WIRELESS SENSOR NETWORKS

"To design an energy efficient routing protocol for military vigilance and security"

Project Report submitted in partial fulfillment of the requirement for the degree of

Bachelor of Technology

in

Electronics and Communication Engineering

Under the Supervision of

Prof. Tapan Kumar Jain

Submitted by:

Archita Chakraborty	081091
Sakshi Mangal	081099
Abhineet Gupta	081128

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY

Jaypee University of Information and Technology

Waknaghat, Solan – 173234, Himachal Pradesh.

CERTIFICATE

This is to certify that project report entitled "To design a routing protocol for military vigilance and security", submitted by Archita Chakraborty (081091), Sakshi Mangal (081099), Abhineet Gupta (081128) in partial fulfillment for the award of degree of Bachelor of Technology in Electronics and Communication Engineering to Jaypee University of Information Technology, Waknaghat, Solan has been carried out under my supervision.

This work has not been submitted partially or fully to any other University or Institute for the award of this or any other degree or diploma.

Date: 01.06.2012

Prof. Tapan Kumar Jain

Department of Electronics and
Communication Engineering.

ACKNOWLEDGEMENT

We wish to express our deep sense of gratitude to our Guide, **Prof. Tapan Kumar Jain** for his able guidance and useful suggestions, which helped us in completing the project work.

Needless to mention the Department Head, **Prof. S.V. Bhooshan** who has been a source of inspiration and for his timely guidance in the conduct of our project work.

Words are inadequate in offering our thanks to our panel members Dr.D.S.Saini, Mrs. Shruti Jain, Ms. Sunita´Sharma for their encouragement and cooperation in carrying out the project work.

Finally, yet importantly, we would like to express our heartfelt thanks to our beloved parents for their blessings, our friends/classmates for their help and wishes for the successful completion of this project.

Chakraborty

(ARCHITA CHAKRABORTY) (ABHINEET GUPTA) (SAKSHI MANGAL)

Jain 01.06.2012

(Tapan Jain)

LIST OF FIGURES

S. No.	Title	Page No.
1.	Figure 1.1: The WSN architecture	2
2.	Figure 2.1: One-hop Model	13
3.	Figure 2.2: Multi-hop Model	14
4.	Figure 2.3: Hierarchical Clustering-based Model	15
5	Figure 3.1: First order radio energy model	21
6.	Figure 5.1: Random deployments of sensor nodes	31
7.	Figure 5.2: Selection of cluster heads	32
8.	Figure 5.3: Joining of cluster heads	32
9.	Figure 5.4: Sensor nodes connecting to their CHs	33
10.	Figure 5.5: Formation of cluster 1	33
11.	Figure 5.6: Formation of cluster 2	34
12.	Figure 5.7: Formation of cluster 3	34
13.	Figure 5.8: Formation of cluster 4	35
14.	Figure 5.9: MATLAB result for CRC coding	37
15.	Figure 5.10: MATLAB result for hamming code	37

LIST OF TABLES

S. No.	Title	Page No.
1.	Table 3.1: Energy considerations in our routing protocol	18
2.	Table 2.1: Routing protocols based on applications	22

ABSTRACT

A wireless sensor network is made of a number of sensor nodes and at least one base station. The most crucial characteristic of sensor nodes is that they are battery-powered and are expected to operate without attendance for a relatively long period of time. In most cases it is very difficult and even impossible to change or recharge batteries for the sensor nodes. Our contribution in this project is designing an energy based routing protocol. The main application of this protocol is military vigilance and security. Energy conservation is the main concern in wireless sensor network protocol design since power resources of sensor nodes are very limited as well as computation, communication capabilities. Dense deployment of high power, low-cost sensor nodes makes wireless sensor network concept good for battle fields. The main security requirements for a military based routing protocol are data confidentiality, and data integrity. Thus, in our project we have emphasized on implementing a routing protocol which is both energy efficient and secured and is best suited for applying in a battlefield.

Table of Content

S. No.	Topic	Page No.
1.	**WIRELESS SENSOR NETWORKS**	1
	1.1. Introduction	1
	1.2. The WSN architecture	2
	1.3. Differences between WSNs and MANETs	3
	1.4. Applications of Wireless Sensor Networks	3
	1.4.1. Military Applications	
	1.4.2. Environmental Applications	
	1.4.3. Health Applications	
	1.4.4. Other Application	
	1.5. Classification of Wireless sensor networks	5
	1.6. Design factors of WSN	6
	1.7. Problem statement	11
	1.8. Thesis Flow	12
2.	**ROUTING PROTOCOLS**	13
	2.1 Sorts of Routing Models	13
	2.1.1One-hop model	
	2.1.2 Multi-hop Planar Model	
	2.1.3 Clustering-based Hierarchical Model	
	2.2 Comparison of the 3 routing models	15
	2.3 Major routing protocols proposed for WSNs	16
	2.3.1 Location based routing	
	2.3.2 Data centric protocols	
	2.3.3 Hierarchical protocols	
	2.4 Application wise usage of different existing routing Protocols	18
	2.5 LEACH-low energy adaptive clustering hierarchy	18

2.5.1 Advantages of leach

2.5.2 Disadvantages of leach

3. **NETWORK DEPLOYMENT** 21

3.1 First order radio energy model 22

3.2 Assumptions 23

3.3 Algorithm for network deployment and energy Computation

4. **SECURITY** 24

4.1 Security requirements 24

4.1.1 Data confidentiality

4.1.2 Data integrity

4.1.3 Data freshness

4.1.4 Self-organization

4.1.5 Time synchronization

4.2 Implementation of data confidentiality 26

4.2.1 Using simple encryption –decryption coding

4.3 Implementation of data integrity 27

4.3.1 Using CRC coding

4.3.2 Using Hamming codes

5. **SIMULATIONS, RESULT & CONCLUSION** 31

5.1 Random deployment of sensor nodes 31

5.2 Formation of clusters within fixed range 33

5.3 CRC coding MATLAB result 36

5.4 Hamming code MATLAB result 36

5.5 Conclusion 37

REFERENCE 38

BIBLIOGRAPHY 40

CHAPTER 1

WIRELESS SENSOR NETWORKS

1.1 Introduction

In 1999 it was called one of "21 ideas for the 21st century" and in 2003 it was heralded as one of "10 emerging technologies that will change the world" [1]. This revolutionary technology is known as Wireless Sensor Networks (WSNs) [2]. Over the past years wireless communication has become of great importance that it is now used in almost every sphere of life.

Wireless sensor networks are coming forth as powerful platforms for distributed embedded computing, encouraging a variety of applications such as disaster/crime prevention and military applications, environmental applications, health applications, etc.

A wireless sensor network is made of a number of sensor nodes and at least one base station. The sensor nodes are small, intelligent, low power, low cost and autonomous devices with sensing, wireless communication and computational capabilities. These sensor nodes communicate over mainly short distances via a wireless medium and join together to accomplish a particular task. Once deployed, the sensor nodes must be able to autonomously organize themselves into a wireless communication and sensing network. The most crucial characteristic of sensor nodes is that they are battery-powered and are expected to operate without attendance for a relatively long period of time. In most cases it is very difficult and even impossible to change or recharge batteries for the sensor nodes.

WSNs are characterized with denser levels of sensor node deployment, higher unreliability of sensor nodes, power consumptions, and memory constraints. Thus, the unparalleled characteristics and constraints present many new challenges for the development and application of WSNs.

Actually the network topology is constantly changing, and it is not a desired solution to replenish it by impregnating new sensors instead the exhausted ones. An appropriate solution for this problem is to implement routing protocols that perform efficiently and utilize less amount of energy as possible for the communication among nodes and to the base station or sink.

1.2 The WSN architecture:

After the initial deployment (ad-hoc or fixed) [2], sensor nodes are responsible for self-organizing an appropriate network base, with multi-hop or single-hop connections between the sensor nodes. The sensors then start collecting acoustic, seismic, infrared or magnetic information about the environment, using either continuous or event driven working modes. Location and positioning information can also be obtained through the global positioning system (GPS) or local positioning algorithms. This information can be gathered from across the network and appropriately processed to construct a global view of the monitoring phenomena or objects. The basic philosophy behind WSNs is that, while the capability of each individual sensor node is limited, the aggregate power of the entire network is sufficient for the required mission.

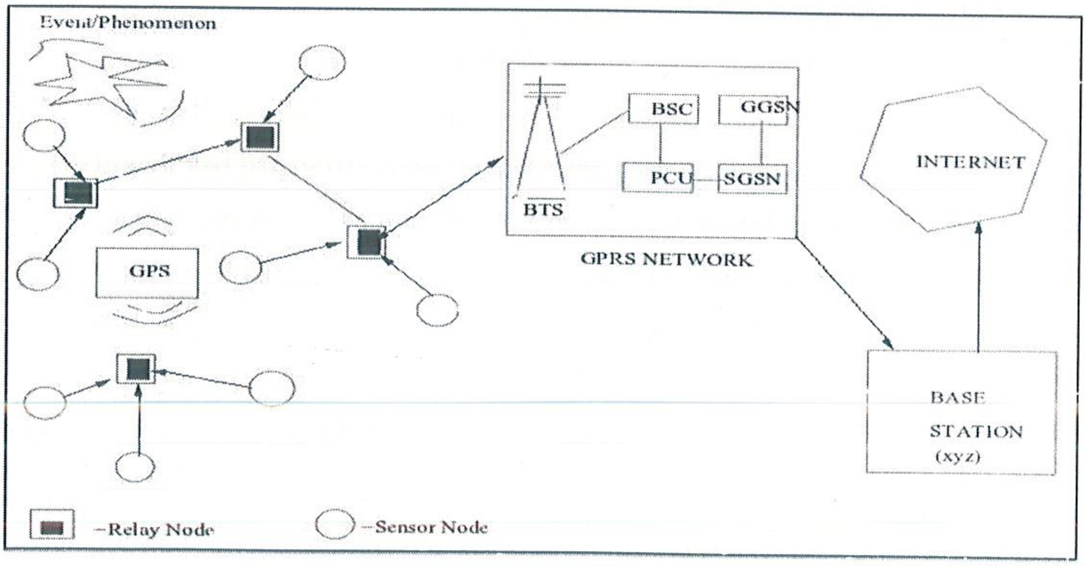


Figure 1.1: The WSN architecture

1.3 Differences between WSNs and MANETs:

An actualization of sensor networks' characteristics, design, and applications require wireless ad hoc networking mechanisms. Among the existing ad hoc networks models, the mobile ad hoc networks (MANETs) are the closest to sensor networks. Although MANETs and Wireless Sensor Networks (WSNs) share some similar characteristics, such as; network topology is ad hoc (i.e., not fixed), power and bandwidth are an expensive resources, wireless communication mediums (i.e., wireless communications links) are used to connect nodes, the protocols and algorithms developed for MANETs are not suitable for the unique features and application requirements of WSNs because these two types of networks have the following differences:

- The number of sensor nodes in WSNs can be several orders of magnitude higher than that in MANETs.
- Unlike a node in MANETs, sensor node may not have a unique global IP address because of the large amount of overhead and the numerous numbers of sensors.
- Sensor nodes are extremely cheaper and more tiny devices, not like ad hoc network nodes (e.g., PDAs, Laptops, etc.), and usually they deployed in thousands.
- The communication paradigm used in WSNs is broadcasting, whereas MANETs are based on point-to-point communications.
- The topology of a WSN changes.
- Energy and bandwidth conservation is the main concern in WSN protocol design since power resources of sensor noses are very limited as well as computation, communication capabilities than their MANETs counterparts because of their low cost.

1.4 Applications of Wireless Sensor Networks:

There are many commercially available sensor types to monitor plenty of conditions including [3]:

- Temperature

- Movement
- Humidity
- Lightning condition
- Pressure
- Noise levels
- Presence or absence of certain kinds of objects
- The current characteristics such as speed, direction and size of an object.

As a result of availability of different kinds of low cost sensors everywhere, there are various applications of WSNs. A general categorization of WSN applications may include military applications, environmental applications, health applications and other commercial applications.

1.4.1 Military Applications:

Dense deployment of high power, low-cost sensor nodes makes WSN concept good for battle fields. Some military applications of WSNs are:

- Supervising friendly forces, equipment and ammunition.
- Battlefield surveillance
- Exploration of opposing forces and land
- Targeting
- Battle damage assessment
- Nuclear, biological and chemical attack detection

1.4.2 Environmental Applications:

Although there are some other techniques to monitor environmental conditions, random distribution and self-organization of WSNs make them suitable for environmental monitoring. Some applications include:

- Bio complexity mapping of environment.
- Detection of natural disasters, such as fire, flood and earthquake detection.
- Precision agriculture

- Habitat monitoring
- Pollution detection
- Planetary exploration

1.4.3 Health Applications:

Tiny sizes and light-weight structure of WSN nodes provides many functionality in health applications, including:

- Tele-monitoring of human physiological data
- Tracking and monitoring doctors and patients
- Drug administration

1.4.4 Other Commercial Applications:

In addition to all of above, there are many commercial applications of WSNs including:

- Home automation for smart home environments
- Interactive museums
- Environmental control in buildings
- Detecting and monitoring burglary/ thieving
- Vehicle tracking and detection

1.5 Classification of Wireless sensor networks:

Classification of sensor networks based on their mode of functioning and the type of application is as follows [4]:

- **Proactive Networks**

  The nodes within this network periodically switch on their sensors and transmitters, sense the environment or event and transmit the data of concern. Hence, they provide a general view of the relevant parameters at regular periods of time. They are well befitted for applications requiring periodic data monitoring.

- **Hybrid Networks**

  The nodes in such a network not only react to time-decisive situations, but also give an overall picture of the network at periodic intervals in a very energy efficient manner. Such a network enables the user to request past, present and future data from the network in the form of historical, one-time and lasting queries respectively.

- **Reactive Networks**

  The nodes of the networks according to this scheme react immediately to sudden and drastic changes in the value of a sensed attribute. They are well suited for time critical applications.

1.6 Design factors of WSN:

A sensor network design is influenced by many factors, which include fault tolerance; scalability; production costs; operating environment; sensor network topology; hardware constraints; transmission media; and power consumption [2]. These factors are important for designing a protocol or an algorithm for sensor networks.

Fault tolerance:

Fault tolerance is the ability to sustain sensor network functionalities without any interruption due to sensor node failures. The fault tolerance level depends on the application of the sensor networks and protocols and algorithms are designed to address the level of fault tolerance required by the sensor networks

Scalability:

Depending on the application, the number of nodes may reach an extreme value of millions. The schemes must be able to work with this number of nodes. They must also utilize the high density nature of the sensor networks which can range from few sensor nodes to few hundred sensor nodes in a region that can be less than 10 m in diameter. In addition, the number of nodes in a region can be used to indicate the node density that depends on the application in which the sensor nodes are deployed

Production costs:

To justify the overall cost of the networks the cost of a single node is very important. If the cost of the network is more expensive than deploying traditional sensors, then the sensor network is not cost-justified therefore the cost of each sensor node has to be kept low. The sensor network may be equipped with a location finding system, mobilizer, or power generator depending on its applications and thus the cost of a sensor node is a very challenging issue

Hardware constraints:

Subunits like location finding system, a power generator and a mobilizer may need to fit into a matchbox-sized module. The required size may be smaller than even a cubic centimeter which is light enough to remain suspended in the air. Apart from the size, there are some other constraints also on sensor node such as:

- consume extremely low power,
- operate in high volumetric densities,
- have low production cost and be dispensable,
- be autonomous and operate unattended,
- be adaptive to the environment

Since the sensor nodes are often inaccessible, the lifetime of a sensor network depends on the lifetime of the power resources of the nodes which is a scarce resource due to the size limitations.

Sensor network topology:

Sheer numbers of inaccessible and unattended sensor nodes, which are prone to frequent failures, make topology maintenance a challenging task. Hundreds to several thousands of nodes are deployed throughout the sensor field. They are deployed within tens of feet of each other Deploying high number of nodes densely requires careful handling of topology maintenance. Sensor nodes can be either thrown in mass or placed one by one in the sensor field. They can be deployed by:

- dropping from a plane,
- delivering in an artillery shell, rocket or missile,
- throwing by a catapult (from a ship board, etc.),
- placing in factory, and
- placing one by one either by a human or a robot.

After deployment, topology changes are due to change in sensor nodes:

- position,
- reach ability (due to jamming, noise, moving obstacles, etc.),
- available energy,
- malfunctioning, and
- task details.

Environment:

Sensor nodes are densely deployed either very close or directly inside the phenomenon to be observed.

Conditions sensor nodes are expected to work are as follows:

- busy intersections,
- interior of a large machinery,
- bottom of an ocean,
- surface of an ocean during a tornado,
- biologically or chemically contaminated field,
- battlefield beyond the enemy lines,
- home or a large building,
- attached to fast moving vehicles, and
- drain or river moving with current.

They work under high pressure in the bottom of an ocean, in harsh environments such as debris or a battlefield, under extreme heat and cold such as in the nozzle of an aircraft engine or in arctic regions, and in an extremely noisy environment such as under intentional jamming.

Transmission media:

In a multi-hop sensor network, communicating nodes are linked by a wireless medium. These links can be formed by radio, infrared or optical media. To enable global operation of these networks, the chosen transmission medium must be available worldwide. One option for radio links is the use of industrial, scientific and medical (ISM) bands, which offer license-free communication in most countries. For sensor networks, a small-sized, low-cost, ultralow power transceiver is required. There are various rules and constraints, like power limitations and harmful interference from existing applications. Much of the current hardware for sensor nodes is based upon RF circuit design. The unusual application requirements of sensor networks make the choice of transmission media more challenging. Inhospitable terrain or battlefield applications might encounter error prone channels and greater interference. Moreover, a sensor antenna might not have the height and radiation power of those in other wireless devices. Hence, the choice of transmission medium must be supported by robust coding and modulation schemes that efficiently model these vastly different channel characteristics.

Power consumption:

The wireless sensor node, being a micro-electronic device, can only be equipped with a limited power source (<0.5 Ah, 1.2 V). In some application scenarios, replenishment of power resources might be impossible and thus sensor node lifetime shows a strong dependence on battery lifetime. The malfunctioning of few nodes can cause significant topological changes as they act as both data originator and data router and might require re-routing of packets and reorganization of the network. Hence, power conservation and power management take on additional importance. Power consumption can hence be divided into three domains:

- **Sensing:** Sensing power varies with the nature of applications. Sporadic sensing might consume lesser power than constant event monitoring. The complexity of event detection also lays a crucial role in determining energy expenditure. Higher ambient noise levels might cause significant corruption and increase detection complexity.

- **Communication:** A sensor node expends maximum energy in data communication which involves both data transmission and reception.

- **Data processing:** Energy expenditure in data processing is much less compared to data communication. Local data processing is crucial in minimizing power consumption in a multi-hop sensor network. A sensor node must therefore have built-in computational abilities and be capable of interacting with its surroundings.

Guarantee of Network Connectivity:

There can be missed or delayed mission critical information due to only a few isolated sensor nodes in the network, and this may result in a wrong decision on the battlefield. Therefore a self-organization algorithm guaranteeing network connectivity is required

Information Flow:

There are 3 types of information flow in WSNs. The first type is one-way communication from sensors to the sink or the gateway. The second type is two-way information flow which can manage sensor nodes by sending control message from the sink to sensor nodes. The last type is multi-way information flow which can be applied to multi-media applications.

Quality of Service (QoS):

Data type can be classified QoS parameters [5] in military WSNs as following:

- **Emergency Data:** This mission critical information should be guaranteed to deliver to the sink with both low delay and high reliability.

- **Monitoring and Tracking Data:** Since sensor nodes cannot distinguish the target whether enemy or others such as animal, military WSNs should monitor and track all targets with guarantee of low delay until the target becomes identified.

- **Periodic Simple Data:** A condition of sensor nodes such as remaining energy could be a simple data type. As this periodic data is not critical to operate the mission, the high reliability is sufficient regardless of real-time delivery.

Security:

Military WSNs, especially distributed in the enemy 's area should consider security factors. Unlike the commercial WSNs, all possible design techniques for LPD, LP1 and Anti-jamming should be considered at each layer of sensor node.

1.7 Problem definition:

1. Sensors must be light weight and compact.
2. Limited Power Supply.
3. Replenishing power is not an option.
4. Important to minimize power consumption of each node to maximize battery life and lifetime of entire network.
5. Energy consumption occurs in three domains: sensing, data processing and communication.
6. Nodes route data destined to the base station through intermediate nodes.
7. Security is also one of the main constraints as the protocol is designed for military application.
8. Our focus is on data link layer as we are dealing with power saving modes of operation and error control codes.

1.8 Thesis Flow:

In the second chapter we have presented what are the types of routing protocols available in a wireless sensor network and their classification and a brief introduction about LEACH protocol.

In the third chapter we have explained the properties and features of the first order radio energy model and its implementation in our algorithm along with the algorithm for our network deployment.

In the fourth chapter we have briefly discussed about the security issues in a wireless sensor network since our aim is to design a routing protocol for military purpose and we have presented algorithms for error correction and encryption and decryption.

In the fifth chapter we have given all the simulations and results performed on MATLAB. And finally, we have drawn our conclusions and also highlighted on the future work that can be done.

Chapter 2
ROUTING PROTOCOLS

The fundamental aim of any routing protocol is to furnish the network useful and efficient. A routing protocol organizes the activities of individual nodes in the network to achieve global goals and do so in a proficient manner. In the following subsection existing routing models are discussed.

2.1 Sorts of Routing Models

All existing routing protocols may be included into one of the following three routing models [4].

2.1.1One-hop model

This is the most elementary approach and corresponds to direct communication as is shown in Figure 2.1. In these networks each and every sensor node transmits directly to the base station. This mode of communication is not only too expensive in terms of energy consumption, but also it is impractical because nodes have restricted or limited transmission range. Therefore direct communication is not a feasible model for routing in WSN.

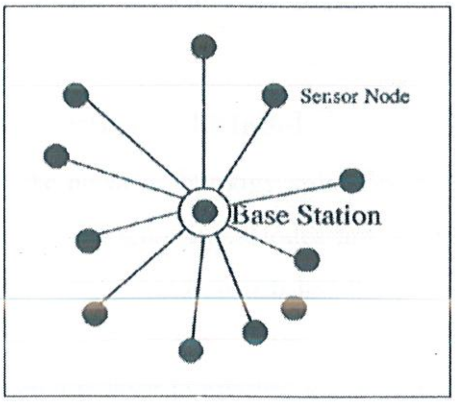


Figure 2.1: One-hop Model.

2.1.2 Multi-hop Planar Model

In this type of model, a node transmits to the base station by forwarding its data to one of its nearest neighbors, which is closer to the base station. The latter then passes on its neighbor that is even closer to the base station as is denoted in Figure 2.2. Thereby the information travels from source to destination through hop by hop from one node to another until it reaches the base station or sink. Considering the energy and the transmission range node restrictions, this multi-hop planar model is a feasible approach. In a network composed by thousands of sensors, this model will exhibit high data dispersion latency due to the long time needed by the node information to arrive to the base station.

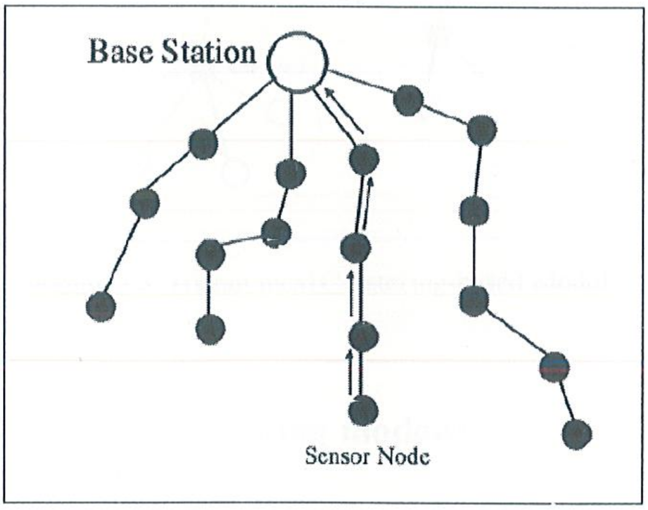


Figure 2.2: Multi-hop Model.

2.1.3 Clustering-based Hierarchical Model

A hierarchical approach for the network topology splits up the network into number of areas called clusters as shown in Figure 2.3. Nodes are grouped depending on some parameter into clusters with a cluster head, which has the province of routing the data from the cluster to other cluster heads or base stations. Data still hops from one node to another, but since it hops from one layer to another it covers larger distances and moves the data faster to the base station than in the previous multi-hop model. The reaction time in this model is theoretically much less than in the multi-hop model. Clustering brings out built-in optimization potentialities at the cluster heads, what results in a more efficient and well integrated network topology. This model is more suitable than the one-hop or multi-hop model.

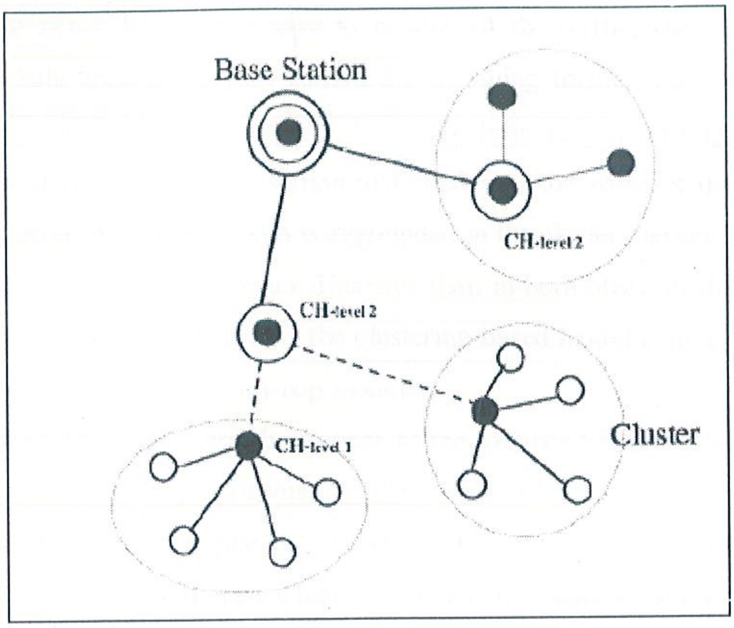


Figure 2.3: Hierarchical Clustering-based Model.

2.2 Comparison of the 3 routing models:

For several reasons direct communication is infeasible for a large sensor network that is formed by thousands of sensors. It is a model that wastes energy and even worse, nodes far from base station do not have enough transmission power to reach the base station what would turn into unreachable the most part of the network. Even though the sensors would be close to the base station, the density of it would create such number of collisions that would seriously degrade the network efficiency. The multi-hop model is a more practical approach than the one-hop. In this case, data is forwarded by hops from one node to another until it reaches the base station. Taking into account the energy constraint nodes that comprise sensor networks, it is a feasible approach. The coverage area is improved over the one-hop model since most nodes are able to connect the network and the amount of collisions is reduced. Some drawbacks of this model are the high latency in networks comprised of thousands of sensors and the serious delay that data experiences. Perhaps the most important drawback is that the closest nodes to the base station would have to act as intermediaries to all traffic being sent to the base station by the rest of the network. As they have to handle all the traffic, they will die first creating a black hole around the base station for incoming traffic. This situation will appear another time with the new closest nodes to the base station causing in the mid-term that no data arrives to the base station and rendering the network useless. In the clustering-based hierarchical model, data is aggregated in the cluster and sent to a higher-level cluster head, thus travelling greater distances than in both other models explained and reducing time and latency. Therefore, the clustering-based model is more suitable for time-critical applications than the multi-hop model.

Nevertheless, this model has one drawback since as the distance between clustering level increases, the spent energy is proportional to the square of the distance [4]. This fact increases energy expenditure. Despite this drawback, this model outperforms by far the one-hop and multi-hop models offering a better approach to routing for sensor networks.

2.3 Major routing protocols proposed for WSNs:

Traditional routing is not applicable to WSNs mainly due to its energy constrained nature. In WSN, the sensor nodes have a limited transmission range, and their processing and storage capabilities as well as their energy resources are also limited.

Categorization of the routing protocols is as follows:

2.3.1 Location based routing:

In location-based protocols [6], sensor nodes are addressed by means of their locations. Location information for sensor nodes is required for sensor networks by most of the routing protocols to calculate the distance between two particular nodes so that energy consumption can be estimated.

Examples of location-aware routing protocols are:

1. Geographic Adaptive Fidelity (GAF)

2. Geographic and Energy-Aware Routing (GEAR)

3. Span
4. Trajectory-Based Forwarding (TBF)
5. Geographic Random Forwarding (GeRaF)
6. Minimum Energy Communication Network (MECN)
7. Small Minimum-Energy Communication Network (SMECN)

2.3.2 Data centric protocols:

In *data-centric* protocols, when the source sensors send their data to the sink, intermediate sensors can perform some form of aggregation on the data originating from multiple source sensors and send the aggregated data toward the sink. This process can result in energy savings because of less transmission required.

Examples of data-centric routing protocols are:

1. Sensor Protocols for Information via Negotiation (SPIN)
2. Cougar
3. Active Query Forwarding in Sensor Networks (ACQUIRE)

2.3.3 Hierarchical protocols:

A hierarchical approach breaks the network into clustered layers [7]. Nodes are grouped into clusters with a cluster head that has the responsibility of routing from the cluster to the other cluster heads. Data travel from a lower clustered layer to a higher one. Although, it hops from one node to another, but as it hops from one layer to another it covers larger distances. This moves the data faster to the base station. Clustering provides inherent optimization capabilities at the cluster heads.

Examples of hierarchical routing protocols are:

1. Low-energy adaptive clustering hierarchy (LEACH)
2. Power-Efficient Gathering in Sensor Information Systems (PEGASIS)

3. Hybrid, Energy-Efficient Distributed Clustering (HEED)

4. Threshold Sensitive Energy Efficient Sensor Network Protocol (TEEN)

5. Adaptive Periodic Threshold Sensitive Energy Efficient Sensor Network Protocol (APTEEN)

2.4 Application wise usage of different existing routing protocols:

Application type	Node deployment	Topology	Routing Protocols
Military	random	Cluster Head	LEACH
Disaster monitoring	manual	Multi-hop/ Multi-path	COUGAR
Health monitoring	Manual one time	Cluster head	LEACH
	Manual	star	SAR
Habitat Monitoring	Manual one time	Cluster head	GAF
Home/office	Manual,	Three	APTEEN

Table 2.1: Routing protocols based on applications

2.5 LEACH-Low energy adaptive clustering hierarchy

LEACH [8] is a self organizing, adaptive clustering protocol that uses randomization to distribute the energy load evenly among the sensors in the network. In LEACH the nodes organize themselves into groups termed as clusters and each cluster have one local base station termed as cluster head. According to conventional clustering algorithms, any node was selected randomly and was made cluster head. In this method there were chances that the cluster head may die quickly which would result in wastage of other nodes which belongs to that cluster. But in LEACH the high energy cluster head position is randomly rotated so that it does not drain energy out of a single sensor. In addition, LEACH performs local data fusion to compress the amount of data being sent from clusters to the base station, further reducing energy dissipation and enhancing system lifetime.

When a sensor node becomes a cluster heads they broadcast their status to other sensors in the network and then the nodes determine to which cluster head they belong to. This criterion for this decision is minimum communication energy. Once all the nodes are organized into clusters, each cluster head creates a schedule for the nodes in its cluster. This minimize the energy dissipation in the individual sensors as the radio components of each non cluster head is turned off at all times except it's transmit time. When cluster heads has received all the data from the nodes of its cluster, then it aggregates the data. It then sends the compressed data to the base station. This is a high energy transmission process as the base station is far away but since there are fewer cluster heads, this only affects a small numbers of nodes.

The system can determine, a priori, the optimal number of clusters to have in the system. This will depend on several parameters, such as network topology and relative costs of computation versus communication.

The main energy savings of the LEACH protocol is due to combining lossy compression with the data routing. There is a probability that some data is lost from individual signal but eventually it results in substantial reduction of the overall energy of the system. In LEACH, the energy usage is distributed among nodes such that the nodes die randomly and at same rate.

2.5.1 Advantages of leach:

In static clustering algorithm as soon as the cluster head dies ,all the nodes in that cluster effectively dies off as they don't have any way to send their data to base station while in

LEACH this is not the case. They give a good first order approximation of the lifetime extension which can be achieved through LEACH.

The position of cluster head is randomly changed. This does not put pressure on any single node.

In LEACH, node dies randomly. With random death, there is no one section of the environment that is not being sensed as nodes die, as in other protocols

The nodes are equal in status and they done need the controlled information from whole network.

The algorithm is simple and easy to implement.

Hierarchy, path selection and storage of information is simple. Nodes need not to store a large amount of routing information.

2.5.2 Disadvantages of leach:

As the cluster head are selected randomly, there is a probability that at some point of time the cluster head is located at the corner of the network. This in turn will consume more energy than required.

Sometimes, it may happen that the broadcast message of cluster head and entry information of any new nod may collide which will result in loss of some information.

Chapter 3

NETWORK DEPLOYMENT

3.1 First order radio energy model:

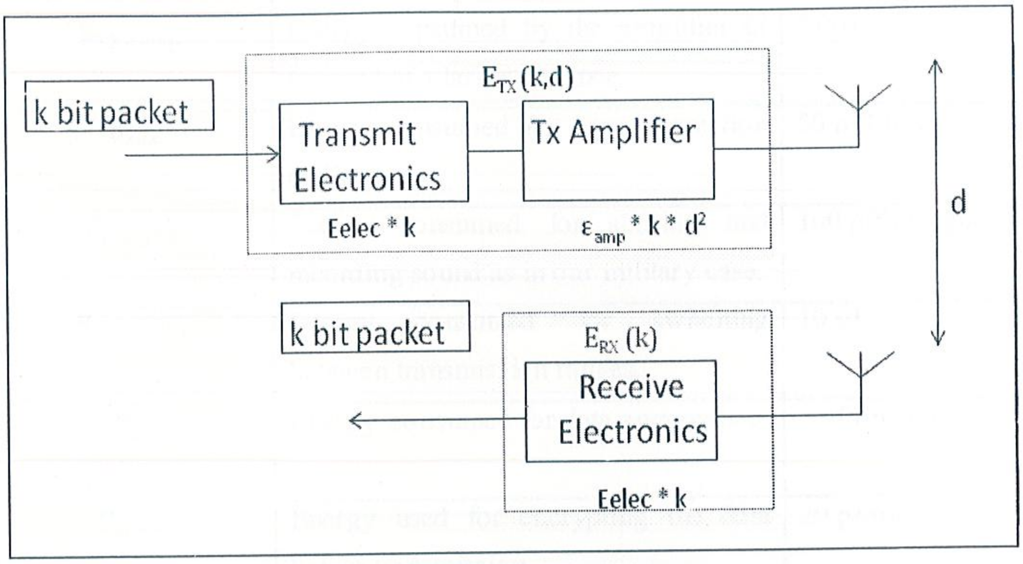


Figure 3.1: First order radio energy model [9]

Transmitting a k-bit message a distance d radio expends:

$$E_{TX}(k, d) = E_{TX-elec}(k) + E_{TX-amp}(k, d) + E_{ecc} + E_{sensing} + E_{switching} + E_{da} + E_{encrp}$$

$$= E_{elec} * k + \varepsilon * k * d^2 + E_{ecc} + E_{sensing} + E_{switching} + E_{da} + E_{encrp}$$

Receiving this message, radio expends:

$$E_{RX}(k) = E_{RX-elec}(k) + E_{processing} + E_{decyp}$$

$$= E_{elec} * k + E_{processing} + E_{decyp}$$

k=number of bits.

d= distance between two nodes.

SYMBOL	DESCRIPTION	VALUE(approx.)
E_{elec}	Energy consumed in the electronics circuitry to transmit or receive signal.	50 nJ/bit
E_{TX-amp}	Energy consumed by the amplifier to transmit at a larger distance.	0.0013 pJ/bit/m^2
E_{ecc}	Energy consumed for error correction coding.	50 pJ/bit/m
$E_{sensing}$	Energy consumed for sensing and recording sound as in our military case.	100 pJ/bit/signal
$E_{switching}$	Energy consumed for switching between transmission ranges.	10 pJ
E_{da}	Energy consumed for data aggregation	5 nJ/bit/signal
E_{encrp}	Energy used for encrypting the data before transmission.	20 pJ/bit
$E_{processing}$	Energy used for processing the data received.	20 pJ/bit
E_{decyp}	Energy consumed for decrypting the data at the receiver end.	20 pJ/bit

Table 3.1: Energy considerations in our routing protocol

For these parameter values, receiving a message is not a low cost operation. Therefore the protocols should try to minimize transmit distances as well as number of transmit and receive operations for each message.

3.2 Assumptions:

1. The radio channel is symmetric such that the energy required to transmit a message from node A to B is same as energy required to transmit energy from node B to A for a given SNR.

2. All the sensors are sensing the environment at a fixed rate and we therefore, they always have some data to send to end-user.
3. Each sensor node in our model has two transmission range 'x' and '2x'.
4. The battlefield area is assumed to be 500m X 500m.
5. All the nodes have same initial power therefore we propose a homogeneous network.
6. Sensor nodes communicate using short data packets.

3.3 Algorithm for Network Deployment and Energy Computation:

Set-Up Phase:

1. Deployment of the SINK at position (0, 0) in the battlefield.
2. Random deployment of sensor nodes in the area of the battlefield.
3. Selection of Cluster Heads (CHs) firstly on the basis of their centralized position.
4. Switching the transmission range of CHs to '2x' and 'x' for the rest of the sensor nodes.
5. Forming a distance matrix for each sensor node.
6. Connecting all the CHs present within the transmission range of '2x' using the distance matrix.
7. A CH is now responsible for discovering other cliques and sharing information within the clique.

Steady State Phase:

8. Use of more comprehensive first order radio model.
9. Calculate energy of each node i.e. transmission energy plus receiving energy gives the total energy of each node.
10. Calculate number of rounds after which each node dies.
11. Change of CH within a cluster if the first CH dies i.e. runs out of energy.
12. Set-up phase for CH selection is repeated.
13. Sensing occurs until the lifetime of the network.

Chapter 4
SECURITY

Wireless Sensor Network is performs not only civilian tasks but military tasks also. Traditional computer security techniques are not applicable as WSN also brings some resource constraints such as power and data storage with itself. The most important constraint in wireless sensor capabilities is Energy. Once the sensors are deployed they cannot be easily replaced or recharged, therefore their battery charge needs to be conserved. In this project we will not only increase the life of the node and but also increase the lifetime of the entire network. On adding a cryptographic code in the network protocol energy impact on the node should also be considered. Energy- Encryption energy, Decryption energy, cryptographic storages, etc.

In our routing protocol for military application security constraints would be equally important as energy constraints. Here are the security requirements for a military based routing protocol.

4.1 Security Requirements:

4.1.1 Data Confidentiality

The most important issue in network security is Data confidentiality [10]. In sensor networks, the confidentiality relates to the following -

- A sensor network should not leak sensor readings to its neighbors. Especially in a military application the data stored in the sensor node may be highly sensitive as in our project.
- It is extremely important to build a secure channel in a wireless sensor network because in many applications nodes communicate highly sensitive data, e.g., key distribution
- Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.

The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, thus achieving confidentiality.

4.1.2 Data Integrity

With the implementation of confidentiality, an adversary may be unable to steal information. But this doesn't mean the data is safe. The data can be changed, so as to send the sensor network into disarray. The data integrity [10] ensures that any received data has not been altered in transit and it is brought about by including error correction codes like CRC, Hamming codes, etc.

4.1.3 Data Freshness

Even if confidentiality and data integrity are assured, we also need to make sure about the freshness of each message. Informally, data freshness states that the data is recent, and it also states that no old messages have been replayed. This requirement is especially important when there are shared-key strategies used in the design. Mostly shared keys need to be changed over time. But it takes time for new shared keys to be propagated to the entire network, so it is easy for the adversary to use a replay attack.

4.1.4 Self-Organization

A wireless sensor network is a typically an ad hoc network, where every sensor node is independent and flexible enough to be self-organizing and self-healing as per situations demand. In a sensor network no fixed infrastructure is available as required by network management. This inherent feature brings a great challenge to wireless sensor network security as well.

4.1.5 Time Synchronization

In order to conserve power, an individual sensor's radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to- end delay of a packet as it travels between two pair-wise sensors. A more collaborative sensor network may need group synchronization for tracking applications, etc.

4.2 Implementation of data confidentiality

4.2.1Using simple encryption –decryption coding:

ALGORITHM:

Encryption:

1. Input the message to be encrypted in bits. E.g. '10111011'.
2. Find length (len) of the message.
3. Find the factors of the length.
4. Create a matrix using magic function with rows and column equal to the first factor of length.
5. Find the product (p) of the rest of the factors of the length.
6. Form a matrix (M) from the above matrix whose inverse always gives positive whole numbers.
7. Convert the input message into its ASCII codes.
8. Reshape the message matrix into a matrix of size (first factor, p).
9. Subtract 32 from each term of the above matrix.
10. Multiply it with M.
11. Find modulus of the above with 95.
12. Add 32 to each element.
13. Reshape the above matrix into size (1, len).
14. Send the encrypted message code.

Decryption:

1. Reshape the encrypted code into matrix size of(first factor, p).
2. Subtract 32 from each element.
3. Multiply inverse (M) with the above matrix.
4. Find its modulus with 95.
5. Add 32 to each element.
6. Reshape the matrix into size (1, len).
7. Send in the decrypted message code.

4.3 Implementation of data integrity

Receiving all sensor data correctly at the sink is more important so that we can prevent taking wrong actions. Unfortunately, this is very difficult in noisy environment, and hence error correcting codes (ECC) is used to improve data integrity. ECC can also have an adverse effect on network lifetime because of the energy consumed in processing (i.e., coding and decoding).

Therefore the fixed data length scheme is examined and its results are compared to the case of fixed frame length.

4.3.1 Using CRC codes:

A **cyclic redundancy check** (CRC) [11] is an error detecting code only used in digital networks and storage devices to detect accidental changes to raw data. Blocks of data entering these systems get a short check value attached, based on the remainder of a polynomial division of their contents; on retrieval the calculation is repeated, and corrective action can be taken against presumed data corruption if the check values do not match.

Algorithm of CRC coding:

1. Take the generator polynomial as $x^3 + x^2 + 1$.
2. Given a message to be transmitted: $b_n\ b_{n-1}\ b_{n-2} \ldots b_2\ b_1\ b_0$
3. Let the bits of the message as the coefficients of a polynomial $B(x) = b_n x^n + b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \ldots b_2 x^2 + b_1 x + b_0$
4. Multiply the polynomial corresponding to the message by x^k where k is the degree of the generator polynomial and then divide this product by the generator to obtain polynomials Q(x) and R(x) such that: $x^k B(x) = Q(x)\ G(x) + R(x)$. Treating all the coefficients not as integers but as integers modulo 2.
5. Finally, treat the coefficients of the remainder polynomial, R(X) as "parity bits". That is, append them to the message before actually transmitting it.
6. Since the degree of R(x) is less than k, the bits of the transmitted message will correspond to the polynomial: $x^k B(x) + R(x)$
7. Since addition and subtraction are identical in the field of integers mod 2, this is the same as $x^k B(x) - R(x)$
8. From the equation that defines division, however, we can conclude that: $x^k B(x) - R(x) = Q(x)\ G(x)$

   In other words, if the transmitted message's bits are viewed as the coefficients of a polynomial, then that polynomial will be divisible by G(x).
9. Finally the basis of error checking using the CRC. When a message is received the corresponding polynomial is divided by G(x). If the remainder is non-zero, an error is detected. Otherwise, the message is assumed to be correct.

CRCs are specifically designed to protect against common types of errors on communication channels, where they can provide quick and reasonable assurance of the integrity of messages delivered. However, they are not suitable for protecting against intentional alteration of data. Firstly, as there is no authentication, an attacker can edit a message and recalculate the CRC without the substitution being detected. Secondly, the linear properties of CRC codes even allow an attacker to modify a message in such a way as to leave the check value unchanged and otherwise permit efficient recalculation of the CRC for compact changes.

Moreover in CRC, the error is only detected and the correction is done by retransmitting data. The processing energy for coding will be investigated based on hardware implementations of coding or decoding circuits. Furthermore, a metric that represents a compromise between the lifetime and the amount of correct received data (throughput) will be introduced. Finally, according to our application, we have extended our error correction coding towards hamming codes, using which we have emphasized on improving network throughput without affecting the lifetime. Hamming code has a negligible effect on network lifetime irrespective of the SNR. In contrast, the CRC with retransmissions reduces the lifetime by 37.3% [12] compared to the un-coded system. Also, Hamming code increases system throughput when compared to the use of CRC.

4.3.2 Using Hamming codes:

Hamming codes [13] can detect up to two and correct up to one bit errors. By contrast, the simple parity code cannot correct errors, and can detect only an odd number of errors. Hamming codes are special in that they are perfect codes, that is, they achieve the highest possible rate for codes with their block length and minimum distance 3.

Algorithm for hamming codes:

The following general algorithm generates a single-error correcting (SEC) code for any number of bits [13].

1. Number the bits starting from 1.
2. Write the bit numbers in binary.
3. All bit positions that are powers of two (have only one 1 bit in the binary form of their position) are parity bits.
4. All other bit positions, with two or more 1 bits in the binary form of their position, are data bits.
5. Each data bit is included in a unique set of 2 or more parity bits, as determined by the binary form of its bit position.

5.1 Parity bit 1 covers all bit positions which have the least significant bit set: bit 1 (the parity bit itself), 3, 5, 7, 9, etc.

5.2 Parity bit 2 covers all bit positions which have the second least significant bit set: bit 2 (the parity bit itself), 3, 6, 7, 10, 11, etc.

5.3 Parity bit 4 covers all bit positions which have the third least significant bit set: bits 4–7, 12–15, 20–23, etc.

5.4 Parity bit 8 covers all bit positions which have the fourth least significant bit set: bits 8–15, 24–31, 40–47, etc.

5.5 In general each parity bit covers all bits where the binary AND of the parity position and the bit position is non-zero.

The form of the parity is irrelevant. Even parity is simpler from the perspective of theoretical mathematics, but there is no difference in practice.

Chapter 5

SIMULATIONS, RESULTS & CONCLUSION

5.1 Random deployment of sensor nodes:

Random deployment of sensor nodes and fixing the base station at position (0,0) because the area of deployment is assumed to be a battlefield therefore base station is secure outside it. We have done our coding in MATLAB. The area of the battlefield is assumed to be 500mX500m. In Figure 5.2 the cluster heads are selected.

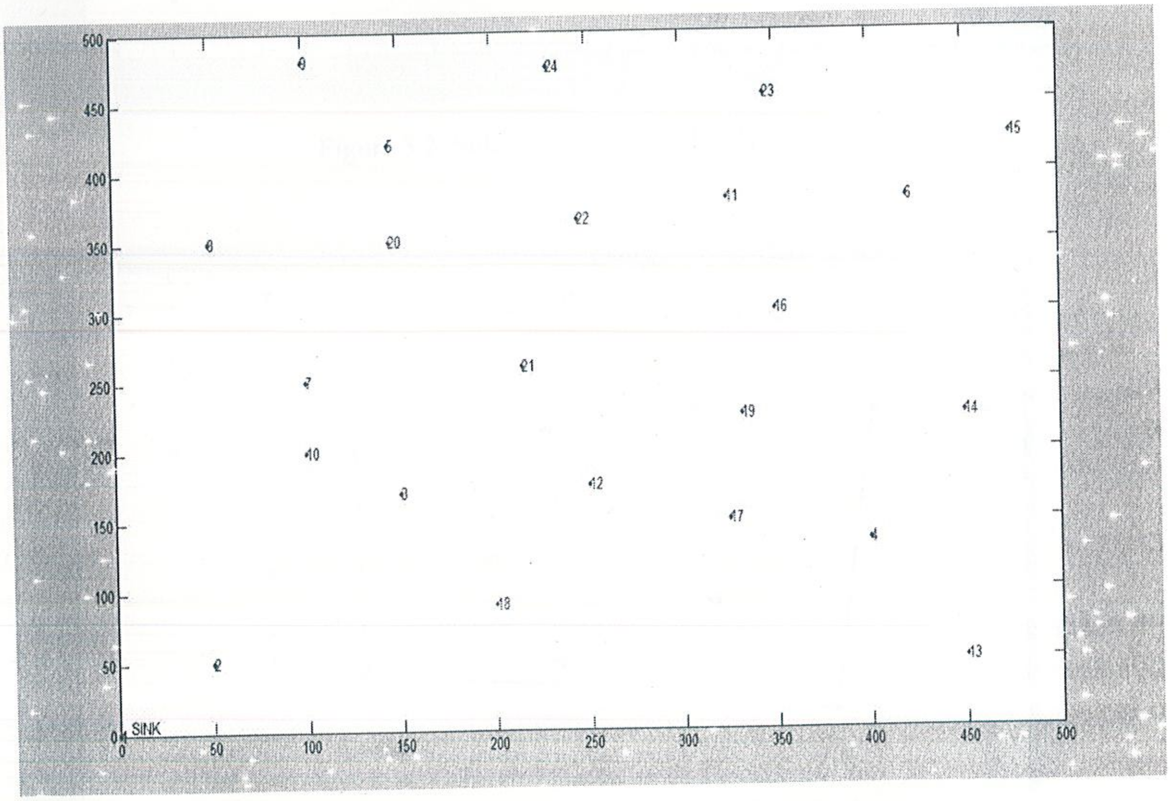


Figure 5.1: Random deployments of sensor nodes

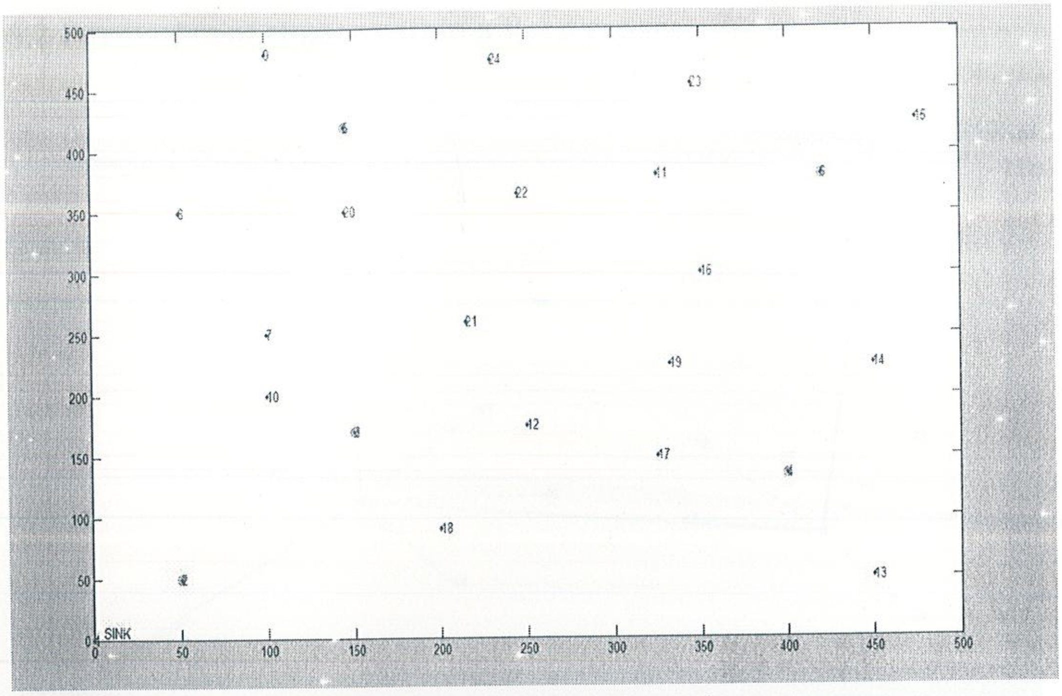


Figure 5.2: Selection of cluster heads

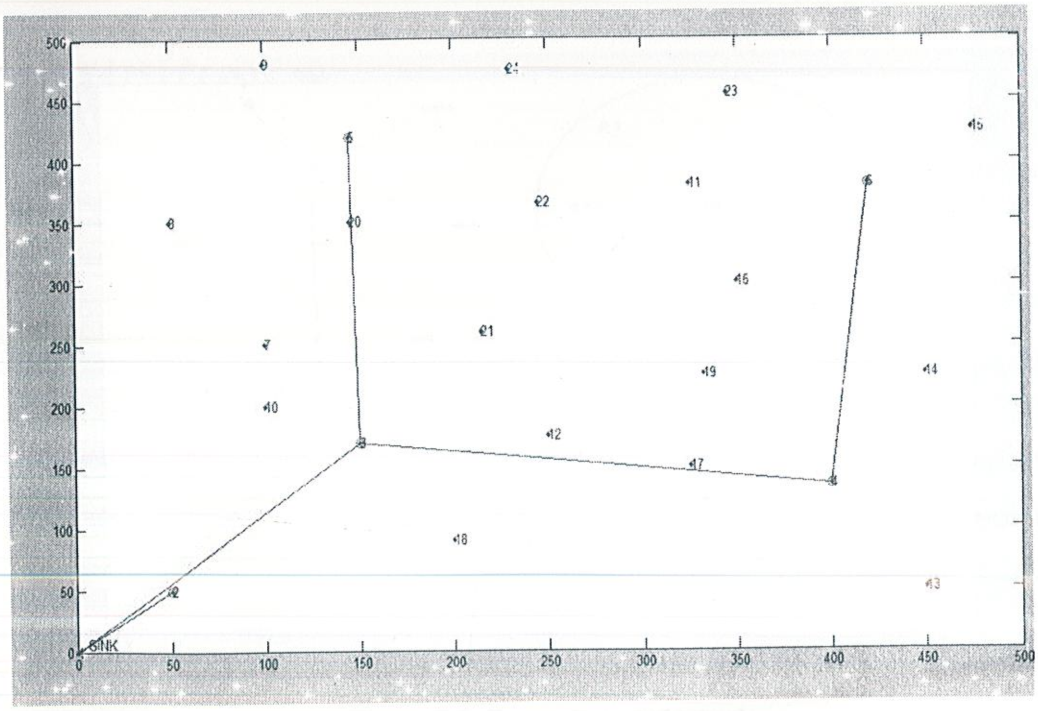


Figure 5.3: Joining of cluster heads

5.2 Formation of cluster within a fixed range:

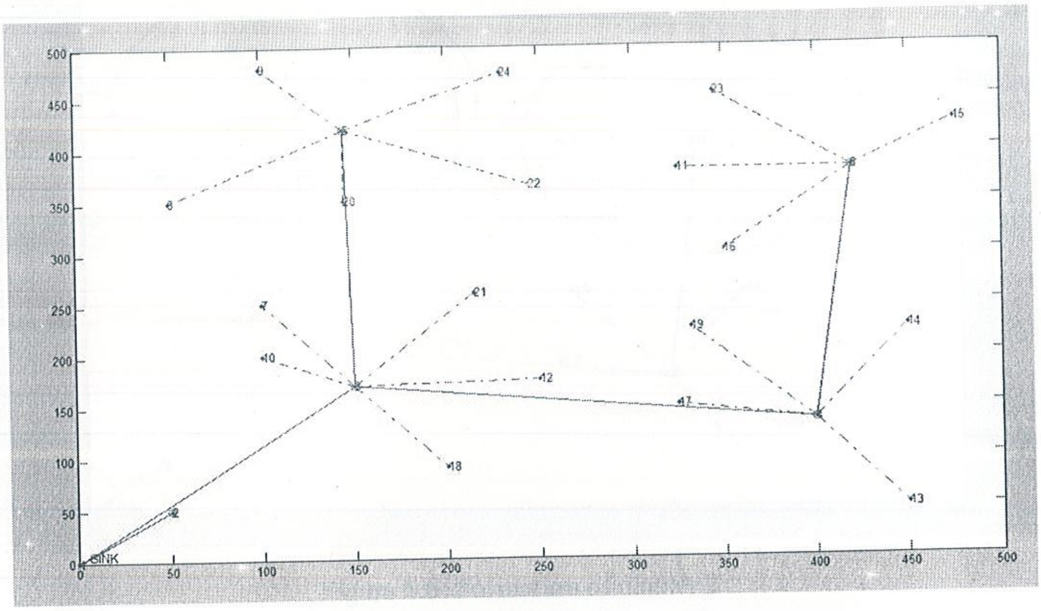


Figure 5.4: Sensor nodes connecting to their CHs

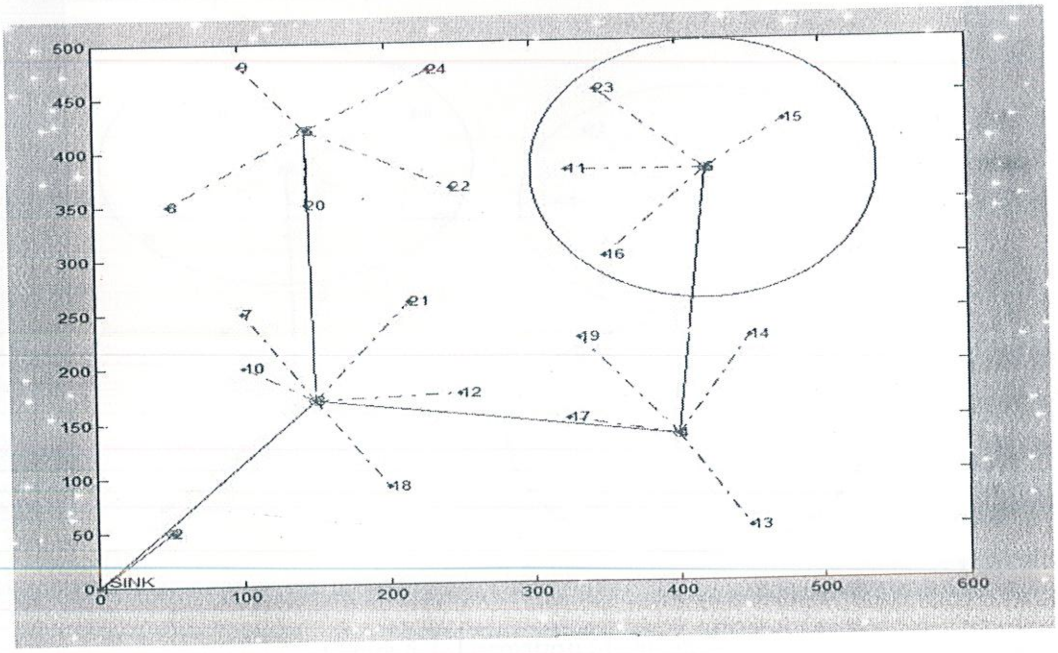


Figure 5.5: Formation of cluster 1

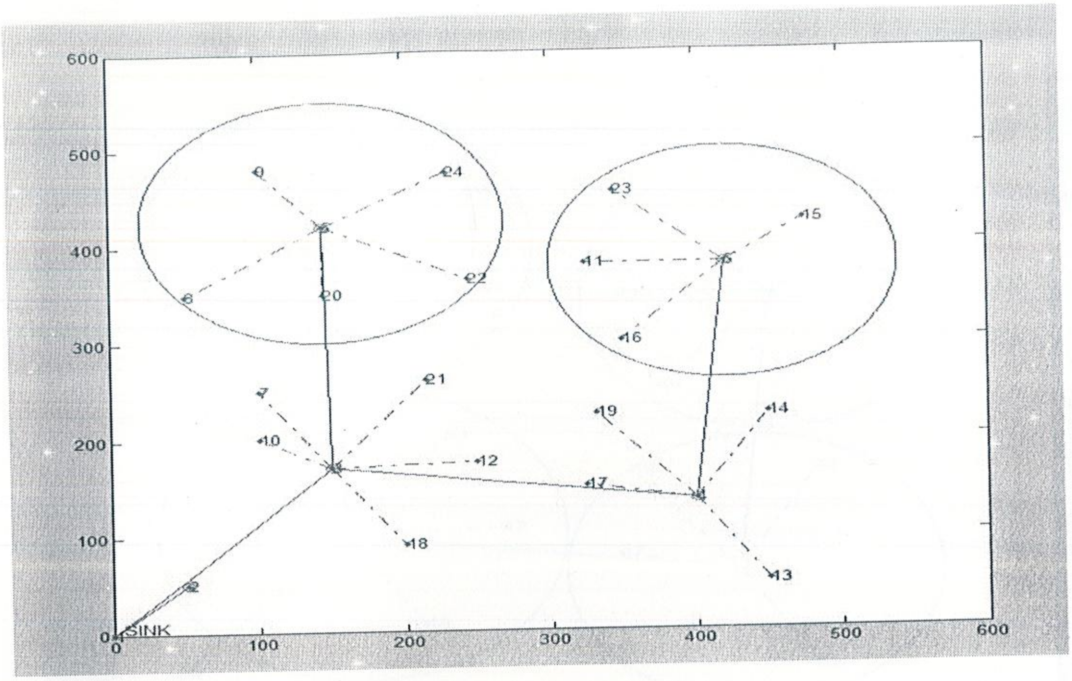


Figure 5.6: Formation of cluster 2

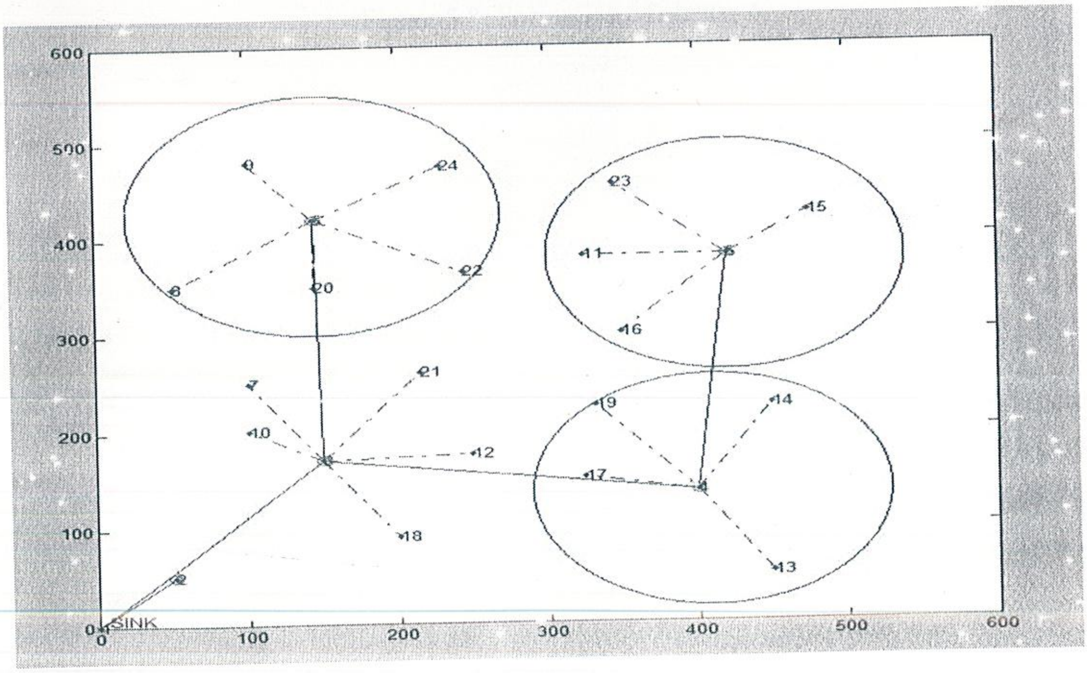


Figure 5.7: Formation of cluster 3

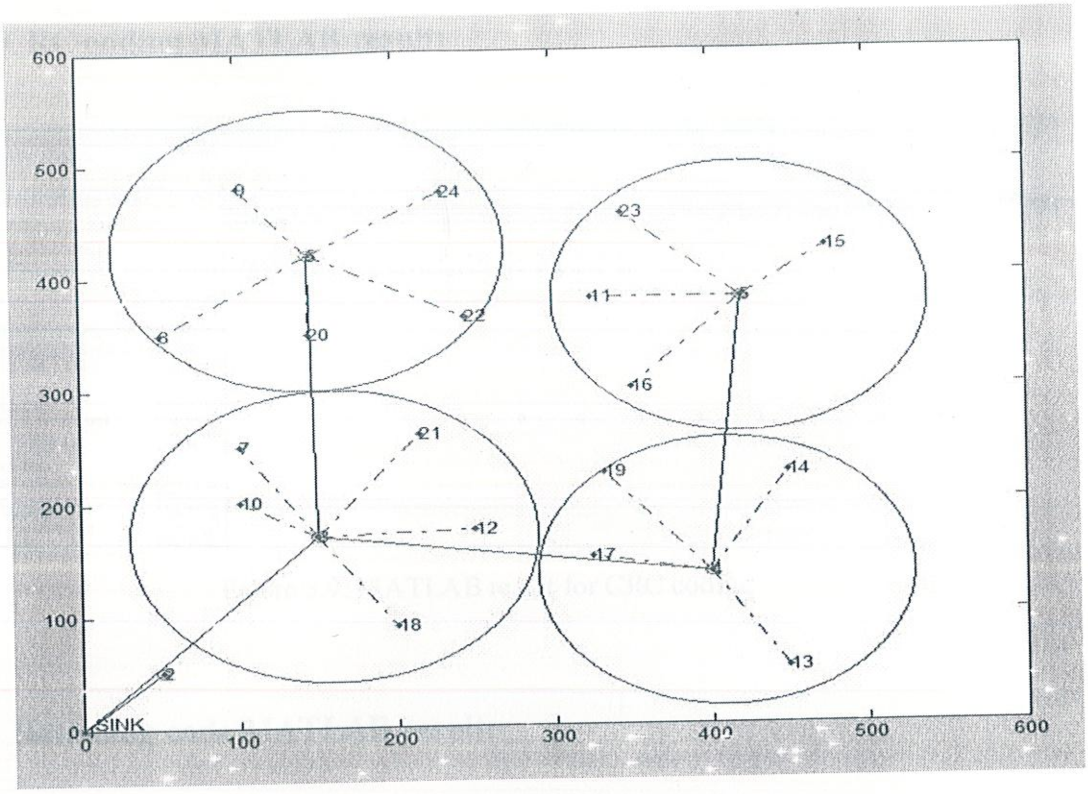
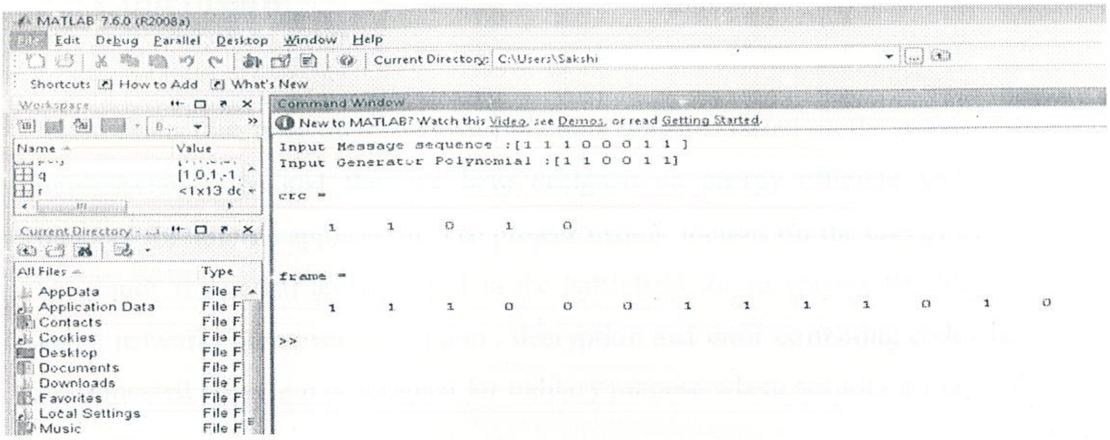


Figure 5.8: Formation of cluster 4

5.3 CRC coding MATLAB result:



```
Input Message sequence :[1 1 1 0 0 0 1 1 ]
Input Generator Polynomial :[1 1 0 0 1 1]

crc =

     1     1     0     1     0


frame =

     1     1     1     0     0     0     1     1     1     1     0     1     0

>>
```

Figure 5.9: MATLAB result for CRC coding

5.4 Hamming code MATLAB result:

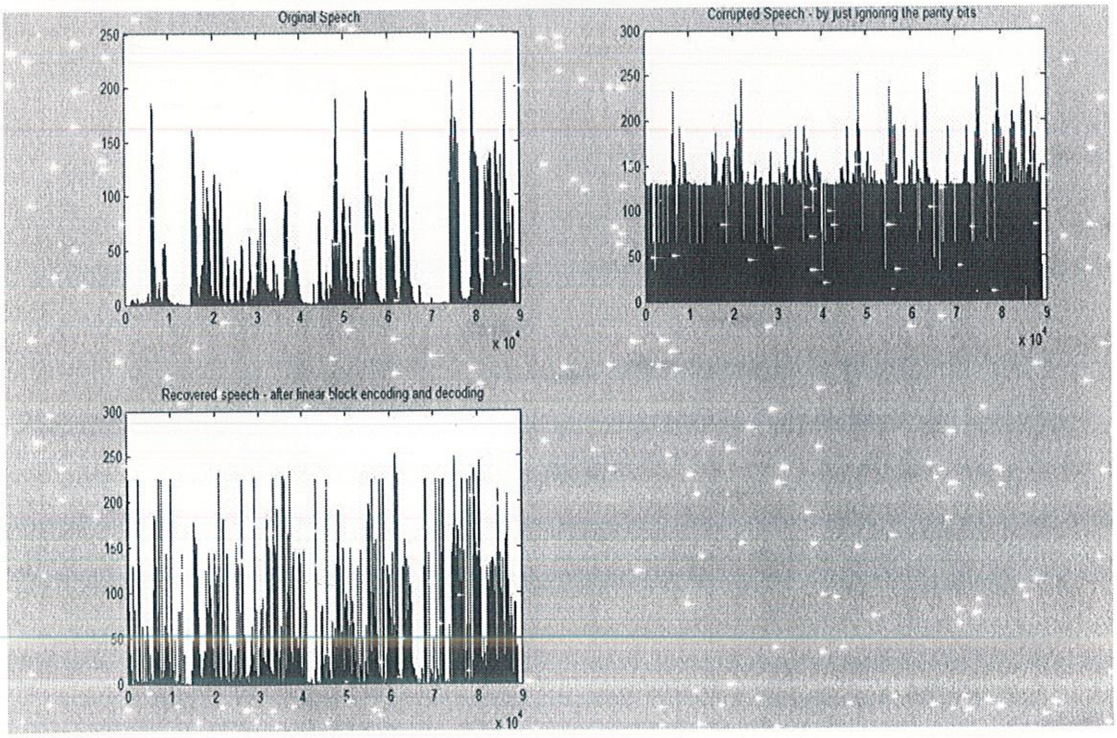


Figure 5.10: MATLAB result for hamming code

5.5 Conclusion:

In our project we have used adaptive switching which is based on the usage of different transmission range and thus we have designed an energy efficient secured routing protocol for defence application. The project mainly focuses on the energy efficiency of the sensor nodes that are deployed in the battlefield for increasing the lifetime of the entire network. Moreover encryption , decryption and error correcting codes have been implemented because it is designed for military purpose where security is one of the main concerns.

As the field of wireless sensor network is progressing with each new day, we wish to implement a heterogeneous network with more high power nodes and data aggregation techniques in our routing protocol as our future work aspect.

REFERENCES

[1] Application Domain of Wireless SensorNetwork:- A Paradigm in Developed and Developing Countries S.Taruna , Kusum Jain, G.N. Purohit, 2005.

[2] Wireless sensor networks: a survey- I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA Received 12 December 2001; accepted 20 December 2001.

[3] Application Domain of Wireless Sensor Network: - A Paradigm in Developed and Developing Countries S.Taruna , Kusum Jain, G.N. Purohit, July 2011.

[4] Initialization algorithms for wireless ad-hoc networks Carlos Agreda Ninot, April 26 th 2010.

[5] Wireless sensor network design for tactical military applications : remote large-scale environments, Sang Hyuk Lee, Soobin Lee, Heecheol Song, and Hwang Soo Lee, Department of Electrical Engineering, Kaist Daejeon, South Korea.

[6] International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010, Routing Protocols in Wireless Sensor Networks – A Survey Shio Kumar Singh, M P Singh, and D K Singh.

[7] Classification and comparison of routing protocols in wireless sensor networks Rajashree.V.Biradar, V.C .Patil, Dr. S. R. Sawant , Dr. R. R. Mudholkar

[8] Haiming Yang, BiplabSikdar," Optimal Cluster Head Selection in the LEACH Architecture", Performance, Computing, and Communications Conference, 2007. IPCCC 2007. IEEE International.

[9] Energy-Efficient Communication Protocol forWireless Microsensor Networks Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan Massachusetts Institute of Technology Cambridge.

[10] Wireless Sensor Network Security: A Survey by John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, Department of Computer Science Wayne State University,2006.

[11] http://en.wikipedia.org/wiki/Cyclic_redundancy_check

[12] Effect of Hamming Coding on WSN Lifetime and Throughput by Nora A. Ali, Hany M. ElSayed, Magdi El-Soudani, Hassanein H. Amer, Electronics a nd Communications Engineering Department, Cairo U niversity, Giza, Egypt,2011.

[13] http://en.wikipedia.org/wiki/Hamming_code

BIBLIOGRAPHY

- Wireless sensor networks-Technology, Protocols, and Applications by Kazem Sohraby, Daniel Minoli, Taieb Znati, A John Wiley & Sons, INC., Publication.

- Design of Network Management Platform and Security Framework for WSN Byunggil Lee, Seungjo Bae and Dongwon Han, Electronics and Telecommunications Research Institute.

- WSN-based Solutions for Security and Surveillance, F. Viani, G. Oliveri, M. Donelli, L. Lizzi, P. Rocca, and A. Massa, Department of Information Engineering and Computer Science, University of TrentoVia Sommarive 14, I-38050, Trento, Italy.

- Literature Survey on Wireless Sensor Networks by Pavlos Papageorgiou.

- A Survey of Application Distribution In Wireless Sensor Networks by Mauri Kuorilehto Marko H¨annik¨ainen and Timo D. H¨am¨al¨ainen.