diffusion by restricting the number of interests sent, and only considering a certain area rather than sending the interests to the whole network. In GEAR, each node keeps an estimated cost and a learning cost of reaching the destination through its neighbours.

A virtual relative position based routing protocol for sensor networks that provides methods for data management is Virtual Cord Protocol (VCP) [**49**]. VCP is a Distributed Hash Table like protocol that offers an efficient routing mechanism, besides standard DHT functions. The key characteristics of VCP are the geographical vicinity of virtual neighbors, which reduces the communication load, VCP only needs information about direct neighbors for routing, and it cannot be stuck with dead ends. The protocol is easy to be implemented on the top of a typical MAC layer. All data items are associated with numbers in a pre-defined range is captured by the available nodes.

2.3.2 The routing protocols for network structure

Flat based routing: In these protocols, all nodes have assigned equal roles in the network. The well known protocols considered in flat based routing are: Sequential Assignment Routing (SAR), .Directed Diffusion, Energy Aware Routing (EAR) etc.

Sequential Assignment Routing [**50**] proposed was one of the first protocols for WSN that considered QoS issues for routing decisions. The objective of SAR algorithm is to minimize the average weighted QoS metric throughout the lifetime of the network .SAR makes a routing decision based on three factors: energy resources, QoS planned for each path, and the packet's traffic type, which is implemented by a priority mechanism. To resolve reliability problems, SAR uses two systems consisting of a multipath approach and localized path restoration done by communicating with neighboring nodes. The multipath tree is defined by avoiding nodes with low-energy or QoS guarantees while taking into account that the root tree is located in the source node and its ends in the sink nodes set. In other words, SAR creates a multipath table whose main objective is to obtain energy efficiency and fault tolerance. Although this ensures fault tolerance and easy recovery, the protocol suffers certain overhead when tables and node states must be maintained or refreshed. This problem increases especially when there are a large number of nodes.

Directed diffusion (DD) [**51**] is a data-centric and application aware paradigm since all data generated by sensor nodes are named by attribute value pairs. The objective of the directed diffusion paradigm is to aggregate the data coming from different sources by deleting redundancy, which drastically reduces the number of transmissions. This has two main consequences: First, the network saves energy and extends its life. Secondly, it counts on a higher bandwidth in the links near the sink node. The latter factor could be quite persuasive in deciding to provide QoS in real-time applications.

The directed diffusion paradigm is based on a query-driven model, which means that the sink node requests data by broadcasting interests. Requests can originate from humans or systems and are defined as pair values, which describe a task to be done by the network. The interests are then disseminated through the network. This dissemination sets up gradients to create data that will satisfy queries to the requesting node. When the events begin to appear, they start to flow toward the originators of interest along multiple paths. This behavior provides reliability for data transmissions in the network. Another feature of directed diffusion is that it caches network data, generally the attribute-value pair's interests. Caching can increase efficiency, robustness, and the scalability of coordination between sensor nodes, which is the essence of the directed diffusion paradigm.

A new energy-aware WSN routing protocol, reliable and energy efficient protocol (REEP) is proposed in [**52**]. REEP is also a fault tolerant. REEP has been motivated by the existing network layer data-centric routing protocol directed diffusion. REEP makes sensor nodes establish more reliable and energy-efficient paths for data transmission. In addition, the energy conservation heuristic of SPIN-2 has been used to maintain an energy threshold value in each REEP node in order to make the sensor nodes energy-aware.

REEP consists of five important elements. These are: sense event, information event, request event, energy threshold value and request priority queue (RPQ). A 'sense event' is a kind of query, which is generated at the sink node and is supported by the sensor network for acquiring information. The response of this query is the 'information event', which is generated at the source node. It specifies the detected object type and the location information of the source node. After receiving this information, 'request events' are generated at the sink node and are used for path setup to retrieve the real data. The real data in any sensor network are the collected or processed information regarding any physical phenomenon. Each node in REEP uses an 'energy threshold value' by checking which node agrees or denies for participating in path setup with adequate energy for data transmission. It gives more reliable transmission of any event information or real data. RPQ is a kind of first-in-first-out (FIFO) queue, which is used in each node to track over the sequence of 'information event' reception from different neighbours. It is used to select a neighbour with highest priority in order to request for path setup in case of failed path, without invoking periodic flooding.

The authors used four performance metrics like average packet transmission, average data loss ratio, average delay and average energy consumption to analyse and compare the performance of both protocols DD and REEP. The performance of REEP has been found to be superior to directed-diffusion routing protocol.

Energy Aware Routing [**53**] is a reactive protocol to increase the lifetime of the network. This protocol maintains a set of paths instead of maintaining or reinforcing one optimal path. The maintenance and selection depends on a certain probability, which relays on how low the energy consumption of each path can be achieved. The protocol creates routing tables about the paths according to the costs. Localized flooding is performed by the destination node to maintain the paths alive.

Hierarchical based routing: It is also known as cluster-based routing. In these protocols, the nodes can play different roles in the network and normally the protocol includes the creation of clusters. Additionally, designations of tasks for the sensor nodes with different characteristics are also performed.

Low Energy Adaptive Clustering Hierarchy (LEACH) is one of the most popular clustering algorithms with distributed cluster formation for WSNs [**54**,**55**]. The algorithm randomly selects cluster heads and rotates the role to distribute the consumption of energy. LEACH uses TDMA/CDMA MAC to reduce inter-cluster and intra-cluster collisions and data collection is centralized with defined periods. It forms clusters based on the received signal strength and uses the CH nodes as routers to the base-station. All the data processing such as data fusion and aggregation are local to the cluster. LEACH forms clusters by using a distributed algorithm, where nodes make autonomous decisions without any centralized control. Initially a node decides to be a CH with a probability P and broadcasts its decision. Each non-CH node determines its cluster by choosing the CH that can be reached using the least communication energy. The role of being a CH is rotated periodically among the nodes of the cluster in order to balance the load.

The rotation is performed by getting each node to choose a random number ''T'' between 0 and 1. A node becomes a CH for the current rotation round if the number is less than the following threshold:

Where P is the desired percentage of CH nodes in the sensor population

r is the current round number

G is the set of nodes that have not been CHs in the last 1/P rounds.

Since the decision to change the CH is probabilistic, there is a good chance that a node with very low energy gets selected as a CH. When this node dies, the whole cell becomes dysfunctional. Also, the CH is assumed to have a long communication range so that the data can reach the base-station from the CH directly. This is not always a realistic assumption since the CHs are regular sensors and the base-station is often not directly reachable to all nodes due to signal propagation problems, e.g., due to the presence of obstacles. LEACH also forms one-hop intra- and inter cluster topology where each node can transmit directly to the CH and thereafter to the base-station. Consequently, it is not applicable to networks deployed in large regions.

The HEED protocol [**56**,**57**] is an energy-efficient clustering protocol designed for WSNs. The aim of the algorithm is to prolong the lifetime of a WSN. In HEED cluster-head selection is based on two different parameters. The primary parameter is the residual energy of each node, while the second parameter measures the intracluster communication cost, i.e., the number of neighbours. The idea is to use the primary parameter to perform a probabilistic choice of an initial set of cluster heads, and the second parameter to break ties between them, e.g., when a node is within the range of multiple cluster heads. This is an iterative algorithm in which nodes change their probability of becoming cluster-head CHprob at each iteration. This value is initially set to is a constant that limits initial cluster-head candidatures

is the residual energy of the node

is its maximum (initial) energy

When nodes elect themselves to become cluster heads, they send an announcement message and then go into tentative_CH status if their CHprob is less than or otherwise into final_CH status. Nodes that receive an announcement consider themselves covered. At each iteration, each uncovered node elects itself as a cluster head with a probability CHprob, then every node doubles its CHprob value. Each node selects the least-cost candidate as its cluster head. Nodes that complete the HEED execution without selecting a cluster head in final_CH status consider themselves uncovered and elect themselves cluster heads with final_CH status. A tentative_CH can also become a non-cluster-head node if it finds a lower-cost cluster head.

This algorithm is proved to guarantee a bounded number of iterations before converging. The selection of cluster heads is energy-aware (so it selects better cluster heads than LEACH) and the clusters obtained are balanced. However, HEED requires multiple iterations, so the overhead and power consumption due to network management is greater than in LEACH. Nevertheless, simulation results show that the higher overhead is compensated for by the better cluster-head selection mechanism and the final result is an increased network lifetime.

Power-Efficient Gathering in Sensor Information Systems (PEGASIS) [**58**] protocol is a LEACH-inspired protocol. PEGASIS is not exactly a cluster-based protocol, as nodes are not explicitly grouped into clusters. PEGASIS is instead a chain based approach, in which each node only communicates with a close neighbour and takes turns to transmit to the BS, thus reducing the amount of energy spent per round. This approach distributes the energy load evenly among the sensor nodes in the network.

The PEGASIS protocol is designed for a WSN containing homogeneous and energy-constrained nodes, with no mobility. The BS (sink) is fixed and far away from nodes. The radio model adopted is the first-order radio model, same as the LEACH protocol. Using this model, energy efficiency can be improved by minimizing the amount of direct transmissions to the sink node. This idea is common to the LEACH protocol, in which clustering is used to reduce both the duty cycle of the nodes and direct transmissions to the BS. A way in which energy efficiency can be further improved is to decrease the number of nodes that perform long-range direct transmissions. So the basic idea of PEGASIS is to have only one designated node that directly transmits to the BS in each round. This can be achieved with a linear chain-based approach, where sensor nodes form a chain, in which gathered data moves from node to node, gets fused, and eventually a designated node will transmit it to the BS. As nodes take turns to transmit to the BS and transmissions are between close neighbours, the average energy spent by each node per round is reduced.

Threshold sensitive energy efficient sensor network protocol (TEEN) [**59**] is a hierarchical protocol. It is useful for time-critical applications in which the network operates in a reactive way. Closer nodes form clusters and elect a cluster head. Each cluster head is responsible for directly sending the data to the sink. After the clusters are formed, the cluster head broadcasts two thresholds to the nodes. These are hard and soft thresholds for sensed attributes. Hard threshold is the minimum possible value of an attribute to trigger a sensor node to switch on its transmitter and transmit to the cluster head. Thus, the hard threshold allows the nodes to transmit only when the sensed attribute is in the range of interest. Hence, the number of transmissions significantly reduced. Once a node senses a value at or beyond the hard threshold, it transmits data only when the value of that attributes changes by an amount equal to or greater than the soft threshold. As a result, soft threshold will further reduce the number of transmissions if there is little or no change in the value of sensed attribute. However, TEEN is not good for applications where periodic reports are needed since the user may not get any data at all if the thresholds are not reached

Adaptive Periodic Threshold-sensitive Energy Efficient sensor Network protocol (APTEEN) is an extension to TEEN presented in [**60**]. The main features of these protocols are that it combines proactive and reactive policies and modification of parameters that allow better control in the cluster heads.

Virtual Grid Architecture (VGA) [**61**] is based on the concept of data aggregation and in-network processing. This routing paradigm considers an extremely low mobility of sensor nodes. Therefore, this protocol arranges the nodes in a fixed topology forming clusters that are fixed, equal, adjacent and non-overlapping with symmetric shapes. One node per zone is considered as cluster head which is in charge of aggregating and transmitting data. It is possible to implement specific strategies for aggregation of data.

Adaptive based routing: In these protocols, the system parameters are controlled to be adapted to the actual network conditions by means of acquired information of the network and negotiation between nodes (e.g. the available energy on the node or QoS of the path).

Adaptive based routing is based on the family of protocols called Sensor Protocols for Information via Negotiation (SPIN) which is described in Negotiation based routing. The SPIN protocols are designed based on two basic ideas:

1. Sensor nodes operate more efficiently and conserve energy by sending metadata instead of sending all the data.
2. Flooding technique wastes energy and bandwidth when sending extra and unnecessary copies of data by sensors covering overlapping areas.

The protocols disseminate all the information at each node to every node in the network assuming that all nodes in network are potential base-stations. With this, the user can query any node and get the needed information immediately. The protocols use data negotiation and resource-adaptive algorithms. The nodes assign a high-level name to describe completely their collected data; this is called meta-data. Then are preformed negotiations before any data is transmitted to avoid redundant data to be transmitted. These protocols distribute the information all over the network, even when the user does not request any data.

Bio-inspired routing: In recent years insect sensory systems have been inspirational to new communications and computing paradigms, which have lead to significant advances like bio inspired routing [**62**]. The most popular ACO (Ant Colony Optimization) is a colony of artificial ants is used to construct solutions guided by the pheromone trails and heuristic information they are not strong or very intelligent; but they successfully make the colony a highly organized society. Swarms are useful in many optimization problems. A swarm of agents is used in a stochastic algorithm to obtain near optimum solutions to complex, non-linear optimization problems [**63**].

Minimum Ant-based Data Fusion Tree (MADFT) [**64**] is a sink selection heuristic routing algorithm .It is based on ACO for gathering correlated data in WSN. It first assigns ants to source nodes. Then, the route is constructed by one of the ants in which other ants search the nearest point of previous discovered route. The chosen formula is Probability function composed of pheromones and costs in order to find the minimum total cost path. MADFT not only optimizes over both the transmission and fusion costs, but also adopts ant colony system to achieve the optimal solution.

The Many-to-One-Improved Adaptive Routing protocol [**65**] is an ant colony-based routing protocol. It is specifically designed to route many-to-one sensory data in a multi-hop WSNs.

Actually, in a many-to-one routing paradigm generates lots of traffic in a multihop WSN that results in greater energy wastage, higher end-to-end delay and packet loss. So, to mitigate the collision, it comes with a lightweight congestion control algorithm. It has the capability of handling both event- based and periodic upstream sensory data flow to the base station. The protocol works in two-phases. During the first phase, the protocol uses ant colony optimization and swarm intelligence to find the shortest and the optimal route within a multi-hop WSN. Here, each node is aware of its location and location of its destination. The ant-routing algorithm is used by each forward ant to find the best next-hop neighbour node, closer to itself and closest to the sink using probabilistic theory. The following nodes use the binary exponential back off algorithm to calculate their channel access time. In the second phase, when the actual many to-one sensory data transmission takes place, the protocol combines the knowledge gained during the first phase with the congestion control mechanism to avoid packet loss and traffic while routing the sensory data. The algorithm outperforms in terms of finding shortest path within least amount of time. The algorithm can be extended considering shortest path by not only distance but also residual energy of nodes.

Swarm Intelligence Optimization Based Routing Algorithm [**66**] works with the objective to balance global energy consumption and avoiding some node’s premature energy exhausting. The algorithm chooses the nodes with less pheromone as next hop, taking less hop numbers into consideration. The algorithm is different from traditional ant colony algorithms. It is better than the directed diffusion routing protocol both in end-to-end delay and global energy balance. It can effectively balance the global energy consumption and prolong the network lifetime.

2.4 Summary and Open research issues:

Routing in wireless sensor networks has attracted a lot of attention to the researchers in the recent years. This section summarized some of the research results on data routing in WSNs. There are mainly three routing categories, namely data-centric, hierarchical and location-based. Important considerations for these routing protocols are energy efficiency and traffic flows. Achieving a good trade-off between energy efficiency and QoS is one of the main issue in WSNs [**57**]. The most effective way to reduce energy consumption is to have a low duty-cycle which in turn causes increase in delay. In order to improve network lifetime, suitable cluster-based approaches have been proposed in the literature.

The main research issue regarding such protocols is how to form the clusters so that the energy consumption and contemporary communication metrics such as latency is optimized. The factors affecting cluster formation and cluster-head communication are open issues for future research. Moreover, the process of data aggregation and fusion among clusters is also an interesting problem to explore. The problem of intelligent utilization of the location information in order to help energy efficient routing is the main research issue. Spatial queries and databases using distributed sensor nodes and interacting with the location-based routing protocol are open issues for further research.

Future research issues should focus on security, QoS and node mobility. Routing techniques for WSNs should address application-dependent security issues such as reliability, authentication, confidentiality etc. should be examined. Currently, there is very little research that looks at handling QoS requirements in a very energy constrained environment like sensor networks. QoS routing in sensor networks have been applied to several applications including multimedia applications like video and imaging sensors. It also applied in real-time applications like target tracking in battle environments, emergent event triggering in monitoring applications etc.

In applications where sensor nodes are mobile, new routing protocols are needed to handle frequent topology changes and reliable delivery. In the literature, most of the protocols assume that the sensor nodes and the sink are stationary. However, there might be situations such as battle environments where the sink and possibly the sensors need to be mobile. In such cases, the frequent update of the position of the command node and the sensor nodes and the propagation of that information through the network may excessively drain the energy of nodes. New routing algorithms are needed in order to handle the overhead of mobility and topology changes in such energy constrained environment.

In the past, many researchers in the WSN field denounced the use of IP as inadequate and in contradiction to the needs of WSNs. Since then the WSN field has matured, standard links have emerged, and IP has evolved. The introduction of 6LoWPANs [**67**], the concept has changed about WSN. The authors present the design of complete IPv6-based network architecture for WSNs in [**68**,**69**]. In future, research for routing protocols includes the integration of WSNs with wired networks (i.e. Internet). It will help applications like security and environmental monitoring, which require the data collected from the sensor nodes to be transmitted to a server so that further analysis can be done and vice versa.

Chapter 3

IEEE 802.15.4 Networks- An Overview

3.1 Introduction

The introduction of IEEE 802.15.4 [**8**] low rate wireless personal area network (LR-WPAN) standard has been implemented for three reasons: the need for low-cost, low-power and short-range communication. Thus it suits for Wireless Sensor Network applications where a large no of tiny sensors having low power, low range and low bandwidth are deployed in an ad hoc manner for the purpose of Automation, Tracking and Surveillance in terrain regions. The standard defines the channel access mechanism, acknowledged frame delivery, network association and disassociation. The standard supports two Direct Sequence Spread Spectrum (DSSS) PHY layers operating in Industrial, Scientific, Medicine (ISM) frequency bands. A low-band PHY operates in the 868 MHz (megahertz) or 915 MHz frequency band and has a raw data rate of 20 kbps or 40 kbps, respectively. A high-band PHY operating in the 2.4 GHz band specifies a data rate of 250 kbps and has nearly worldwide availability. The 2.4 GHz frequency band has the most potential for large-scale WSN applications, since the high radio data rate reduces frame transmission time and usually also the energy per transmitted and received bit of data. This standard now enjoys extensive silicon support, primarily in the 2.4GHz band [**70**] . On top of this PHY and MAC layer standard, several proprietary and standards-based sensor network systems emerged. The one with the most vendor and end-product support is the ZigBee standard.

3.2 IEEE 802.15.4 PHY Layer

PHY layer provides an interface between the MAC layer and the physical radio channel. It provides two services, accessed through two service access points (SAPs). These are the PHY data service and the PHY management service.

3.2.1 Modulations Schemes and Operational Frequencies

The IEEE 802.15.4 standard specifies the multiple PHYs for 868, 915 and 2400 MHz three frequency bands, they use different modulation schemes and different spread spectrum methods to transmit data in different data rates with different chip rates. There are total 37 channels with different bandwidth specified in the standard, which includes one channel in 868 MHz frequency band and 10 channels in 915 MHz frequency band and 16 channels in 2.4 GHz frequency band.

The 868/915 MHz PHY uses a simple DSSS approach in which each transmitted bit is represented by a 15-chip maximum length sequence. Binary data is encoded by multiplying each m-sequence by +1 or -1 and the resulting chip sequence is modulated onto the carrier using binary phase shift keying (BPSK). Differential data encoding is used prior to modulation to allow low-complexity differential coherent reception.

The 2.4 GHz PHY uses a 16-ary quasi-orthogonal modulation technique based on DSSS methods. Binary data is grouped into 4-bit symbols, and each symbol specifies one of sixteen nearly orthogonal 32-chip, pseudo-random noise (PN) sequences for transmission. PN sequences for successive data symbols are concatenated, and the aggregate chip sequence is modulated onto the carrier using, offset-quadrature phase shift keying (OQPSK).The standard specifies the following mandatory multiple PHYs:

Table 3. 1 Frequency bands of IEEE 802.15.4 Physical Layer

PHY (MHz)	Frequency Band (MHz)	Spreading Parameters		Data Parameters		
		Chip Rate (kchip/s)	Modulation	Bit Rate (kb/s)	Symbol Rate (Ksymbol/s)	Symbols
868/915	868-868.6	300	BPSK	20	20	Binary
	902-928	600	BPSK	40	40	Binary
2450	2400-2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

3.2.2 IEEE 802.15.4 Physical layer Packet structure

To maintain a common simple interface with MAC, both PHY share a single packet structure As shown in Figure 3.1. Each PPDU contains a synchronization header (preamble plus start of packet delimiter), a PHY header to indicate the packet length, and the payload, or PHY

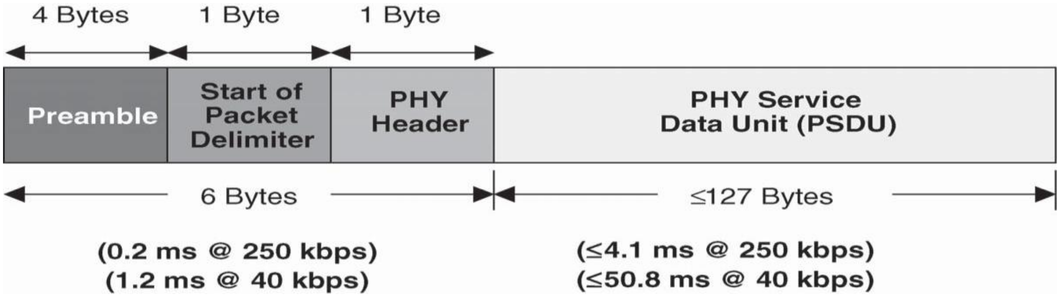


Figure 3.1: IEEE 802.15.4 PHY packet structure [71]

service data unit (PSDU). The 32-bit preamble is designed for the acquisition of symbol and chip timing, and in some cases may be used for coarse frequency adjustment. Channel equalization is not required for either PHY due to the combination of small coverage area and relatively low chip rates.

Within the PHY header, 7 bits are used to specify the length of the payload (in bytes). This supports packets of length 0–127 bytes, although, due to MAC layer overhead, zero-length packets will not occur in practice. Typical packet sizes for home applications such as monitoring and control security, lighting, air conditioning, and other appliances are expected to be of the order of 30–60 bytes, while more demanding applications such as interactive games and computer peripherals, or multihop applications with more address overhead, may require larger packet sizes. Adjusting transmission rates in each frequency band, the maximum packet durations are 4.25 ms for the 2.4 GHz band, 26.6 ms for the 915 MHz band, and 53.2 ms for the 868 MHz band.

3.2.3 The IEEE PHY layer functions:

The IEEE 802.15.4 physical layer has been responsible for the following functions:

- **Activation and deactivation of the radio transceiver**

Turn the radio transceiver into one of the three states, i.e. transmitting, receiving or off (sleeping) according to the request from MAC sublayer. The turnaround time from transmitting to receiving, or vice versa, is less than 12 symbol periods.

- **Energy Detection (ED) within the current channel**

It is an estimate of the received signal power within the bandwidth of an IEEE 802.15.4 channel. No attempt is made to identify or decode signals on the channel in this procedure. The energy detection time is equal to 8 symbol periods. The result from energy detection can be used by a network layer as part of a channel selection algorithm, or for the purpose of clear channel assessment (CCA).

- **Link Quality Indication (LQI) for received packets**

Link quality indication measurement is performed for each received packet. The Physical layer uses receiver energy detection (ED), a signal-to-noise ratio, or a combination of these to measure the strength and/or quality of a link from which a packet is received. However, the use of LQI result by the network or application layers is not specified in the standard.

- **Clear Channel Assessment (CCA) for CSMA-CA**

The PHY layer is required to perform CCA using energy detection, carrier sense, or a combination of these two. In energy detection mode, the medium is considered busy if any energy above a predefined energy threshold is detected. In carrier sense mode, the medium is considered busy if a signal with the modulation and spreading characteristics of IEEE 802.15.4 is detected. In the combined mode, both conditions aforementioned need to be met in order to conclude that the medium is busy.

- **Channel frequency selection**

Wireless links under 802.15.4 can operate in 27 different channels (but a specific network can choose to support part of the channels). Hence the PHY layer should be able to tune its transceiver into a certain channel upon receiving the request from MAC sublayer.

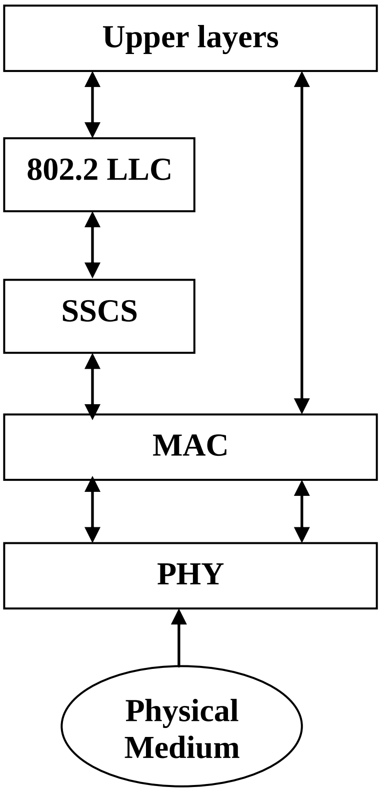
- **Data transmission and reception**

This is the essential task of the PHY layer. Modulation and spreading techniques are used in this part. The 2.4 GHz PHY employs a 16-ary quasi-orthogonal modulation technique, in which each four information bits are mapped into a 32-chip pseudo-random noise (PN) sequence. The PN sequences for successive data symbols are then concatenated and modulated onto the carrier using offset quadrature phase shift keying (O-QPSK). The 868/915 MHz PHY employs direct sequence spread spectrum (DSSS) with binary phase shift keying (BPSK) used for chip modulation and differential encoding used for data symbol encoding. Each data symbol is mapped into a 15-chip PN sequence and the concatenated PN sequences are then modulated onto the carrier using BPSK with raised cosine pulse shaping.

3.3 IEEE 802.15.4 MAC Sublayer

The IEEE 802.15.4 MAC sub layer provides an interface between the service specific convergence sublayer (SSCS) and the PHY layer [**72**] as shown in Figure 3.2. Like the PHY layer, the MAC sublayer also provides two services, namely the MAC data service and the MAC management service. The MAC sublayer of 802.15.4 defines how the medium should be accessed by devices participating in a WPAN. A MAC sublayer provides access to the physical channel for all types of transfer. The upper layers consist of a network layer, which provides network configuration, manipulation, and message routing, and an application layer, which provides the intended function of a device. An IEEE 802.2 logical link control (LLC) can access the MAC through the service specific convergence sublayer (SSCS). It is designed to support a vast number of industrial and home applications for control and monitoring. These applications typically require low to medium data rates and moderate average delay requirements with flexible delay guarantees. Furthermore, the complexity and implementation cost of the IEEE 802.15.4 standard compliant devices must be low to minimize energy consumption and enable the deployment of these devices on a large scale.
To address the needs of its intended applications while enabling the deployment over a large number of monitoring and control devices at reduced implementation cost, the IEEE 802.15.4 MAC-layer specification embeds in its design several unique features for flexible network configurations and low-power operations.
These features include [**73**]:

- Support for various network topologies and network devices
- The availability of an optional superframe structure to control the network devices duty cycle
- Support for direct and indirect data transmissions
- Contention- and schedule-based media access control methods
- Beaconed and non beaconed modes of operation
- Efficient energy management schemes for an extended battery life
- adaptive sleep for extended period of time over multiple beacons



LLC: Logical link Control

MAC:Medium access control

SSCS:Service Specific convergence sublayer

Figure 3.2: IEEE 802.15.4 LR-WPAN device architecture

3.3.1 Network Devices and Topology of IEEE 802.15.4 MAC

There are three categories of logical devices:

1. PAN coordinator: The PAN coordinator is the node (strictly speaking, the coordinator node) that initiates the network and is the primary controller of the network. It can operate as a gateway to other networks. Each PAN must have exactly one PAN coordinator. The PAN coordinator may transmit beacons and can communicate directly with any device in range. Depending on the network design, it may have memory sufficient to store information of all devices in the network as well as routing information required by the algorithm employed by the network . It also stores information about the network and acts as the repository for security keys.

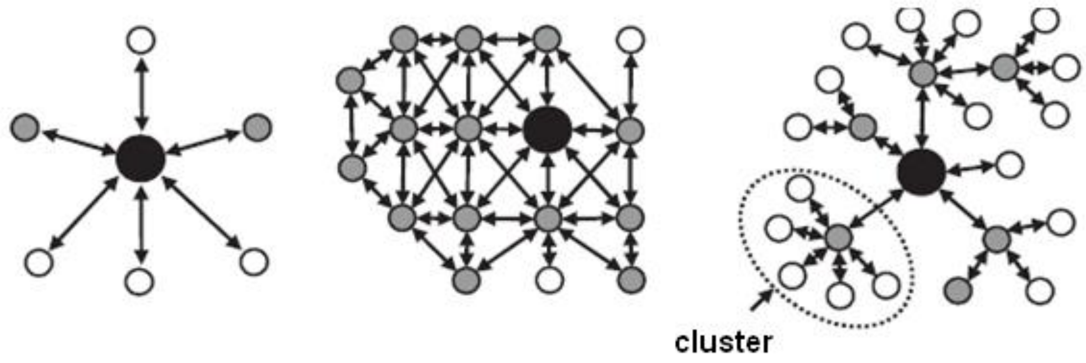
2.Cordinator: The FFD device that supports the data routing functionality, including acting as an intermediate device to link different components of the network and forwarding message between remote devices across multihop paths. A router can communicate with other routers and end devices.

3. End devices: The RFD device that contains just enough functionality to communicate with its parent node: the PAN Coordinator or a Coordinator. An end device does not have the capability to relay data messages to other end devices.

IEEE 802.1.54 MAC supports mainly two topology based on these logical devices.

- Star topology
- Peer to Peer topology

In the star topology, shown in Figure 3.3(a), every device in the network can communicate only with the PAN coordinator. A typical scenario in a star network formation is that an FFD, programmed to be a PAN coordinator, is activated and starts establishing its network.



(a) Star Topology (b) Peer to Peer Topology (c) Cluster –Tree Topology

PAN Coordinator Full functional device Reduced functional device

Figure 3.3: Topology supported by IEEE 802.15.4 and ZigBee [74**]**

The first thing this PAN coordinator does is select a unique PAN identifier that is not used by any other network in its radio sphere of influence —the region around the device in which its radio can successfully communicate with other radios. In other words, it ensures that the PAN identifier is not used by any other nearby networks.

In a peer-to-peer topology as shown in Figure 3.3(b), each device can communicate directly with any other device if the devices are placed close enough together to establish a successful communication link. Any FFD in a peer-to-peer network can play the role of the PAN coordinator. One way to decide which device will be the PAN coordinator is to pick the first FFD device that starts communicating as the PAN coordinator. In a peer-to-peer network, all the devices that participate in relaying the messages are FFDs because RFDs are not capable of relaying the messages. However, an RFD can be part of the network and communicate only with one particular device (a coordinator or a router) in the network.

A peer-to-peer network can take different shapes by defining restrictions on the devices that can communicate with each other. If there is no restriction, the peer-to-peer network is known as a mesh topology. Another form of peer-to-peer network is a Clustered-*tree* topology as shown in Figure 3.3(c). In this case, a PAN coordinator establishes the initial network. Coordinators form the branches and relay the messages. End devices act as leaves of the tree and do not participate in message routing. Coordinator can grow the network beyond the initial network established by the PAN Coordinator.

An IEEE 802.15.4 network, regardless of its topology, is always created by a PAN coordinator. There is only one PAN coordinator in the entire network. A PAN coordinator may need to have long active periods. Therefore, it is usually connected to a main supply. rather than a battery. All other devices are normally battery powered. The smallest possible network includes two devices: a PAN coordinator and a device.

3.3.2 IEEE 802.15.4 MAC layer functions:

IEEE 802.15.4 MAC layer is responsible for the following tasks [**75**]:

- **Generating network beacons if the device is a coordinator**

A coordinator can determine whether to work in a beacon enabled mode, in which a superframe structure is used. The superframe is bounded by network beacons and divided into slots of equal size. By default, the number of slots is 16. A coordinator sends out beacons periodically to synchronize the attached devices and for other purposes. A Full Function Device (FFD) that is not the PAN coordinator shall begin transmitting beacon frames only when it has successfully associated with a PAN.

The Superframe is divided into active and inactive periods. Active period is further divided into Contention Access Period (CAP) and Contention Free Period (CFP). Any device must use CSMA/CA to communicate during CAP. Guaranteed Time Slot (GTS) mechanism is used for CFP. During the inactive period, the coordinator does not interact with the network and goes to power saving mode.

- **Synchronizing to the beacons**

A device attached to a coordinator operating in a beacon enabled mode can track the beacons to synchronize with the coordinator. This synchronization is important for data polling, energy saving and detection of orphans. Upper layer may either direct MAC to keep a track of beacons, in which case the device will have to listen to every beacon sent by the coordinator to maintain synchronization.

- **Supporting Personal Area Network (PAN) association and disassociation**

To support self configuration, 802.15.4 embeds association and disassociation functions in its MAC layer. This not only enables a star to be setup automatically, but also allows for the creation of a self-configuring, peer-to-peer network.

A coordinator may indicate presence of a PAN by sending periodic beacons. The devices wishing to attach to the PAN listen to these beacons to extract necessary information to connect to the PAN. The device can associate to a PAN after performing a scan which gives the list of available PAN ids to upper layer (SSCS).

An unassociated device sends an association request to the selected PAN's coordinator. The PAN coordinator sends back a response depending on availability of resources, using indirect transmission. Disassociation can be initiated either by the PAN coordinator or the device itself. Disassociation is always considered successful.

- **Employing CSMA-CA mechanism for channel access**

Like most other protocols designed for wireless networks, 802.15.4 uses CSMA-CA mechanism for channel access. However, the new standard does not include the Request-To-Send (RTS) and Clear-To-Send (CTS) mechanism, in consideration of the low data rate used in LR-WPANs. Devices will use slotted or unslotted CSMA-CA depending whether the PAN is beacon-enabled or not, respectively. In slotted CSMA-CA channel access mechanism, the backoff period boundaries of every device in the PAN are aligned with the superframe slot boundaries of the PAN coordinator.

- **Providing a reliable link between two peer MAC entities**

The MAC layer employs various mechanisms to enhance the reliability of the link between two peers among them are the frame acknowledgment and retransmission, data verification by using a 16-bit CRC, as well as CSMA-CA. MAC maintains a sequence number which is used to transmit a data frame. Similarly another sequence number is maintained for sending beacon frames. A device can request for an acknowledgment by setting acknowledgment request field to 1 in the frame. The receiver should send the acknowledgment using the same sequence number as present in the original frame.

- **Handling and maintaining GTS mechanism**

When working in a beacon enabled mode, a coordinator can allocate portions of the active superframe to a device. These portions are called GTSs, and comprise the contention free period (CFP) of the superframe.

A GTS shall be allocated only by the PAN coordinator and it shall be used only for communications between the PAN coordinator and a device. A single GTS can extend over one or more superframe slots. The PAN coordinator may allocate up to seven GTSs at the same time. The GTS direction is specified as either transmit or receive. A GTS descriptor is specified in the beacon on successful allocation of a GTS.

- **Direct data transmission**

This applies to data transfers from a device to a coordinator, unslotted CSMA-CA or slotted CSMA-CA is used for data transmission, depending whether non-beacon enabled mode or beacon enabled mode is used.

- **Indirect data transmission**

This only applies to data transfer from a coordinator to its devices. In this mode, a data frame is kept in a transaction list by the coordinator, waiting for extraction by the corresponding device. A device can find out if it has a packet pending in the transaction list by checking the beacon frames received from its coordinator. Occasionally, indirect data transmission can also happen in non-beacon enabled mode.

3.3.3 IEEE 802.1.5.4 MAC data format

IEEE 802.15.4 defines four frame types, including the beacon, command, acknowledgment, and data frames. Only the data and beacon frames actually contain information sent by higher layers; the acknowledgment and MAC command frames originate in the MAC and are used for MAC peer-to-peer communication. The format of the 802.15.4 data frame [**76**] is shown in Figure 3.4

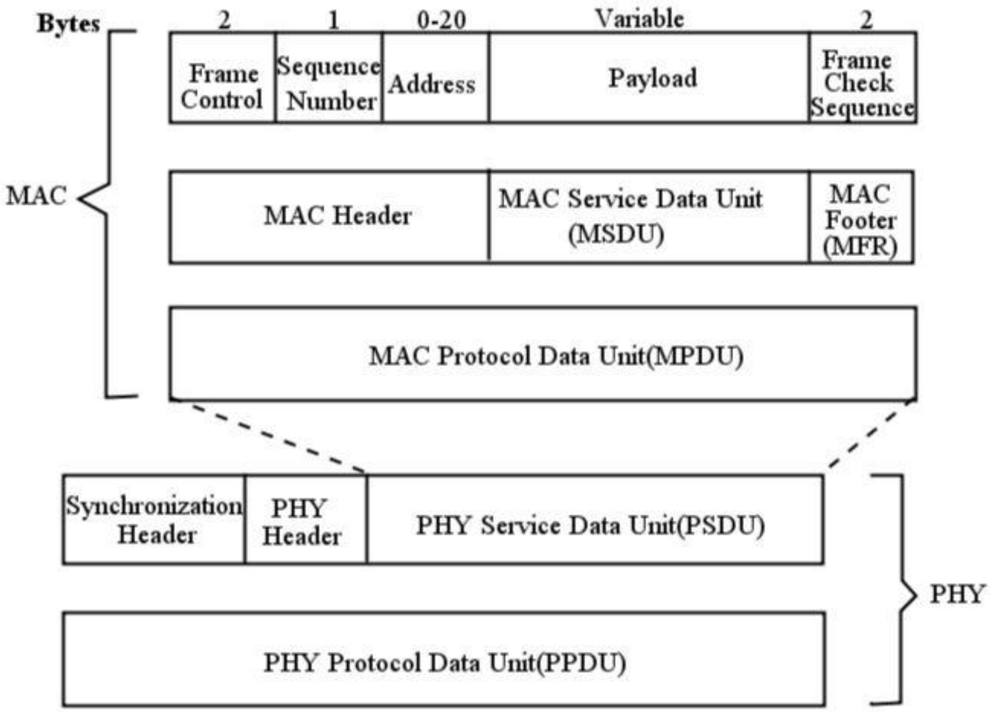


Figure 3.4: Data frame format of IEEE 802.15.4

The MAC frame, i.e. the MPDU, is composed of an MAC header (MHR), MAC service data unit (MSDU), and MAC footer (MFR). The first field of the MAC header is the frame control field. It indicates the type of MAC frame being transmitted, specifies the format of the address field, and controls the acknowledgment. In short, the frame control field specifies how the rest of the frame looks and what it contains. A data frame may contain both source and destination information with the size of the address field between 4 and 20 bytes. The payload field is variable in length. However, the maximum MAC data payload (that is the maximum size of the MSDU), *aMaxMACFrameSize*, is equal to *aMaxPHYPacketSize* (127 bytes) – *aMaxFrameOverhead* (25 bytes) = 102 bytes . The IEEE 802.15.4 MAC has four different frame types. These are the *beacon frame*, *data frame*, *acknowledgment frame* and *MAC command frame*. The MPDU is then passed to the PHY as the PHY data frame payload, i.e., PSDU. The PSDU is prefixed with a synchronization header (SHR) and a PHY header (PHR), together with PSDU to form the PHY data packet, i.e. PPDU.

3.3.4 IEEE 802.15.4 MAC sublayer operational modes

The IEEE 802.15.4 MAC sublayer has two operational modes. They are

(a) Beacon-enabled mode
(b) Nonbeacon –enabled mode

The beacon-enabled mode: Beacon is a message with specific format that is used to synchronize the clocks of the nodes in the network. A coordinator has the option to transmit beacon signals to synchronize the devices attached to it. This is called a *beacon-enabled PAN.* In this mode, beacons are periodically sent by the PAN or Coordinator to synchronize nodes that are associated with it, and to identify the PAN. The superframe structure is shown in Figure 3.6. A beacon frame delimits the beginning of a superframe defining a time interval during which frames are exchanged between different nodes in the PAN. Medium access is basically ruled by Slotted CSMA/CA. However, the beacon-enabled mode also enables the allocation of contention free time slots, called Guaranteed Time Slots (GTSs) for nodes requiring guaranteed bandwidth.

The disadvantage of using beacons is that all the devices in the network must wake up on a regular basis, listen for the beacon, synchronize their clocks, and go back to sleep. This means that many of the devices in the network may wake up only for synchronization and not perform any other task while they are active. Therefore, the battery life of a device in a beacon enabled network is normally less than a network with no beaconing.

Nonbeacon enabled mode: A network in which the PAN coordinator does not transmit beacons is known as a nonbeacon network . A nonbeacon network cannot have GTSs and therefore contentionfree periods because the devices cannot be synchronized with one another. The battery life in a nonbeacon network can be noticeably better than in a beacon-enabled network because in a nonbeacon network, the devices wake up less often.

The superframe is defined between two beacon frames and has an active period and an inactive period. The active portion of the superframe structure is composed of three parts.

- Beacon
- Contention Access Period (CAP) and
- Contention Free Period (CFP)

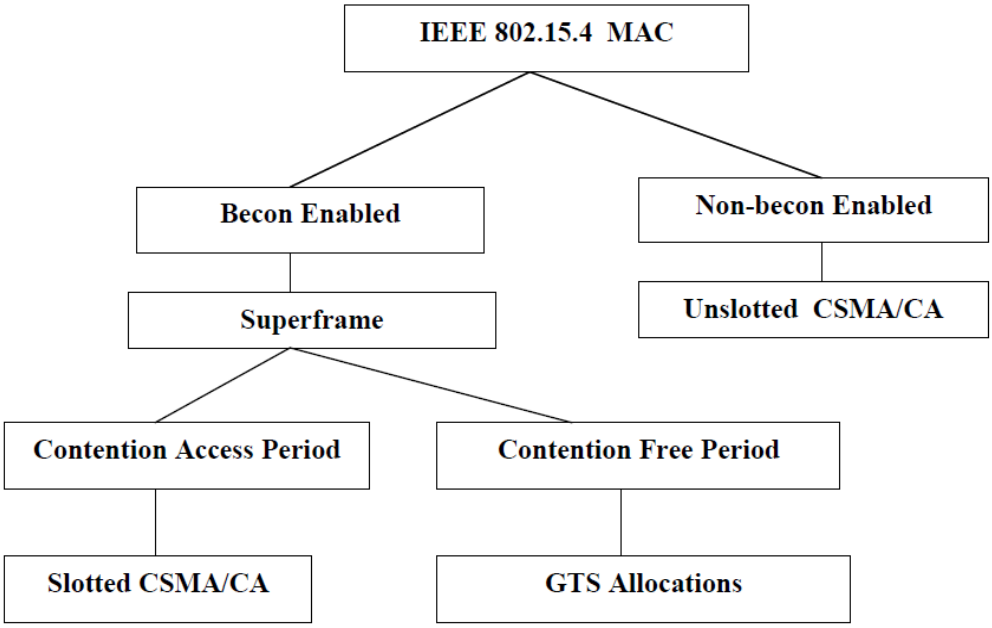


Figure 3.5: IEEE 802.15.4 Operational modes

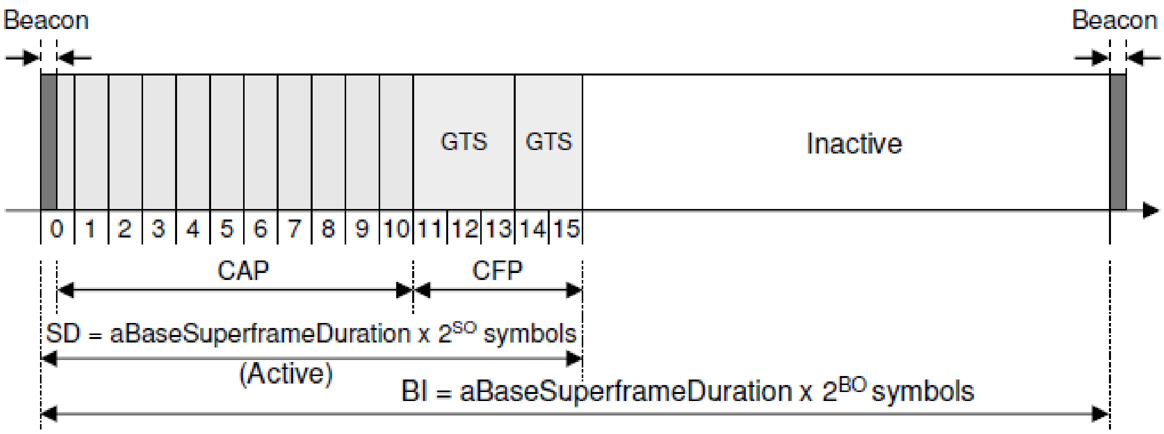


Figure 3.6: IEEE 802.15.4 Superframe structure [72]

Beacon: The beacon frame is transmitted at the start of slot 0. It contains the information on the addressing fields, the superframe specification, the GTS fields, the pending address fields and other PAN related.

Contention Access Period (CAP): The CAP starts immediately after the beacon frame and ends before the beginning of the CFP, if it exists. Otherwise, the CAP ends at the end of the active part of the superframe. The minimum length of the CAP is fixed at *aMinCAPLength = 440 symbols.* This minimum length ensures that MAC commands can still be transmitted when GTSs are being used. A temporary violation of this minimum may be allowed if additional space is needed to temporarily accommodate an increase in the beacon frame length, needed to perform GTS management.

In contention-based channel access, all the devices that want to transmit in the same frequency channel are made using the Slotted CSMA/CA mechanism and the first one that finds the channel clear starts transmitting. However, the acknowledgement frames and any data that immediately follows the acknowledgement of a data request command are transmitted without contention. If a transmission cannot be completed before the end of the CAP, it must be deferred until the next superframe.

Contention Free Period (CFP): In the contention-free method, the PAN coordinator dedicates a specific time slot to a particular device. This is called a ***guaranteed time slot*** (GTS). Therefore, a device with an allocated GTS will start transmitting during that GTS without using the CSMA-CA mechanism. To provide a GTS, the PAN coordinator needs to ensure that all the devices in the network are synchronized. The CFP starts immediately after the end of the CAP and must complete before the start of the next beacon frame (if *BO* equals *SO*) or the end of the superframe. Transmissions are contention-free since they use reserved time slots (GTS) that must be previously allocated by the ZC or ZR of each cluster. All the GTSs that may be allocated by the Coordinator are located in the CFP and must occupy contiguous slots. The CFP may therefore grow or shrink depending on the total length of all GTSs.

In beacon-enabled mode, each Coordinator defines a superframe structure as shown in Figure 3.6 is constructed based on:

The *Beacon Interval* (*BI*): It defines the time between two consecutive beacon frames.

The *Superframe Duration* (*SD*): It defines the active portion in the *BI*, and is divided into 16 equally-sized time slots, during which frame transmissions are allowed. Optionally, an inactive period is defined if *BI* > *SD*. During the inactive period (if it exists), all nodes may enter in a sleep mode (to save energy). *BI* and *SD* are determined by two parameters, the Beacon Order (*BO*) and the Superframe Order (*SO*), respectively, Where,

aBaseSuperframeDuration = 960 symbols

BO = beacon order

SO = superframe order

For 250kbps, 2.4 GHz frequency band, aBaseSuperframeDuration = 15.36 ms denotes the minimum duration of the superframe, corresponding to *SO=0*. Hence, BI and SD may be between 15.36 ms (milliseconds) and 251.7 s (seconds)

Low duty cycles can be configured by setting small values of the *SO* as compared to *BO*, resulting in greater sleep (inactive) periods..This feature is particularly interesting for WSN applications, where energy consumption and network lifetime are main concerns. Additionally, the Guaranteed Time Slot (GTS) mechanism is quite attractive for time-sensitive WSNs, since it is possible to guarantee end-to-end message delay bounds both in Star and Cluster-Tree topologies.

3.3.5 CSMA-CA Mechanism

IEEE 802.15.4 implements a simple method to allow multiple devices to use the same frequency channel for their communication medium. The channel access mechanism used is Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) [**77**] . In CSMA-CA, anytime a device wants to transmit, it first performs a clear channel assessment (CCA) to ensure that the channel is not in use by any other device. Then the device starts transmitting its own signal. The decision to declare a channel clear or not can be based on measuring the spectral energy in the frequency channel of interest or detecting the type of the occupying signal. When a device plans to transmit a signal, it first goes into receive mode to detect and estimate the signal energy level in the desired channel. This task is known energy detection (ED). In ED, the receiver does not try to decode the signal, and only the signal energy level is estimated. If there is a signal already in the band of interest, ED does not determine whether or not this is an IEEE 802.15.4 signal.

IEEE 802.15.4 MAC provides an alternative way to declare a frequency channel clear or busy is *carrier sense* (CS). In CS, in contrast with ED, the type of the occupying signal is determined and, if this signal is an IEEE 802.15.4 signal, then the device may decide to consider the channel busy even if the signal energy is below a user-defined threshold. If the channel is not clear, the device backs off for a random period of time and tries again. The random back-off and retry are repeated until either the channel becomes clear or the device reaches its user-defined maximum number of retries.

There are two types of CSMA-CA: slotted and unslotted. *Slotted CSMA-CA* is referred to as performing CSMA-CA while there is a superframe structure in place. The *unslotted CSMA-CA* algorithm is used when there is no superframe structure; consequently, no back-off slot alignment is necessary. A nonbeacon-enabled network always uses the unslotted CSMA-CA algorithm for channel access. If the CCA indicates a busy channel, the device will back off for a random period of time and then try again. This random back-off period in both slotted and unslotted CSMA-CA is an integer multiple of the unit back-off period. The unit back-off period is equal to *aUnitBackoffPeriod* (a MAC constant) symbols. Figure 3.7 provides the flowchart of the CSMA-CA algorithm. In the first step of the algorithm, a decision is made to use either slotted or unslotted CSMA-CA.

For accessing a channel, each node maintains three variables: NB, BE, and CW. NB is the number of times the CSMA-CA algorithm was required to backoff while attempting the current transmission. It is initialized to 0 before every new transmission. BE is the backoff exponent, which defines the number of backoff periods a node should wait before attempting Clear Channel Assessment (CCA). CW is the contention window length, which defines the number of consecutive backoff periods that the channel must be available before starting to transmit [**78**].

The backoff period length (BOP) is defined as 0.32 ms in the 2.4 GHz band. Default values are $BE = 3$ and $CW = 2$. Before transmission, a node locates a backoff period boundary by the received beacon, waits for a random number of backoff periods (0 to $2^{BE} - 1$) and senses the channel by CCA for *CW* times. Every time the algorithm faces a busy channel, it backs off for a random period of time.

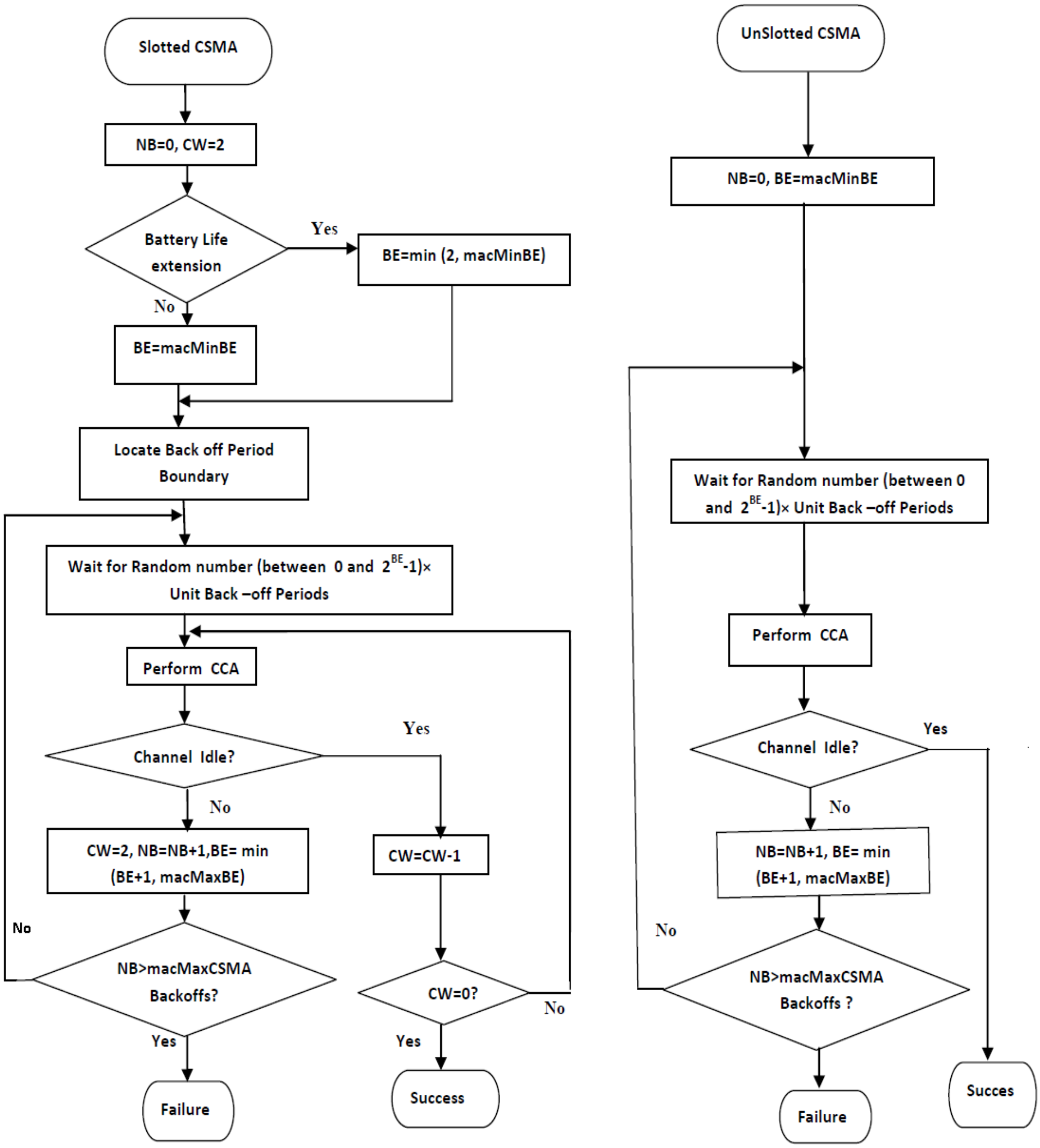


Figure 3.7: Slotted/Un-slotted CSMA-CA Algorithm [77]

The slotted CSMA/CA can be summarised in five steps as follows.

Step 1 -Initialisation of NB, CW and BE: The number of backoffs and the contention window are initialised (*NB* = 0 and *CW* = 2). The backoff exponent is also initialised to *BE* = 2 or *BE* = min (2, *macMinBE*) depending on the value of the *Battery Life Extension* MAC attribute. *macMinBE* is a constant defined in the standard. After the initialisation, the algorithm locates the boundary of the next backoff period.

Step 2 - random waiting delay for collision avoidance: The algorithm starts counting down a random number of BPs uniformly generated within [0, 2^{BE}-1].The countdown must start at the boundary of a BP. To disable the collision avoidance procedure at the first iteration, BE must be set to 0, and thus the waiting delay is null and the algorithm goes directly to Step 3.

Step 3 - Clear Channel Assessment (CCA): When the timer expires, the algorithm then performs one CCA operation at the BP boundary to assess channel activity. If the channel is busy, the algorithm goes to Step 4, otherwise, i.e. the channel is idle, and the algorithm goes to Step 5.

Step 4 - busy channel: If the channel is assessed to be *busy*, *CW* is re-initialised to 2, NB and BE are incremented. *BE* must not exceed *aMaxBE* (default value equal to 5). Incrementing *BE* increases the probability of having greater backoff delays. If the maximum number of backoffs (*NB* = *macMaxCSMABackoffs* = 5) is reached, the algorithm reports a failure to the higher layer, otherwise, it goes back to (Step 2) and the backoff operation is restarted.

Step 5- idle channel: If the channel is assessed to be idle, CW is decremented. The CCA is repeated if CW $\neq$ 0 (Step 3). This ensures performing two CCA operations to prevent potential collisions of acknowledgement frames. If the channel is again sensed as idle (CW = 0), the node attempts to transmit. Nevertheless, collisions may still occur if two or more nodes are transmitting at the same time.

The non-slotted algorithm is similar to slotted CSMA with a few exceptions as follows.

Step 1. The *CW* variable is not used, since the non-slotted has no need to iterate the CCA procedure after detecting an idle channel. Hence, in Step 3, if the channel is assessed to be idle, the MAC protocol immediately starts the transmission of the current frame. Second, the non-slotted CSMA/CA does not support *macBattLife-Ext* mode and, hence, *BE* is always initialised to the *macMinBE* value.

Steps 2, 3 and 4. It is similar to the slotted CSMA/CA version. The only difference is that the CCA starts immediately after the expiration of the random backoff delay generated in Step 2.

Step 5. The MAC sub-layer starts immediately transmitting its current frame just after a channel is assessed to be *idle* by the CCA procedure.

3.3.6 Data Transfer Models

There are three types of data transfer in IEEE 802.15.4 [**77**] :

● Data transfer to a coordinator from a device

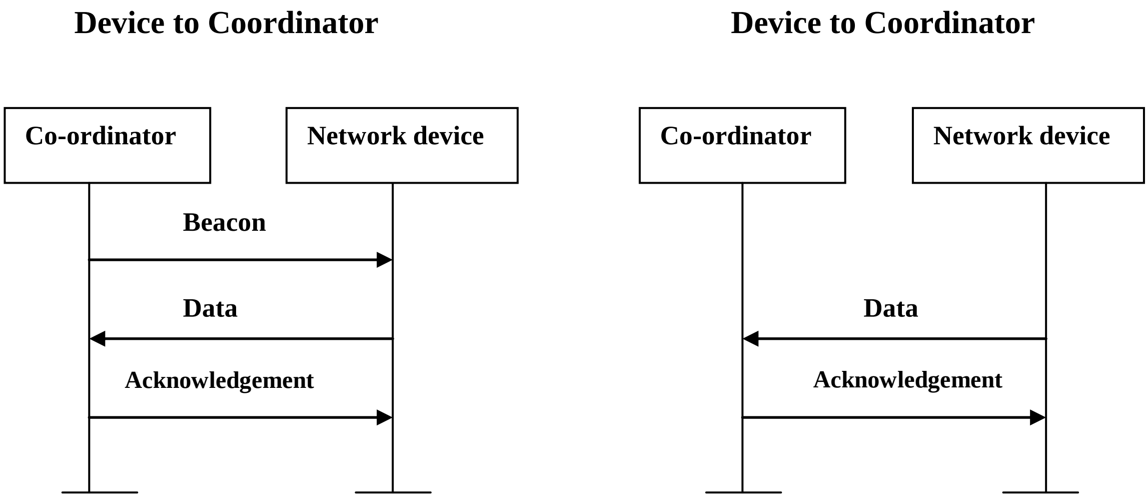
● Data transfer from a coordinator to a device

● Data transfer between two peer devices

All three methods can be used in a peer-to-peer topology. In a star topology, only the first two are used, because no direct peer-to-peer communication is allowed.

Data Transfer to a Coordinator

In a beacon-enabled network, when a device decides to transmit data to the coordinator, the device synchronizes its clock on a regular basis and transmits the data to the coordinator using the CSMA-CA method. It has been assumed that the transmission does not occur during a GTS. The coordinator may acknowledge the reception of the date only if it is requested by the data transmitter. This basic sequence chart is shown in Figure 3.8(a).



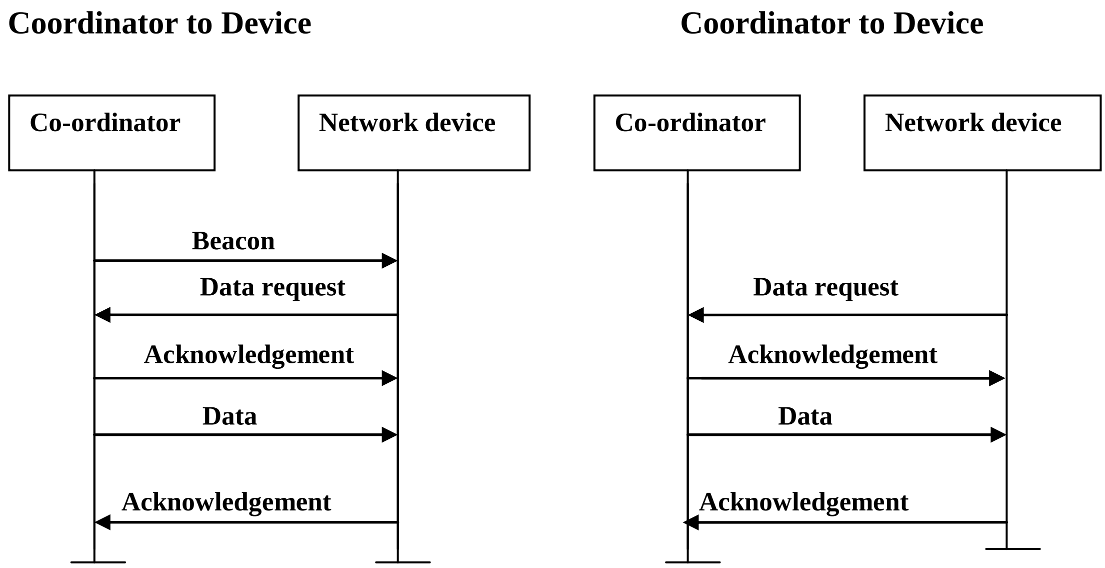
(a) Beacon Enabled **(b)** Nonbeacon Enabled

Figure 3.8: Data transfer to a Coordinator in IEEE 802.15.4 :(a) Beacon Enabled and (b) Non beacon Enabled

The data transfer sequence in a nonbeacon-enabled network is shown in Figure 3.8(b). In this scenario, the device transmits the data as soon as the channel is clear. The transmission of an acknowledgment by the PAN coordinator is optional.

Data Transfer from a Coordinator

Figure 3.9(a) illustrates the data transmission steps to transfer data from a coordinator to a device in a beacon-enabled network. If the coordinator needs to transmit data to a particular device, it indicates in its beacon message that a data message is pending for that device. The device then sends a data request message to the coordinator indicating that it is active and ready to receive the data. The coordinator acknowledges the receipt of the data request and sends the data to the device. Sending the acknowledgment by the device is optional.



(a) Beacon Enabled (b) Nonbeacon Enabled

Figure 3.9: Data Transfer from a Coordinator to a device :(a) Beacon Enabled and (b) Nonbeacon Enabled

In a nonbeacon-enabled network as shown in Figure 3.9(b), the coordinator needs to wait for the device to request the data. If the device requests the data but there is no data pending for that device, the coordinator sends an acknowledgment message with a specific format that Indicates there is no data pending for that device. Alternatively, the coordinator may send a data message with a zero-length payload.

3.4 SSCS Layer

This is the interface between MAC 802.15.4 and upper layers. It provides a way to access all the MAC primitives, but it can also serve as a wrapper of those primitives for convenient operations. It is an implementation specific module and its function should be tailored to the requirements of specific applications.

The SSCS functions are given below:

- **Starting PAN coordinator:** When starting a new PAN, a PAN coordinator must be present. Configurable options will be passed to MAC layer before starting the coordinator.
- **Starting Device:** A device can be started as either a RFD or an FFD. An FFD by default becomes a coordinator. A coordinator, like PAN coordinator, might be beacon enabled or non-beacon enabled.
- **Stopping Device:** This feature allows a device to be stopped at a given point of time.
- **Starting and Stopping Beacon:** A coordinator can change itself from non-beacon mode to beacon mode or otherwise. It can also change beacon parameters, if originally in beacon mode.

3.5 ZigBee

ZigBee wireless network is based on IEEE 802.15.4 standards, which is aimed for Low Rate Wireless Personal Area networks (LR-WPAN). IEEE 802.15.4 standard focuses on the lower two layers of the protocol stack for defining the basic communication methods for instrument networks but requires much more additional work to produce marketable product. On top of IEEE 802.15.4 radio communication standards, the ZigBee Alliance (an industry consortium of semiconductor manufacturers), other providers, and manufacturing companies provide this additional work. The ZigBee specification is designed to utilize the features supported by IEEE 802.15.4, particularly the low data transmission rate and energy consumption features. It targets control and monitoring applications, where low-power consumption is a key requirement. The candidate applications are wireless sensors, lighting controls, and surveillance. It also targets market areas like residential home control, commercial building control, and industrial plant management.

3.5.1 ZigBee Protocol Stack

The ZigBee protocol stack is given below in Figure 3.10.

The Physical layer, which is referred to as IEEE 802.15.4 PHY, is concerned with the interface to the physical transmission medium and exchanging data bits with the layer above. It consists of two PHY layers which operate in two separate frequency ranges: 868/915 MHz

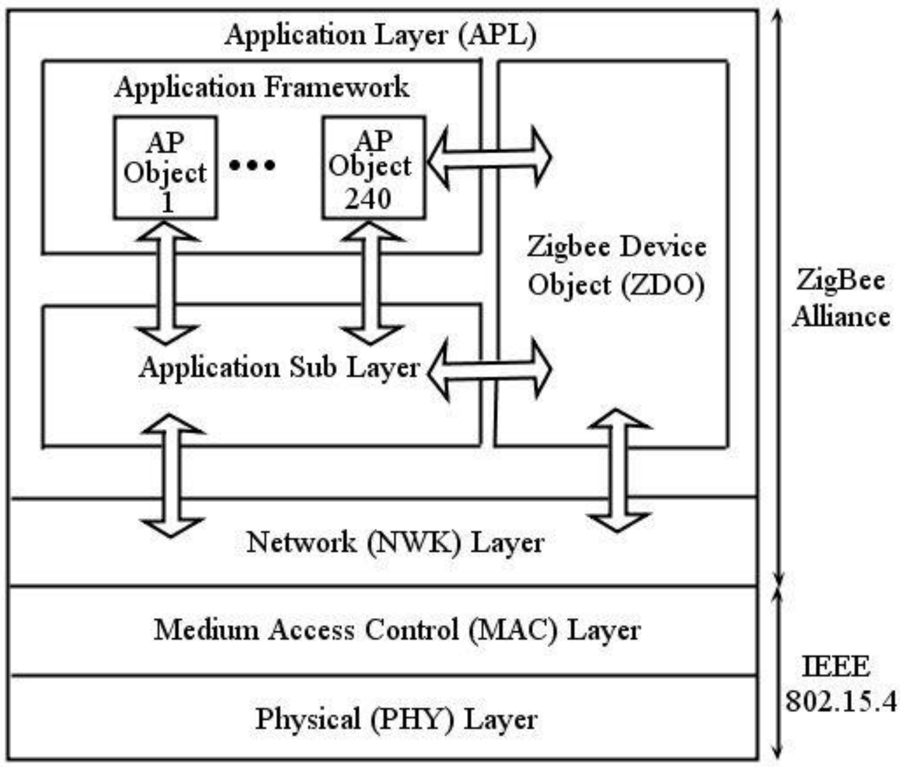


Figure 3.10: ZigBee functional layer architecture and protocol stack

and 2.4GHz. The Medium Access Control (MAC) layer is also known as the Data Link Layer. This layer is concerned with the addressing. It determines where the data is going for outgoing data and where the data is coming from for incoming for data. It is also responsible for assembling data packets or frames to be transmitted and decomposing received frames.

The Network (NWK) layer which is right above MAC specified by IEEE 802.15.4 .It is defined by the ZigBee Alliance. It allows devices to communicate with each other. It is involved in the initialization of the device, network self-organization and routing of data and network discovery within the network.

ZigBee denotes the network device types differently from IEEE 802.15.4. A PAN coordinator is called a ZigBee coordinator, while coordinators and devices are called ZigBee routers and ZigBee end-devices respectively. The NWK layer supports three network topologies: star, peer-to-peer (mesh), and cluster-tree. In the star topology, communication is controlled by a ZigBee coordinator that operates as a network master, while ZigBee end-devices operate as slaves and communicate only with the ZigBee coordinator. This network is most suitable for delay critical applications, where a large network coverage area is not required.

A peer-to-peer topology allows mesh-type of networks, where any ZigBee router may communicate with any other router within its range. By routing data through nodes using multiple hops, network coverage can be extended far longer than a radio range. This enables the formation of complex self-organizing network topologies. In addition, peer-to-peer topologies have high robustness against node failures and interferences, since routes can be freely changed. The mesh configuration allows path formation from any source device to any destination device, using tree and table-driven routing algorithms. The table-driven routing algorithm employs a simplified version of the on-demand distance vector routing (AODV) and Internet Engineering Task Force (IETF) proposal for mobile ad hoc networking (MANET). In the mesh topology, the radio receivers of the coordinator and the routers must always be on. Peer-to-peer topologies are suitable for industrial and commercial applications, where efficient self-configurability and large coverage are important. A disadvantage is the increased network latency due to message relaying.

A cluster-tree or hybrid network is a combination of star and mesh topologies. The network consists of clusters, each having a ZigBee router as a cluster head and multiple ZigBee end devices as leaf nodes. A ZigBee coordinator initiates the network and serves as the root. The network is formed by parent–child relationships, where new nodes associate as children with the existing routers. A ZigBee coordinator may instruct a new child to become the head of a new cluster. Otherwise, the child operates as an end device.

The Application (APS) layer at the top of the stack contains application profiles, defined by ZigBee Alliance contains the applications that run on the network node. This layer determines device relationships and supervises network initiation and association functions. The profiles define which messages are sent over the air, application environment, and the types of utilized devices and clusters. Each ZigBee device should have one or more application profiles, which may consists of ZigBee-specified public profiles and manufacturer-specific private profile. Only the devices equipped with the same application profiles interoperate end-to-end. The manufacturers may still add more features on public profiles and implement additional profiles at the application layer, which live on different endpoints within the device. This allows the creation of manufacturer-specific extensions on the ZigBee. A single node can run up to 240 applications on endpoints.

Security Service Provider (SSP) performs security functions. Security is a major stepping stone for industrial applications .Security includes encryption of data, key generation and distribution, and authentication. ZigBee provides key generation and distribution services, which utilize 128-bit Advanced Encryption Standard (AES) encryption provided by IEEE 802.15.4. In addition, ZigBee supports access control lists and packet freshness timers. Security modes are supported for residential, commercial, and industrial applications.

3.5.2 Application of ZigBee

ZigBee networking has a diverse range of applications, including but not limited to home automation, structural monitoring , inventory tracking, and healthcare etc.

One application of ZigBee is in-home patient monitoring. Consider a patient who is staying at his home but for whom it is important that his physician monitor his heart rate and blood pressure continuously. A patient's blood pressure and heart rate can be measured by IEEE 802.15.4 based wearable devices. The patient wears a ZigBee device that interfaces with a sensor that gathers health-related information such as blood pressure on a periodic basis. Then the data is wirelessly transmitted to a local server, such as a personal computer inside the patient's home, where initial analysis is performed. Finally, the vital information is sent to the patient's nurse or physician via the Internet for further analysis [**79**]. The 802.15.4 standard uses 128-bit Advanced Encryption Standard (AES) technology to securely transfer data between ZigBee devices and other networks.

Figure 3.11 is a simplified diagram of a remote monitoring system. A patient wears a ZigBee device that interfaces with a sensor, such as a blood pressure sensor, that gathers the information on a periodic basis. Then this information is transmitted to a ZigBee gateway.

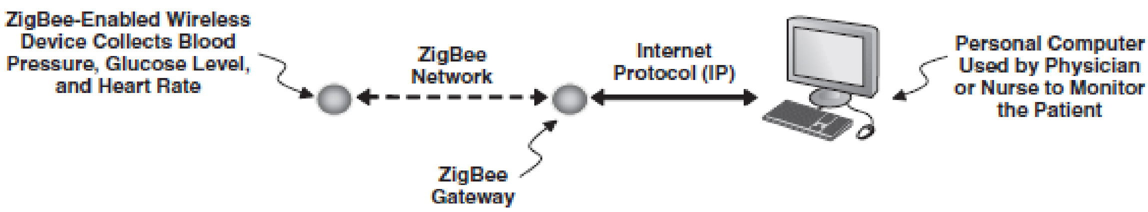


Figure 3.11:In-Home Patient monitoring using ZigBee Wireless Networking [77**]**

A ZigBee gateway provides the interface between a ZigBee network and other networks, such as an Internet Protocol (IP) network. The patient information is then transmitted over the Internet to a personal computer that the physician or nurse uses to monitor the patient.

This system could help hospitals improve patient care and relieve hospital overcrowding by enabling them to monitor patients at home.

At the industrial level, ZigBee mesh networking can help in areas such as energy management, light control, process control, and asset management. At the industrial level, ZigBee mesh networking can help in areas such as energy management, light control, process control, and asset management. A passive RFID tag can transmit only simple information such as an ID number, which is sufficient for many asset management applications. Active RFIDs, such as ZigBee devices, are battery powered and generally are more expensive than passive RFIDs. ZigBee-based active RFIDs have longer range than passive RFIDs and can provide additional services such as estimating the location of assets or personnel.

Another example of a ZigBee application is monitoring the structural health of large scale buildings. In this application, several ZigBee-enabled wireless sensors (e.g. accelerometers) can be installed in a building and all these sensors can form a single wireless network to gather the information that will be used to evaluate the building's structural health and detect signs of possible damage. After an earthquake, for example, a building could require inspection before it reopens to the public. The data gathered by the sensors could help expedite and reduce the cost of the inspection.

3.6 Summary: This section described about the IEEE 802.15.4 Physical, MAC and SSCS layer standard. It also discussed ZigBee protocol stack and its application. Featuring its simplicity, low power consumption, low cost connectivity, and device-level networking will make IEEE 802.15.4 suitable for WSN applications in the practical industry.

Chapter 4

Cluster Head Selection for Energy efficiency in WSN using BFO

4.1 Introduction

Evolutionary algorithms are stochastic search methods that mimic the metaphor of natural biological evolution. Evolutionary algorithms operate on a population of potential solutions applying the principle of survival of the fittest to produce better and better approximations to a solution. At each generation, a new set of approximations is created by the process of selecting individuals according to their level of fitness in the problem domain and breeding them together using operators borrowed from natural genetics. This process leads to the evolution of populations of individuals that are better suited to their environment than the individuals that they were created from, just as in natural adaptation [**80**].

4.2 Principle of Evolutionary Algorithms

Evolutionary algorithms model natural processes, such as selection, recombination, mutation, migration, locality and neighbourhood. Figure 4.1 shows the structure of a simple evolutionary algorithm. Evolutionary algorithms work on populations of individuals instead of single solutions. In this way the search is performed in a parallel manner.

At the beginning of the computation a number of individuals (the population) are randomly initialized. The objective function is then evaluated for these individuals. The first/initial generation is produced.

If the optimization criteria are not met the creation of a new generation starts. Individuals are selected according to their fitness for the production of offspring. Parents are recombined to produce offspring. All offspring will be mutated with a certain probability. The fitness of the offspring is then computed. The offspring are inserted into the population replacing the parents, producing a new generation. This cycle is performed until the optimization criteria are reached.

Such a single population evolutionary algorithm is powerful and performs well on a wide variety of problems. However, better results can be obtained by introducing multiple subpopulations. Every subpopulation evolves over a few generations isolated (like the single population evolutionary algorithm) before one or more individuals are exchanged between the subpopulation. The multi-population evolutionary algorithm models the evolution of a species in a way more similar to nature than the single population evolutionary algorithm.

From the above discussion, it can be seen that evolutionary algorithms differ substantially from more traditional search and optimization methods.

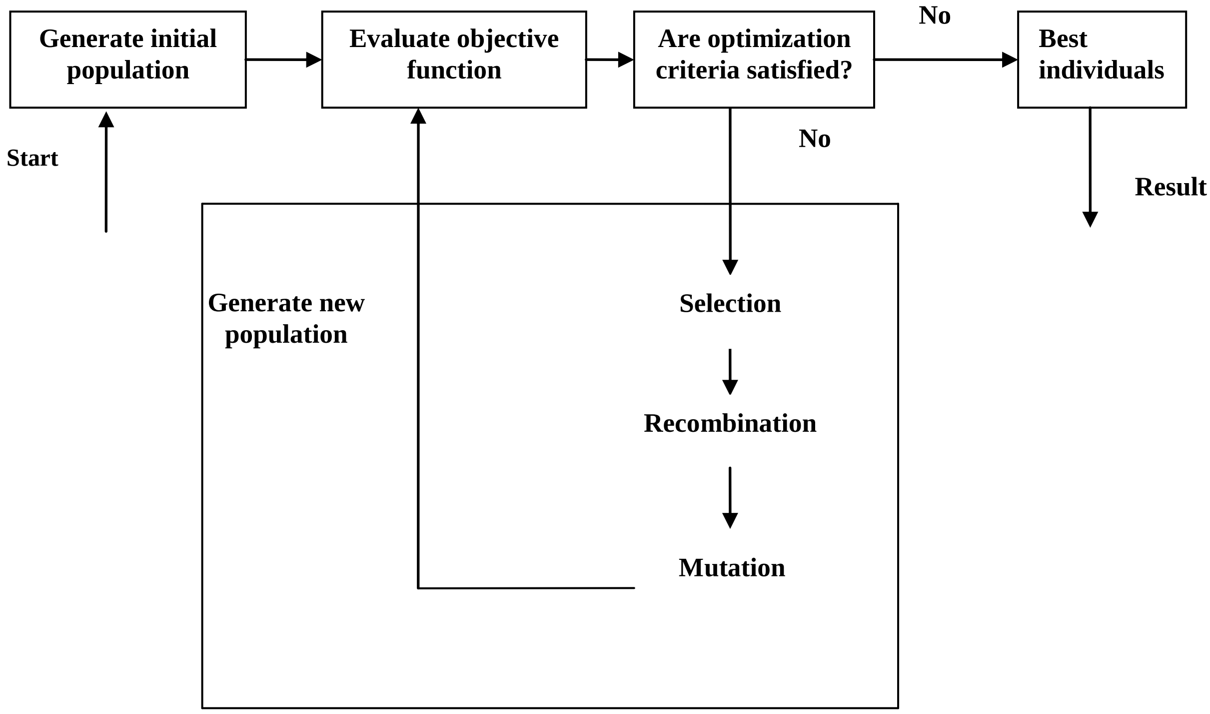


Figure 4.1: Structure of a single population evolutionary algorithm

From the above discussion, it can be seen that evolutionary algorithms differ substantially from more traditional search and optimization methods. The most significant differences are:

- Evolutionary algorithms search a population of points in parallel, not just a single point. These algorithms do not require derivative information or other auxiliary knowledge; only the objective function and corresponding fitness levels influence the directions of search.
- Evolutionary algorithms use probabilistic transition rules, not deterministic ones.

- Evolutionary algorithms are generally more straightforward to apply, because no restrictions for the definition of the objective function exist.

4.2.1 Some examples of EA

Genetic algorithm: This is the most popular type of EA. One seeks the solution of a problem in the form of strings of numbers (traditionally binary, although the best representations are usually those that reflect something about the problem being solved - these are not normally binary), virtually always applying recombination operators in addition to selection and mutation.

Evolutionary programming: Like genetic programming, only the structure of the program is fixed and its numerical parameters are allowed to evolve.

Evolution strategy: This works with vectors of real numbers as representations of solutions, and typically uses self-adaptive mutation rates.

Genetic programming: Here the solutions are in the form of computer programs, and their fitness is determined by their ability to solve a computational problem.

Learning classifier system - Instead of a using fitness function, rule utility is decided by a reinforcement learning technique

4.2.2 Related techniques

Differential evolution: This is based on vector differences and is therefore generally suited for numerical optimization problems.

Particle swarm optimization: This is based on the ideas of animal flocking behaviour. They are generally suited for numerical optimization problems.

Ant colony optimization: This is based on the ideas of ant foraging by pheromone communication to form path. They are generally suited for combinatorial optimization problems.

Bacterial foraging optimization: This is based on the ideas of bacteria foraging by swimming and tumbling. It is primarily suited for combinatorial optimization problems [**81**].

4.3 Bacterial Foraging Optimization for cluster head selection

Bacterial Foraging Optimization (BFO) [**81**] is a population-based numerical optimization algorithm. In recent years, bacterial foraging behaviour has provided rich source of solution in many engineering applications and computational model. It has been applied for solving practical engineering problems like optimal control [**81**], harmonic estimation [**82**], channel equalization [**83**] etc. In this thesis, BFO has been used for cluster head selection to provide improved energy efficiency in routing. This section discusses process of cluster head selection using BFO algorithm. The process of cluster head selection involves application of a clustering algorithm. This has been classically done with LEACH, K-Means and direct method.

4.3.1 Bacteria Foraging Optimization

The process of natural selection tends to eliminate animals with poor foraging strategies and favour the propagation of genes of those animals that have successful foraging strategies, since they are more likely to enjoy reproductive success. After many generations, poor foraging strategies are either eliminated or shaped into good ones. This activity of foraging led the researchers to use it as optimization process. The *Escherichia Coli or E. coli* bacteria that are present in our intestines also undergo a foraging strategy. The control system of these bacteria that dictates how foraging should proceed can be subdivided into four sections, namely, chemotaxis, swarming, reproduction, and elimination and dispersal.

Chemotaxis: This process in the control system is achieved through swimming and tumbling via Flagella. Each flagellum is a left-handed helix configured so that as the base of the flagellum (i.e., where it is connected to the cell) rotates counterclockwise, as viewed from the free end of the flagellum looking toward the cell, it produces a force against the bacterium so it pushes the cell. On the other hand, if they rotate clockwise, each flagellum pulls on the cell, and the net effect is that each flagellum operates relatively independently of others, and so the bacterium tumbles about. Therefore, an *E. coli* bacterium can move in two different ways; it can run (swim for a period of time) or it can tumble, and alternate between these two modes of operation in the entire lifetime. To represent a tumble, a unit length random direction, say $\phi(j)$, is generated; this will be used to define the direction of movement after a tumble. In particular

$$\theta^i(j+1,k,l) = \theta^i(j,k,l) + c(i)\phi(j) \tag{4.1}$$

where $\theta^i(j+1,k,l)$ represents the i^{th} bacterium at j^{th} chemotactic, k^{th} reproductive and l^{th} elimination and dispersal step. *c(i)* is the size of the step taken in the random direction specified by the tumble (run length unit).

Swarming: When a group of *E. coli* cells is placed in the center of a semisolid agar with a single nutrient chemo-effecter (sensor), they move out from the center in a traveling ring of cells by moving up the nutrient gradient created by consumption of the nutrient by the group. Moreover, if high levels of succinate are used as the nutrient, then the cells release the attractant aspartate so that they congregate into groups and, hence, move as concentric patterns of groups with high bacterial density. The spatial order results from outward movement of the ring and the local releases of the attractant; the cells provide an attraction signal to each other so they swarm together. The mathematical representation for swarming can be represented by

$$J_{cc}(\theta, P(j,k,l)) = \sum_{i=1}^{S} J_{cc}^{i}(\theta, \theta^{i}(j,k,l))$$

$$= \sum_{i=1}^{S}[-d_{attrac\tan t}\exp(-w_{attrac\tan t}\sum_{m=1}^{p}(\theta_m - \theta_m^i)^2)]$$

$$+ \sum_{i=1}^{S}[h_{repellent}\exp(-w_{attrac\tan t}\sum_{m=1}^{p}(\theta_m - \theta_m^i)^2)] \tag{4.2}$$

where $J_{cc}(\theta, P(j,k,l))$ is the cost function value to be added to the actual cost function to be minimized to present a time varying cost function, S is the total number of bacteria, P is the number of parameters to be optimized which are present in each bacterium, and $d_{attarct}, w_{attract}, h_{repellent}, w_{repellent}$ are different coefficients that are to be chosen properly.

Reproduction: The least healthy bacteria die and the other healthier bacteria each split into two bacteria, which are placed in the same location. This makes the population of bacteria constant.

Elimination and Dispersal: It is possible that in the local environment, the lives of a population of bacteria changes either gradually (e.g., via consumption of nutrients) or suddenly due to some other influence. Events can occur such that all the bacteria in a region are killed or a group is dispersed into a new part of the environment. They have the effect of possibly destroying the chemotactic progress, but they also have the effect of assisting in chemotaxis, since dispersal may place bacteria near good food sources. From a broad perspective, elimination and dispersal are parts of the population-level long-distance motile behaviour.

4.3.2 Bacterial Foraging Optimization Algorithm

The algorithm that models bacterial population chemotaxis, swarming, reproduction, elimination, and dispersal is given here (initially $j=k=l=0$). For the algorithm, updates to the θ^i automatically result in updates to P number of sensor nodes. The flowchart of the BFO is shown in Figure 4.2.The procedure of BFO is as follows.

1) First of all, get sample no of sensor nodes to be optimized

2) Initialize, the value of $p, S, N_c, N_s, N_{re}\ N_{ed}, P_{ed}$ and the $c(i)$, i=1,2… S. The initial values for the θ^i, i = 12…. S must be chosen.

3) *Elimination-dispersal loop*: $l = l + 1$

4) *Reproduction loop*: $k = k + 1$

5) *Chemotaxis loop*: $j = j + 1$

a) For i =1, 2….S, take a chemotactic step for bacterium i as follows.

b) Compute cost function $J(i, j, k, l)$. The cost function of the BFO is calculated in the following way: First sum the distance squares from each node to the CH for an one cluster. Then this value for all the clusters should be summed over.

Let $J(i, j, k, l) = J(i, j+1, k, l) + J_{cc}(\theta^i(j+1, k, l).P(j+1, k, l)$

c) Let $J_{last} = J(i, j, k, l)$ to save this value since we may find a better value via a run.

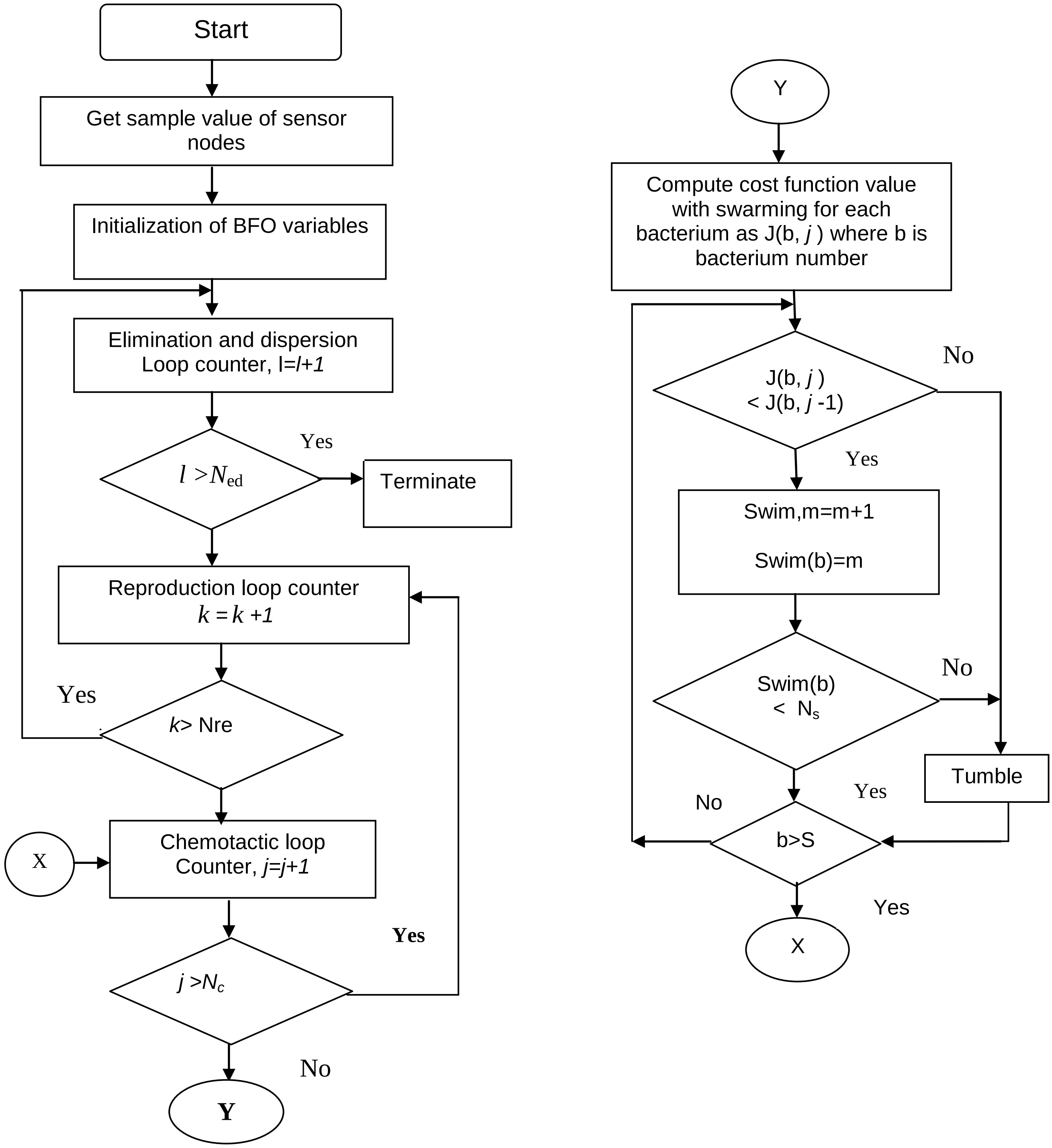


Figure 4.2: Flowchart of BFO algorithm

d) ***Tumble***: Generate a random vector Δ(i) $\in R^p$ with each element $\Delta_m(i)$, m=1,2…..*p,* a random number on [-1,1].

e) ***Move***: Let $\theta^i(j+1,k,l) = \theta^i(j+1,k,l) + c(i)\,\Delta(i)\dfrac{1}{\sqrt{\Delta^t(i)\Delta(i)}}$

This results in a step of size *c(i)* in the direction of the tumble for bacterium *i*.

$J(i,j+1,k,l) = J(i,j+1,k,l) + J_{cc}(\theta^i(j+1,k,l).P(j+1,k,l)$

g) **Swim** : Let m = 0 (counter for swim length).

I. While m < N_s (if have not climbed down too long)

• Let m = m + 1

• I f $J(i,j+1,k,l) < J_{last}$ (if doing better),

Let $J_{last} = J(i,j+1,k,l)$ and let $\theta^i(j+1,k,l) = \theta^i(j,k,l) + c(i)\,\Delta(i)\dfrac{1}{\sqrt{\Delta^t(i)\Delta(i)}}$ and use this $\theta^i(j+1,k,l)$ to compute the new $J(i,j+1,k,l)$ as mentioned in above f step).

• Else, let m= N_s this is the end of the while statement.

h) Go to next bacterium $(i+1)$ if $i \neq S$ (i.e., go to b) to process the next bacterium).

6) If $j < N_c$, go to step 3. In this case, continue chemotaxis, since the life of the bacteria is not over.

7) Reproduction: a) For the given k and l, and for each i =1, 2….. S . Let $J^i_{health} = \sum_{j=1}^{N_c+1} J(i,j,k,l)$ be the health of bacterium i (a measure of how many nutrients it got over its lifetime and how successful it was at avoiding noxious substances). Sort bacteria and chemotactic parameters *c(i)* in order of ascending cost J_{health} (higher cost means lower health).

b) The S_r bacteria with the highest J_{health} values die and the other S_r bacteria with the best values split (and the copies that are made are placed at the same location as their parent).

8) If $k < N_{re}$ go to step 2. In this case, we have not reached the number of specified reproduction steps, so we start the next generation in the chemotactic loop.

9) Elimination-dispersal: For $i = 1, 2\ldots S$ .With probability P_{ed} , eliminate and disperse each bacterium (this keeps the number of bacteria in the population constant). To do this, if you eliminate a bacterium, simply disperse one to a random location on the optimization domain.

10) If $l < N_{ed}$ then go to step 1; otherwise end.

4.3.3 BFO parameters for WSN cluster head optimization

Size of population 'S': Increasing the size of S can significantly increase the computational complexity of the algorithm. However, for larger values of S , it is more likely at least some bacteria near an optimum point should be started, and over time, it is then more likely that many bacterium will be in that region, due to either chemotaxis or reproduction. Here, the population size has been taken as 10 bacteria. Each representing 5 centres and each centre has two dimensions. One bacterium is used for each direction per centre.

Length of chemotactic step '*c(i)*': If the *c(i)* values are too large, then if the optimum value lies in a valley with steep edges, the search will tend to jump out of the valley, or it may simply miss possible local minima by swimming through them without stopping. On the other hand, if the *c(i)* values are too small, convergence can be slow, but if the search finds a local minimum it will typically not deviate too far from it. *c(i)* can be treated as a type of "step size" for the optimization algorithm. Here, the step size *c(i)* for all bacteria is a constant i.e 0.03.

Chemotactic step 'N_c': If the size of N_c is chosen to be too short, the algorithm will generally rely more on luck and reproduction and in some cases, it could more easily get trapped in a local minimum (premature convergence). N_s creates a bias in the random walk, with large values tending to bias the walk more in the direction of climbing down the hill. Here, the total number of chemotactic steps Nc in a loop has been taken as 10 and N_s=4.

Reproduction number 'N_{re}': The small value of N_{re} will converge the algorithm prematurely, while large values of N_{re} increase computational complexity. Here, *Nre* has been taken as 4. It means during simulation E.coli evolve four generations.

Elimination and dispersal number 'N_{ed}': A low value for N_{ed} dictates that the algorithm will not rely on random elimination-dispersal events to try to find favourable regions. A high value increases computational complexity but allows the bacteria to look in more regions to find good nutrient concentrations. Clearly, if probability of elimination and dispersal P_{ed} is large, the algorithm can degrade to random exhaustive search. However, it is chosen appropriately, it can help the algorithm jump out of local optima and into a global optimum. Here, N_{ed} =2 and P_{ed} = 0.1.

Cell-to-cell attractant functions 'J_{cc}^{i}':

If the attractant width is high and very deep, the cells will have a strong tendency to swarm (they may even avoid going after nutrients and favour swarming). On the other hand, if the attractant width is small and the depth shallow, there will be little tendency to swarm and each cell will search on its own. This parameter has not been used for simulation.

4.4 Simulation setup

To validate the proposed BFO for cluster head selection, the performance of BFO was compared with standard clustering algorithm like LEACH along with direct method, K-Means. Performance metrics "Total Energy dissipation in nodes" and "Number of alive nodes" were considered to evaluate the performance. LEACH, K-Means, direct method and BFO simulation were carried out in MATLAB 8.0. First of all, 100 WSN nodes were randomly distributed in a spatial region of 50mx50m network area. In LEACH and K-Means algorithm, 5% of the nodes have been taken as cluster-heads. Each node transmits 2000 bits in 1 round and E_{elec}=50 nJ/bit, ε_{amp}=50 nJ/bit and E_{Rx}=100nJ/bit. All parameters are presented in Table 4.1.

The radio energy model for our simulation is as given below. For transmission of k bits message to a distance, radio expends

$$E_{Tx}(k,d)=E_{Tx\text{-}elec}(k)+E_{Tx\text{-}amp}(k,d) \qquad (4.3)$$

$E_{Tx}(k,d) = E_{elec} * k + E_{amp} * k * d^2$ (4.4)

Where $E_{Tx}(k,d)$ is the energy dissipated to transmit a k-bit message over distance d

$E_{Tx-elec}(k)$ is the energy dissipated by transmitter electronics

$E_{Tx-amp}(k,d)$ is the energy dissipated by amplifier electronics

E_{elec} is the constant energy of 50 nJ expended to run the amp and transmitter circuitry

For reception, radio expends

$E_{Rx}(k) = E_{Rx-elec}(k)$ (4.5)

$E_{Rx}(k) = E_{elec} * k$ (4.6)

where $E_{Rx-elec}$ is the energy dissipated by receiver electronics

Table 4.1 Network parameters for simulations

Parameter	value
No of nodes	100
Area	50m×50m
Desired CH	5%
Energy of battery	0.5J
No of bits transmitted in one round From one node	2000 bits
Location of base station	[25,-100]
Eelec	50nJ/bit
Eamp	100 pJ/bit/

Figure 4.3 shows the initial nodes distribution in LEACH method. Figure 4.4 shows sensors that are alive (dotted circles) and dead sensors (dots) after 1200 rounds in LEACH algorithm. Position of sensor nodes and formation of cluster head have been shown in Figure 4.5 and Figure 4.6 respectively. Figure 4.7 shows the change of cluster head while executing K-Means algorithm. Figure 4.8 shows the initial position of sensor nodes while Figure 4.9 shows clustering of sensor nodes using BFO.

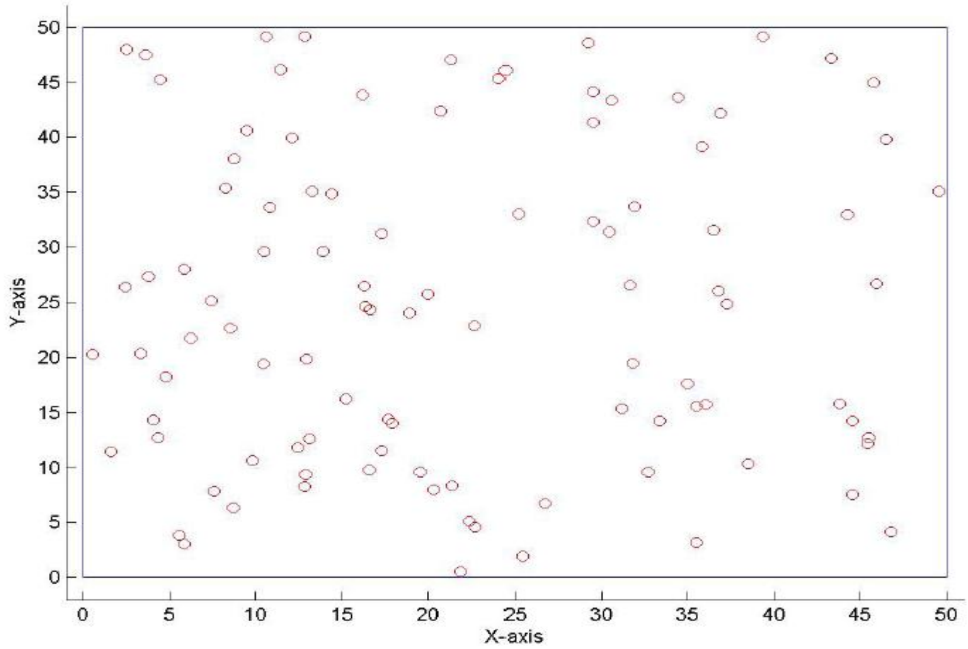


Figure 4.3: Initial positions of sensor nodes during simulation

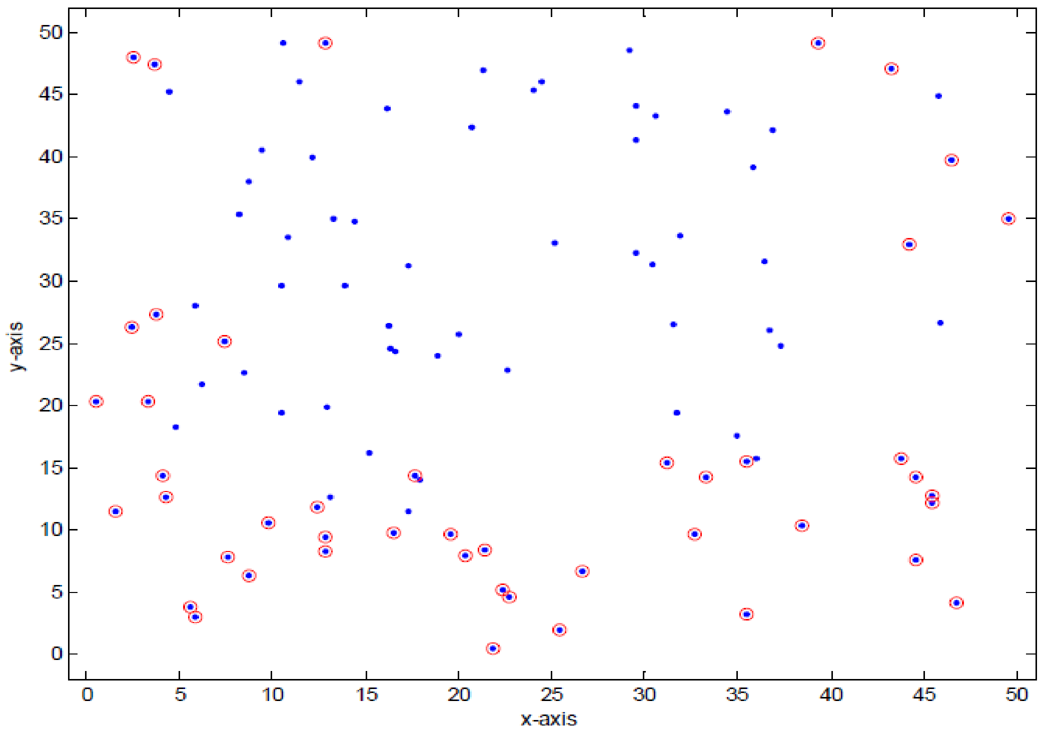


Figure 4.4: Sensors that are alive (dotted circles) and dead sensors (dots) after 1200 simulation rounds

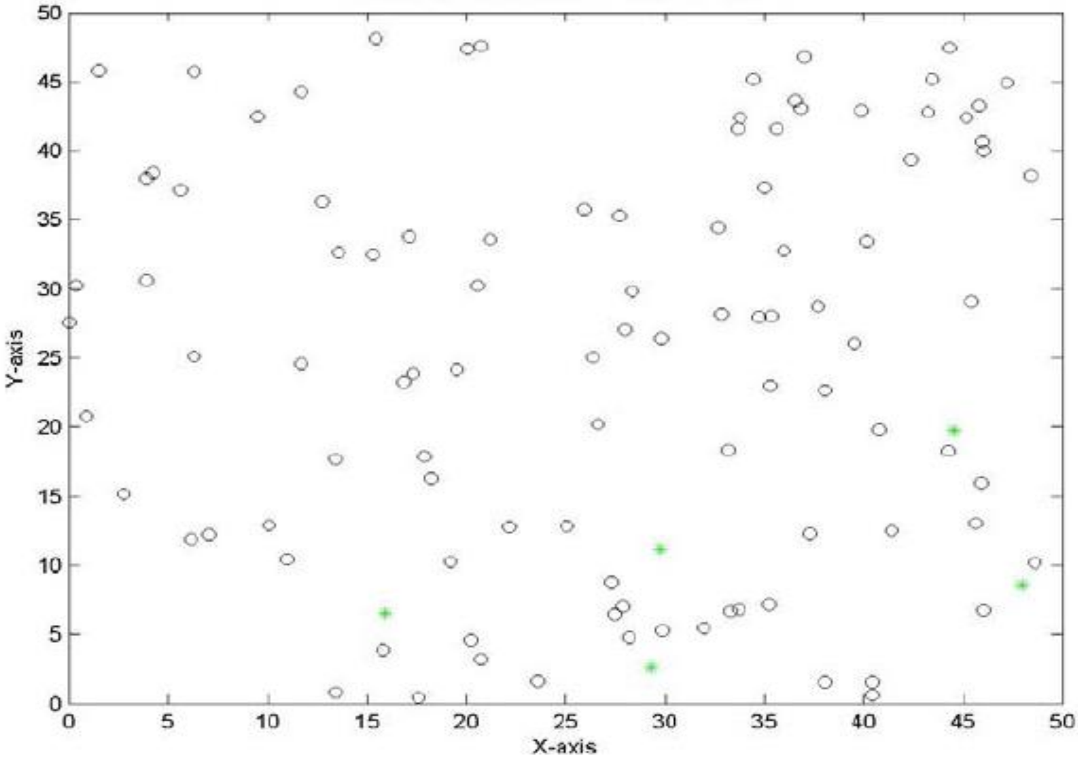


Figure 4.5: Initial positions of sensor nodes during K-Means Clustering

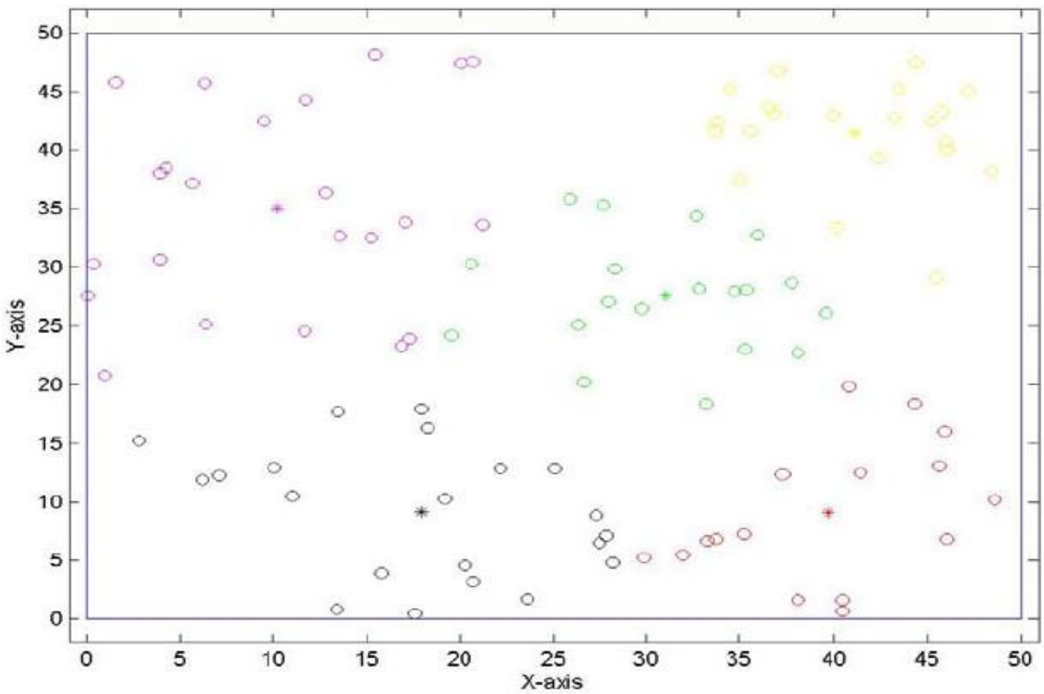


Figure 4.6: Clustering formation of sensor nodes using K-Means Clustering

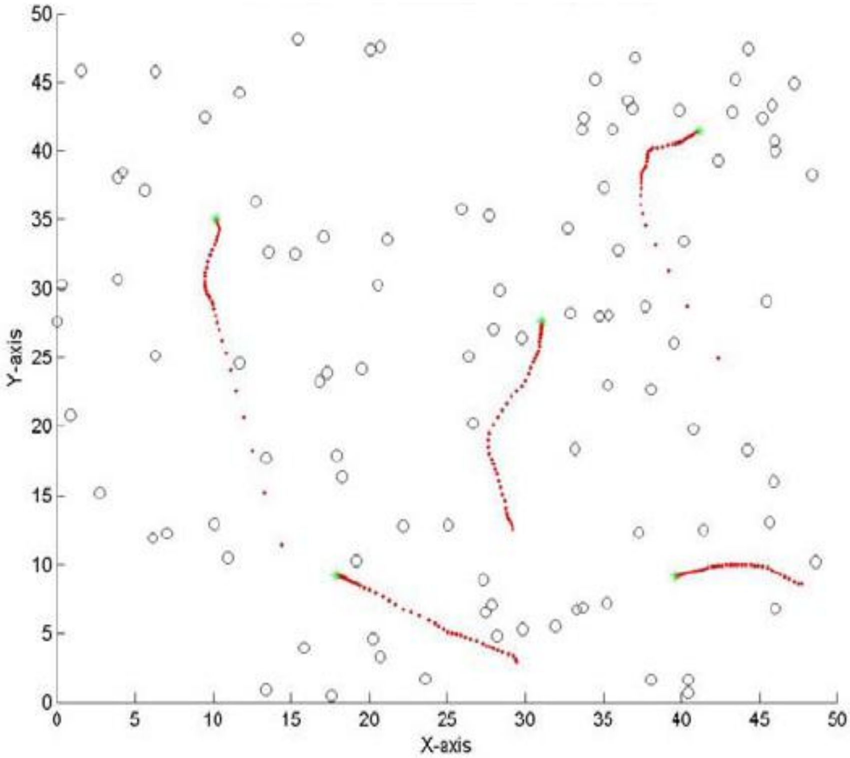


Figure 4.7: Cluster head formation while executing K-Means Clustering

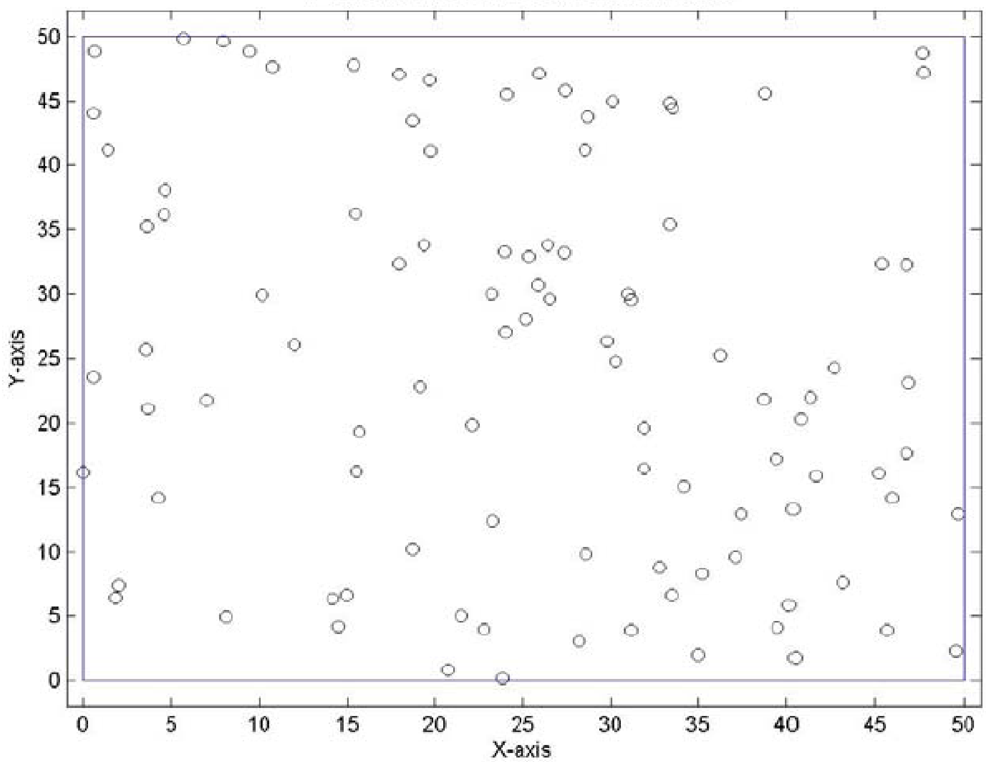


Figure 4.8: Random placement of sensor nodes in BFO

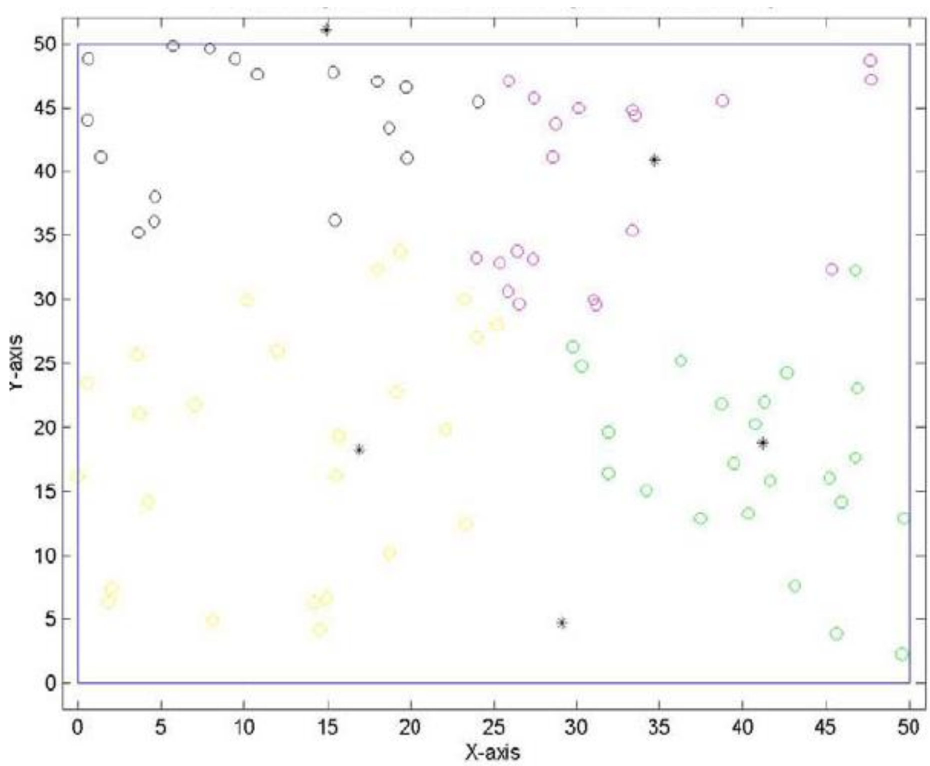


Figure 4.9: Clustering of sensor nodes in BFO

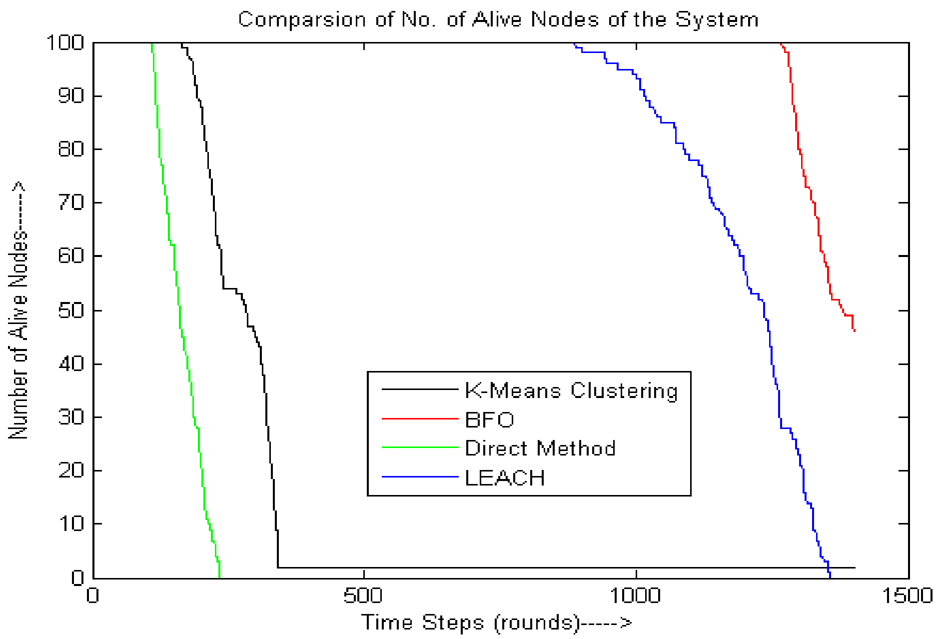


Figure 4.10: Comparison of number of alive nodes of the network system among different algorithms

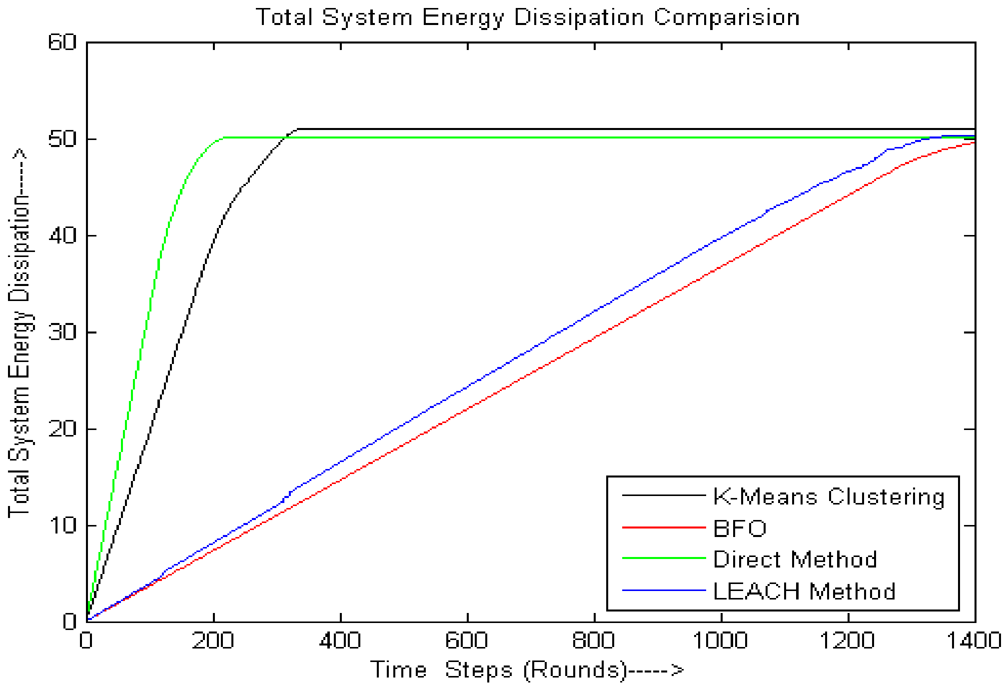


Figure 4.11: Comparison of Total system energy dissipation in the network system among different algorithms

4.5 Results and discussion

Figure 4.10 compares the number of alive nodes of the network system for four methods viz: BFO, direct method, LEACH and K-Means algorithm. Here number of nodes that are alive has been plotted against time.

From the simulation results, it is seen that K-means provides better performance than the direct method. However it performs poorly compared to LEACH. It is seen that LEACH provides a considerably higher lifetime compared to K-Means clustering. In addition to reducing energy dissipation, LEACH successfully distributes energy-usage among the nodes in the network such that the nodes die randomly and at essentially the same rate. While these simulations do not account for the setup time to configure the dynamic clusters (nor do they account for any necessary routing start-up costs or updates as nodes die), they give a good first order approximation of the lifetime extension we can achieve using LEACH. Another important advantage of LEACH is the fact that nodes die in essentially a “random” fashion. It is also seen that BFO provide better lifetime for nodes compared to other three methods. BFO is able to provide 100% live nodes for maximum duration. Since all nodes are alive for long duration, there is sharp drop in live nodes at the end. However at any point of time BFO provides equal or more live nodes compared to LEACH algorithm.

The total energy dissipation in the network system is presented in Figure 4.11. From this, it can be seen that at any time instant total energy dissipation with BFO algorithm is less than other algorithms. Additionally, it is seen that LEACH perform better than K-Means clustering which in turn outperforms direct method.

4.6 Conclusion

Bacteria based optimization (BFO) based cluster head selection has been presented in this chapter. It is seen that BFO provides better performance than other popular techniques. However, the computational complexity of BFO for applicability to WSNs still remains a challenge.

Chapter 5

Quality of Service Evaluation in IEEE 802.15.4 Networks

5.1 Introduction

The term "QoS" is used in different meanings, ranging from the user's perception of the service to a set of connection parameters necessary to achieve particular service quality. ITU-T (Recommendation E.800 [ITU-TE.800]) and ETSI [ETSI-ETR003] basically defines Quality of Service (QoS) [**84**] as "the collective effect of service performance which determines the degree of satisfaction of a user of the service". The goal of QoS provisioning is to achieve a more deterministic network behaviour so that information carried by the network can be better delivered and network resources can be better utilized. It is becoming an important service of any communications system. Providing QoS in WSN is a challenging task due to its severe resource constraints in terms of energy, network bandwidth, memory, and CPU cycles. WSNs have also unstable radio ranges, transient connectivity and unidirectional links. So, a new set of QoS parameters, mechanisms and protocols are needed. Energy-efficiency is crucial in WSNs, which require a long network lifetime, data accuracy and the avoidance of maintenance. Moreover, certain service properties such as the delay, reliability, network lifetime, and quality of data may conflict by nature. For example, multi-path routing can improve the reliability. However, it can increase the energy consumption and delay due to duplicate transmissions. The high resolution sensor readings may also incur more energy consumptions and delays. Modeling such relationships, measuring the provided quality and providing means to control the balance is essential for QoS support in WSN [**85**].

5.2 Quality of Service Requirements in WSNs

A WSN node consists of different kinds of sensors for different unique applications. For example, it may be acceptable to lose some measurements in repeatedly transmitted environmental data, but transmitted events and one-shot queries must be reliable. In addition, critical alert messages from possibly life-threatening conditions require high reliability as well as low delay. The simplest method for providing a sufficient service is to make sure that a network has enough resources for each application. Thus, the capacity is fitted for the worst-case network usage; but this is not applicable to energy constraint WSN nodes. As wired devices are AC powered and wireless devices (such as laptops) can be easily recharged, the energy is not of significant issue. In a WSN, the majority of energy consumption is caused by wireless communications, therefore requiring *energy awareness*. Computer networks route most of their data in a wired-backbone network, while only end nodes may be wireless (such as in wireless LANs or cellular networks).The nodes of WSN are energy constraint in resource. So, in WSN data is usually routed via multihop due to its low transmission range. The wireless links of WSN nodes are prone to effects of radio interference, node mobility, changing environmental conditions or unexpected failure of a sensor node due to low energy. Even if a link has a small probability of failure, the probability accumulates on each link, which makes end-to-end communication unreliable. Due to the *unreliability*, the connection oriented approach like TCP used in traditional networks is impractical in WSNs. A WSN node has significant resource constraints as memory and processing power are limited. This significantly limits the available approaches for QoS. For example, storing states of each flow that passes a node is impossible. The memory constraints and the unreliability prevent using many protocols that rely on end-to-end resource reservation mechanisms [**74**].

5.3 Challenges for QoS Support in WSNs

Since WSNs have to interact with the environment, their characteristics can be expected to be very different from other conventional data networks. Thus, while WSNs inherit most of the QoS challenges from general wireless networks, their particular characteristics pose unique challenges as follows [**86**].

Severe resource constraints*:* The constraints on resources involve energy, bandwidth, memory, buffer size, processing capability, and limited transmission power. Among them, energy is a primary concern since energy is severely constrained at sensor nodes and it may not be feasible to replace or recharge the battery for sensor nodes that are often expected to work in a remote or inhospitable environment. So, these constraints impose an essential requirement on any QoS support mechanisms in WSNs simplicity. Hence, computation intensive algorithms, expensive signaling protocols, or overwhelming network states maintained at sensors are not feasible.

Unbalanced traffic*:* In most applications of WSNs, traffic mainly flows from a large number of sensor nodes to a small subset of sink nodes. QoS mechanisms should be designed for an unbalanced QoS-constrained traffic.

Data redundancy*:* WSNs are characterized by high redundancy in the sensor data. However, while the redundancy in the data does help loosen the reliability/robustness requirement of data delivery, it unnecessarily spends much precious energy. Data fusion or data aggregation is a solution to maintain robustness while decreasing redundancy in the data, but it introduces latency and complicates QoS design in WSNs.

Energy balance*:* To prolong the network lifetime of WSNs, energy load must be evenly distributed among all sensor nodes so that the energy at a single sensor node or a small set of sensor nodes will not be drained out quickly. So, load balancing techniques should be applied to support this feature.

Scalability*:* A wireless sensor network usually consisting of hundreds or thousands of sensor nodes densely distributed in phenomena. Therefore, QoS support designed for WSNs should be able to scale up to a large number of sensor nodes, i. e. QoS support should not degrade quickly when the number of nodes or their density increases.

Multiple traffic types*:* In WSN, inclusion of heterogeneous sets of sensors raises challenges for QoS support. For instance, some applications may require a diverse mixture of sensors for monitoring temperature, pressure and humidity, thereby introducing different reading rates at these sensors. Such a heterogeneous environment makes QoS support more challenging.

Multiple sinks*:* Wireless Sensor networks may have multiple sink nodes, which impose different requirements on the network. For example, one sink may query sensor nodes located in the southwest of the sensor field to send a temperature report every one minute, while another sink node may only be interested in an exceptionally high temperature event in the northeast area. WSNs should be able to support different QoS levels associated with different sinks.

Network dynamics*:* Network dynamics may arise from node failures, wireless link failures, node mobility, and node state transitions due to the use of power management or energy efficient schemes. Such a highly dynamic network greatly increases the complexity of QoS support.

Packet criticality: The content of data or high-level description reflects the criticality of the real physical phenomena with respect to the quality of the applications. QoS mechanisms may be required to differentiate packet importance and set up a priority structure.

5.4 Parameters Defining WSN QoS

The QoS service parameters used in traditional wired networks are throughput, reliability, delay and jitter. Security and mobility are essential in any wireless network, while data accuracy is especially relevant to the WSNs. The Network lifetime is usually shortened by decreasing latency or increasing any of the other parameters which affects energy consumption of WSN nodes in terms of processing, transmission and reception of data packets.

The QoS parameters for WSN are listed below as given in [**74**]:

• **Data accuracy**: A node detects a physical phenomenon within certain sensing coverage that is affected by the physical sensor and environmental obstacles. As a network may have redundant sensors and as the measurements in all areas are not equally important, energy efficiency can be improved by switching off some of the nodes. For example, the majority of the nodes in an intruder detection WSN are initially on power-save mode (sleep and low-sensing interval), while border nodes may be more active than the other nodes. When an intruder is detected, nodes are switched on for tracking movement and to determine the type of intruder.

• **Energy usage**: As computation is often much less energy consuming than transmitting, some of the communications may be traded against computation. For example, data may be pre-processed to fit into smaller packets or by performing data aggregation. However, the aggregation has a trade-off between energy usage and reliability, as a large amount of data may be lost on a missed packet.

• **Reliability**: In communications networks common methods for increasing reliability are using acknowledgments and error correction. Also, adding redundancy increases reliability as the network is able to recover from the loss of a single packet, but this method increases energy usage.

• **Latency**: Latency is the time taken for the network to transfer a packet from a source node to the destination node. For critical messages, networks may need to provide delivery guarantees. As sensor networks rarely use real-time streaming applications (e.g. audio, video), the variation of the latency is less important.

• **Security**: Security is achieved by encrypting messages and verifying that a message is authentic. However, these may require significant processing power. In addition, encryption may widen data size and authentication requires additional messaging, thus causing more communicational overheads.

• **Mobility**: The mobility support may range from partial mobility to full mobility support. In partial mobility support, only a part of the nodes can be moved. The maximum degree of mobility may be limited to a maximum amount of mobile nodes. Also, the protocol stack and the utilized transceiver may limit mobility speed, as the communication range is limited and a node may move outside the range before having a chance to send or receive data.

• **Throughput:** In WSN, throughput is not usually as significant as other parameters. A sensor node send typically small packets; but the use of acoustic and imaging sensors requires significant throughput, as data must be streamed through the network. Thus, certain WSN applications require maximizing throughput and possibly throughput guarantees.

5.5 Quality of Service support in protocol layers

5.5.1 Application Layer

The application layer has the best knowledge regarding the importance of the data. Therefore, an application associates a generated packet with its QoS requirements. The network aims to satisfy these requirements, while minimizing the energy consumption. The application layer is also responsible for making the sensor measurements and controlling sensors. There will be trade-off between the data accuracy and energy usage if an application configures sensors based on measurement accuracy versus time interval.

5.5.2 Transport Layer

The two main tasks for the transport layer are congestion control and reliable transmission. Typically, congestion control limits the sending of traffic to reduce bandwidth utilization. As the congestion is reduced, the overall reliability in the network is increased since the data link layer does not have to drop frames. However, throughput limitations may increase delays as the source node must hold onto the generated packets that much longer. Therefore, QoS awareness is required to make a decision regarding which traffic is being more limited than the other.

The energy efficiency of a transport protocol depends on the number of transmissions required to deliver a message. This is greatly affected by the acknowledgment scheme being utilized. With the positive acknowledgment scheme, the receiver acknowledges each packet. If an acknowledgment is not received within a certain time interval, the packet is resent. With the negative acknowledgment scheme, missing packets are requested by the receiver node. This reduces messaging as acknowledgments are sent only when required.

5.5.3 Network Layer

The network layer controls QoS with traffic shaping and routing protocol. The traffic shaping performs congestion control by classifying packets and providing queuing disciplines that provide per class QoS and fairness. For example, a node may drop low-priority traffic to ensure enough resources for higher priority data. The routing protocol is responsible for selecting an end-to-end routing path fulfilling the desired QoS characteristics. As a route that maximizes one QoS metric may not be optimal on others, the route selection has to make a trade-off between different QoS metrics.

For maximizing network lifetime, a routing protocol not only tries to minimize the energy used for routing the packet, but also performs load balancing between nodes to prevent heavily loaded nodes from dying prematurely. Meanwhile, the shortest path route is not always the most energy efficient. It is due to the fact that the transmission power requirement is proportional to the square of the distance. It might be more energy efficient to forward data through two short hops than through one long hop. As longer routes usually have higher latency, the route selection therefore has to make a trade-off between energy and delay. The routing protocol design can make the selection between maintenance and routing energy consumption to determine how dynamic the protocol is.

5.5.4 Data Link Layer

The data link layer achieves energy efficiency by good designs of the channel access scheme. It consists of the selection between synchronized and unsynchronized data exchanges, and the usage of the low duty-cycle operation. Low duty-cycle operation has a significant impact on available QoS. While a smaller duty cycle requires less energy, it also decreases available throughput, as there are less transmission opportunities per access cycle. In addition, duty cycling also increases latency because a node must wait until the receiver wakes up before it can send a frame. Longer access cycles increase the waiting time, thus further increasing the delay. Therefore, low duty-cycle operation has a trade-off between latency, throughput, and energy usage.

The data link layer is responsible for dividing bandwidth to the traffic based on their priority and QoS requirements. The data link layer mainly controls reliability with the used retransmission scheme, but also by avoiding the collisions and hidden node problems. In addition, the adjustment of transmission power affects reliability. High transmission power enables more reliable transmission, but on the other hand, might cause additional interference within a network. The mobility support on the MAC layer is largely dependent on how often a node can communicate with its neighbours. Low duty-cycle operation and long access cycles are bad for mobility because a node might have already moved outside the communication range before it has the chance to communicate. In addition, the requirement for extensive association hand-shaking or transmission slot reservation may also limit mobility.

5.5.5 Physical Layer

The physical layer comprises not only the transceiver, but also Microprocessor, sensors, and the energy source. Therefore, the physical layer put limits on other layers capacity. While the transceiver causes most of the energy usage, it also imposes several other limitations to the communication protocols. The data rate limits maximum achievable throughput, whereas the used coding scheme affects reliability. As the communication range is limited, the transceiver determines the minimum network density that is needed to route data. MCU puts limits to computational capabilities and available memory so as to avoid complex protocols and applications. Energy consumptions in sleep and active modes have a significant impact on energy usage.

Physical sensors have certain accuracy and acquisition time-limiting sampling intervals. To overcome these limitations, the network may need to sample data in several nodes on the same region and combine this data to get more detailed values, thus consuming more energy. Still, if a sensor supports selecting sensing accuracy, the accuracy may be purposefully reduced to make a trade-off against energy.

5.6 MANET REACTIVE ROUTING PROTOCOLS

5.6.1 Ad-hoc On-demand Distance Vector Routing (AODV)

Ad–hoc on demand distance vector routing (AODV) is a stateless on-demand routing protocol [**87**]. It establishes routes on as desired by a source node, using route request (RREQ) and route reply (RREP) messages. When the source node needs a route to another node, it broadcasts a RREQ message with a unique RREQ identification number. The message will reach the neighbouring nodes, which will update the sequence number for this source node. At same time, each neighbour node can also set up a reverse route to the source node in the routing table. Under the following two conditions, the neighbour node that receives a RREQ will send back a RREP to the requesting source node:

(1) The neighbour node is the destination node.

(2) The node has a route to the destination node that meets the freshness requirement specified in the RREQ message. On the other hand, if the node cannot send back the RREP packet, it will broadcast the received RREQ packet so that the message can spread wider in the network, until the message can reach the destination node or a node with a good route. The source node and the intermediate nodes that receive a RREP will update its routing table for the destination node. Before receiving a RREP, the source node will keep broadcasting RREQs with a given interval, with increasing identification numbers in the message. If a node receives a RREQ message that has already been processed, it will discard the message and do not forward it.

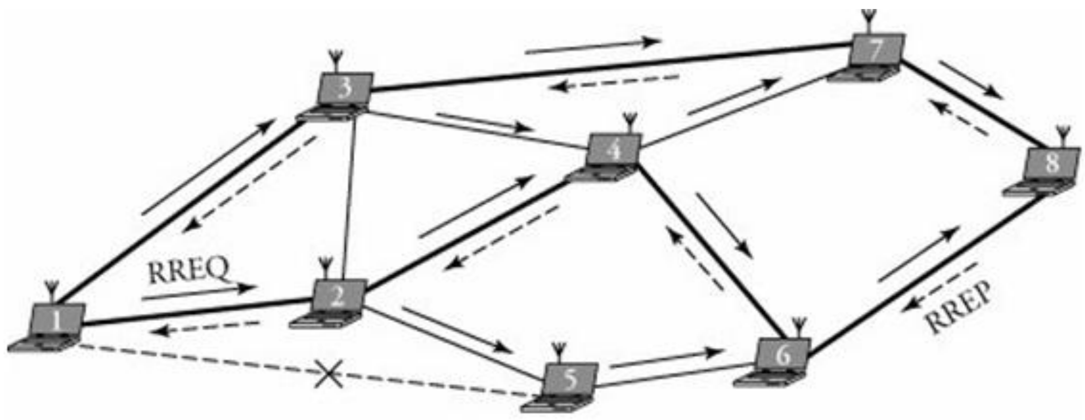


Figure 5.1: AODV Communication signaling from node 1 to node 8 [88**]**

Figure 5.1 shows the process of signals with AODV from node 1 to node 8. To establish a connection, source node 1 searches in its table for a valid route to destination node 8. RREQ reaches the destination for the first time through path 1-2-4-6-8. The destination then issues an RREP packet to the source. After a while, the destination receives another RREQ, this time through path 1-3-7-8. The destination evaluates this path, and finds that path 1-3-7-8 is better, and then issues a new RREP packet, telling the source to discard the other reply.

5.6.2 Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR) [**89**] is an on demand reactive routing protocol based on the concept of source routing . That is, the sender knows the complete hop-by-hop route to the destination for data packets to be transverse in the whole network. These routes are stored in a route cache. The data packets carry the source route in the packet header. The nodes can dynamically discover a source route across multiple network hops to any destination in the network. This makes the network completely self-organizing and self-configuring without the need for a network infrastructure or administration. DSR protocol is composed of two mechanisms: route discovery and route maintenance. Route discovery is based on flooding of route request messages and return of route reply messages. Route discovery is performed when a source has a packet to send, but does not know a route to its destination. The source broadcasts a query called a Route Request (RREQ) to each of its immediate neighbour, which on receiving, checks whether it is the destination, or has a route to the destination. If so, the node unicasts a response called a Route Reply (RREP) back to the source, informing it of the route to the destination.

The RREP follows a path that is typically the reverse of that followed by the RREQ. Otherwise, the node appends its own address to the RREQ and rebroadcasts the packet to its neighbours, which in turn process in the same manner. Each node only processes a given RREQ once and discards duplicates of the same RREQ received from its neighbours. Nodes detect a duplicate RREQ by tracking and comparing the ID and source address of each received RREQ. A RREQ having reached its hop-limit or maximum number of traversable hops upon arrival at a node will be automatically dropped. Once a RREP is received, the source immediately sends out the packet to its destination using the route obtained. Route maintenance is then carried out on the route in use to detect any link breaks. It is due to the fact that some node in the route has moved out of wireless transmission range of the previous node in the route. When a link on the source route is broken, a Route Error (RERR) identifying this broken link is returned to the original sender. The original sender then removes this broken link from its route cache. For subsequent packets to this same destination, the sender may use an alternate route that it may already have in its route cache or may reinvoke route discovery to discover a new source route to the destination. Together with route discovery, there are a number of optimizations that improve the performance of the protocol. For example, after a node detects a broken link and returns a RERR to the original sender of a packet, the node may attempt to salvage the packet if it has in its own route cache a different route to the packet's destination; to do so, the node replaces the original route with the route from its cache and transmits the packet to the new next hop node. In DSR, route maintenance may also involve allowing an intermediate node to send a gratuitous RREP to the source, informing it of a shorter route it detects during a packet's journey across the network.

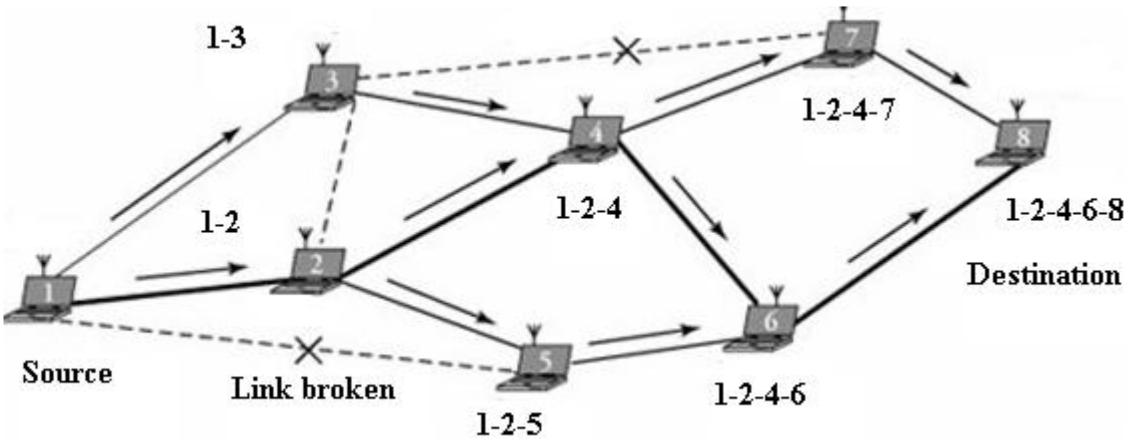


Figure 5.2: DSR Communication signaling from node 1 to node 8 [88**]**

Figure 5.2 shows an ad-hoc wireless network with eight nodes and a broken link (3-7).
Node 1 wants to send a message to the destination, node 8. Node 1 looks at its routing table, finds an expired route to node 8, and then propagates route-request packets to nodes 3 and 2. Node 3 finds no route to the destination and so appends the route record 1-3 to the route-request packet and forwards it to node 4. On receiving this packet, node 7 finds a route to the destination and so stops propagating any route-request packet and instead sends a route-reply packet to the source. The same happens when a route-request packet reaches the destination node 8 with a route record 1-2-4-6. When the source, node 1, compares all the route-reply packets, it concludes that the best route is 1-2-4-6-8 and establishes this path. Route maintenance in this protocol is fast and simple. In case of a fatal error in the data-link layer, a route-error packet is generated from a failing node. When the route-error packet is received, the failing node is removed from its route cache, and all routes containing that node are truncated. Another route-maintenance signal is the acknowledgment packets sent to verify the correct operation of the route links.

5.6.3 The Dynamic MANET On-demand (DYMO) routing protocol

The Dynamic MANET On-demand (DYMO) routing protocol [**90**] is a unicast reactive routing protocol which is intended for used by mobile nodes in wireless multihop networks. DYMO is a reactive routing protocol. In this routing message (control packet) is generated only when the node receives a data packet and it does not have any routing information. The basic operation of DYMO protocol is route discovery and route management.

During route discovery, the originator's DYMO router initiates dissemination of a Route Request (RREQ) throughout the network to find a route to the target's DYMO router. During this hop-by-hop dissemination process, each intermediate DYMO router records a route to the originator. When the target's DYMO router receives the RREQ, it responds with a Route Reply (RREP) sent hop-by-hop toward the originator. Each intermediate DYMO router that receives the RREP creates a route to the target, and then the RREP is unicast hop-by-hop toward the originator. When the originator's DYMO router receives the RREP, routes have then been established between the originating DYMO router and the target DYMO router in both directions.

Route maintenance consists of two operations. In order to preserve routes in use, DYMO routers extend route lifetimes upon successfully forwarding a packet. In order to react to changes in the network topology, DYMO routers monitor links over which traffic is flowing. When a data packet is received for forwarding and a route for the destination is not known or the route is broken, then the DYMO router of source of the packet is notified. A Route Error (RERR) is sent toward the packet source to indicate the current route to a particular destination is invalid or missing. When the source's DYMO router receives the RERR, it deletes the route. If the source’s DYMO router later receives a packet for forwarding to the same destination, it will need to perform route discovery again for that destination. DYMO uses sequence numbers to ensure loop freedom. Sequence numbers enable DYMO routers to determine the order of DYMO route discovery messages, thereby avoiding use of stale routing information.

5.7 Related Work

J. Zheng and M.J. Lee [**72**] implemented the IEEE 802.15.4 standard on NS2 simulator and subsequently produced the comprehensive performance evaluation on 802.15.4. The literature comprehensively defines the 802.15.4 protocol as well as simulations on various aspects of the standard. It mainly confined to performance of IEEE 802.15.4 MAC. Similarly in [**91**], the authors provided performance evaluations of IEEE 802.15.4 MAC in beacon-enabled mode for a star topology. The performance evaluation study revealed some of the key throughput-energy-delay tradeoff inherent in IEEE 802.15.4 MAC. J.S.Lee [**92**] attempted to make a preliminary performance study via several sets of practical experiments, including the effects of the direct and indirect data transmissions, CSMA-CA mechanism, data payload size, and beacon-enabled mode. T.H.Woon and T.C. Wan [**93**] extended existing efforts but focuses on evaluating the performance of peer-to-peer networks on a small scale basis using NS2 simulator. The author analyzed the performance based on commonly known metrics such as throughput, packet delivery ratio, and average delay. In addition, they proposed ad hoc sensor networks (AD-WSNs) paradigm as part of the extension to the IEEE 802.15.4 standard. A Mathematical Model for performance analysis of IEEE 802.15. 4 non-beacon enabled mode has been presented in [**94**] . This model allows the evaluation of the statistical distribution of the traffic generated by the nodes, the success probability for the transmission of a packet, and the mean energy spent by a node for a transmission which is validated through simulations. In [**95**], the authors presented a novel mechanism intended to provide Quality of Service (QoS) for IEEE 802.15.4 based Wireless Body Sensor Networks (WBSN) used for pervasive healthcare applications. The mechanism was implemented and validated on the AquisGrain WBSN platform.

5.8 QoS analysis in IEEE 8021.5.4 Star topology

5.8.1 Simulations set up

The main Objective of this simulation study is to evaluate the performance of IEEE 8021.5.4 star topology on different popular reactive wireless mobile ad hoc routing protocols like AODV, DSR and DYMO with varying traffic load. The simulations was carried out QualNet version 4.5 [**96**], a software that provides scalable simulations of wireless networks. For simulation, a star topology with one PAN Co-ordinator and 100 devices , uniformly deployed in an area of 50mx50m as shown in Figure 5.3 was considered. PAN is a static mains powered device placed at the centre of the simulation area. Only the uplink traffics i.e. devices to PAN Co-ordinator was considered in the simulation which suits WSN applications like automation industry where a large number of devices communicates to a single sink server for data delivery and processing. The devices have transmission range of one hop away from PAN Coordinator in star topology. The simulation parameters are listed in Table

5.1. The fact that BO = SO assures that no inactive part of the superframe is present. A low value of this parameter implies a great probability of collisions of beacons of beacon frames as these would be transmitted very frequently by coordinators. On the contrary, a high value of the BO introduce a significant delay in the time required to perform the MAC association procedure since channel duration which is a part of association procedure is proportional to BO. In our simulation model, function for acknowledging the receipt of packets is disabled. It is due to the fact that RTS/CTS overhead mechanism is too expensive for low data rate WSN application for which 802.15.4 is designed [**8**]. The CBR traffic with the following average packet rates: 0.1 packet per second (pps), 0.2 pps, 1 pps, 5 pps and 10 pps are used. Multiple-to-one CBR application traffic, which consists of 20 application sessions from farthest side nodes like 1,2,4,6,8,10,20,21,40,60,61,80,81,91,92,94,96,98,99 and 100 to PAN Co-ordinator node 55. The simulation results have been averaged over 10 different seed values varying from 1 to 10.

TABLE 5.1: IEEE 802.15.4 Star topology simulation parameters

Parameter	Value
Area	50m *50m
Transmission range	30meter
Simulation Time	170M,85M,18M,5M and 3M
Channel Frequency	2.4GHz
Data rate	250Kbps
TX-Power	0dBm
Path Loss Model	Two Ray Model
Phy and MAC Model	IEEE 802.15.4
Energy Model	MICAZ Mote
Battery Model	Simple Linear,1200mAhr
Payload Size	1000 and 50 bytes
BO and SO	5

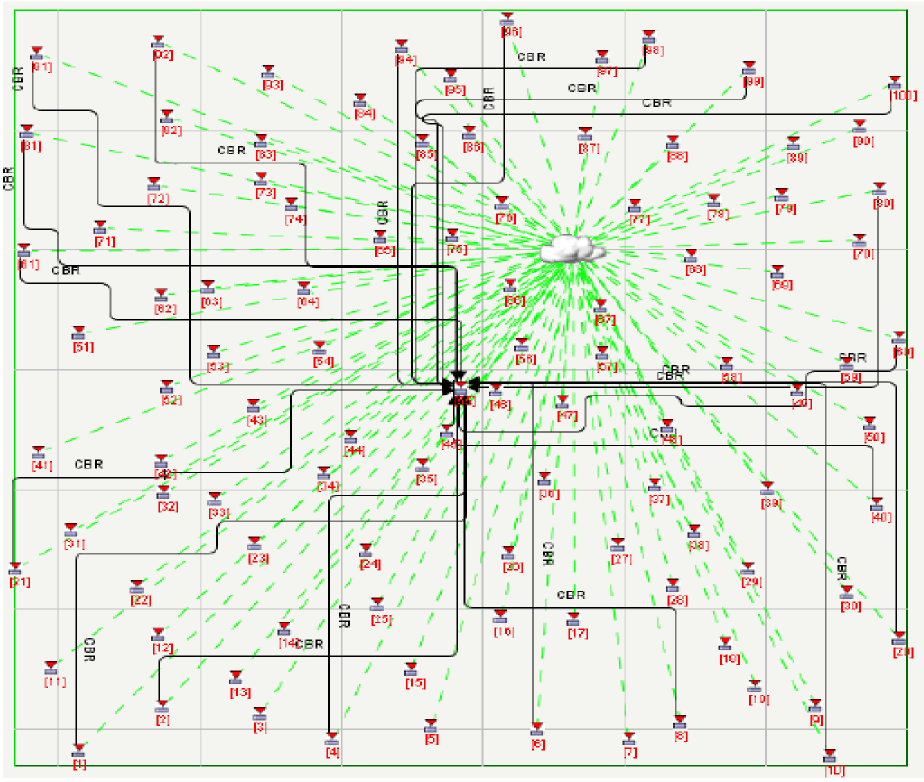


Figure 5.3: Simulation set up for Star Topology

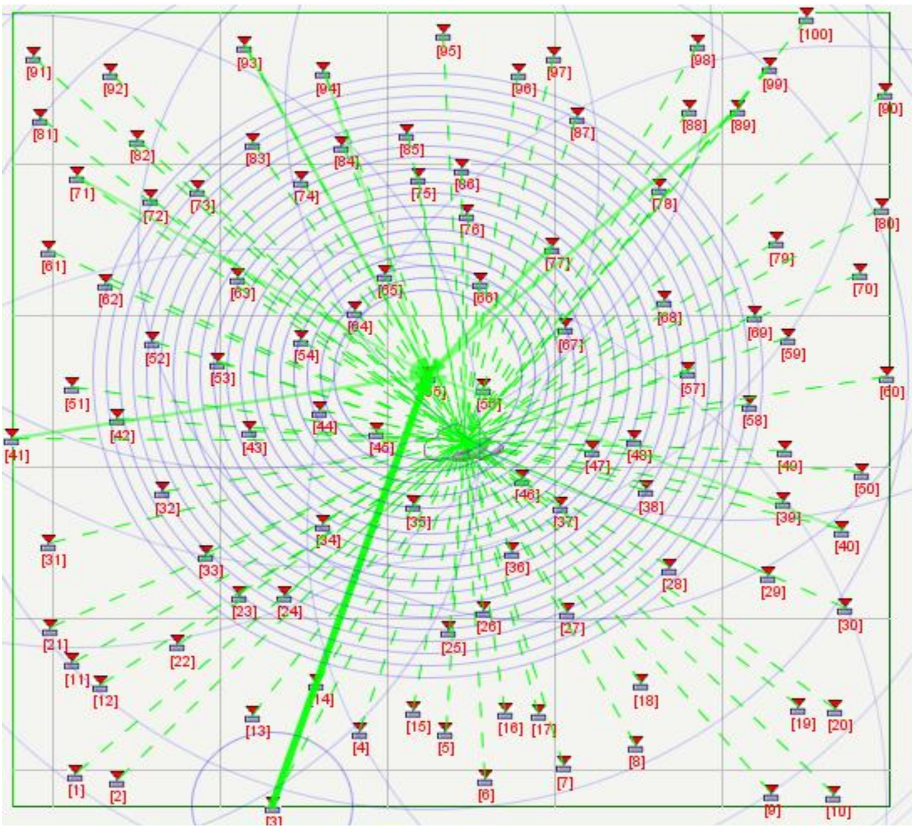


Figure 5.4: QualNet animator during simulation execution

5.8.2 Performance Metrics

Following performance metrics are considered to evaluate the QoS in IEEE 802.15.4 networks.

Packet delivery ratio (PDR): It is the ratio of number of data packets successfully received by the PAN Coordinator to the total number of data packets sent by RFD.

Average End-to-End delay: It indicates the length of time taken for a packet to travel from the CBR (Constant Bit Rate) source to the destination. It represents the average data delay an application experiences when transmitting data.

Throughput: It is the number of bits passed through a network in one second. It is the measurement of how fast data can pass through an entity (such as a point or a network).

Energy Consumption: This is amount of energy consumed by MICAZ Mote devices during the periods of transmitting, receiving, idle and sleep. The unit of energy consumption used in the simulations is mJoule.

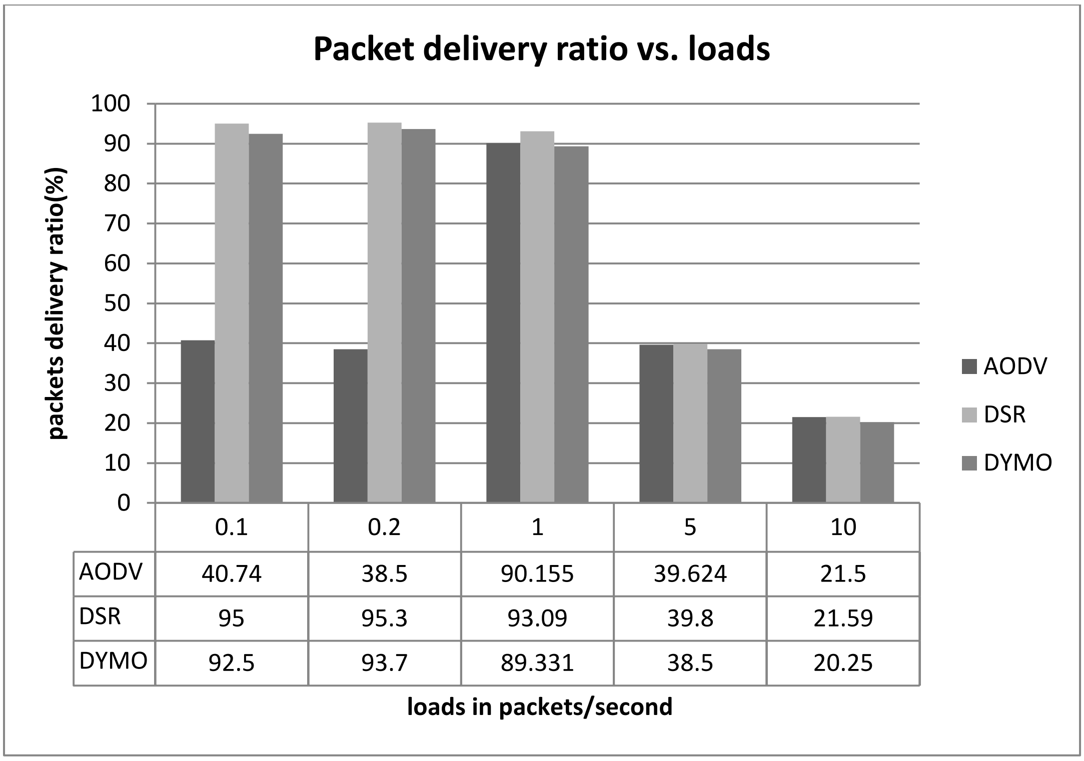
Energy per goodput bit: It is the ratio of total energy consumed to total bits received. It is used as a figure of merit to compare the performance of various network methods based on battery powered devices

Network Lifetime: This is defined as the minimum time at which maximum numbers of sensor nodes are dead or shut down during a long run of simulations.

5.8.3 Simulation results discussion

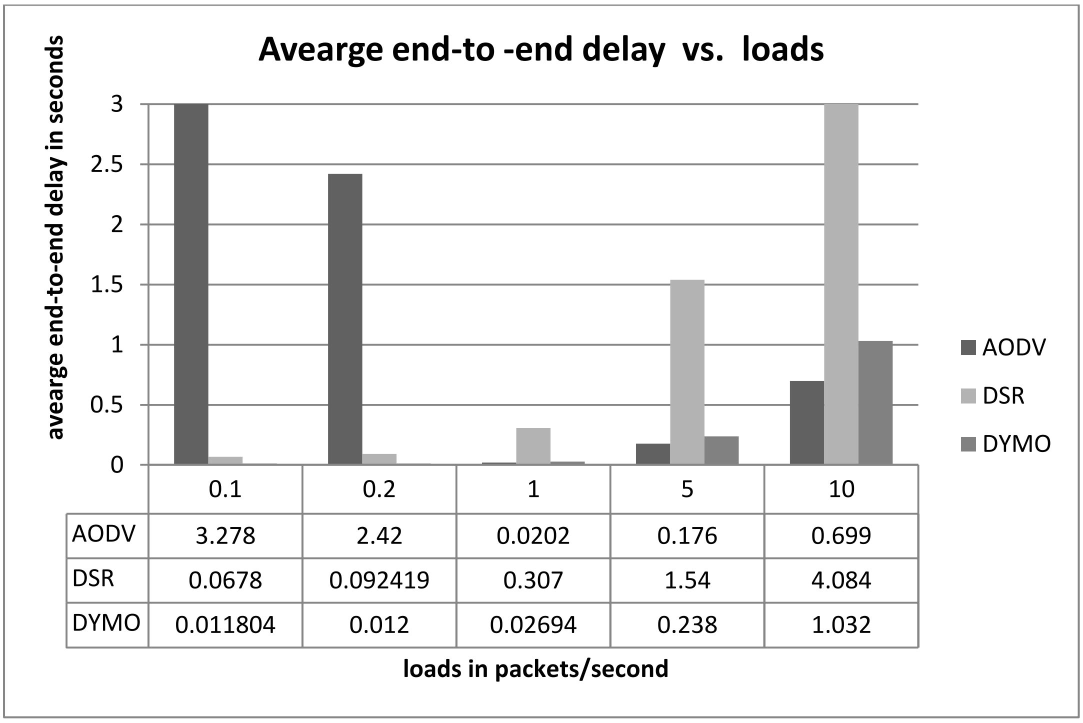
Packet delivery ratio: The performance of packet delivery ratio vs. load for varying traffic is shown in Figure 5.5. It is observed from the figure that DSR performs better than AODV and DYMO. The PDR of AODV increases from 40.74% to 90.15% when the load changes from 0.1 packets per second to 1 packet per second and then decreases. On the other hand, DSR shows nearly 95% packet delivery ratio at low traffic loads; but at higher loads i.e. at 5pps and 10pps, decreases to 21.5%. DYMO shows better performance of PDR at lower traffic rather than at higher traffic loads as comparison to AODV. The better performance of DSR is due to its source routing based aggressive caching approach which is very effective as the cached routes never expire.

Average end to end delay: The plot for average end-to- end delay for varying traffic loads is shown in Figure 5.6. The average end- to- end delay of a packet depends on route discovery latency, besides delays at each hop (comprising of queuing, channel access and transmission delays) and the number of hops. At low loads, queuing and channel access delays do not contribute much to the overall delay.



	0.1	0.2	1	5	10
AODV	40.74	38.5	90.155	39.624	21.5
DSR	95	95.3	93.09	39.8	21.59
DYMO	92.5	93.7	89.331	38.5	20.25

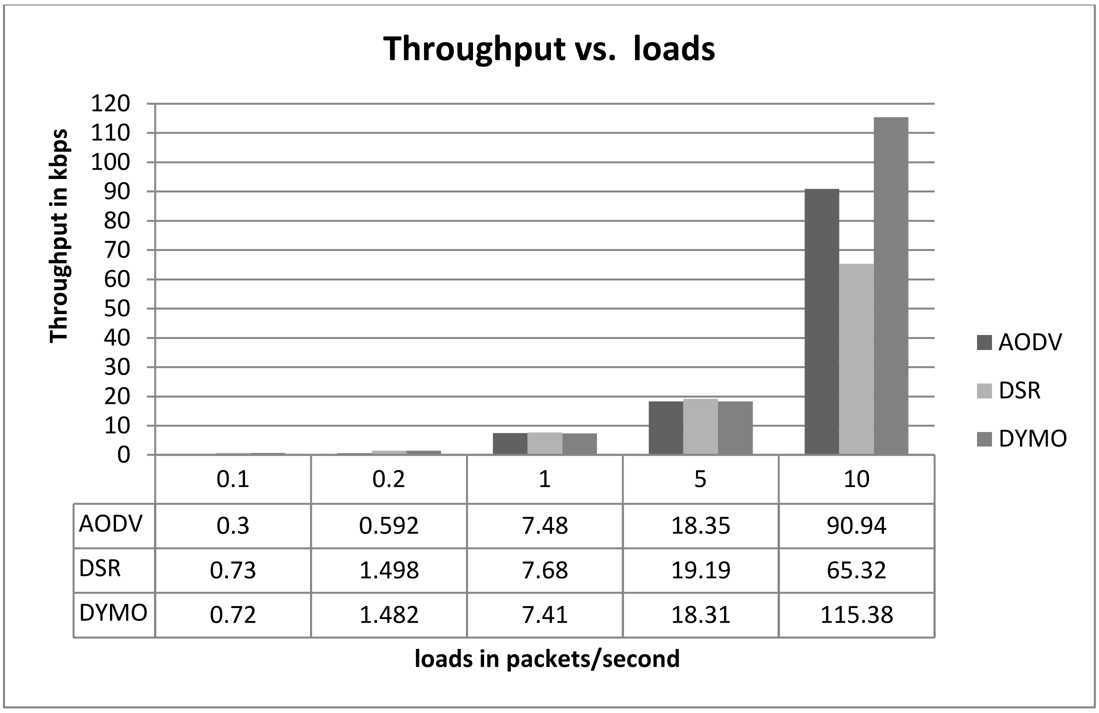
Figure 5.5: Packet delivery ratio vs. loads (packets/second)



	0.1	0.2	1	5	10
AODV	3.278	2.42	0.0202	0.176	0.699
DSR	0.0678	0.092419	0.307	1.54	4.084
DYMO	0.011804	0.012	0.02694	0.238	1.032

Figure 5.6: Average end to end delay vs. loads (packets/second)

From the figure, it is observed that DYMO, AODV and DSR is lower for a load of one packet per second. Lesser delay is attributed to its source routing mechanism.



	0.1	0.2	1	5	10
AODV	0.3	0.592	7.48	18.35	90.94
DSR	0.73	1.498	7.68	19.19	65.32
DYMO	0.72	1.482	7.41	18.31	115.38

Figure 5.7: Throughput vs. loads (packets/second)

Throughput: Figure 5.7 shows performance of throughput (in kbps) vs. loads in packets per second. From the graph, it is observed that maximum throughput is achieved when the load is at 10 packets per second. For DYMO, maximum throughput is 115.63kbps, it shows maximum throughput 115 kps is achieved at high traffic loads i.e. at 10 packets per second by DYMO. DYMO shows better throughput in comparison to AODV and DSR. Better throughput is due to lower average end to end delay as shown in Figure 5.6. In practice, a collision probability is high due to shorter backoff time. In addition, throughput is limited because of to a very short CAP. Thus, this option is suitable only for small and very low data rate networks. While a smaller duty cycle requires less energy, it also decreases available throughput, as there are less transmission opportunities per access cycle.

Total energy consumption: The plot for total energy consumption vs. load of three routing protocols is shown in Figure 5.8. The total energy consumption includes energy consumption in transmission, reception, idle and sleep modes of operation. It is noticed that the maximum energy dissipation occurred during idle mode while reception consumes greater energy than transmission for transferring data packets while calculating total energy consumption in our simulation. During sleep time, there is no energy consumption. The total energy consumption of three routing protocols decreases exponentially when it transferred packets from low traffic loads to high traffic loads. Routing protocols have an indirect effect on battery and energy models.

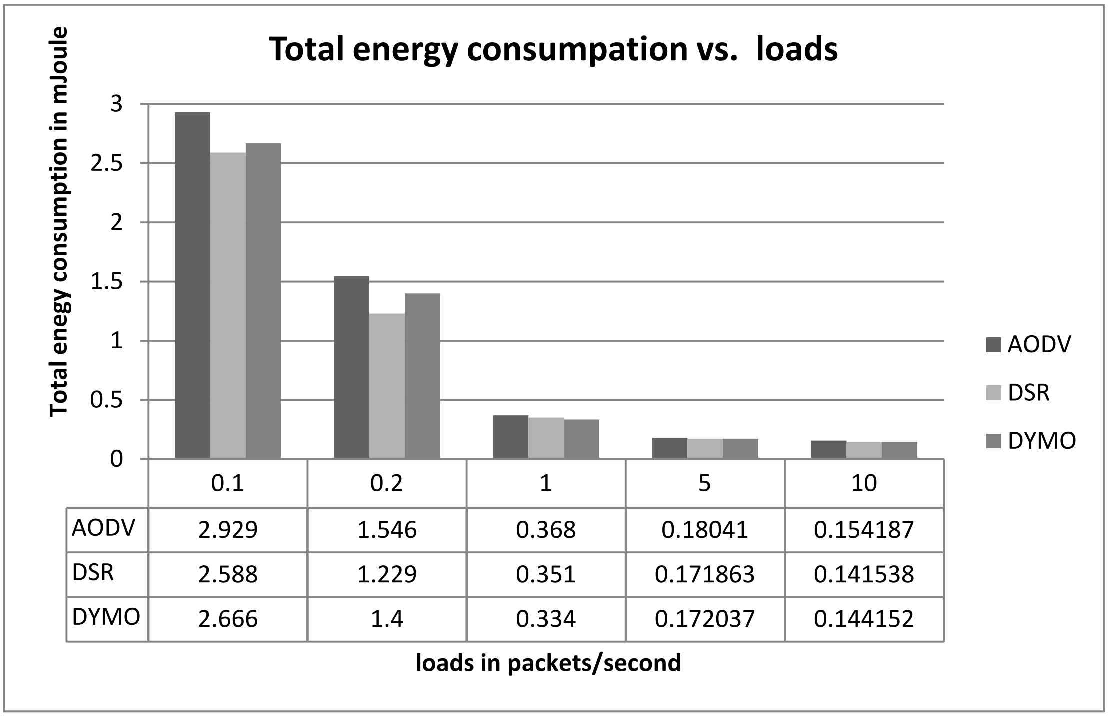


Figure 5.8: Total energy consumption vs. loads (packets/second)

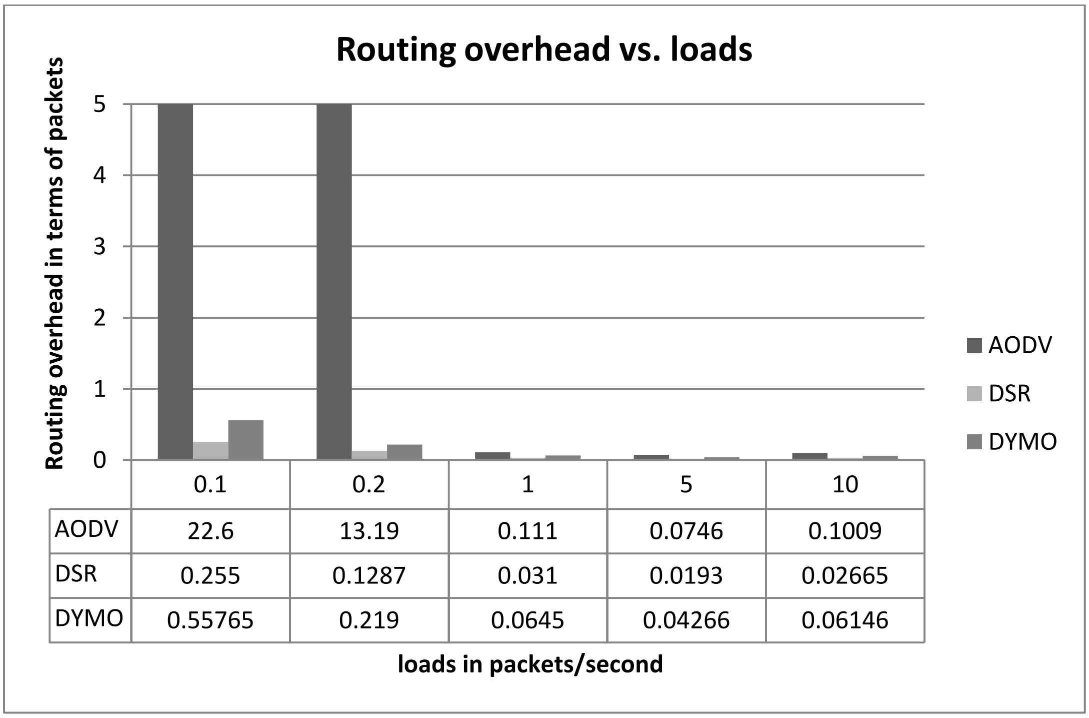
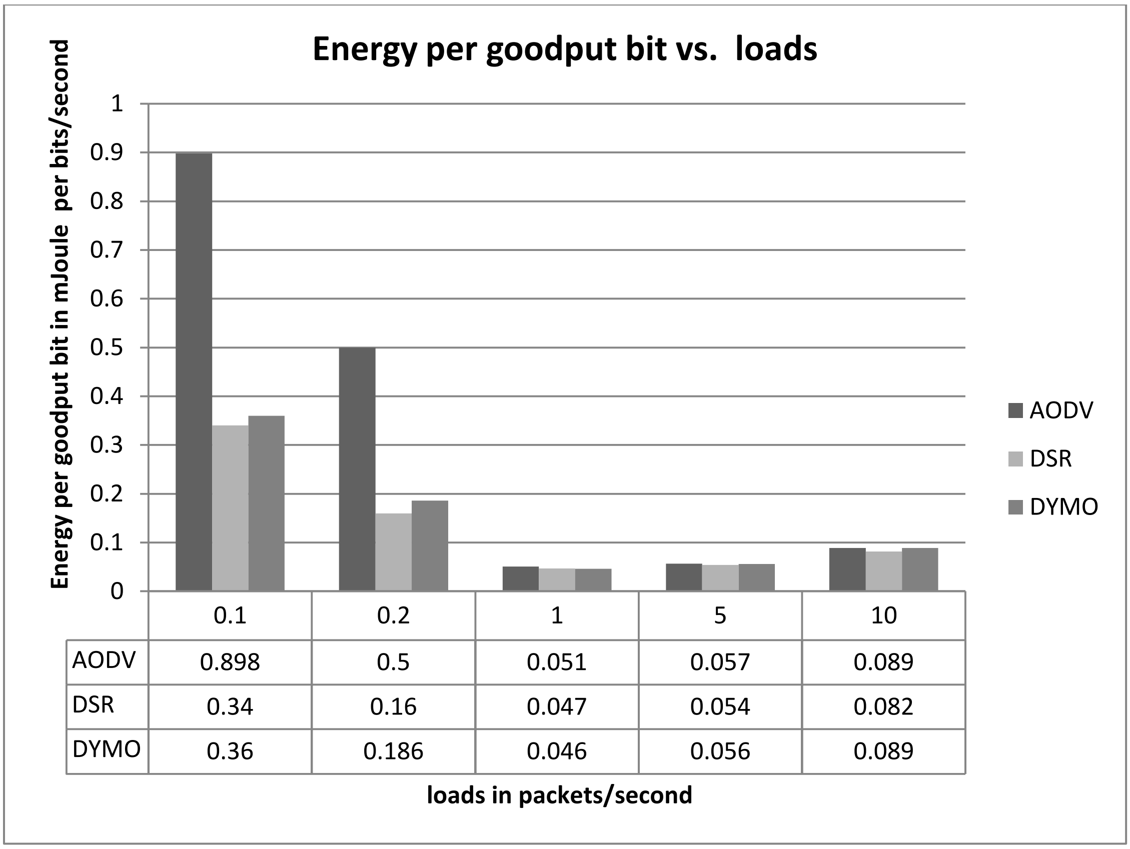


Figure 5.9: Routing overhead vs. loads (packets/second)

A routing protocol with more routing overhead would consume more energy than the routing protocol with less routing overhead. Hence, the statistics of energy and battery model could



	0.1	0.2	1	5	10
AODV	0.898	0.5	0.051	0.057	0.089
DSR	0.34	0.16	0.047	0.054	0.082
DYMO	0.36	0.186	0.046	0.056	0.089

Figure 5.10: Energy per goodput bit verses loads (packets/second)

be different for different routing protocols. The DSR routing protocols performs better than AODV and DYMO at all specified traffic loads due to its low routing overhead which is clear from Figure 5.9. AODV consume more power because routing overhead in AODV is more than DSR and DYMO.

Energy per goodput bit: The Figure 5.10 shows performance of energy per goodput bit verses traffic loads. The energy per goodput bit tells how much energy that one node has to consume per one bit of payload data. The result has been obtained by the taking the ratio of total energy consumed in transmission of data to the total bits delivered to the receiver. DSR routing protocol shows least energy per goodput bit in comparison to AODV and DYMO routing protocol. It is due to lower energy consumption and higher packet delivery ratio. The best value of energy per goodput bit is obtained when the load is 1 packet per second for all three routing protocols.

Percentage of time in sleep mode: The performance of the percentage of time in sleep mode vs. loads is shown in Figure 5.11. From the figure, it can be noticed that less than 1 mAhr is required to send data at different traffic loads. The IEEE 802.15.4 supports a Battery Life Extension (BLE) mode, in which the back-off exponent is limited to the range 0-2. This greatly reduces the receiver duty cycle in low traffic rate applications.

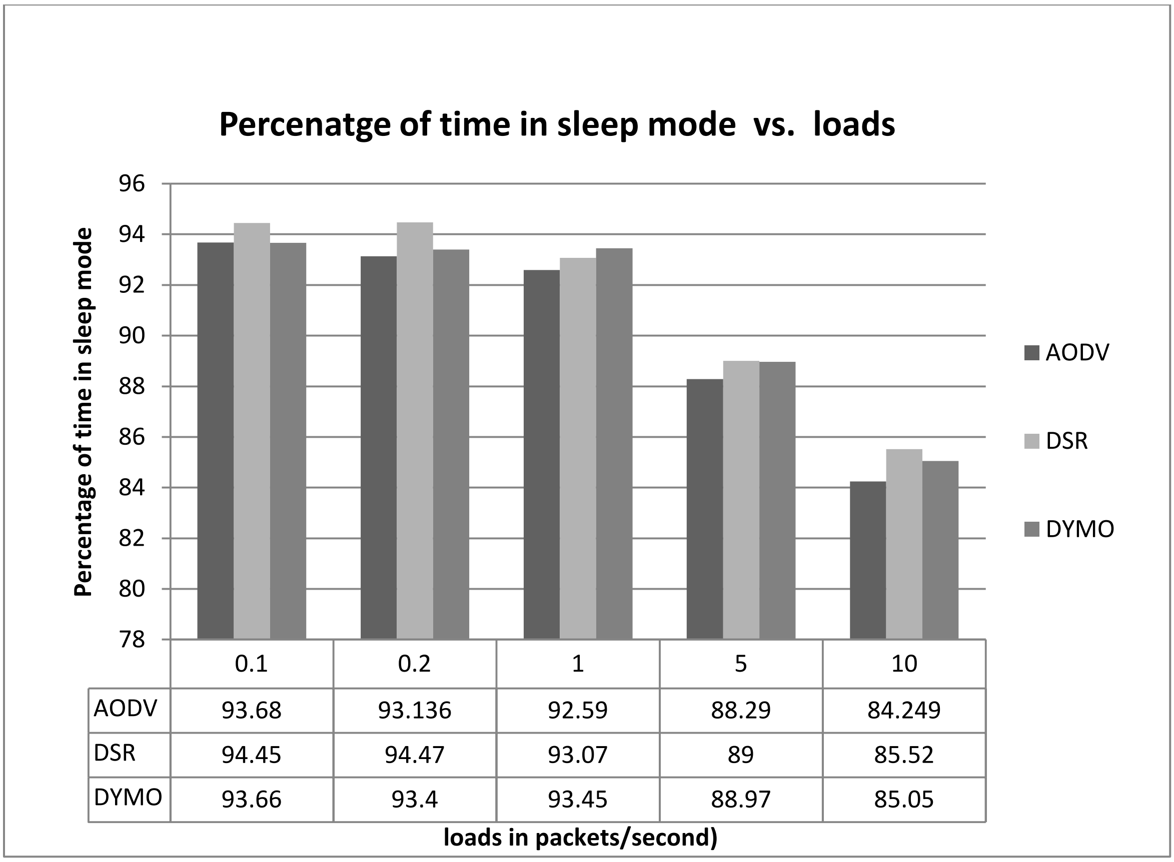


Figure 5.11: Percentage of time in sleep mode verses loads (packets/second)

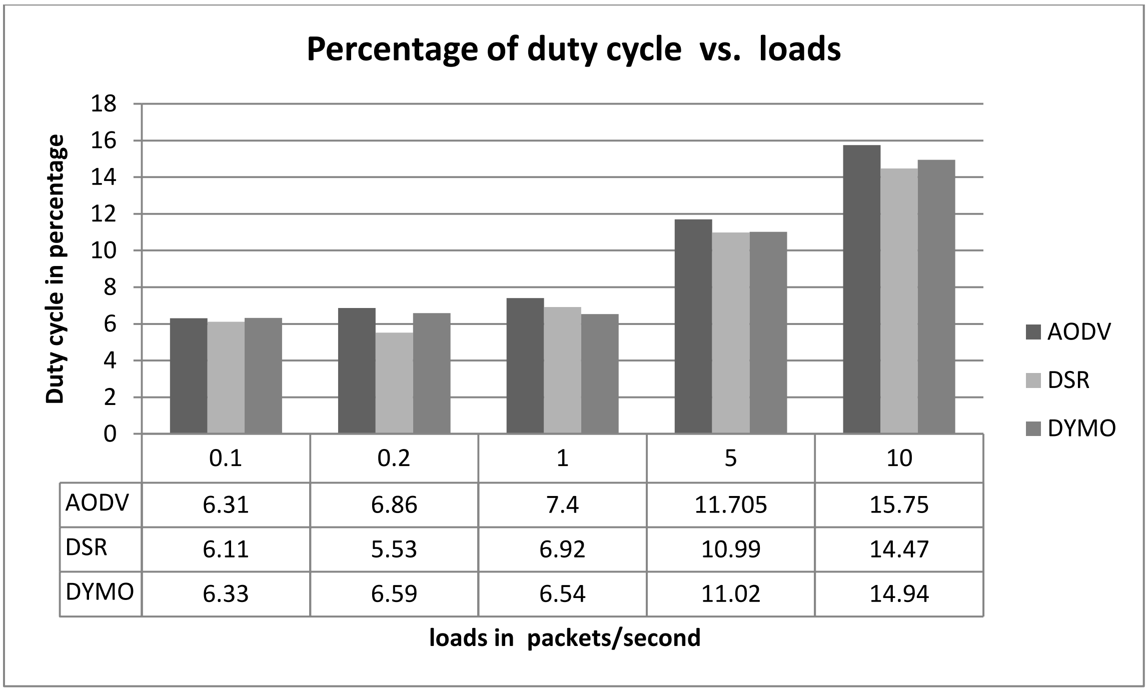
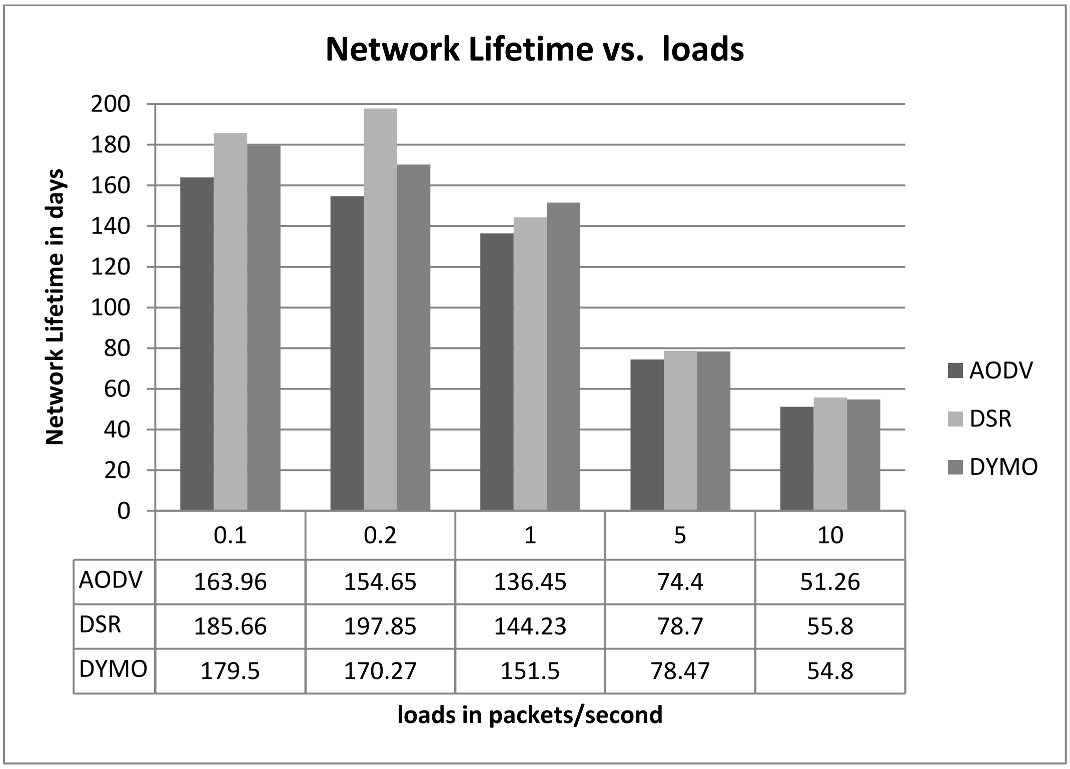


Figure 5.12: Percentage of duty cycle verses loads (packets/second)

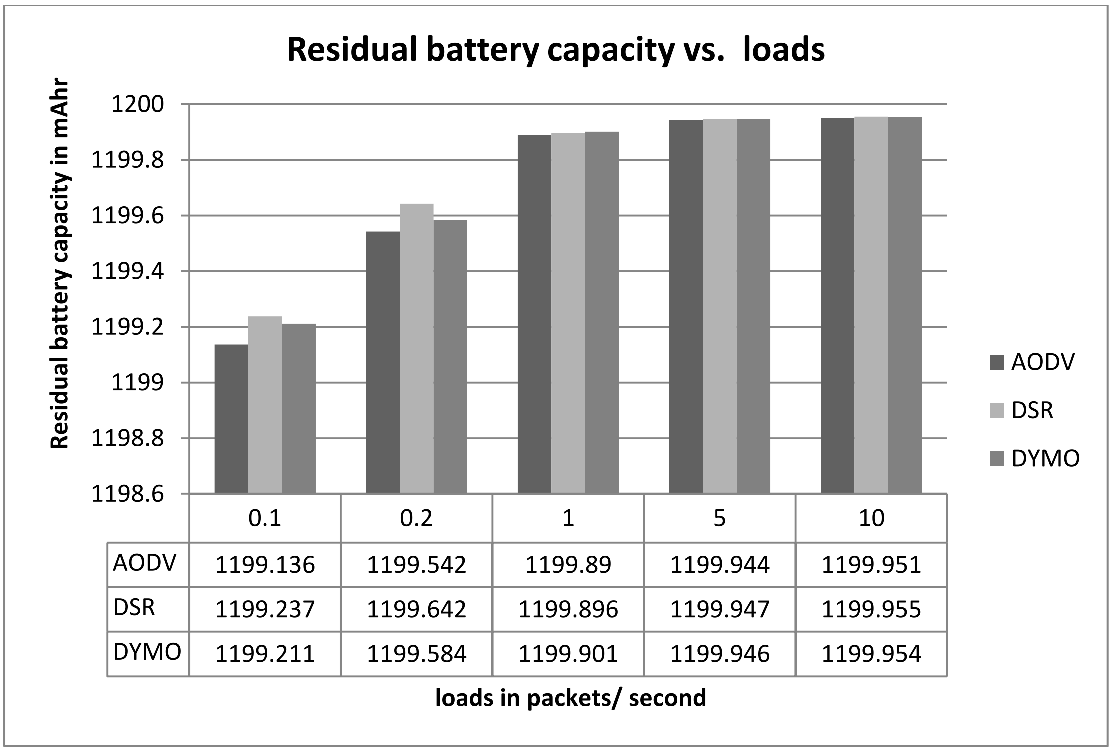
However, in dense networks, this mode results into excessive collision rates. It is due to energy efficient IEEE 802.15.4 MAC which minimizes low duty cycle on RFD to send data packets.

It clearly shows that DSR performs better than other two routing protocols. The lower duty cycle of DSR as shown in Figure 5.12 indicates that nodes in DSR remain in sleep mode for longer period.



	0.1	0.2	1	5	10
AODV	163.96	154.65	136.45	74.4	51.26
DSR	185.66	197.85	144.23	78.7	55.8
DYMO	179.5	170.27	151.5	78.47	54.8

Figure 5.13: Network lifetime vs. loads (packets/second)



	0.1	0.2	1	5	10
AODV	1199.136	1199.542	1199.89	1199.944	1199.951
DSR	1199.237	1199.642	1199.896	1199.947	1199.955
DYMO	1199.211	1199.584	1199.901	1199.946	1199.954

Figure 5.14: Residual battery capacity vs. loads (packets/second)

Network Lifetime: The Figure 5.13 describes performance of the network lifetime verses the traffic loads. The network lifetime calculation in our simulation based on residual battery capacity as shown in Figure 5.14 after running it full battery capacity 1200mAHr to the respective simulation time for varying traffic loads. The DSR routing protocol has higher lifetime in comparison to ADOV and DYMO. This is due to low control packet overhead and higher percentage of time nodes are in sleep mode. DSR also minimizes the overall network bandwidth as it does not use periodic routing messages. By doing so, DSR also tries to conserve battery power as well as avoidance of routing updates that are large enough.

5.9 Performance analysis of QoS for peer to peer Topology

5.9.1 Simulations Set up

In this section, performance evaluation of different popular reactive wireless mobile ad hoc routing protocols like AODV, DSR and DYMO on static IEEE 802.15.4 mesh topology has been done for varying traffic loads. The simulations have been performed using QualNet version 4.5, a scalable wireless networks simulator. In the mesh topology simulation model, 200 FFD devices are uniformly deployed in an area of 1000x100m^2. One of them is a PAN, static mains powered device placed at the centre of the simulation area. The simulation parameters are listed in Table 5.2. In our simulation model, function for acknowledging the receipt of packets is disabled. It is due to the fact that RTS/CTS overhead mechanism is too expensive for low data a rate WSN application for which 802.15.4 is designed. The CBR traffic with the following average packet rates: 0.1 packet per second (pps), 0.2 pps, 1 pps, 5 pps and 10 pps are used. There are 20 CBR applications between FFD nodes which are separated by an average of 8 hops away from each other to establish peer to peer communication as shown in Figure 5.15.

To evaluate performance of different reactive MANET routing on IEEE 802.15.4 mesh topology, we have used the following performance metrics.

Packet delivery ratio: It is the ratio of the number of data packets successfully delivered to the destination nodes to the total number of data packets sent by source nodes.

Average End-to-End delay: It indicates the length of time taken for a packet to travel from the CBR (Constant Bit Rate) source to the destination. It represents the average data delay an application or a user experiences when transmitting data.

Throughput: It is the number of bits passed through a network in one second. It is the measurement of how fast data can pass through an entity (such as a point or a network).

Energy Consumption: This is amount of energy consumed by MICAZ Mote devices for the periods of transmitting, receiving, idle and sleep. The unit of energy consumption used in the simulations is mJoule.

Energy per goodput bit: It is the ratio of total energy consumed to total bits received. It is used as a figure of merit to compare the performance of various network methods based on battery powered devices.

Network Lifetime: This is defined as the minimum time at which maximum number of sensor nodes will be dead or shut down during a long run of simulations

TABLE 5.2: IEEE 802.15.4 Mesh topology simulation parameters

Parameter	value
No. of Nodes and Area	200 and 100m*100m
Channel frequency and data rate	2.4GHz and 250kbps
Transmission range	10meter
TX-Power	0dBm
Antenna height	0.05meter
Path Loss Model	Two Ray Model
Phy and MAC Model	IEEE 802.15.4
Energy Model	MICAZ Mote
Battery Model	Simple Linear,1200 mAhr ,
Traffic	CBR
No. of items and Payload Size	1000 and 50 bytes
BO and SO	15
Simulation time	170Minute,85M,18M,5M and 3M

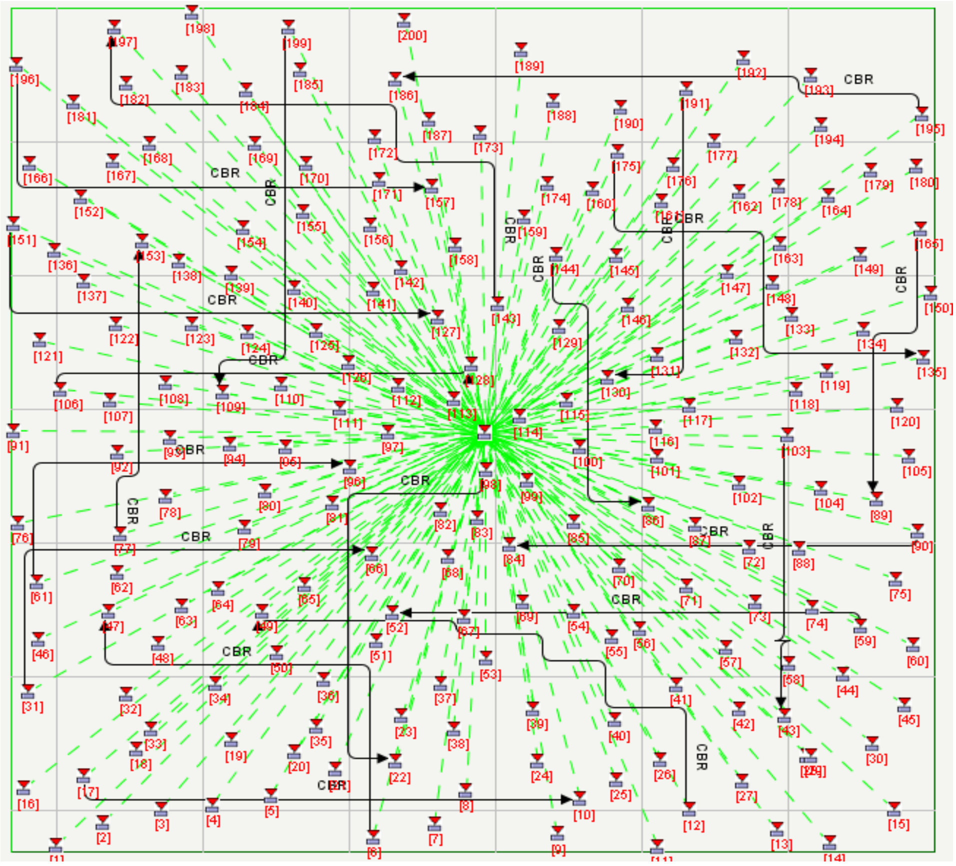


Figure 5.15: Simulation setup for Mesh topology

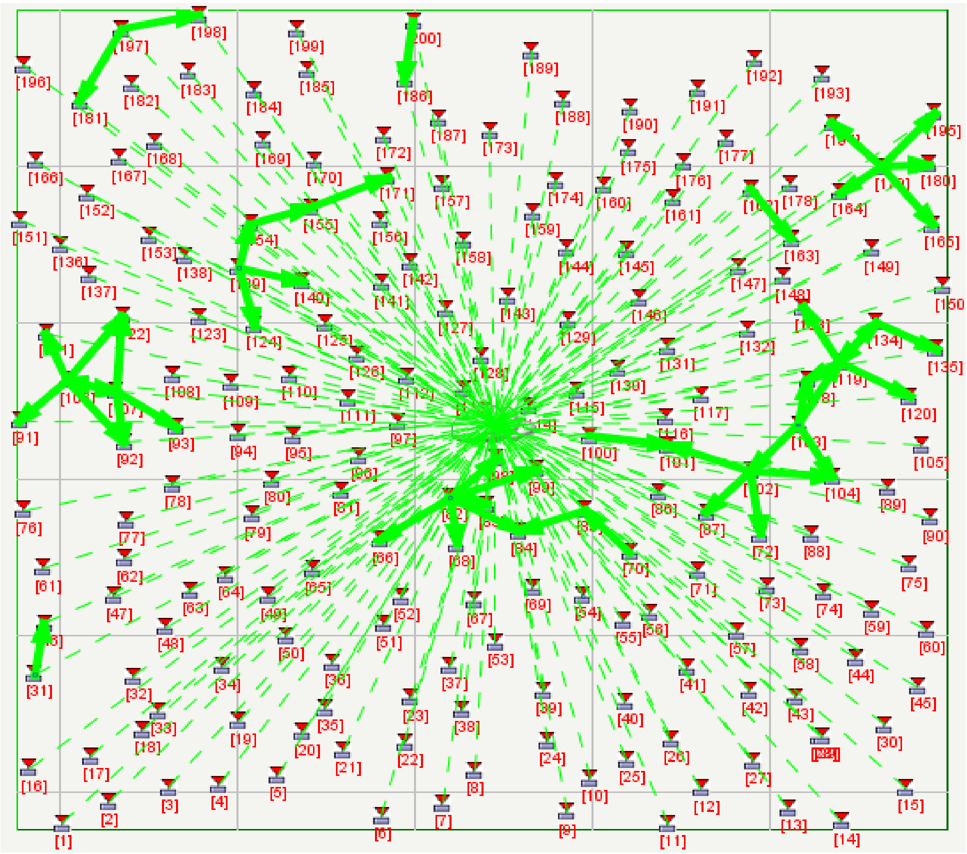
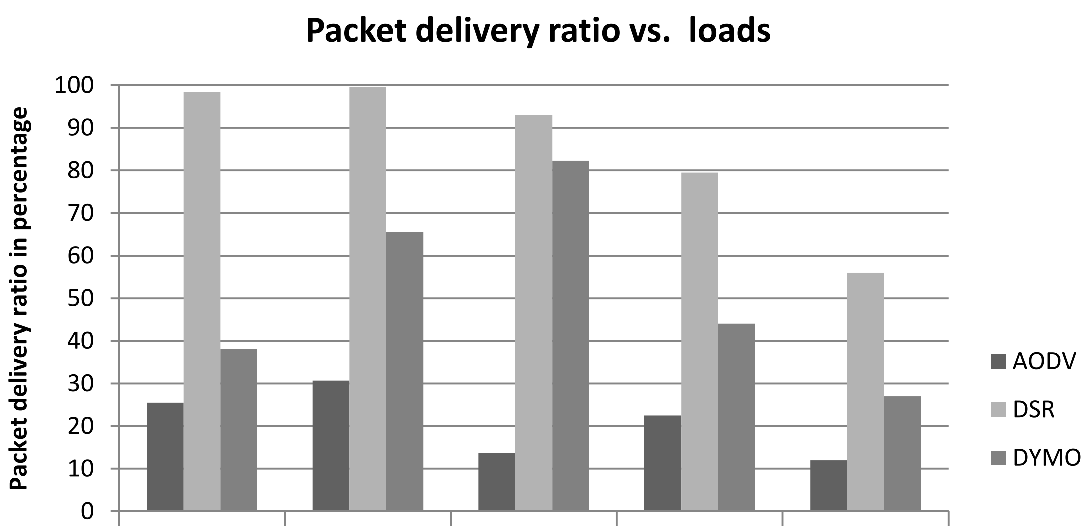


Figure 5.16: QualNet animator during Mesh topology simulation execution

5.9.2 Simulation results and discussion

In this section, the simulation results of various performance metrics for on demand routing protocols like ADOV, DSR and DYMO routing protocols on IEEE 802.15.4 mesh topology using varying traffic load is presented.

Packet delivery ratio (PDR): Figure 5.17 shows performance of the packet delivery ratio vs. loads for different types of applications. For all types of traffic load, DSR performs better than AODV and DYMO. DSR attained a PDR of 99.5 % at low traffic load of 0.2 i.e. when the inter arrival of packet is 5 seconds. Then it decreases to 56% at a higher traffic load of 10 packets per second. The packet delivery ratio drops at high traffic due to well-known hidden terminal problem in multihop environments. DSR also performs well due to its beaconless mechanism. It does not require transmission of hello packets to neighbour nodes as in AODV protocol. DSR source routing based on aggressive caching approach is also effective in better performance of PDR; but when it encounters a large number hops for data delivery between source and destination, PDR performance degrades severely. This is because when the payloads size goes beyond standard IEEE 802.15.4 *MaxMACFrameSize* which is equal to 102 bytes, then it simply drops the packet.



	0.1	0.2	1	5	10
AODV	25.5	30.7	13.7	22.47	12
DSR	98.4	99.65	93	79.5	56
DYMO	38	65.595	82.3	44.03	27

loads in packets/second

Figure 5.17: Packet delivery ratio vs. loads (packets/second)

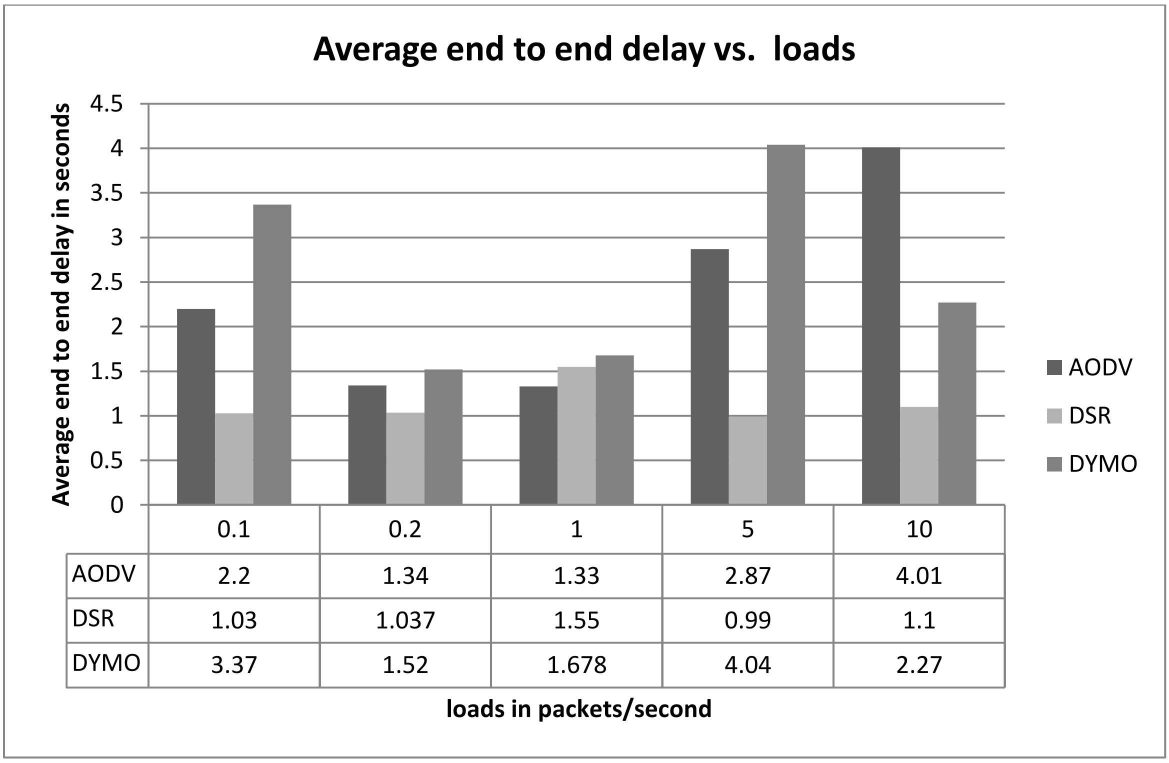
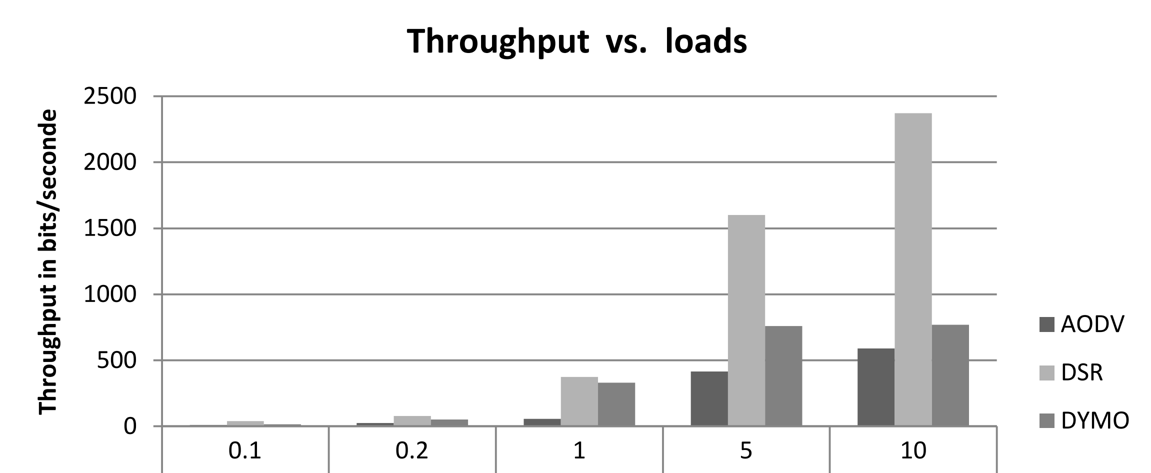


Figure 5.18: Average end to end delay vs. loads (packets/second)

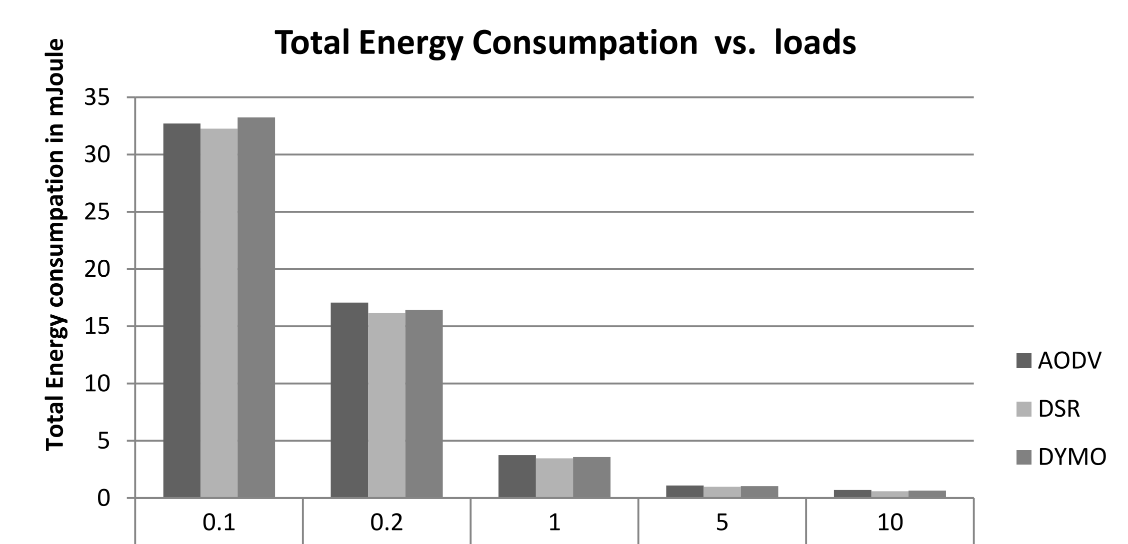
Average end-to- end delay: Figure 5.18 shows performance of the average end-to- end delay vs. varying traffic loads. The average end- to- end delay of a packet depends on route discovery latency, besides delays at each hop (comprising of queuing, channel access and transmission delays), and the number of hops. At low loads, queuing and channel access delays does not contribute much to the overall delay. The overall average end-to-end delay performance of the DSR is lower than DYMO and AODV. The average end to end delay is lower at traffic of 1 packet per second for all three routing protocols considered. DSR has a significantly low delay due to its source routing, which helps to know the complete path to the destination node for data transferring rather than AODV approach.

Throughput: Figure 5.19 shows performance of the throughput in kbps vs. traffic loads in packets per second. From the graph, it is observed that maximum throughput of 2.3kbps is achieved at a rate of 10 packets per second. DSR shows higher throughput in comparison to AODV and DYMO. Throughput to be maximum, when the average end to end delay is low which can be seen in Figure 5.18.



	0.1	0.2	1	5	10
AODV	10	24.37	56.46	416	590
DSR	39	79.33	374.33	1600	2372
DYMO	14.5	51.75	330	758.75	770

Figure 5.19: Throughput vs. loads (packets/second)



	0.1	0.2	1	5	10
AODV	32.7	17.069	3.746	1.1	0.703
DSR	32.271	16.16	3.462	1	0.588
DYMO	33.25	16.44	3.6	1.05	0.662

Figure 5.20: Total energy consumption vs. loads (packets/second)

Total energy consumption: The total energy consumption vs. load for three routing is shown in Figure 5.20. The total energy consumption is the energy consumption in transmission, reception, idle and sleep. The total energy consumption of three routing protocols decreases gradually from lower traffic loads to higher traffic loads.

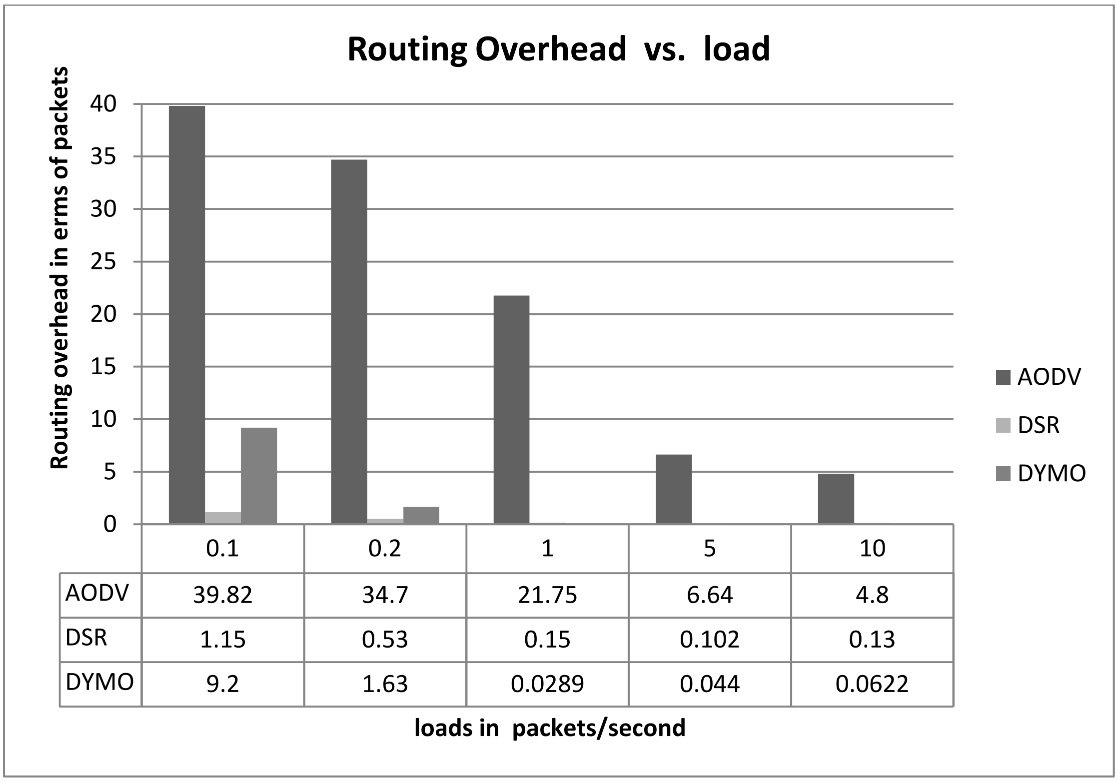
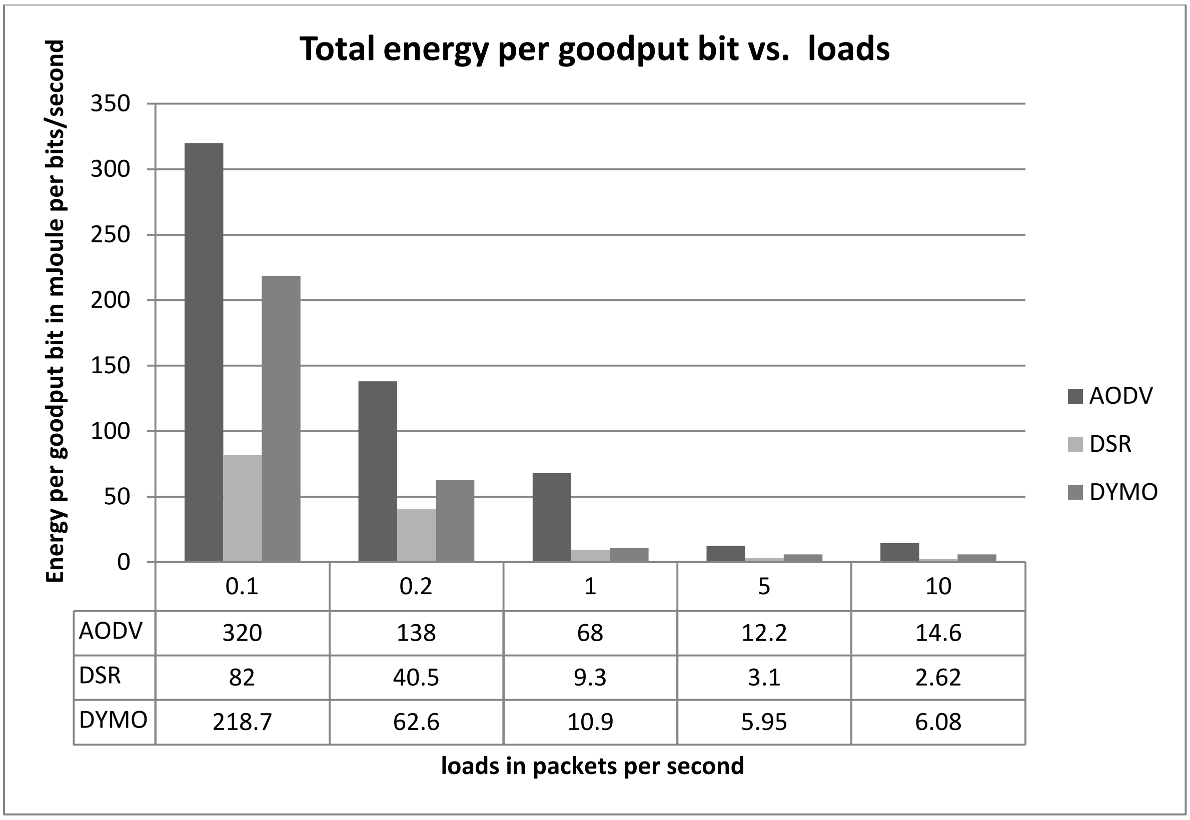


Figure 5.21: Routing overhead vs. loads (packets/second)

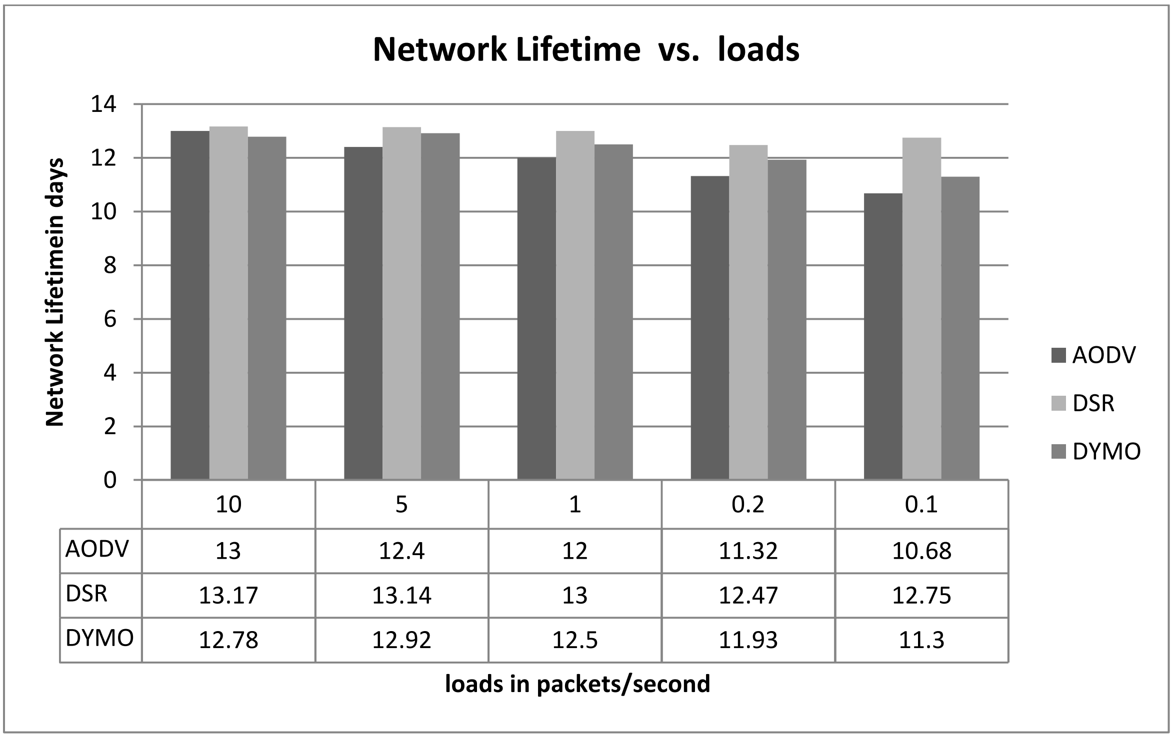
The total energy consumption in three routing protocols is almost same. However, DSR and DYMO perform better than AODV at all specified traffic loads due to its low routing overhead as shown in Figure 5.21. This is due to the fact that a routing protocol with more routing overhead would consume more energy than the routing protocol with less routing overhead.

Energy per goodput bit: Figure 5.22 shows performance of energy per goodput bit vs. traffic loads. The energy per goodput bit is the metric to measure the amount of energy consumed per one bit of payload data. The result has been obtained by the taking the ratio of total energy consumed in transmission of data to the total bits delivered to the receiver. DSR routing protocol shows least energy per goodput bit in comparison to AODV and DYMO routing protocol. It is due to the protocol low energy consumptions and high number of packets received at the destination in DSR. The energy per goodput bit value decreases when traffic loads is low to high .The best value of energy per goodput bit is obtained when the load is 5 packets per second for all the three routing protocols.



	0.1	0.2	1	5	10
AODV	320	138	68	12.2	14.6
DSR	82	40.5	9.3	3.1	2.62
DYMO	218.7	62.6	10.9	5.95	6.08

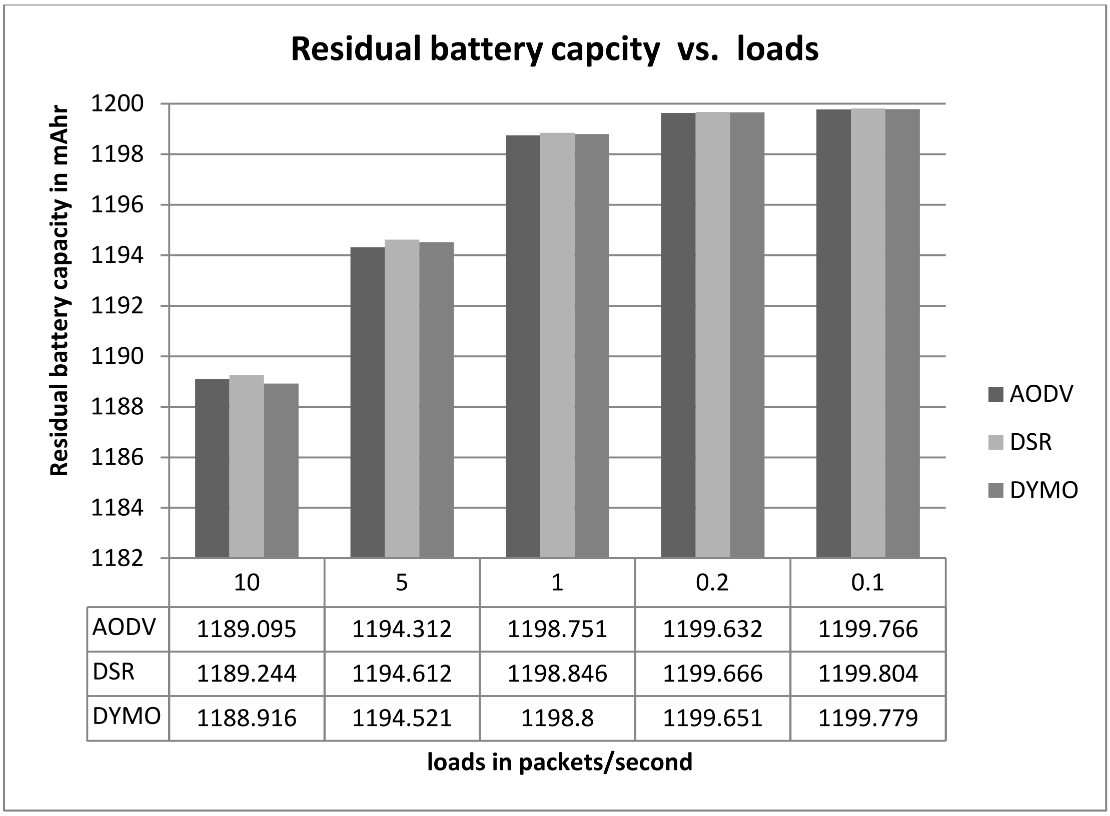
Figure 5.22: Energy per goodput bit vs. loads (packets/second)



	10	5	1	0.2	0.1
AODV	13	12.4	12	11.32	10.68
DSR	13.17	13.14	13	12.47	12.75
DYMO	12.78	12.92	12.5	11.93	11.3

Figure 5.23: Network lifetime vs. loads (packets/second)

Network Lifetime: The Figure 5.23 shows performance of network lifetime vs. traffic loads. Network lifetime calculation in our simulation based on residual battery capacity as shown



	10	5	1	0.2	0.1
AODV	1189.095	1194.312	1198.751	1199.632	1199.766
DSR	1189.244	1194.612	1198.846	1199.666	1199.804
DYMO	1188.916	1194.521	1198.8	1199.651	1199.779

Figure 5.24: Residual battery capacity vs. loads (packets/second)

in Figure 5.24 after running it full battery capacity 1200mAHr to the respective simulation time for varying traffic loads. For the mesh topology considered, all nodes are FFD so as to relay data to the nearest radio range devices. They are always on active router device and never goes to sleep mode. Therefore, the network lifetime is lesser in comparison to RFD in star topology. The network lifetime can be increased if end users are assigned as RFD. The DSR routing protocol has maximum lifetime in comparison to ADOV and DYMO. This is due to fact of lower control overhead of DSR. DSR does not use periodic routing messages and conserve the battery power by not sending or receiving any advertisement.

5.10 Conclusion: The Wireless Sensor Networks Quality of service is significantly different from traditional wired and wireless networks. This chapter discussed the challenges for quality of service support and parameters for defining QoS in WSNs. It also discussed support and design choices of different layers like application layer, network layer, transport layer, data link layer and physical layer. To support QoS, cooperation between layers is essential. Otherwise, each layer may try to maximize different QoS metrics, which will have unpredictable and possibly undesirable results. The QoS is more challenging in heterogeneous wireless sensors networks where a diverse mixture of sensors for monitoring temperature, pressure, and humidity are deployed to monitor the phenomena, thereby introducing different reading rates at these sensors.

This section evaluated the performance analysis of Quality of Service parameters of WSN based on IEEE 802.15.4 star (beacon enabled) mode and mesh topology (non-beacon enabled mode) topology respectively. Simulations have been performed using reactive MANET routing like AODV, DSR and DYMO in QualNet 4.5 for varying loads**.** From the simulation results, it can be concluded that on an average DSR performs better than DYMO and AODV for different rates of traffic loads. The simulations are performed for 200 nodes and 20 application per sessions. For mesh topology, maximum of 10 hops were considered because DSR and AODV performance is not better in comparison to DYMO when it encounters a large number of hops. If the payload size goes beyond standard IEEE 802.15.4 *MaxMACFrameSize* which is equal to 102 bytes, then it simply drop the packet. So, the overall performance of the three protocols on IEEE 802.15.4 for standardizing for WSNs is not promising. The major reason behind the performance degradation is all these protocols are designed mainly for mobile ad-hoc network where topology changes frequently. To meet these challenges of performance degradations, new routing protocols should be designed for IEEE 802.15.4 networks keeping in view of above routing protocols key features.

Chapter 6

Conclusion

6.1 Introduction

The research carried out for this thesis, investigates energy efficient clustering algorithms related to WSNs. A bio-inspired clustering algorithm based on BFO has been proposed. This increases Network life of WSNs. Secondly, quality of service for IEEE 802.15.4 networks has been investigated for star and mesh topology using MANET routing. These chapter summaries the work reported in this thesis, specifying the limitations of the study and provides some suggestions to future work.

Following this introduction, section 6.2 lists the achievements of the research work. Section 6.3 provides the limitations in the study and section 6.4 presents some of the future research area that can be extended to this thesis.

6.2 Contribution of Thesis

The first chapter of the thesis introduced to Wireless Sensor Networks, literature survey and its applications. It also provides a brief overview of the thesis. The second chapter discussed routing algorithms in Wireless Sensor Networks. It presented energy efficient clustering routing algorithms related to Wireless Sensor Networks. The IEEE 802.15.4 standard, ZigBee and its applications were presented in chapter 3.It mainly discussed physical and medium access control (MAC) protocol of IEEE 802.15.4.The chapter 4 described a Bio-inspired clustering algorithm called **Bacteria Foraging Optimization (BFO)** for minimization of total energy consumption and increasing Network Lifetime of Wireless Sensor Networks . Chapter-5 presented a performance evaluation of Quality of Service for IEEE 802.15.4 in star and mesh using on demand MANET routing protocols like AODV, DSR and DYMO. The results of simulation studies have been presented.

The first contribution of the thesis related to use of Bacteria foraging algorithm firstly for WSNs for enhancing network lifetime of sensor nodes. To validate the algorithm, simulations had been carried out using MATLAB. Simulation results showed better performance of BFO as compared to other clustering protocols like LEACH, K-Means and direct method in terms of performance metrics like number of alive nodes and total energy dissipation in the system.

BFO provides better lifetime for nodes compared to other three methods. It is also seen that BFO is able to provide 100% live nodes for maximum duration. LEACH provides a considerably higher lifetime compared to K-Means clustering. In addition to reducing energy dissipation, LEACH successfully distributes energy-usage among the nodes in the network such that the nodes die randomly and at essentially the same rate.

The second contribution related to Quality of Service (QoS) performance analysis for IEEE 802.15.4 networks based on star and mesh topology. The performance has been evaluated using simulations for MANET reactive routing protocols like AODV, DSR and DYMO in QualNet 4.5 software. Performance evaluations metrics like packet delivery ratio (PDR), throughput, average end to end delay, energy per goodput bit, network lifetime of battery model and total energy consumption which includes transmission, reception, idle, sleep mode etc. were considered. From the simulation studies and analysis, it can be seen that on an average DSR and DYMO performs better than AODV for different traffic load rates. Hence, it suits most of application of WSNs which require constant monitoring and sending sensed data packets to a sink at regular intervals of time.

6.3 Limitation of work

This section presents some of the limitations of the work reported in this thesis. In this thesis, cluster head count of 5% of total nodes has been assumed. This has been done considering available literature [**55**]. Performance of the network for higher or lower head count has not been investigated. We have used only BFO for head selection procedure. Presently, BFO consumes higher computational power due to its complexity. Addressing the computational complexity for BFO still remains a challenge.

The second limitation is that the performances have been compared with standard LEACH algorithm. Performance of other sensor network head selection like PEGASIS, HEED, TEEN etc. have not been considered. The clustering algorithms were simulated in MATLAB [**97**]; but to get a realistic network performance, it can be simulated in QualNet, NS2 [**98**], OPNET [**99**], EXata [**100**] as well as TinyOS [**11**] through MICA motes [**7**].

Thirdly, MANET has been designed for highly mobile ad hoc network. Wireless sensor networks nodes can be mix of mobile and stationary nodes depending upon applications. Hence, it is suitable for fixed wireless network can also be analyzed. For QoS study, QualNet simulation has been used. The limitations associated with the software are inherent to the study like hardware resources RAM and CPU to get a realistic simulation of higher number of nodes. The protocols that have analyzed to the investigation were AODV, DSR and DYMO. This has been done due to absence of any standard for 802.15.4.

6.4 Future directions

To conclude the thesis, the following are some suggestions for the future work which can be done. In this thesis, bio-inspired clustering algorithm Bacteria Foraging has been used. Other bio-inspired algorithms like Ant colony optimization, artificial Immune system, Genetic algorithm (significant time and power consuming) can also be compared to BFO; but the challenge of reducing computational complexity still remains. Comparable study of computational complexity of different algorithm need to be analysed.

Secondly, security as a QoS parameter has not been evaluated in this thesis. So, new security based routing protocols for IEEE 802.1 5.4 networks and its validation can be a field of study.

Recently, 6LoWPAN standard turns IEEE 802.15.4 networks into the next IP-enabled networks. Low power device can communicate directly with IP devices using IPv6 based protocols. So, future work can be done by developing a 6LoWPAN standard in QualNet and its performance study for next generation networks like body sensor networks (BSN),battle field surveillance system etc.

Bibliography

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *Communications Magazine,IEEE*, vol. 40, pp. 102-114, 2002.

[2] I.F.Akyildiz, W.Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks,Elsevier*, vol. 38, pp. 393-422, 2002.

[3] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, "Wireless sensor network survey," *Computer Networks,Elsevier,* vol. 52, pp. 2292-2330, 2008.

[4] K. Martinez,J.K. Hart, and R. Ong, "Environmental Sensor Networks," *Computer Magazine,IEEE*, vol. 37, no. 8, pp. 50-56, 2004.

[5] D. Culler, D. Estrin, M.Srivastava, "Overview of Sensor Networks," *Computer Magazine,IEEE*, vol. 37, no. 8, pp. 41-49, August 2004.

[6] J. L.Hill, "System architecture for wireless sensor networks," University of California, Berkeley, Ph.D. dissertation 2003.

[7] http://www.xbow.com.

[8] IEEE Standard 802.15.4, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)," 2006.

[9] Brian Otis, Jan Rabaey, *Ultra-Low Power Wireless Technologies for Sensor Networks*.: Springer, 2007.

[10] G. Simon, M. Maroti, "Sensor network-based counter sniper system," in *Proceedings of the 2nd international conference on Embedded networked sensor systems,* Baltimore, MD, 2004, pp. 1-12.

[11] http://www.tinyos.net/TinyOS.

[12] G. Tolle, D. Culler, W. Hong, et al., "A macroscope in the redwoods," in *Proceedings of the 3rd international conference on Embedded networked sensor systems*, San Diego, CA, 2005, pp. 51-63.

[13] I. Vasilescu, K. Kotay, D. Rus, M. Dunbabin, P. Corke, "Data collection, storage, retrieval with an underwater sensor network," in *Proceedings of the Third International Conference on Embedded Networked Sensor Systems (Sensys),* San Diego, CA, 2005.

[14] P. Zhang, C.M. Sadler, S.A. Lyon, M. Martonosi, "Hardware design experiences in ZebraNet," in *Proceedings of the SenSys'04*, Baltimore, MD, 2004.

[15] Welsh, K. Lorincz and M., "Motetrack: A robust, decentralized approach to RF-based location tracking," *Personal and Ubiquitous Computing,Springer*, vol. 11, pp. 489-503, 2007.

[16] http://www.zigbee.org.

[17] D.J. Baker, A. Ephremides, "The architectural organization of a mobile radio network via a distributed algorithm," *Transactions on Communications,IEEE*, vol. 29, no. 11, pp. 1694-1701, 1981.

[18] C.R. Lin, M. Gerla, "Adaptive clustering for mobile wireless networks," *Journal on Selected Areas Communications,IEEE*, vol. 15, no. 7, pp. 1265-1275, 1997.

[19] K. Xu, M. Gerla, "A heterogeneous routing protocol based on a new stable clustering scheme," in *Proceeding of IEEE Military Communications Conference*, vol. 2, Anaheim,CA, 2002, pp. 838-843.

[20] C. C. Chiang and M.Gerla, "Routing and Multicast in Multihop Mobile Wireless Networks," in *Proceedings of 6th International Conference on Universal Personal Communications*, vol. 2, 1997, pp. 546-551.

[21] L. Jiang, J. Y. Li, and Y. C. Tay, Cluster Based Routing Protocol, 2004, draft-ietf-manet-dsr-10.txt,work-in-progress.

[22] M. Chatterjee, S. K. Das and D. Turgut, "WCA: A Weighted Clustering Algorithm for Mobile Ad Hoc Networks," *Cluster computing,Springer Netherlands*, vol. 5, pp. 193-204, April 2002.

[23] J. Y. Yu and P. H. J. Chong, "A survey of clustering schemes for mobile ad hoc networks," *Communication Surveys and Tutorials,IEEE*, vol. 7, no. 1, pp. 32-48, 2005.

[24] B. Atakan, O.B. Akan, and Tuna Tugcu, "Bio-inspired Communications in Wireless," in *Guide to Wireless Sensor Networks*.: Springer-Verlag London Limited, 2009, ch. 26, pp. 659-687.

[25] M. Gunes, U. Sorges, I. Bouazizi, "ARA – the ant-colony based routing algorithm for MANETs," in *Proceedings of IEEE ICPPW,IEEE Computer Society*, Los Alamitos, CA,USA, 2002, pp. 79-85.

[26] G.A. Di Caro, M. Dorigo, "AntNet: distributed stigmergetic control for

communications networks," *Artificial Intelligence*, vol. 9, pp. 317-365, 1998.

[27] G. Di Caro, F. Ducatelle, L.M. Gambardella, "AntHocNet: an ant-based hybrid routing algorithm for mobile ad hoc networks," *Parallel Problem Solving from Nature - PPSN VIII,Springer*, pp. 461-470, 2004.

[28] R. Muraleedharan, L.A Osadciw, "Balancing the performance of a sensor network using an ant system," in *Annual Conference on Information Sciences and Systems*, Baltimore, MD, USA, 2003.

[29] Y.W Hong, A. Scaglione, "A scalable synchronization protocol for large scale sensor networks and its applications," *Selected Areas in Communications,IEEE*, vol. 23, pp. 1085-1099, 2005.

[30] G.W Allen, G.Tewari, A. Patel, M. Welsh, R. Nagpal, "FireflyInspired Sensor Network Synchronicity with Realistic Radio Effects," *Proceedings of the 3rd international conference on Embedded networked sensor systems,SenSys'05*, pp. 142-153, 2005.

[31] I. Carreras, I. Chlamtac, H. Woesner, C. Kiraly, "BIONETS: Bio-inspired next generation networks," *Lecture Notes in Computer Science,Springer*, vol. 3457, pp. 245-252, 2005.

[32] F. Dressler, B. Kruger, G. Fuchs, and R. German, "Self-Organization in Sensor Networks using Bio-Inspired Mechanisms," in *18th International Conference on Architecture of Computing Systems,Springer*, Innsbruck, Austria, March 2005, pp. 139-144.

[33] I. Wokoma, L.L. Shum, et al., "A biologically inspired clustering algorithm dependent on spatial data in sensor networks," in *Proceedings of the Second European Workshop on Wireless Sensor Networks*, 2005, pp. 386-390.

[34] S. Chen, "Routing Support for Providing Guaranteed End-to-End Quality-of-Service," University of Illionois , Urbana-Champaign, Ph.D. thesis 1999.

[35] S. Chakrabarti and A. Mishra, "QoS Issues in Ad Hoc Wireless Networks," *Communication Magazine*, vol. 39, pp. 142-148, February 2001.

[36] S. Chakrabarti and A. Mishra, "Quality of Service Challenges for Wireless Mobile Ad Hoc Networks," *Wireless Communication and Mobile Computing*, vol. 4, pp. 129-153, March 2004.

[37] J. N. Al-Karaki and A. E.Kamal, "Quality of Service Routing in Mobile Ad Hoc

Networks: Current and Future Trends," in *Mobile Computing Handbook,CRC*., 2004.

[38] T.B Reddy, I. Karthigeyan , B.S Manoj,C.S.R Murthy, "Quality of service provisioning in ad hoc wireless networks: a survey of issues and solutions. Ad Hoc Networks," *Ad Hoc Networks,Elsevier*, vol. 4, pp. 83-124, 2006.

[39] R.Tafazolli l. Hanzo, "A survey of QoS routing solutions for mobile ad hoc networks," *Communications Surveys & Tutorials*, vol. 9, pp. 50-70, 2007.

[40] M. Younis K.Akkaya, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks*, vol. 3, no. 3, pp. 325-349, 2005.

[41] A.A Mohamed, Y. Abbasi, "A survey on clustering algorithms for wireless sensor networks," *Computer communications,Elsevier*, vol. 30, pp. 2826- 2841, october 2007.

[42] W. Heinzelman, J. Kulik, H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks," in *Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking* , Seattle, WA, 1999.

[43] J.H. Chang, L. Tassiulas, "Maximum lifetime routing in wireless sensor networks," in *Proceedings of the Advanced Telecommunications and Information Distribution Research*, College Park, MD, 2000.

[44] Q. Li and J. Aslam and D. Rus, "Hierarchical Power-aware Routing in Sensor Networks," in *Proceedings of the DIMACS Workshop on Pervasive Networking*, 2001.

[45] D. Braginsky, D. Estrin, "Rumor routing algorithm for sensor networks," in *Proceedings of the First Workshop on Sensor Networks and Applications (WSNA)*, Atlanta, 2002.

[46] L. Li, J. Y Halpern, "Minimum energy mobile wireless networks revisited," in *Proceedings of IEEE International Conference on Communications*, vol. 1, Helsinki,Finland, June 2001, pp. 278-283.

[47] J. Heidemann, D. Estrin Y. Xu, "Geography-informed Energy Conservation for Ad-hoc Routing," in *Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking*, Rome, Italy, July,2001, pp. 70-84.

[48] Y. Yu, D. Estrin, and R. Govindan, "Geographical and Energy-Aware Routing: a recursive data dissemination protocol for Wireless Sensor Networks," UCLA Computer Science Department, Technical Report UCLA-CSD TR-01-0023, May 2001.

[49] Abdalkarim Awad, Christoph Sommer, Reinhard German and Falko Dressler, "Virtual Cord Protocol (VCP): A flexible DHT-like routing service for sensor networks," in *5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, 2008, pp. 133-142.

[50] K. Sohrabi, J. Pottie, "Protocols for self-organization of a wireless sensor network," *Personal Communications, IEEE*, vol. 7, pp. 16-27, 2000.

[51] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, 2000, pp. 56-67.

[52] F. Zabin, S.Misra,I. Woungang, H.F. Rashvand, N.W. Ma,M. Ahsan Ali, "REEP: data-centric, energy-efficient and reliable routing protocol for wireless sensor networks," *IET Communications*, vol. 2, no. 8, pp. 995-1008, September 2008.

[53] C. Rahul, J. Rabaey, "Energy Aware Routing for Low Energy Ad Hoc Sensor Networks," in *Wireless Communications and Networking Conference,IEEE*, vol. 1, 2002, pp. 350-355.

[54] W.Heinzelman, A.Chandrakasanand and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, Maui, HI, 2000, pp. 3005-3014.

[55] W.B. Heinzelman, A.P. Chandrakasan, H. Balakrishnan, "Application specific protocol architecture for wireless microsensor networks," *Wireless Communications,IEEE*, vol. 1, pp. 660-670, october 2002.

[56] O.Younis and S. Fahmy, "Distributed Clustering for Scalable, Long-Lived Sensor Networks," *Mobile Computing,IEEE*, vol. 3, no. 4, pp. 366-379, 2004.

[57] Richard Zurawski, *NETWORKED EMBEDDED SYSTEMS*.: CRC Press, 2009.

[58] S. Lindesy and C. Raghavendra, "PEGASIS: Power-Efficient Gathering in Sensor Information System," in *Proceedings of the Aerospace Conference,IEEE*, vol. 3, Big Sky, Montana, 2002, pp. 9-16.

[59] A. Manjeshwar and D. Agrawal, "TEEN: a Routing Protocol for Enhanced Efficient in Wireless Sensor Networks," in *Proceedings of the 15th International Parallel and Distributed Processing Symposium*, San Francisco, April 2001, pp. 2009-2015.

[60] A. Manjeshwar, D.P. Agrawal, "APTEEN: a hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks," in *Proceedings of the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile computing*, Ft. Lauderdale, FL, April 2002.

[61] J. N. Al-Karaki, Raza Ul-Mustafa, Ahmed E. Kamal, "Data Aggregation in Wireless Sensor Networks - Exact and Approximate Algorithms," in *Proceedings of IEEE Workshop on High Performance Switching and Routing (HPSR)*, Phoenix, Arizona, USA, 2004, pp. 241-245.

[62] A.W. Krings Z. (Sam) Ma, "Bio-Inspired Computing and Communication in Wireless Ad Hoc and Sensor Networks," *Ad Hoc Networks,Elsevier*, vol. 7, no. 4, pp. 742-755 , June 2009.

[63] S. Selvakennedy, S. Sinnappan, Yi Shang, "A biologically-inspired clustering protocol for wireless sensor networks," *Computer Communications,Elsevier*, vol. 30, pp. 2786-2801, 2007.

[64] Luo Juan and Song Chen and Zhou Chao, "Ant System Based Anycast Routing in Wireless Sensor Networks," in *International Conference on Wireless Communications, Networking and Mobile Computing*, 2007, pp. 2420-2423.

[65] Reza GhasemAghaei, ASM Mahfujur Rahman, Md. Abdur Rahman, "Ant Colony-Based Many-to-One Sensory Data Routing in Wireless Sensor Networks," in *proceedings of International Conference on Computer Systems,AICCSA 2008. IEEE/ACS*, April 2008, pp. 1005-1010.

[66] Chao Wang and Qiang Lin, "Swarm intelligence optimization based routing algorithm for Wireless Sensor Networks," in *proceedings of International Conference on Neural Networks and Signal Processing*, 2008, pp. 136-141.

[67] G. Montenegro, N. Kushalnagar, J. Hui, and D.Culler, "IPv6 over low-power wireless personal area networks (6LoWPANs):Overview, assumptions, problem statement, and goals," RFC 4919, 2007.

[68] J. W. Hui and D. E. Culler, "IP is dead, long live IP for wireless sensor networks," in *Proceedings of the 6th ACM conference on Embedded network sensor systems,ACM*, 2008, pp. 15-28.

[69] J.W Hui , D.E Culler, "Extending IP to Low-Power, Wireless Personal Area Networks," *Internet computing, IEEE*, vol. 12, pp. 37-45, 2008.

[70] Andrew Wheeler, "Commercial Applications of Wireless Sensor Networks Using Zigbee," *Communication Magazine, IEEE*, vol. 45, pp. 70-77, April 2007.

[71] K. Sohraby, D. Minoli, T. Znati, *WIRELESS SENSOR NETWORKS-Technology, Protocols, and Applications*.: Wiley-interscience, 2007.

[72] J. Zheng and M.J. Lee, "A Comprehensive Performance Study of 802.15.4," in *Sensor Network Operations*.: IEEE Press, 2006, ch. 4, pp. 218-237.

[73] H. Karl, A. Willig, *Protocols and Architectures for Wireless Sensor Networks*. New York: John-Wiley, 2007.

[74] Mauri Kuorilehto, Mikko Kohvakka, *Ultra-Low Energy Wireless Sensor Networks in Practice Theory, Realization and Deployment*. England: John-Wiley, 2007.

[75] www.scalablenetworks.com/QualNet/documentation.

[76] Vijay K. Garg, *Wireless Communications and Networking*. USA: Elsevier, 2008.

[77] Shahin Farahani, *ZigBee Wireless Networks and Transceivers*.: Elsevier, 2008.

[78] Nitaigour P. Mahalik, *Sensor Networks and Configuration Fundamentals, Standards, Platforms, and Applications*.: Springer, 2007.

[79] S. Dagtas, "Multi-stage Real Time Health Monitoring via ZigBee in Smart Homes," in *proceedings of IEEE International Conference on Advanced Information Networking and Applications Workshops (AINAW)*, 2007, pp. 82-86.

[80] http://www.geatbx.com/docu/algindex-01.html.

[81] K. M. Passino, "Biomimicry of bacterial foraging for distributed optimization and control," *Control System Magazine,IEEE*, vol. 22, pp. 52-67, June 2002.

[82] S. Mishra, "A Hybrid Least Square-Fuzzy Bacterial Foraging Strategy for Harmonic Estimation," *IEEE TRANSACTIONS ON EVOLUTIONARY COMPUTATION*, vol. 9, no. 1, pp. 61-73, February 2005.

[83] Babita Majhi and G. Panda and A. Choubey, "On the Development of a New Adaptive Channel Equalizer using Bacterial Foraging Optimization Technique," in *Annual IEEE india conference*, 2006, pp. 1-6.

[84] Mario Marchese, *QoS over heterogeneous networks*.: John &Wiley sons Limited, 2007.

[85] S. Misra, S. C. Misra, I. Woungang, *Guide to Wireless Sensor Networks*.: Springer, 2009.

[86] Dazhi Chen, Pramod K. Varshney, "QoS Support in Wireless Sensor Networks: A

Survey," in *Proceedings of the International Conference on Wireless Networks*, vol. 1, Las Vegas, Nevada, USA, 2004, pp. 227-233.

[87] C.Perkins, E.Belding-Royer and S.Das, "Ad Hoc On-demand Distance Vector Routing (AODV)," IETF RFC 3561, July 2008.

[88] Nader F. Mir, *Computer and Communication Networks*.: Prentice Hall, November 02, 2006.

[89] D.B.Johnson, D.A. Maltz, Y. Hu, and J. G. Jetcheva, "The Dynamic Source routing protocol for Mobile Ad Hoc Networks (DSR)," IETF RFC 4728, February 2007.

[90] I.Chakeres, C.Perkins, "Dynamic MANET On-demand (DYMO) Routing protocols for Mobile Ad Hoc Networks(DYMO)," draft- ietf-manet-dymo-09 November 2007.

[91] G. Lu, B. Krishnamachari, and C. S. Raghavendra, "Performance evaluation of the IEEE 802.15.4 MAC for low-rate low power wireless networks," in *Proceedings of the 23rd IEEE International Performance Computing and Communications Conference*, Phoenix, Ariz, USA, April 2004, pp. 701-706.

[92] J.S. Lee, "Performance evaluation of IEEE 802.15.4 for low-rate wireless personal area networks," *IEEE Transactions on Consumer Electronics*, vol. 52, no. 3, pp. 742- 749, August 2006.

[93] W.T.H Woon, T.C. Wan, "Performance Evaluation of IEEE 802.15.4 Ad Hoc Wireless Sensor Networks: Simulation Approach," in *IEEE International Conference on Systems, Man and Cybernetics*, vol. 2, october 2006, pp. 1443-1448.

[94] C. Buratti and R.Verdone, "A Mathematical Model for Performance Analysis of IEEE 802.15. 4 Non-Beacon Enabled mode," in *European Wireless Conference* , June 2009, pp. 1- 7.

[95] Jose Javier Garcia, Thomas Falck, "Quality of Service for IEEE 802.15.4-based Wireless Body Sensor Networks," in *Proceedings of 3rd International Conference on Pervasive Computing Technologies for Healthcare*, UK,London, April 2009, pp. 1-6.

[96] www.scalable-networls.com/QualNet.

[97] http://www.mathworks.com/.

[98] http://www.isi.edu/nsnam/ns/.

[99] http://www.opnet.com/.

[100] http://www.scalable-networks.com/EXata.

Publication

[1] S.Mohanty and S.K.Patra, "Performance analysis of Quality of Service Parameters for IEEE 802.15.4 Star Topology using MANET routing," in *Proceedings of the 1st ACM International Conference on Wireless and Workshop on Emerging trends in Technology,* Mumbai, India*, 2010, Pages-115-120.*

[2] S.Mohanty and S.K. Patra, "Quality of Service analysis in IEEE 802.15.4 Mesh Topology using MANET routing," *in Proceeding of 2nd IEEE* International Conference on Computing, Communication and Networking Technologies, Karur, India *(ICCCNT'10).*

[3] S.Mohanty and S.K.Patra, "A novel Bio-inspired Clustering algorithm for Wireless Sensor Networks," *accepted in 3rd International Conference on Intelligent and Advanced Systems,* Kuala Lumpur, Malaysia *(ICIAS 2010).*

[4] S.Mohanty and S.K. Patra, "Quality of Service analysis in IEEE 802.15.4 Mesh Topology using MANET routing," *accepted in International Journal of Technology and Engineering System (IJTES),* vol.1, no.2, Jan– June 2010.