PERFORMANCE ANALYSIS OF VARIOUS HIERARCHICAL ROUTING PROTOCOLS IN HOMOGENEOUS WIRELESS SENSOR NETWORKS

ROHIT JAIN (15UCS161)
AVINASH KUMAR (15UCS166)
ASHOK BHADU (15UCS170)
VIKASH SINGH (15UCS181)

COMPUTER SCIENCE & ENGINEERING DEPARTMENT
NATIONAL INSTITUTE OF TECHNOLOGY, AGARTALA
INDIA-799046

MAY, 2019

PERFORMANCE ANALYSIS OF VARIOUS HIERARCHICAL ROUTING PROTOCOLS IN HOMOGENEOUS WIRELESS SENSOR NETWORKS

Report submitted to the
National Institute of Technology, Agartala
for the award of the degree

of

Bachelor of Technology

by

ROHIT JAIN (15UCS161)
AVINASH KUMAR (15UCS166)
ASHOK BHADU (15UCS170)
VIKASH SINGH (15UCS181)

Supervisor

Mrs. SMITA DAS

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
NATIONAL INSTITUTE OF TECHNOLOGY, AGARTALA
INDIA-799046

MAY, 2019

.

Dedicated to

Our Project Supervisor, Mrs. Smita Das, Assistant Professor, Computer Science & Engineering Department, NIT Agartala for sharing her valuable knowledge, encouragement & showing confidence on us all the time. Each faculty of the department has contributed to our development as a professional and helped us to achieve this goal.

To all those people who have somehow contributed to the creation of this project and who have supported us.

Somewhere in me is a curiosity sensor. I want to know what's over the next hill. You know, people can live longer without food than without information.

_Arthur C. Clarke

Approval

Date:..........................

Certified that the report entitled **PERFORMANCE ANALYSIS OF VARIOUS HIERARCHICAL ROUTING PROTOCOLS IN HOMOGENEOUS WIRELESS SENSOR NETWORKS**, submitted by **Rohit Jain (15UCS161), Avinash Kumar (15UCS166), Ashok Bhadu (15UCS170), Vikash Singh (15UCS181)** to the National Institute of Technology, Agartala, for the award of the degree Bachelor of Technology has been approved.

Signature	Signature
Mrs. SMITA DAS	**Dr. DEBASISH BHATTACHARYA**
(Project Supervisor)	(Head of the Department, CSE Dept.)
Assistant Professor	Associate Professor
Computer Science & Engineering Department	Mathematics Department
NIT Agartala	NIT Agartala

Declaration

We declare that this written submission represents our own ideas in our own words and where others' ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Signature
ROHIT JAIN
(15UCS161)

Signature
AVINASH KUMAR
(15UCS166)

Signature
ASHOK BHADU
(15UCS170)

Signature
VIKASH SINGH
(15UCS181)

Certificate

This is to certify that the report entitled **PERFORMANCE ANALYSIS OF VARIOUS HIERARCHICAL ROUTING PROTOCOLS IN HOMOGENEOUS WIRELESS SENSOR NETWORKS**, submitted by **ROHIT JAIN (15UCS161), AVINASH KUMAR (15UCS166), ASHOK BHADU (15UCS170), VIKASH SINGH (15UCS181)** to National Institute of Technology, Agartala, is carried out under my supervision. I consider it worthy of consideration for the award of the degree of Bachelor of Technology of the Institute.

Signature
Mrs. SMITA DAS
(Project Supervisor)
Assistant Professor
Computer Science & Engineering Department
NIT Agartala

Signature
Dr. DEBASISH BHATTACHARYA
(Head of the Department, CSE Dept.)
Associate Professor
Mathematics Department
NIT Agartala

Acknowledgments

We take the privilege to express our gratitude towards our supervisor Mrs. Smita Das Assistant Professor, Computer Science and Engineering, NIT Agartala. Her constant support was the prime reason behind the successful completion of this report.

Last but not the least, we would like to express our sincere gratitude to all of them, who directly and indirectly helped us for the successful completion of our work.

- Rohit Jain
- Vikash Singh
- Avinash Kumar
- Ashok Bhadu

Contents

List of Figures

List of Tables

Abstract

Wireless Sensor Networks (WSN) is one of the most emerging and fastest growing fields in the scientific world. In the past few years, WSN have explored different application areas from home automation, environment monitoring, target tracking, pipeline (water, oil, gas) monitoring, structural health monitoring, precision agriculture, health care monitoring, supply chain management, active volcano monitoring, transportation, and underground mining to Internet of Things (IoT). The constraint most often associated with sensor network design is that sensor nodes operate with limited energy budgets. Typically, the limited battery power of a sensor node becomes a critical issue when it is not possible to replace or recharge its battery. The efficient use of energy source in a sensor node is a desirable criteria for scalability and prolonging the lifetime of WSN. Therefore, designing an efficient routing protocol for reducing energy consumption is one of the important issues in the network. A large number of routing protocols has been proposed in the last few decades. Some of the most popular and energy efficient routing protocols are hierarchical routing protocols like LEACH (Low Energy Adaptive Clustering Hierarchy), SEP (Stable Election Protocol), PEGASIS (Power Efficient GAthering in Sensor Information Systems), GAF (Geographic Adaptive Fidelity) and HEED (Hybrid Energy Efficient Distributed clustering protocol).

In this project we have studied various hierarchical routing protocols for their pros and cons. Subsequently, we have selected LEACH, PEGASIS and HEED routing protocols, based on their usefulness and have done a comparative study among them. Finally, a comparative study on the selected protocols are done based on several metrics such as: Load Balancing, Energy Consumption, Stability Period, Scalability and Network Lifetime through simulations of these routing protocols in OCTAVE on various simulation parameters and different simulation environments.

Chapter 1

Introduction

1.1 Wireless Sensor Networks

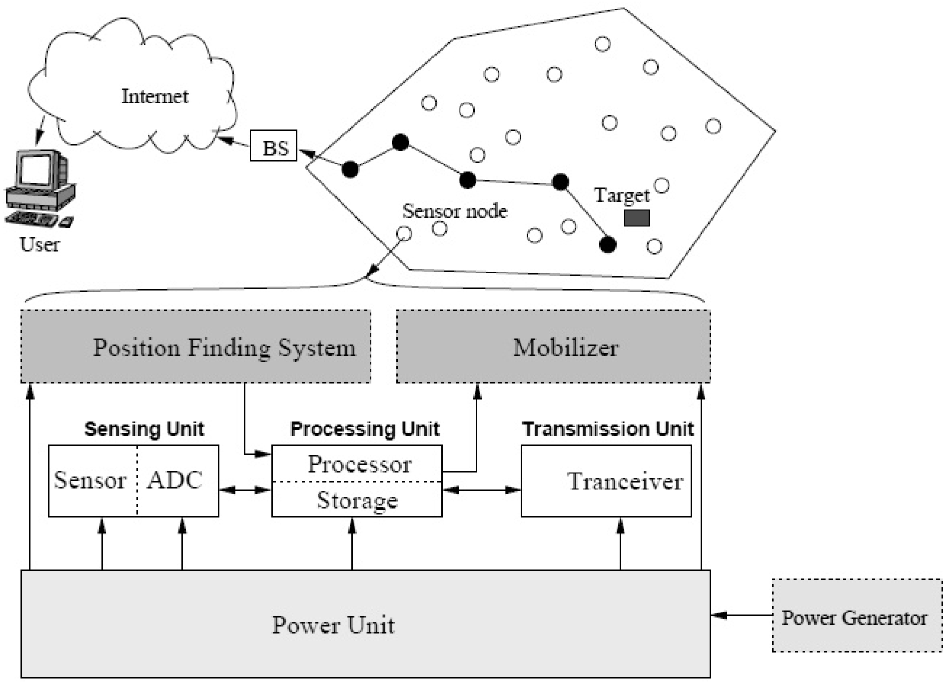


Figure 1.1: Components Of Sensor Node in WSN [1]

A wireless sensor network(WSN) is a self-configured and infrastructure-less wireless network and is a group of specialized transducers called sensors. These sensors are equipped with four basic components such as sensing unit, processing unit, transceiver unit and a power unit which is shown in figure 1.1 for monitoring and recording conditions at diverse locations. The individual nodes in WSN are inherently resource constrained: they have limited processing speed, storage capacity, and communication bandwidth. After the sensor nodes are deployed, they are responsible for self-organizing an appropriate network infrastructure often with multi-hop communication with them. Then the on-board sensors start collecting information of interest. Commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions.

The sensor network can be homogeneous or heterogeneous in nature depending upon the differences the sensor nodes have in terms of computation power, bandwidth and storage of energy.

1.1.1 Common applications of Wireless Sensor Networks

- **Military applications:** WSN be likely an integral part of military command, control, communications, computing, intelligence, battlefield surveillance, reconnaissance and targeting systems.
- **Environmental sensing:** The term Environmental Sensor Networks has developed to cover many applications of WSNs to earth science research. This includes sensing volcanoes, oceans, glaciers, forests etc. Some other major areas are listed below:
  - Air pollution monitoring
  - Forest fires detection
  - Landslide detection
  - Water quality monitoring
- **Structural monitoring:** Wireless sensors can be utilized to monitor the movement within buildings and infrastructure such as bridges, flyovers, embankments, tunnels etc enabling engineering practices to monitor assets remotely with out the need for costly site visits.
- **Data Logging:** Wireless sensor networks are also used for the collection of data for monitoring of environmental information. This can be as simple as the monitoring of the temperature in a fridge to the level of water in overflow tanks in nuclear power plants.
- **Industrial monitoring:** Wireless sensor networks have been developed for machinery condition-based maintenance(CBM) as they offer significant cost savings and enable new functionalities. In wired systems, the installation of enough sensors is often limited by the cost of wiring [1].

1.1.2 Design issues in Wireless Sensor Networks

- **Fault Tolerance:** Sensor nodes are vulnerable and frequently deployed in dangerous environment. Nodes can fail due to hardware problems or physical damage or by exhausting their energy supply. We expect the node failures to be much higher than the one normally considered in wired or infrastructure-based wireless networks. The protocols deployed in a sensor network should be able to detect these failures as soon as possible and be robust enough to handle a relatively large number of failures while maintaining the overall functionality of the network. This is especially relevant to the routing protocol design, which has to ensure that alternate paths are available for rerouting of the packets. Different deployment environments pose different fault tolerance requirements [1].

- **Scalability:** Sensor networks vary in scale from several nodes to potentially several hundred thousand. In addition, the deployment density is also variable. For collecting high-resolution data, the node density might reach the level where a node has several thousand neighbours in their transmission range. The protocols deployed in sensor networks need to be scalable to these levels and be able to maintain adequate performance.

- **Hardware Constraints:** At minimum, every sensor node needs to have a sensing unit, a processing unit, a transmission unit, and a power supply. Optionally, the nodes may have several built-in sensors or additional devices such as a localization system to enable location-aware routing. However, every additional functionality comes with additional cost and increases the power consumption and physical size of the node. Thus, additional functionality needs to be always balanced against cost and low-power requirements.

- **Network Topology:** Although WSNs have evolved in many aspects, they continue to be networks with constrained resources in terms of energy, computing power, memory, and communications capabilities. Of these constraints, energy consumption is of paramount importance, which is demonstrated by the large number of algorithms, techniques, and protocols that have been developed to save energy, and thereby extend the lifetime of the network. Topology Maintenance is one of the most important issues researched to reduce energy consumption in wireless sensor networks.

- **Production Costs:** As many deployment models consider the sensor nodes to be disposable devices, sensor networks can compete with traditional information gathering approaches only if the individual sensor nodes can be produced very cheaply. The target price envisioned for a sensor node should ideally be less than $1.

- **Power Consumption:** Many of the challenges of sensor networks revolve around the limited power resources. The size of the nodes limits the size of the battery. The software and hardware design needs to carefully consider the issues of efficient energy use. For instance, data compression might reduce the amount of energy used for radio transmission, but uses additional energy for computation and/or filtering.

1.1.3 Security issues in Wireless Sensor Networks

Security issues in WSN depend on the need to know what we are going to protect [1]. **The four security goals of sensor networks are :**

- **Confidentiality:** It is the ability to conceal message from a passive attacker, where the message communicated on sensor networks remain confidential.
- **Integrity:** It refers to the ability to confirm the message has not been tampered, altered or changed while it was on the network.
- **Authentication:** It is the need to know if the messages are from the node it claims to be from, determining the reliability of messages origin.
- **Availability:** It is to determine if a node has the ability to use the resources and the network is available for the messages to move on.

Common security attacks which prevents us from achieving these goals are [1] :

- **Routing loops attacks:** It target the information exchanged between nodes. False error messages are generated when an attacker alters and replays the routing information. Routing loops attract or repel the network traffic and increases node to node latency.
- **Selective forwarding attacks:** It influences the network traffic by believing that all the participating nodes in network are reliable to forward the message. In this attack malicious nodes simply drop certain messages instead of forwarding every message.
- **Sinkhole attacks:** In this attack, adversary attracts the traffic to a compromised node. The simplest way of creating sinkhole is to place a malicious node where it can attract most of the traffic, possibly closer to the base station or malicious node itself deceiving as a base station. One reason for sinkhole attacks is to make selective forwarding possible to attract the traffic towards a compromised node.
- **Sybil attacks:** These are a type of attacks where a node creates multiple illegitimate identities in sensor networks either by fabricating or stealing the identities of legitimate nodes. Sybil attacks can be used against routing algorithms and topology maintenance;

it reduces the effectiveness of fault tolerant schemes such as distributed storage and disparity.

- **Denial of service DoS) attacks:** It occurs at physical level causing radio jamming, interfering with the network protocol, battery exhaustion etc thereby reducing the availability of sensor nodes. Mostly the target is a sensor nodes power supply. Attacks of this type can reduce the sensor lifetime from years to days and have a devastating impact on a sensor network.

1.1.4 Routing Techniques in Wireless Sensor Networks

The data sensed by the sensor nodes in a WSN is typically required to be forwarded to the base station where the data is collected, analyzed and some action is taken accordingly. This forwarding of data can be done in single-hop if network area is small and all nodes are closer to base station, but if the coverage area is large and base station is far away from most of the nodes then multi-hop communication is required.

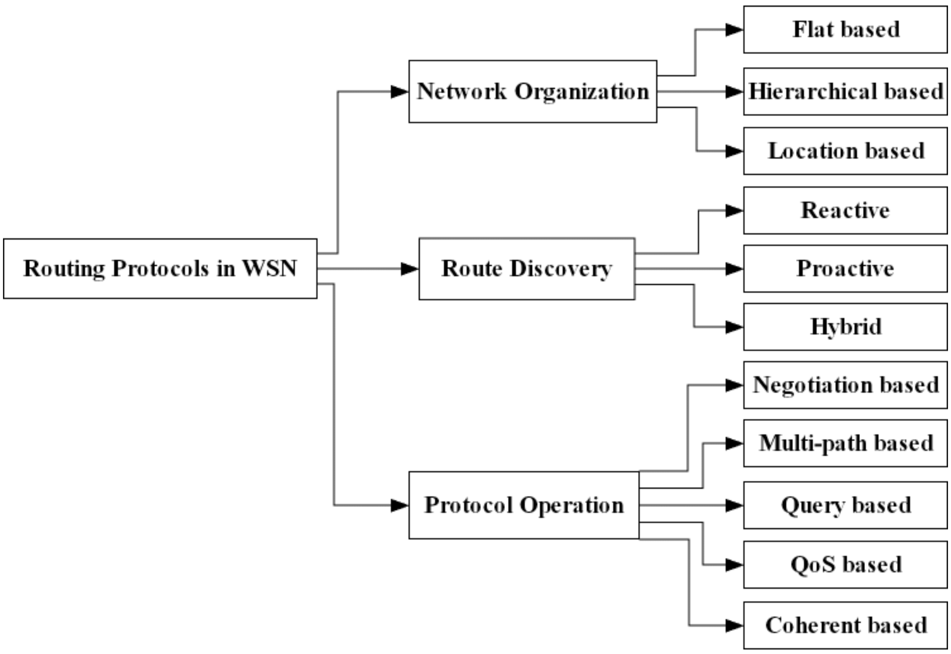


Figure 1.2: Classification of Routing Protocols [2]

In multi-hop communication the sensor nodes not only produce and deliver their data but also serve as a path for other sensor nodes towards the base station. The process of finding suitable path from source node to destination node is called routing and this is the primary responsibility of the network layer. The routing depends upon, type of network, channel characteristics and metrics such as energy efficiency, delay, robustness, scalability and complexity.

Routing protocols are mainly classified on the basis of Network Organization, Route Discovery and Operation Based as shown in figure 1.2 [2]

- **Flat Based protocols:** Each node assumes the same task in network and the sensor nodes team up to carry out the sensing task. The BS keeps waiting for information from the sensor situated selected areas after it sent queries to those certain areas.
- **Hierarchical Based Protocols:** Cluster based or hierarchical based routing is advantageous in relation to energy-efficiency as well as scalability. Nodes lower in energy can be utilized to sense data close to target whereas nodes with higher energy for processing and sending the information. The forming of clusters and appointing unique tasks to cluster heads can enormously contribute to the whole network scalability and energy efficiency.
- **Location Based Protocols:** In location based routing the nodes have capability to locate their present location using various localization protocols.If the sensor nodes are outfitted with a little low-power GPS receiver,their location may be accessible straight forward by corresponding with a satellite utilizing GPS.
- **Reactive Protocols:** Reactive routing protocols do not maintain the whole network topology they are activated just on demand when any node wants to send data to any other node. So the routes are created on demand when queries are initiated.
- **Proactive Protocols:** They are also known as table driven routing protocols, because they maintains the routing tables for the complete network by passing the network information from node to node and the routes are predefined prior to their use and even when there is no traffic flow.
- **Hybrid Protocols:** Hybrid Routing Protocols have the merits of proactive and reactive routing protocols by neglecting their demerits.
- **Negotiation Based Protocols:** In these types of protocols to keep the redundant data transmission level at minimum, the sensor nodes negotiate with the other nodes a and share their information with the neighboring nodes about the resources available and data transmission decisions are made after the negotiation process.
- **Multi-path Based Protocols:** Multi-path routing protocols provide multiple paths for data to reach the destination providing load balancing, low delay and improved network performance as a result. The multiple routing protocol also provide alternate path in case of failure of any path. Dense networks more interested in multiple path networks. To keep the paths alive some sort of periodic messages have to a send after some specific intervals hence multiple path routing is not more energy efficient.

- **Query Based Protocols:** These type of routing protocols are mostly receiver-initiated. The sensor nodes will only send data in response to queries generated by the destination node. The destination node sends query of interest for receiving some information through the network and the target node sense the information and send back to the node that has initiated the request.

- **QoS Based Protocols:** To get good Quality of Service these protocols are used. QoS aware protocols try to discover path from source to sink that satisfies the level of metrics related to good QoS like throughput, data delivery, energy and delay, but also making the optimum use of the network resources.

- **Coherent Based Protocols:** In coherent data processing routing protocol the nodes perform minimum processing (time stamping, data compression etc.) on the data before transmitting it towards the other sensor nodes or aggregators. Aggregator performs aggregation of data from different nodes and then passes to the sink node.

Out of all these, hierarchical clustering protocols are widely used to improve overall network scalability as well as to increase the lifetime of the network by enhancing the energy efficiency of each sensor node.

1.2 Motivation

Considering the design issues in WSNs and the shear number of protocols available to tackle them, it is very difficult to find a routing protocol which suits a specific purpose or fulfills certain requirements with better results as compared to other protocols.

Moreover, there are many surveys such as [6], [7] and [8] on energy-efficient hierarchical routing protocols analysing their strengths and weakness depending upon their implementation, but none of them focused on their performance in energy-efficiency and prolonging network lifetime for large scale WSNs. That is, the scalability of a network is also an important criteria in deciding which routing protocol is more energy-efficient than the other.

This motivated us to work on this project , where we select three known hierarchical routing protocols ,LEACH, PEGASIS and HEED and do a simulation for 100 to 1000 nodes over a network area of (100 X 100) to (1000 X 1000) square metres and compare them on metrics such as load balancing, average energy consumption and lifetime of the network.

1.3 Goal

The goal of this project is to find out which among these three protocols: LEACH, PEGASIS and HEED, is better in terms of load balancing, energy-efficiency, stability period, network lifetime and scalability. It also discusses the challenges faced by the existing routing protocols and wireless sensor networks as a whole and what can be done to create a better and energy-efficient wireless sensor networks that can be utilized at a greater scale in the existing scientific and industrial areas in the real world.

1.4 Contribution of dissertation

- Our work includes simulation of network for various simulation parameters such as number of nodes, network area, initial energy, location of base station, crossover distance, electronics energy per bit, aggregation energy per bit, length of packets.
- Then we simulated the LEACH, PEGASIS and HEED as directed in their original paper and ran these protocols over the above mentioned simulated network.
- We then, stored the statistics such as residual energy of network per round, dead nodes per round, average residual energy of a node per round, variance of residual energy per round for each protocol in different simulation environments.
- Finally, the conclusion was drawn after analysing the statistics obtained by plotting the graphs for each protocol after every simulation.

1.5 Outline of the project

This report is organized in the following manner: Chapter 2 deals with the related work done on routing protocols in WSN. Chapter 3 discusses the background of our project. Chapter 4 describes simulation details. Chapter 5 is on results analysis, Chapter 6 gives the conclusion drawn from the project and possible directions for future work.

Chapter 2

Related Work

2.1 A Chain-Based Routing Protocol to maximize the lifetime of wireless sensor networks

To extend the lifespan of WSN, the author [3] proposed an algorithm that forms multiple chains in the direction of the sink each with a leader node, which is the last, and the nearest node to the sink. Data transmission is performed from node to node and the last node sends directly to the sink. An improved scheme of this latter consists at forming a main chain grouping the leader nodes as shown in figure 2.1 and further reducing the energy consumption of the network.

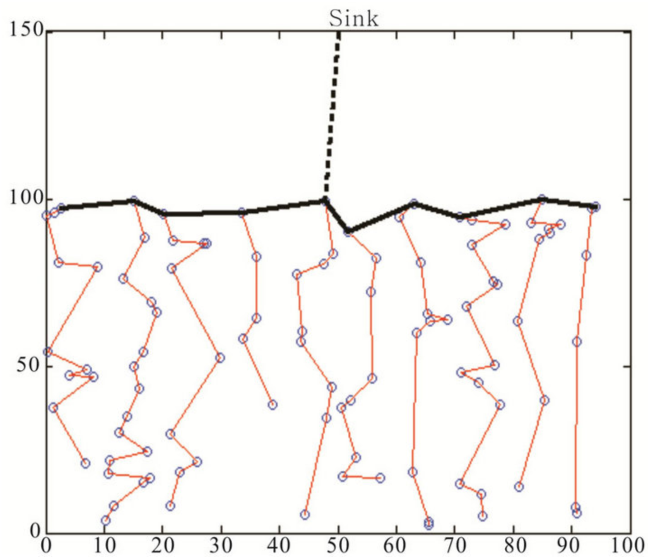


Figure 2.1: Multiple Chain Formation in WSN [3]

The simulation results revealed that the improved algorithm reduced the energy consumption as compared to the former chain schemes and consequently maximized the lifetime of the WSNs.

2.2 Energy-Efficient Routing Control algorithm in large-scale WSN for Water Environment Monitoring

The application of wireless sensor networks for water environment monitoring in the Three Gorges Reservoir area [9] is a typical case of large-scale wireless sensor networks research. And it has the typical characteristics of zonal distribution and large coverage area. Author's research is based on the achievements they already obtained and deeply study on the existing routing algorithms, such as, LEACH [5] and PARPEW [10] algorithms, and the focus is on the energy saving routing algorithm for large-scale WSN. So an improved energy-saving routing algorithm based on maximum energy-welfare optimization clustering has been proposed. There are three aspects of the major improvements:

- firstly, remaining energy and the distance from base station of nodes were both considered when selecting cluster heads. So it is more reasonable.

- Secondly, the cluster heads adjustment and clustering optimization based on improved maximum energy-welfare made the distribution of cluster heads more uniform, and the energy consumption of network has been balanced efficiently.

- Thirdly, the factors such as path costs, remaining energy, and angle deviation between node and base station were taken into consideration in the clustering routing construction, so that the energy efficiency of nodes has been increased.

Simulation results show that, compared with LEACH and PARPEW algorithms, the proposed algorithm in this paper can efficiently save energy of each node, balance the energy consumption, and prolong the lifetime of the network. It is suitable to the Three Gorges Reservoir water environment monitoring network with zonal structure.

2.3 SEP: A Stable Election Protocol for clustered heterogeneous wireless sensor networks

In this paper the author assumes that the sink is not energy limited and that the coordinates of the sink and the dimensions of the field are known. They also assume that the nodes are uniformly distributed over the field and they are not mobile. Under this model, they propose a new protocol, called SEP [11], for electing cluster heads in a distributed fashion in two-level hierarchical wireless sensor networks. Unlike prior work, SEP is heterogeneous-aware, in the sense that election probabilities are weighted by the initial energy of a node relative to that of other nodes in the network i.e. it improves the stable region of the clustering hierarchy process using the characteristic parameters of heterogeneity, namely the fraction of advanced nodes (m) and the additional energy factor between advanced and normal nodes (a). This prolongs the time interval before the death of the first node (referred as stability period), which is crucial for many applications where the feedback from the sensor network must be reliable.

Simulation results show for the case of **m = 0.2** and **a = 1** that the stable region of SEP is extended compared to that of LEACH by **8%**, even though the gain is not very large and for the case of **m = 0.2** and **a = 3**, SEP takes full advantage of heterogeneity (extra energy of advanced nodes) and the stable region is increased significantly by **26%** in comparison with that of LEACH. SEP provides longer stability period and higher average throughput than current clustering heterogeneous-oblivious protocols. Authors also studied the sensitivity of SEP [11] protocol to heterogeneity parameters capturing energy imbalance in the network. It is shown that SEP is more resilient than LEACH [5] in judiciously consuming the extra energy of advanced nodes. SEP yields longer stability period for higher values of extra energy in the advanced nodes present in the network.

2.4 Design of a Distributed Energy-Efficient Clustering algorithm for heterogeneous wireless sensor networks

The clustering algorithm is a kind of key technique used to reduce energy consumption. It can increase the scalability and lifetime of the network. Energy-efficient clustering protocols should be designed for the characteristic of heterogeneous wireless sensor networks.

In this paper, the author proposed and evaluated a new distributed energy-efficient clustering scheme for heterogeneous wireless sensor networks, which is called DEEC [12]. Following the thoughts of LEACH, DEEC lets each node expend energy uniformly by rotating the cluster-head role among all nodes. In DEEC, the cluster-heads are elected by a probability based on the ratio between the residual energy of each node and the average energy of the network. Thus, DEEC does not require any global knowledge of energy at every election round. The round number of the rotating epoch for each node is different according to its initial and residual energy, i.e., DEEC adapt the rotating epoch of each node to its energy. The nodes with high initial and residual energy will have more chances to be the cluster-heads than the low-energy nodes.Thus DEEC can prolong the network lifetime, especially the stability period, by heterogeneous-aware clustering algorithm.

Simulations results show that DEEC increases the stability period by **15%** more number of rounds and **20%** more number of total rounds of network lifetime as compared to LEACH and SEP and hence it achieves longer network lifetime and more effective messages than other classical clustering algorithms in two-level heterogeneous environments. Unlike SEP [11] and LEACH [5] , DEEC can perform well in multi-level heterogeneous wireless sensor networks.

2.5 Enhanced LEACH Multi-path Based Energy-Efficient Routing for wireless sensor network

In this paper, authors have proposed multi-path LEACH protocol [13] based on LEACH. The main intention of this protocol is to offer energy efficient and robust communication. The multi-path technique overcomes the problems raised in single path or multi hop routing algorithm. As we know that in sensor network, in between sensor node and base station multiple number of paths are available. This gives information about how far the cluster head exist from the sensing node. This knowledge is helpful for selecting the nearest cluster-head node. Due to this energy gets saved and decreases the number of hops needed to communicate between cluster head and sensor node. This is achieved by traffic multiplexing over multiple paths and introducing alternation of the cluster-heads for every given interval of time.

Simulation results show that multi-path LEACH protocol performs better than LEACH in terms of energy-efficiency and prolonging the lifetime of the network.

Chapter 3

Background

3.1 LEACH Protocol

3.1.1 Overview of LEACH

One of the oldest and first hierarchical protocols, LEACH(Low-Energy Adaptive Clustering Hierarchy) is a simple TDMA based routing protocol used in WSN. It was proposed by Heinzelman [5] in the year 2000. This cluster based protocol emerged as an energy efficient communication protocol for wireless micro-sensor networks that utilizes randomized rotation of local cluster base stations known as cluster heads to uniformly distribute the energy load among sensor nodes in the network.

The key features of LEACH are:

- Localized coordination and control for cluster-set up and operation.
- Randomized rotation of the cluster heads and the corresponding clusters.
- Local compression to reduce global communication.

LEACH is considered to be a self-organizing protocol in which the sensor nodes organize themselves to form clusters and one node is chosen as a cluster head (CH). The CH acts as a local Base Station (BS) in a way that data is transmitted by each sensor node to its corresponding cluster head. The cluster head position is rotated among different sensor nodes within the cluster to ensure that just a single node does not die out due to loss of its whole energy. The rotation is done in a random manner. The CHs also compress the data received by it from the other nodes before sending it to the base station to ensure less energy dissipation in the network. Once the CHs are chosen, they broadcast their position or status to other sensor nodes within the network. Each sensor node then calculates the amount of energy required to communicate data to the CHs and chooses the one with minimum. In this way the clusters are formed. The CHs then create schedule for its sensor nodes to transmit the data and the nodes remain turned off until their turn for transmitting data comes. This saves a large amount of energy dissipated by each sensor node. After collecting data from each node within the cluster, the CH then aggregates it and sends it to the BS.

3.1.2 LEACH Algorithm

The operation of LEACH is broken up into rounds, where each round begins with a set-up phase, when the clusters are formed, followed by a steady-state phase, when data transfers to the base station occurs through the cluster heads.

Cluster Set-Up Phase:

- Each node will generate a random number between 0 and 1. This node will be selected as Cluster Head (CH) if the generated random number is less than the specified threshold for that round. The threshold is given by 3.1 [5].

$$T(n) = \begin{cases} \frac{P}{1-P*(r mod \frac{1}{P})} & \text{if } n \in G \\ 0 & otherwise \end{cases} \tag{3.1}$$

  Here, 'P' is the desired percentage of cluster heads, 'r' is the round number and 'G' is the set of nodes that have not been cluster heads in the last 1/P rounds. This makes sure that every node will become cluster head at some point within 1/P rounds.

- Next, each node that has selected itself as CH will advertise a message of being a CH using CSMA MAC protocol and every non CH node has to put their receiver on during the entire set-up phase to listen for the advertisement and then decide which CH is nearest depending upon the received signal strength. The node selects that CH for this round which is nearest or say, has the highest received signal strength.

- Every non CH node then informs the selected CH using CSMA MAC protocol that this node belongs to its cluster. For this, every CH node has to put its receiver on during the entire phase.

- The CH node after receiving messages from all node that would like to be in its cluster, creates a CDMA code to prevent inter-cluster interference along with a TDMA schedule for each node in its cluster for the purpose of data transfer and broadcast this schedule and CDMA code to every node in the cluster.

Steady State Phase: Once the clusters are created and the TDMA schedule is fixed, data transmission can begin.

- Assuming non CH nodes always have data to transfer, they send it during their allocated transmission time to CH. This transmission uses minimal amount of energy and the radio can be turned off untill the next transmission time and hence minimizing energy dissipation in these nodes.
- Every CH has to keep their receiver on during the entire phase to receive data from every node in the cluster. Once every node has send its data, CH can compress all the data into a composite signal using any beamforming algorithm [[14] [15]] and send it to the base station (BS). As BS is far away, this is a high energy transmission.

3.2 PEGASIS Protocol

3.2.1 Overview of PEGASIS

The protocol PEGASIS (Power-Efficient GAthering in Sensor Information Systems) was proposed by Lindsey and Raghavendra [4] in which a chain of sensor nodes is formed and each node communicates only with its close neighbors. Data transmission is done from node to node and only a designated node sends it to the BS. The leader node responsible for transmission changes turn by turn. The chain formation is either determined by the BS or the nodes themselves form chain using greedy algorithm. While data gathering, each node gathers data from its neighbor and further transmits it to next neighboring node after fusing it with its own sensed data. To make the scheme robust, the sensor nodes die out at random locations. This is achieved by changing the data transmission leader in each communication round.

3.2.2 PEGASIS Algorithm

The main idea in PEGASIS is for each node to receive from and transmit to close neighbors and take turns being the leader for transmission to the BS. This approach will distribute the energy load evenly among the sensor nodes in the network.

Formation of a Chain:

- Firstly, a chain is formed before the start of any data communication using a greedy approach among the nodes.
- The furthest node from the sink or BS is chosen as a starting point for the chain in order to make sure that the nodes farther from the BS have close neighbors.
- As in the greedy algorithm the neighbor distances will increase gradually since nodes already on the chain cannot be revisited. Therefore not every node in the chain will have the closest neighbor among all the nodes in the surroundings.

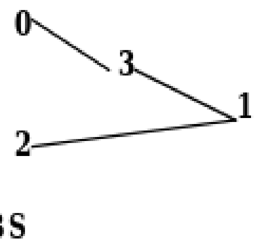


Figure 3.1: Chain Formation in PEGASIS [4]

- Figure 3.1 shows node 0 connecting to node 3, node 3 connecting to node 1, and node 1 connecting to node 2 in that order.
- When a node dies, the chain is reconstructed in the same manner to bypass the dead node.

Data Transmission:

- For gathering data in each round, each node receives data from one neighbor, fuses with its own data, and transmits to the other neighbor on the chain.
- Note that node i will be in some random position j on the chain. Nodes take turns transmitting to the BS, and node number i mod N (N represents the number of nodes) will transmit to the BS in round i. Thus, the leader in each round of communication will be at a random position on the chain, which is important for nodes to die at random locations. The idea in nodes dieing at random places is to make the sensor network robust to failures.

- In any given round, a simple control token passing approach initiated by the leader can be used to start the data transmission from the ends of the chain. The cost is very small since the token size is very small.

- PEGASIS performs data fusion at every node except the end nodes in the chain. Each node will fuse its neighbors data with its own to generate a single packet of the same length and then transmit that to its other neighbor (if it has two neighbors).

$$\begin{array}{c} c0 \rightarrow c1 \rightarrow c2 \leftarrow c3 \leftarrow c4 \\ \downarrow \\ BS \end{array}$$

Figure 3.2: Token Passing Approach in PEGASIS [4]

- In figure 3.2, node c2 is the leader, and it will pass the token along the chain to node c0. Node c0 will pass its data to node c1. Node c1 fuses node c0s data with its own and then transmits to the leader c2. After node c2 receives data from node c1, it will pass the token to node c4, and node c4 will pass its data similarly towards node c2.

- Finally, node c2 transmits one message to the BS. Thus, in PEGASIS each node will receive and transmit one packet in each round and be the leader once every 'N' (N is the number of remaining nodes in the chain) rounds.

3.3 HEED Protocol

3.3.1 Overview of HEED

The basic assumption in HEED (Hybrid Energy-Efficient Distributed clustering) is that each sensor node is capable of controlling its transmission power level but they are location unaware. It was proposed by Younis & Fahmy [16] in 2004, this technique was developed as a distributed and energy efficient cluster formation. HEED employs a combination of two different parameters for CH selection i.e. residual energy of each node and node degree. A node can be selected as a CH depending on its residual energy together with some probability. The cluster formation occurs when other nodes in the network choose their respective CHs maintaining minimum cost of communication. The main objective of HEED is to prolong network lifetime as well as supporting scalable data aggregation.

3.3.2 HEED Algorithm

The two clustering parameters which are used in the algorithm are **Residual Energy of the node** as a primary parameter and **Intra Cluster Communication Cost** as a secondary parameter.

Higher the residual energy of the node, higher the probability of that node to become a cluster head (CH). The probability function for the n^{th} node is given by 3.2 [16].

$$CH_{prob}(n) = C_{prob} * \frac{E_{residual}}{E_{max}} \tag{3.2}$$

where , CH_{prob} is the probability of the node, C_{prob} is the initial probability of the node, $E_{residual}$ is the residual energy of the node and E_{max} is the maximum energy of the node initially.

Intra Cluster Communication Cost depends upon node degree and the Average Minimum Reachability Power (AMRP) of the cluster head (CH). That is, lower the node degree and AMRP, higher the chance of a node to become a cluster head. Here, node degree is defined as the number of neighboring nodes in the range of the node in consideration, and AMRP of n^{th} node is given by 3.3 [16].

$$AMRP(n) = \frac{\sum_{i=1}^{M} MinPower_i}{M} \tag{3.3}$$

where, AMRP is the average minimum reachability power of the n^{th} node if it becomes CH, $MinPower_i$ is the minimum power required by i^{th} node in the range of n^{th} node to communicate with it and M is the total number of nodes in the range of the n^{th} node.

At the start of each round, CH selection happens as described below:

INITIALIZE: Each node is initialized as described below.

- Each node calculates its cost(node degree and AMRP) and send it to every other node in its range.
- Each node is initialize with a starting or initial probability given by 3.2 (usually C_{prob} is 0.05).
- The probability should never be minimum than a threshold probability P_{min} (usually 0.0001).

REPEAT: The process described below is repeated for each node until it has CH_{prob} = 1 or the maximum number of iterations (usually 6-10) is reached for that node which is set prior to start of the network.

- Each node will select its CH with the lowest cost from a set of tentative CHs which are in its range. It may select itself if it is a part of that set.
- Otherwise, Each node will generate a random number and if that number is less than or equal to its own CH_{prob}, then it becomes a part of the tentative CHs set.
- At the end of each iteration, every node will double its CH_{prob} value (max limit is 1).
- If any node reached to $CH_{prob} = 1$, it puts itself in the set of final CHs and this process is stopped for this node.

FINALIZE: To conclude the CH selection process.

- Each node will find a CH with lowest cost from the set of final CHs which are in its range and join it.
- If a node doesn't have a CH in its range then it becomes a final CH to communicate with the base station(BS) directly and joins the set of final CH for other nodes in the range.

Thus, with appropriate choice of max iterations, minimum probability(P_{min}) and initial probability(C_{prob}), High energy nodes will exit HEED in short number of iterations by becoming a CH and lower energy nodes have to choose CH from the set of final CHs.

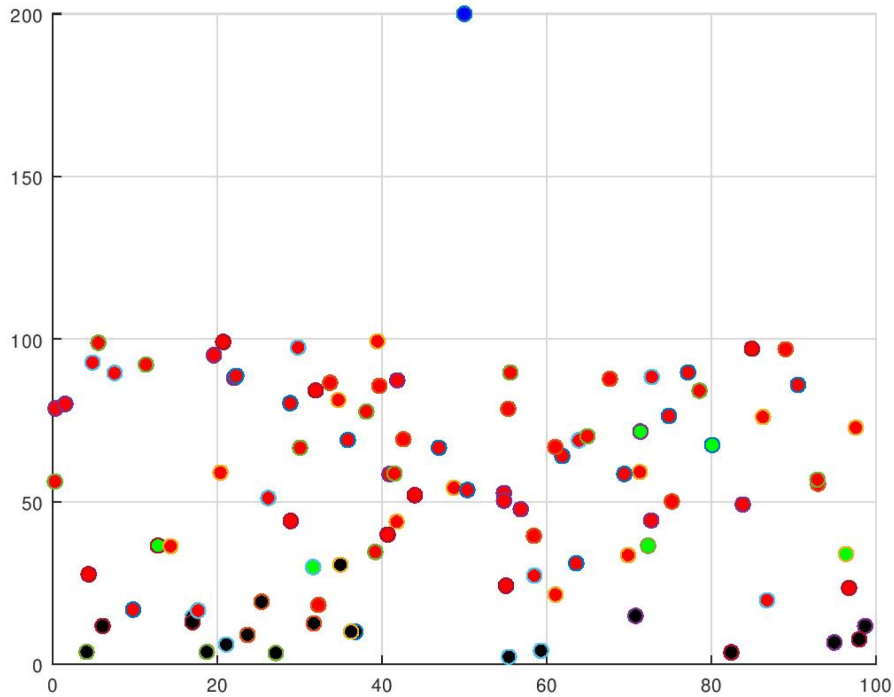
Chapter 4

Simulation Details

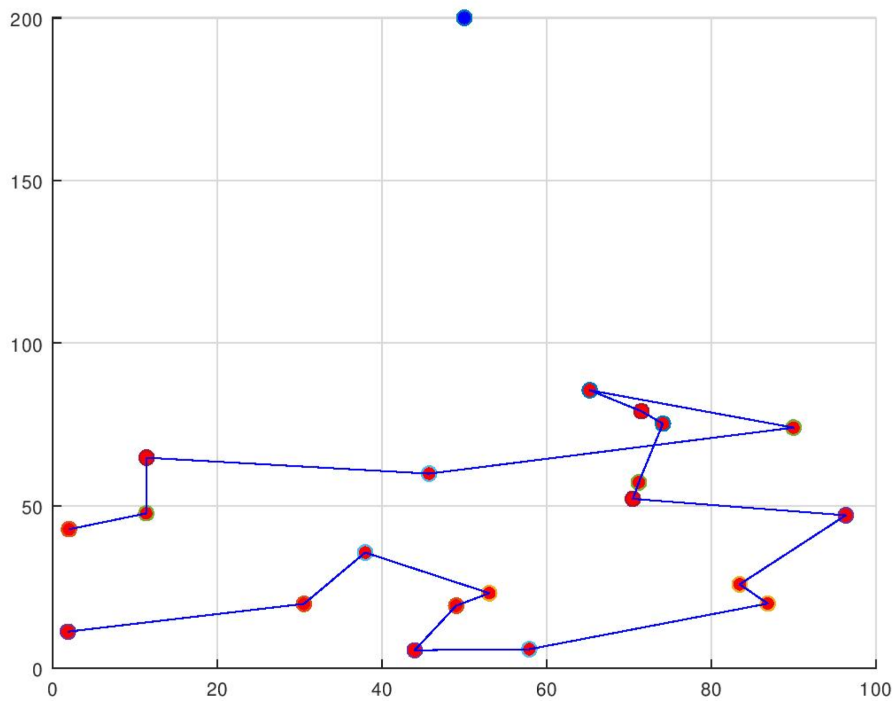
The simulation of LEACH, PEGASIS and HEED was done in GNU OCTAVE. Some simulation plots has been shown in figure 4.1. Here, we are going to describe some of the important aspects of the simulation like assumptions, simulation parameters, simulation network environments and energy dissipation model.

4.1 Assumptions

- The network is homogeneous i.e. all nodes have equal initial energy at the time of deployment.
- The network is static and nodes are distributed randomly.
- There exists only one static base station which is positioned depending upon the environment (described later) chosen.
- The energy of sensor nodes cannot be recharged after deployment of network. i.e. the sensors are not reusable.
- Sensor nodes are not equipped with GPS so they are location unaware.
- No power and computational constraints on Base Station (BS).
- Deployed nodes can use power control to vary the amount of transmission power, which depends on the distance to the receiver.
- we assume all sensors are sensing at a fixed rate and thus always have data to send to base station.



(a) LEACH plot for 100 nodes at round 1334, dead nodes 20, cluster heads 6



(b) Chain formation in PEGASIS for 20 nodes

Figure 4.1: Some simulation plots

4.2 Simulation Parameters

The simulation parameters which were used in our simulation are described below in table 4.1.

Sr.no.	Simulation Parameters	Values
1	E_{elec} (Electronics energy loss per bit)	50 nJ
2	E_{fs} (Free space energy loss per bit per m^2)	10 pJ
3	E_{mp} (Multi-path fading energy loss per bit per m^4)	0.0013 pJ
4	E_{aggr} (Data Aggregation energy loss per bit)	5 nJ
5	Packet length (bits)	2000
6	P (Desired fraction of cluster heads in LEACH)	0.05
7	P_{min} (Minimum probability to be a cluster head in HEED)	$5*10^{-4}$
8	C_{prob} (Initial probability to be a cluster head in HEED)	0.05
9	Iterations (Number of iterations to select cluster heads)	6

Table 4.1: Simulation Parameters

4.3 Network Environments

We selected four network environments and simulated the above mentioned routing protocols in these environments. They are described below in table 4.2. Also, the nodes were given randomized locations each time the network was initialized.

Environment	Number of nodes	Area (m^2)	Base station location(m)	Initial energy(J)	Cluster Range (For HEED)(m)
1	100	100 X 100	(50 , 200)	0.5	25
2	200	200 X 200	(100 , 400)	1	50
3	500	500 X 500	(250 , 1000)	5	125
4	1000	1000X1000	(500 , 2000)	10	250

Table 4.2: Four kinds of simulation environments

4.4 Radio Energy Dissipation Model

Wireless communication is the main part of energy dissipation in WSN. The energy dissipation model used in our simulation is shown in figure 4.2 [5] and is described below in eqn. 4.1 , 4.2 , 4.3 and 4.4. Also we assume that the radio channel is symmetric in nature i.e. energy required to send a packet from node A to node B will be equal to energy required to send a packet of same length from node B to node A.

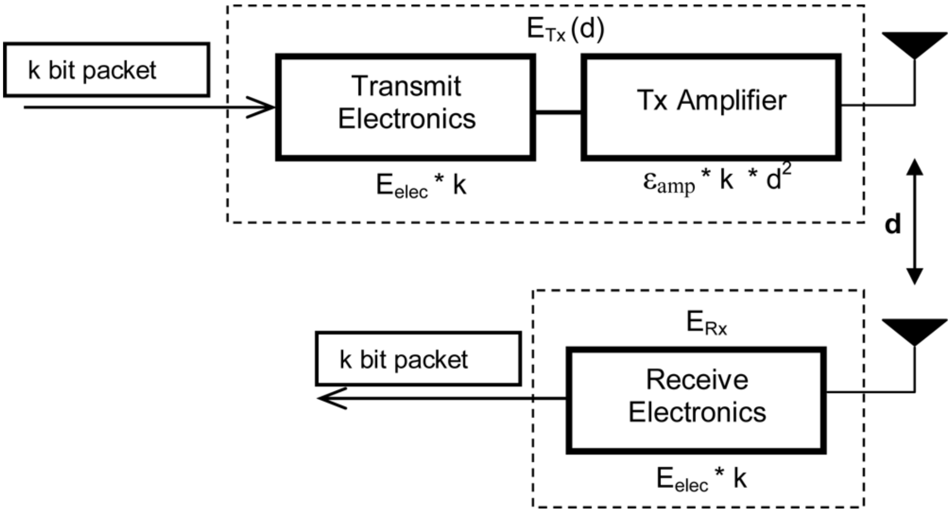


Figure 4.2: Radio Energy Dissipation Model in WSN [5]

The energy cost of transmission (E_{Tx}) is given below in eqn. 4.1 [16].

$$E_{\text{Tx}} = \begin{cases} k * E_{\text{elec}} + k * E_{\text{fs}} * d^2 & \text{if } d <= d_0 \\ k * E_{\text{elec}} + k * E_{\text{mp}} * d^4 & \text{if } d > d_0 \end{cases} \tag{4.1}$$

Here, 'k' is packet length in bits, 'E_{elec}' is the electronics energy loss per bit, 'd' is the distance upto which the data has to be transferred, 'E_{fs}' is the free space energy loss per bit per m^2, 'E_{mp}' is the multi-path fading energy loss per bit per m^4, and d_0 is the crossover distance which is defined below in eqn. 4.2 [16].

$$d_0 = \sqrt{\frac{E_{\text{fs}}}{E_{\text{mp}}}} \tag{4.2}$$

Therefore, Depending upon the transmission distance, both the free space (E_{fs}) and multi-path fading (E_{mp}) models are used in our energy dissipation model.

The energy cost for reception (E_{Rx}) is given below in eqn. 4.3 [16].

$$E_{\text{Rx}} = k * E_{\text{elec}} \tag{4.3}$$

Here, 'k' is packet length in bits, 'E_{elec}' is the electronics energy loss per bit.

The energy cost for data aggregation (E_{aggr}) is given below in eqn. 4.4 [16].

$$E_{\text{aggr}} = k * E_{\text{da}} \tag{4.4}$$

Here, 'k' is packet length in bits, 'E_{da}' is the data aggregation energy loss per bit.

Chapter 5

Result Analysis

5.1 Result of the Simulation

The simulation results obtained from the 4 network environments shows the overall relative behaviour of LEACH, PEGASIS and HEED and is compared on metrics such as Load Balancing, Network Lifetime, Energy Consumption, and Scalability. The table 5.1 shows a summarized result of nodes death and the number of rounds of each protocol in each environment for comparing their behaviour.

Environment No.	Protocols	No. of rounds		
		First Node Dies	Half Node Dies	Last Node Dies
Env.:1	LEACH	1165	1611	2209
	PEGASIS	1877	2090	2362
	HEED	207	947	2384
Env.:2	LEACH	255	669	1729
	PEGASIS	1236	2663	3600
	HEED	63	498	1867
Env.:3	LEACH	22	114	432
	PEGASIS	507	1919	3412
	HEED	6	192	673
Env.:4	LEACH	1	17	80
	PEGASIS	1	324	882
	HEED	1	59	236

Table 5.1: Dead Nodes vs. Number Of Rounds

5.1.1 Graph Plots of LEACH, PEGASIS and HEED :

Figure 5.1, 5.2, 5.3 and 5.4 shows the graph of each protocol in the 4 environments. Each figure has 4 sub plots describing the Total Energy, Dead Nodes, Average Energy and Variance of Nodes Energy in the Network vs. Number of Rounds of protocol operations.

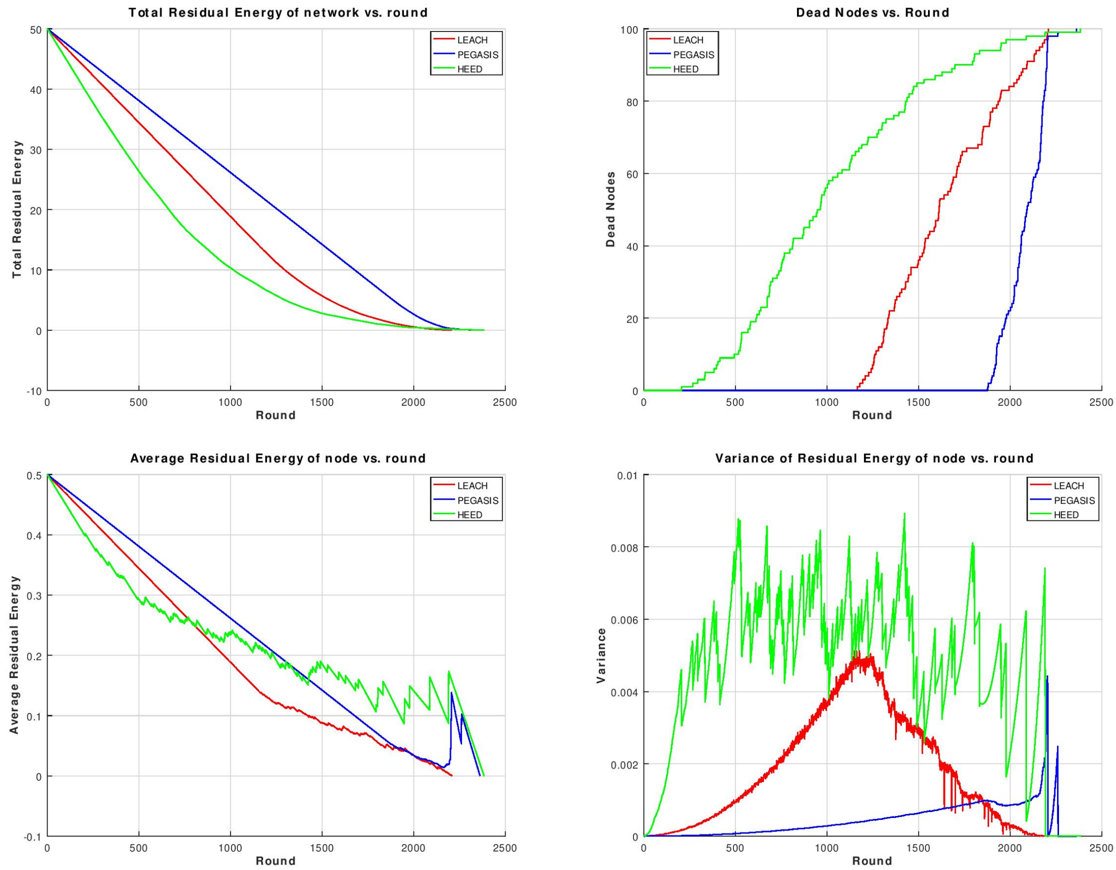


Figure 5.1: Graphs for Environment: 1

5.2 Interpretation of the Result

The graph plots obtained from the simulation describes the performance of each protocol in the simulated environment and can be interpreted on the following metrics :-

Energy Consumption: The higher the total residual energy of the network for any protocol at any given round, the lower the energy consumption and higher the energy efficiency of the protocol. From the sub plots of Total Residual Energy vs. Round, we can observe that the PEGASIS residual energy curve is above the other two curves in every environment, even when the size of network was increased to 1000 nodes and the network area to 1000

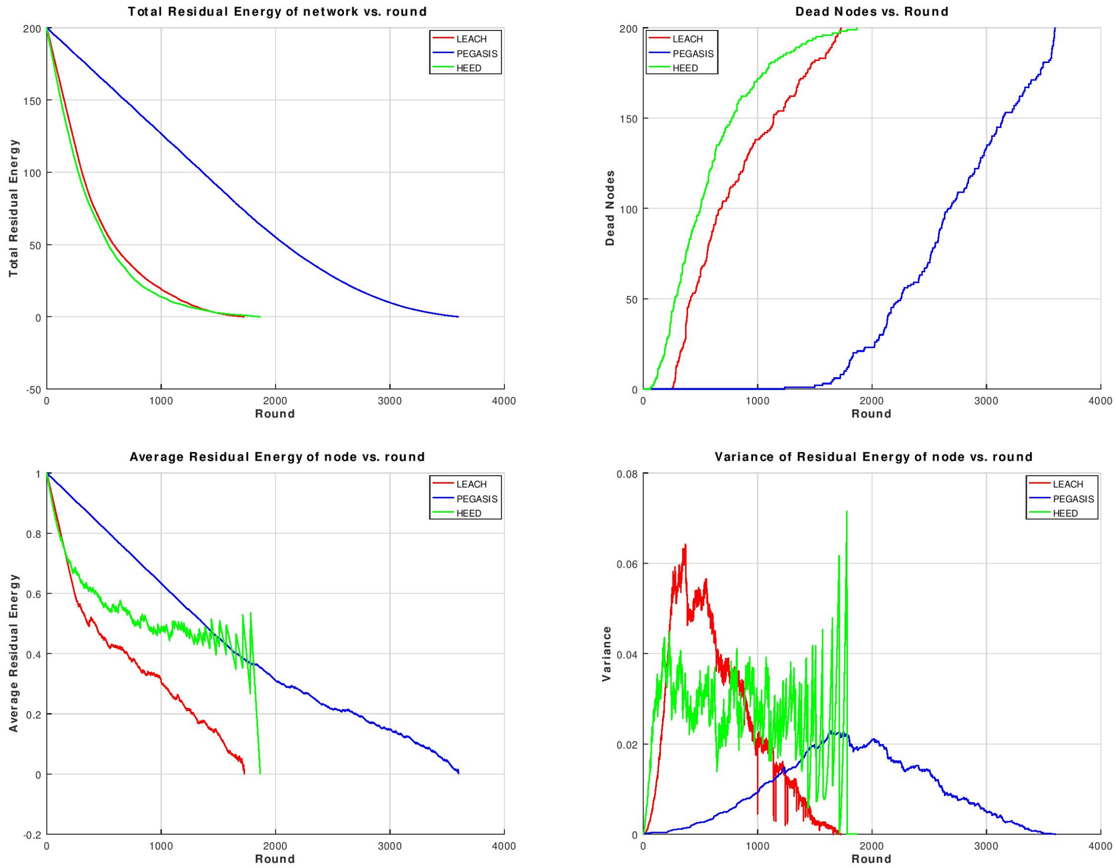


Figure 5.2: Graphs for Environment: 2

X 1000 m^2, so it is highly energy efficient as compared to other two protocols. LEACH on the other hand is better than HEED for smaller network like Environment 1 and 2 but, as the network size increases, HEED becomes better than LEACH as we can observe in graph plots of Environment 3 and 4.

Load Balancing: Load balancing in WSN [9] is the act of balancing the network traffic load on the entire network such that most of the nodes survive longer and consume similar amount of energy in transferring of data from one point to the other. From the sub plots of Average Residual Energy vs. Round and the Variance of the Nodes Residual Energy vs. Round, we can observe that the average residual energy of the nodes at any given round is higher in PEGASIS and the variation in each nodes' residual energy is lower, than in LEACH and HEED in every environment i.e. PEGASIS balances the network load better than other two protocols in every environment.

Stability Period: It is defined as the number of rounds from the starting round after which the first node dies [11]. For many applications, the stability period should be higher to cover the entire network for most of the rounds to get better quality of service from the network. From the data shown in table 5.1 and the sub plots of Dead Nodes vs. Round of

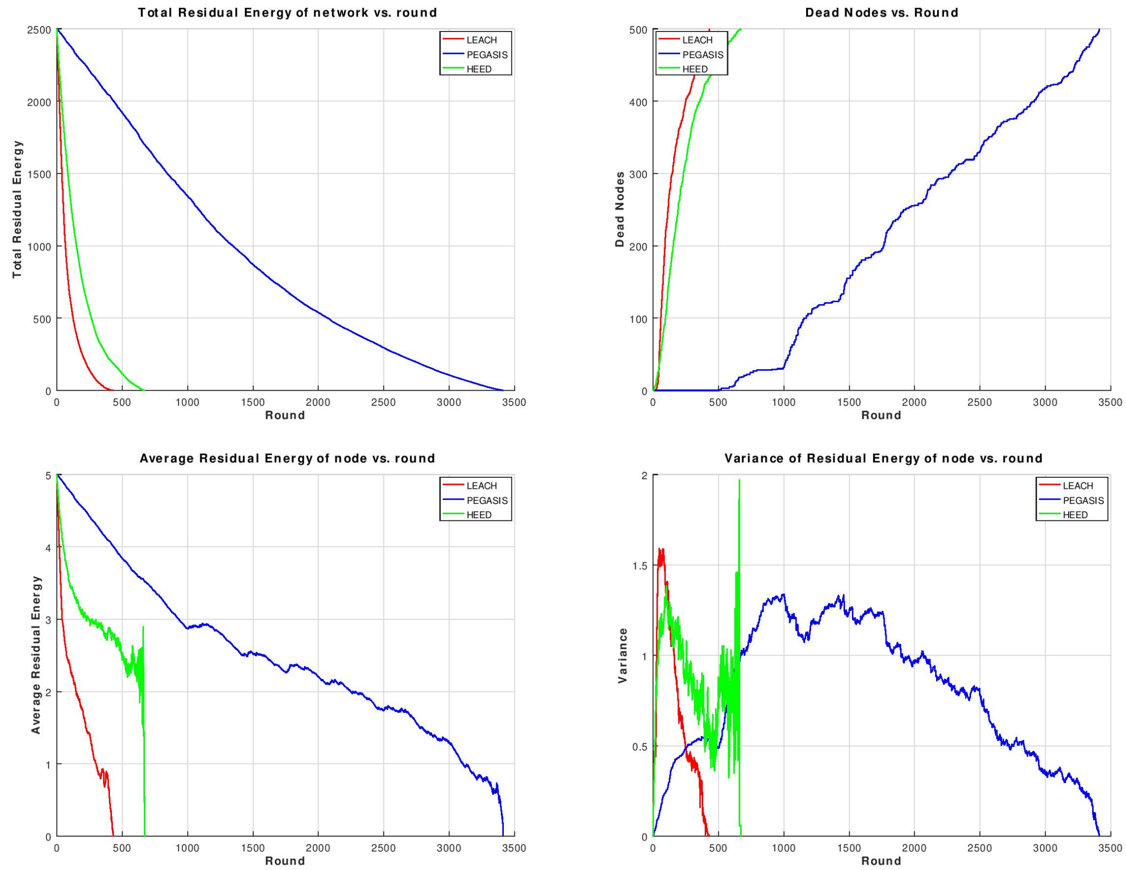


Figure 5.3: Graphs for Environment: 3

each environment, we can observer that the stability period of PEGASIS is far better than the other two protocols.

Network Lifetime: It is defined as the total number of rounds for which the protocol runs until the last node dies [16]. From the sub plots Dead Nodes vs. Round in every graph, we can observe that PEGASIS has the highest network lifetime, followed by HEED and the lowest network lifetime is for LEACH in every environment.

Scalability: Scalability is the property of a system to handle a growing amount of work by adding resources to the system [9]. In WSN, increasing the network size should not reduce the effective performance of the network. From the graph, we can observe that although the total rounds decrease as size increases, but the gap in performance of all the protocols becomes more noteworthy. PEGASIS is scalable as compared to other two protocols as their total rounds decreases heavily and could not withstand higher network sizes.

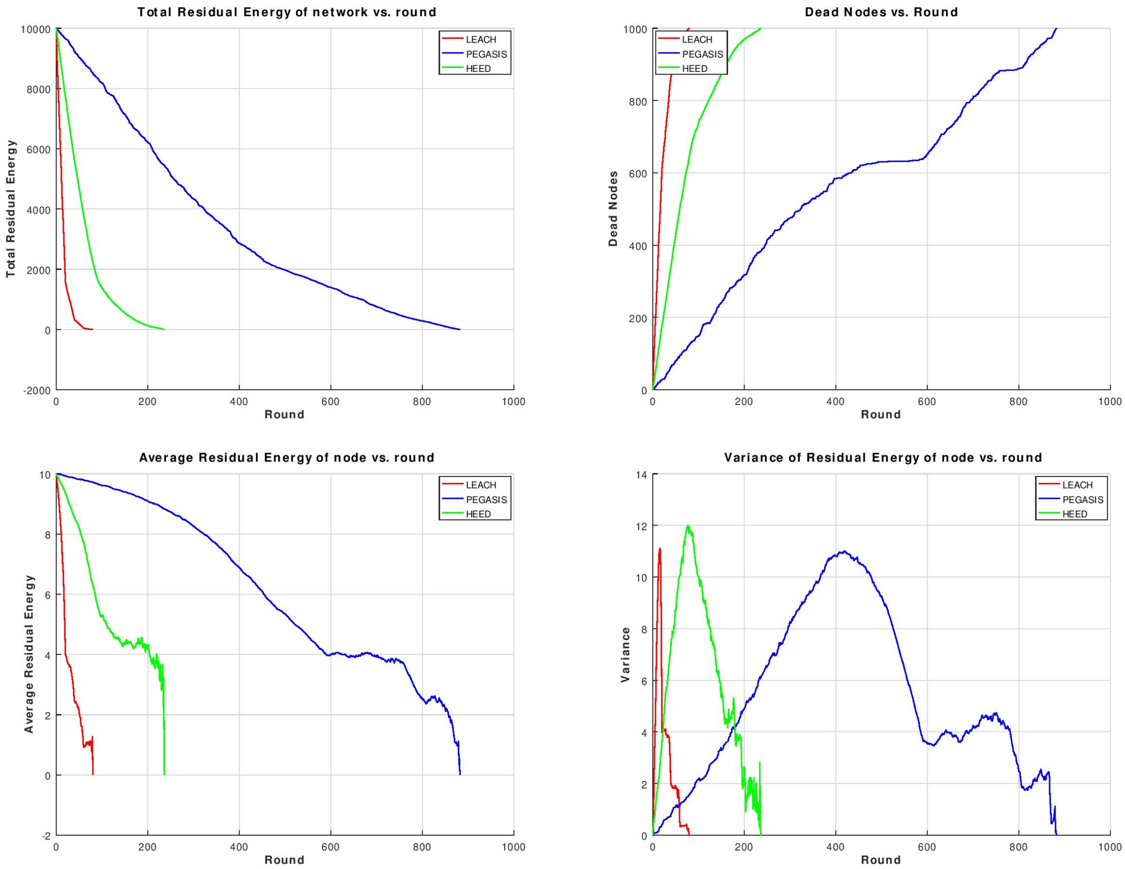


Figure 5.4: Graphs for Environment: 4

Chapter 6

Conclusion and Future Direction of Work

6.1 Conclusion

From the simulation results, we can conclude that PEGASIS is highly energy-efficient protocol as compared to LEACH and HEED when scalability is also one of the factors or design issues of WSN. This is because PEGASIS has two main objectives. First, reduce the power required by each node to transmit data per round by using collaborative techniques and spread the power draining uniformly over all nodes. Second, allow only local coordination between nodes that are close together so that the bandwidth consumed in communication is reduced. Also, The aggregated data is sent to the base-station by only one node in the chain and every node in the chain takes turns in sending the data to the base-station. Unlike, LEACH and HEED, it avoids cluster formation and thus reduces clustering overheads too. Hence, PEGASIS performs better on all the metrics in consideration i.e. load balancing, stability period, network lifetime and scalability. Although more mature results can be found out if the analysis was done on the field sensor networks instead of simulation. Furthermore, WSN routing protocols is still a vast field of research and more scalable and energy-efficient protocols is needed for data gathering in wireless sensor networks.

6.2 Future Direction of Work

There are many potential applications in the field of wireless sensor networks and a number of directions for future work.

One possible future work is to analyse the contention and schedule based protocols at MAC layer when the deployment of the sensor nodes are randomized for a delay constrained, reliable, high throughput and energy-efficient wireless sensor network protocols.

Another possible work is to analyze the localization algorithms in WSN so that local location information can be found out without the use of GPS on energy-constrained sensors and use it to develop a better, energy-efficient and low latency routing protocols in order to increase the life span of network nodes in harsh environments like oil fields, gas fields, forests, chemical factories and underground mines etc, and how to find the position of mobile node with Distributed, Range-based and Beacon-based localization technique in harsh environments which can further increase the quality of service given by wireless sensor networks.

One can also work on analysis of security issues and their possible solutions in WSN as with the increasing development of ubiquitous computing, the demand for WSN and their possible applications will also increase, which will then demand the security of such applications.

Bibliography

[1] M.A. Matin and M.M. Islam. Overview of wireless sensor network. In Mohammad A. Matin, editor, *Wireless Sensor Networks*, chapter 1. IntechOpen, Rijeka, 2012. doi: 10.5772/49376. URL `https://doi.org/10.5772/49376`.

[2] Noman Shabbir and Syed Rizwan Hassan. Routing protocols for wireless sensor networks (wsns). In Philip Sallis, editor, *Wireless Sensor Networks*, chapter 2. IntechOpen, Rijeka, 2017. doi: 10.5772/intechopen.70208. URL `https://doi.org/10.5772/intechopen.70208`.

[3] H. Guyennet M. Hadjila and M. Feham. A chain-based routing protocol to maximize the lifetime of wireless sensor networks. *Wireless Sensor Network*, 5(5):116–120, 2013. doi: 10.4236/wsn.2013.55014. URL `http://www.scirp.org/journal/PaperInformation.aspx?PaperID=31780`.

[4] S. Lindsey and C. S. Raghavendra. Pegasis: Power-efficient gathering in sensor information systems. In *Proceedings, IEEE Aerospace Conference*, volume 3, pages 3–3, March 2002. doi: 10.1109/AERO.2002.1035242.

[5] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. In *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, volume 2, page 10, Jan 2000. doi: 10.1109/HICSS.2000.926982.

[6] Bhanu Pratap Singh Jyoti Singh and Subhadra Bose Shaw. A survey on leach-based hierarchical routing protocols in wireless sensor networks. *International Journal of Engineering Research & Technology (IJERT*, 3(6), JUNE 2014. ISSN 2278-0181.

[7] Ali Newaz Bahar Shamim Sardar, Angona Sarker. Hierarchical routing protocol in wireless sensor network a survey. *International Journal of Scientific & Engineering Research*, 6(2), FEB 2015. ISSN 2229-5518.

[8] Dr.A.E.Narayanan C.Narmadha, Dr.P.Marichamy. A survey on hierarchical-based routing protocols for wireless sensor networks. *International Journal of Pure and Applied Mathematics*, 119(16), 2018. ISSN 663-3676.

[9] Yuanchang Zhong, Lin Cheng, Liang Zhang, Yongduan Song, and Hamid Reza Karimi. Energy-efficient routing control algorithm in large-scale wsn for water environment monitoring with application to three gorges reservoir area. *The Scientific World Journal*,

2014:9, 2014. doi: 10.1155/2014/802915. URL http://dx.doi.org/10.1155/2014/802915.

[10] Pu-Tai Yang and Seokcheon Lee. A distributed reclustering hierarchy routing protocol using social welfare in wireless sensor networks. *International Journal of Distributed Sensor Networks*, 8(4), 2012. doi: 10.1155/2012/681026. URL https://doi.org/10.1155/2012/681026.

[11] Georgios Smaragdakis, Ibrahim Matta, and Azer Bestavros. Sep: A stable election protocol for clustered heterogeneous wireless sensor networks. 2004.

[12] Li Qing, Qingxin Zhu, and Mingwen Wang. Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks. *Computer Communications*, 29(12):2230 – 2237, 2006. ISSN 0140-3664. doi: https://doi.org/10.1016/j.comcom.2006.02.017. URL http://www.sciencedirect.com/science/article/pii/S0140366406000727.

[13] Satish Kannale Gaikwad Ranjitkumar Sharnappa and Vireshkumar Swamy. Enhanced leach multipath based energy efficient routing for wireless sensor network. *International Journal of Advanced Research in Computer and Communication Engineering*, 4(6):6, 2015. ISSN 2278-1021. doi: 10.17148/IJARCCE.2015.4613. URL https://www.ijarcce.com/upload/2015/june-15/IJARCCE\%2013.pdf.

[14] D. Dudgeon and R.Mersereau. In *Multidimensional Digital Signal Processing*, chapter 6. Prentice-Hall,Inc., 1984.

[15] C.Reed D.Chen K.Yao, R.Hudson and F. Lorenzelli. Blind beamforming on a randomly distributed sensor array system. In *Proceedings of SiPS*, Oct 1998.

[16] O. Younis and S. Fahmy. Heed: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. *IEEE Transactions on Mobile Computing*, 3(4): 366–379, Oct 2004. ISSN 1536-1233. doi: 10.1109/TMC.2004.41.

Curriculum Vitae

Name:	**Rohit Jain**
Contact Address:	75/141, Sanganer , Jaipur-302033 Rajasthan, India
email:	rohitjain9314@gmail.com
contact number:	9929899222
Academics:	Pursuing B.Tech. in Computer Sc. & Engg. branch from N.I.T, Agartala with CPI of 8.16/10. Intermediate from Rawat Public School, Jaipur under (C.B.S.E),Rajasthan with 87% in 2014. High School from Rawat Public School, Jaipur under (C.B.S.E),Rajasthan with 93.1% in 2012.

Name:	**Avinash Kumar**
Contact Address:	Munger , Patna - 811213 Bihar, India
email:	avinasnita115@gmail.com
contact:	7085808029
Academics:	Pursuing B.Tech. in Computer Sc. & Engg. branch from N.I.T, Agartala with CPI of 7.13/10. Intermediate from N.S college H.kharagpur,Munger under (B.S.E.B), Bihar with 74.8% in 2015.

High School from Sri Krishna ram Ruchi High school, Manachater Jamui
under (B.S.E.B), Bihar with 61.2% in 2013.

Name:	**Ashok Bhadu**
Contact Address:	Gugariyali, Jayal, Nagaur-341023 Rajasthan, India
email:	ashokbhadu29d@gmail.com
contact:	8769638218

Academics:	Pursuing B.Tech. in Computer Sc. & Engg. branch from N.I.T, Agartala with CPI of 7.05/10. Intermediate from from Vivekananda Public School Fatehpur, Sikar under (R.B.S.E), Rajasthan with 87.60% in 2014. High School from Govt. Sec School Tanwara,Nagaur under (R.B.S.E), Rajasthan with 67.50% in 2012.

Name:	**Vikash Singh**
Contact Address:	441, Kathariya , Ballia - 221713 Uttar Pradesh, India
email:	vikassingh8112@gmail.com
contact:	8413011254

Academics:	Pursuing B.Tech. in Computer Sc. & Engg. branch from N.I.T, Agartala with CPI of 8.49/10. Intermediate from Central Hindu Boys School, Varanasi under (C.B.S.E), Uttar Pradesh with 88.40% in 2014. High School from Foundation School, Buxar under (C.B.S.E), Bihar with 95% in 2012.