EESCDE: An Energy Efficient SNR-Based Clustering With Data Encryption

Bandita Sahu

Roll. 213CS2169

under the guidance of

Prof. Pabitra Mohan Khilar

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela – 769 008, India

EESCDE: An Energy Efficient SNR-Based Clustering With Data Encryption

Dissertation submitted in

June 2015

to the department of

Computer Science and Engineering

of

National Institute of Technology Rourkela

in partial fulfillment of the requirements

for the degree of

Master of Technology

by

Bandita Sahu

(Roll. 213CS2169)

under the supervision of

Prof. Pabitra Mohan Khilar

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela – 769008, India

Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, India. `www.nitrkl.ac.in`

Dr. Pabitra Mohan Khilar
Professor

May 30, 2015

Certificate

This is to certify that the work in the thesis entitled *EESCDE: An Energy Efficient SNR-Based Clustering With Data Encryption* by *Bandita Sahu*, bearing roll number 213CS2169, is a record of an original research work carried out by her under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of *Master of Technology* in *Computer Science and Engineering Department*. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Pabitra Mohan Khilar

Acknowledgment

First of all, I would like to express my deep sense of respect and gratitude towards my supervisor Prof. Pabitra Mohan Khilar, who has been the guiding and supporting pillar behind this work. From the core of my heart,I thank him for introducing me to the field Wireless Sensor Network and giving me the opportunity to work under him. His confidence and faith in this field and ability to bring out the best of analytical and practical skills in people has been invaluable in tough periods. Without his invaluable advice and assistance it would not have been possible for me to complete this thesis. I am greatly indebted to him for his constant encouragement and invaluable advice in every aspect of my academic life. I consider it my good fortune to got an opportunity to work with such a nice and wonderful person.

I thank our H.O.D. Prof. Shantanu Kumar Rath, Prof. Ashok Kumar Turuk and Prof Bibhudutta Sahoo for their constant support in my thesis work. They have been great sources of inspiration to me and I thank them from the bottom of my heart.

I would also like to thank all faculty members, PhD scholars Sourav ku Bhoi,Soubhagya Shekhar Barpanda and Sampa Sahoo and all colleagues to provide me their regular suggestions and encouragements during the whole work.

At last but not the least I am in debt to my Husband and my son for their support during my hard times.

I wish to thank all faculty members and secretarial staff of the CSE Department for their sympathetic cooperation.

Bandita Sahu

Abstract

In this decade, Under Water Sensor Network (UWSN) has become important in order to explore the underwater environment. The characteristics of UWSN such as limited energy, low bandwidth, high propagation delay, and error rate has made the design of clustering protocol challenging, due to the energy constrained sensor nodes. As the unpleasant environmental condition of the underwater, replacement of the battery is neither simple nor cheap. Therefore, energy saving is considered to be an important issue. A new clustering protocol is proposed which is named as energy efficient SNR based clustering in UWSN with Data Encryption (EESCDE). The residual energy of the nodes is considered for the improvement of the network lifetime of the sensor network. Using the proposed scheme, the improvement in the residual energy is achieved by reducing the number of transmission of the cluster head as well as the sensor nodes. The sensor nodes are partitioned into clusters and the cluster heads (CH) are chosen depending on the SNR values. Symmetric encipherment is implemented using the hill cipher to achieve the security of the sensed data.

In Clustered-Underwater Wireless sensor networks (CUWSNs), battery operated sensing devices are grouped and connected with each other through wireless interfaces. Energy and processing efficiency are the two important parameters in these systems. CUWSNs with reduced number of transmissions utilize less energy and prolong the lifetime of the network. A new protocol is proposed which is named as selective data transmission in SNR based cluster (SCSD). In this protocol, clusters are formed and the cluster heads (CH) are chosen depending on the SNR values. The number of transmissions of the cluster head and the sensor nodes are reduced by selectively transmitting the data. It also avoids congestion problem. This scheme has been implemented using NS3 and it is observed that the residual energy of the sensor nodes are improved by 10 percent as compared to the algorithm, Efficient Secure Routing Protocol For SNR based Dynamic Cluster (ESRPSDC), and by 2 percent as compared to direct data transmission.

Keywords: Signal-To-Noise Ratio (SNR), Underwater Sensor Network(UWSN), Residual Energy, Data Encryption

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 INTRODUCTION

1.2 Introduction

Wireless Network, Ad-Hoc network, and Wireless Sensor Network (WSN) related to each other. Wireless network is the superset of all. Ad-Hoc network is the middle one between wireless network and WSN as described in figure 1.1. These networks have certain constraints on the memory capacity, available source energy and processing capability of the sensor node. The sensor nodes are placed in human inaccessible and hostile environment so, the Wireless networks are usually assumed to be energy restrained.

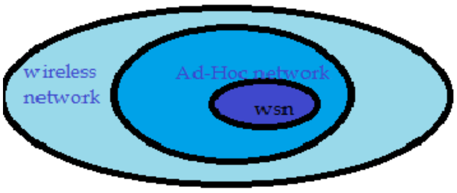


Figure 1.1: Wireless Sensor Network as Subset of Wireless Network.

A WSN consists of a set of autonomous sensor nodes, distributed spatially. Those nodes monitor the physical or the environmental conditions cooperatively. The nodes communicate with each other wirelessly. A WSN may include hundreds or even thousands of nodes. Data are transmitted from the Source nodes to destination nodes through some intermediate nodes. This destination node is connected to base station.

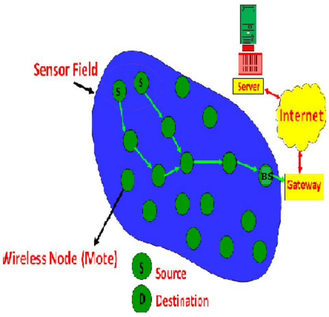


Figure 1.2: A Wireless Sensor Network.

1.3 Basic Components of WSN

The WSN consist of two main components:

- Sensor Nodes
- Base Station (Central Gateway).

1.3.1 Sensor nodes

A sensor network is a network of sensor nodes, which are capable for processing, and gathering the sensory information. They communicate with other nodes connected in the network.

Various components of a sensor node are as follows

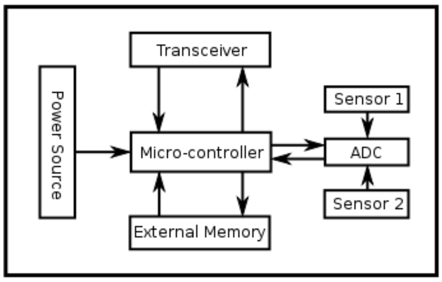


Figure 1.3: Architecture of a sensor node.

- Microcontroller
- Transceiver
- External memory
- Power source
- Sensor

Microcontroller

The responsibility of the microcontroller is to perform tasks, process data and control the functionality of other components in the sensor node. Microcontroller is commonly used, as it is less costly, flexible, ease of programming, and consumes less power. Whereas, microprocessor is considered not to be suitable for sensor node as it consumes more power.

Transceiver

The wireless transmission media used for communication are as follows

- Radio Frequency (RF): Most of the WSN applications relevantly communicate using this signal. WSNs tend to use license-free communication frequencies: 173, 433, 868, and 915MHz; and 2.4GHz.

- Optical Communication (laser): It takes less energy. For such communication Line -Of -Sight is needed. This signal is sensitive to atmospheric conditions.
- Infrared: It has limited broadcasting capacity but no antenna is needed like lasers. Generally, transceivers have built-in state machine. These machines are capable to perform operations automatically. If the transceivers are operating in idle mode,then the amount of power consumed is almost equal to the power consumed in receiving mode. Thus, when it is not transmitting or receiving any data,it is better to shut down. To transmit a data packet, A significant amount of power is consumed as the transceiver switches from sleep mode to transmit mode.

1.3.2 E

xternal memory: Memory requirement is application dependent. Generally Flash memories are used due to low cost and storage capacity. Based on storage purpose memory can be of two types.(i) User memory: Those are used for storing application related or personal data, and (ii) Program memory: Those are used for programming the device.It also contains the device identification data, if present.

1.3.3 P

ower source: Batteries or capacitors are used to store power.Both rechargeable and non-rechargeable batteries are used to supply power to the sensor nodes. Since the wireless sensor nodes are deployed in a human inaccessible location, Charging and changing the battery become costly and inconvenient.

1.3.4 S

ensors: Sensors are the hardware devices that sense data from the surrounding environment. If there is any change in physical or environmental condition, it creats its response for each change. Sensors measure physical data of the parameter to be monitored. A sensor node is generally small in size. These are autonomous, consume low energy, and operate unattended. These are very much adaptive to the environment. As wireless sensor nodes are typically very small electronic devices, they can only be equipped with a limited power source of 1.2-3.7 volts less than and 0.5-2 ampere-hour .Sensors are of three types:

- Passive omnidirectional sensors
- Passive narrow-beam sensors
- Active sensors

Passive sensors sense the data passively. They do not manipulate the environment actually by active probing. These are considered to be self powered. The energy is needed for those sensors are only to amplify the analog signal. Whereas, the active sensors manipulate the surrounding by sending actively probe to the environment. A sonar or radar sensor is of this type. They require continuous energy from a power source. Narrow-beam sensors have a predefined notion of direction of measurement, similar to a camera. Omnidirectional sensors measures the data from any direction.

1.3.5 Base Station

In wireless communications, the Base Station is assumed to be a transceiver that is connected to a number of other devices to one another. It also acts as a router for computers the network to connect them to the internet. As compared to sensor nodes the base station has larger memory and more computational power. It is connected to a better energy source than batteries. The base station is considered as an entry point to the WSN where its primary task is to collect data from sensor nodes in WSN. It forwards the gathered data to a remote server. The basic components of a base station are as follows

- Transceiver: It is also called a gateway node. The gateway node is a special, sensorless node which is connected to the host computer and provides an interface between the base station and sensor network.

- Base station software: Software is to be understood as a program running on the host computer which communicates with sensor nodes through the gateway node and stores received data to a database.

- Host computer: A host computer is imagined as a regular personal computer.

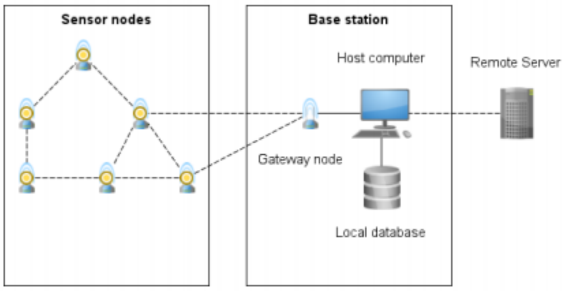


Figure 1.4: Architecture of a Base station.

1.4 Underwater Sensor Network

In this decade, UWSN has become one of the most attractive research areas for exploring the underwater environmental condition . A large number of applications are enabled by UWSN such as monitoring the environmental condition for scientific application, navigation assistance, oil monitoring disaster prevention, and much more. UWSN can be categorized into three types [2] such as: i) mobile UWSN for long term application, ii) static UWSN for short term application and iii) Mobile UWSN for short term application. The proposed protocol comes under the second type of UWSN which is able to resolve various issues related to UWSN's characteristics. The basic task of this is to improve the residual energy of the nodes and the lifetime of the sensor network. When the battery is depleted, it becomes difficult and also expensive to replace it due to the unpleasant environmental condition underwater. Therefore, efficient energy utilization is to be implemented to improve the residual energy. For better energy utilization and improving the lifetime of the network, the following approaches are considered. i) The workloads of all the sensor nodes are equally divided among themselves in the route from source to destination. ii) Reducing the number of transmissions.

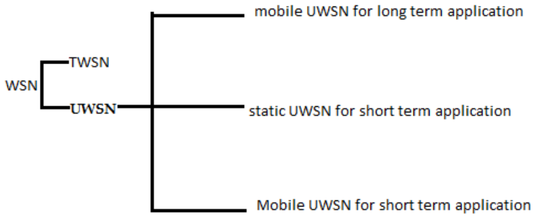

WSN
TWSN
UWSN
mobile UWSN for long term application
static UWSN for short term application
Mobile UWSN for short term application

Figure 1.5: Hierarchy of WSN.

1.4.1 Communication Media in UWSN

In underwater communication systems informations are transmitted in the form of sound, electromagnetic (EM), or optical waves. However, each technique has some advantages and disadvantages.

- Acoustic communication: It is a widely used technique in underwater environments due to its less signal reduction (attenuation) of sound in water. This is suitable for thermally stable, and depth water environment. In shallow water acoustic waves can be affected by temperature gradients and surface ambient noise. The slower speed of acoustic propagation in water is about 1500 m/s.

- Electromagnetic (EM) waves: Due to the conducting nature of the medium, conventional radio signal is not suitable in an underwater environment.

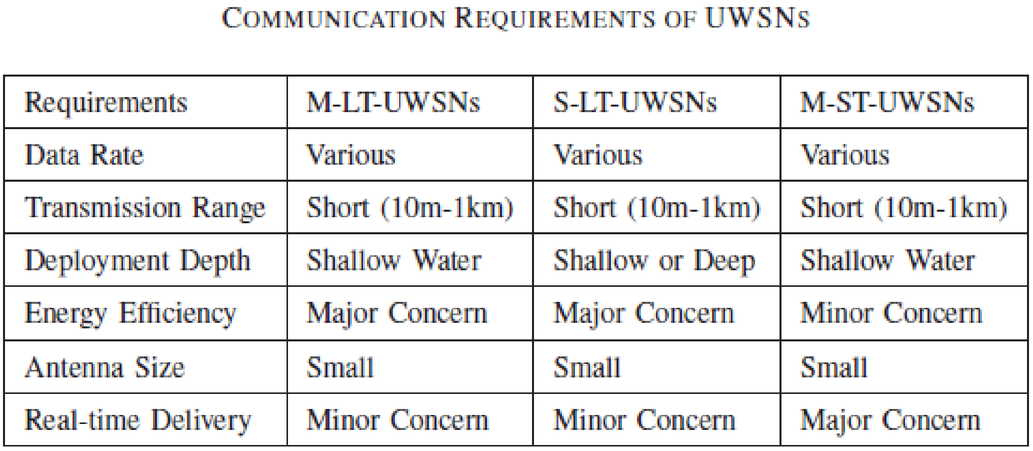
However, it has high propagation speed. Nodes are communicated efficiently using this wave.

- Free-space optical (FSO) waves:

  These are used as the communication carriers wireless medium. Due to the severe water absorption at the optical frequency band such waves are limited to very short distances . It provides a high-bandwidth communication (10-150 Mbps) .

1.4.2 Communication Requirements

The UWSNs also include sparse mobile AUV (autonomous underwater vehicle) or UUV (unmanned underwater vehicle) networks, where vehicles or the sensor nodes can be spaced out by several kilometers. The communication requirements for such networks are listed in the following table.



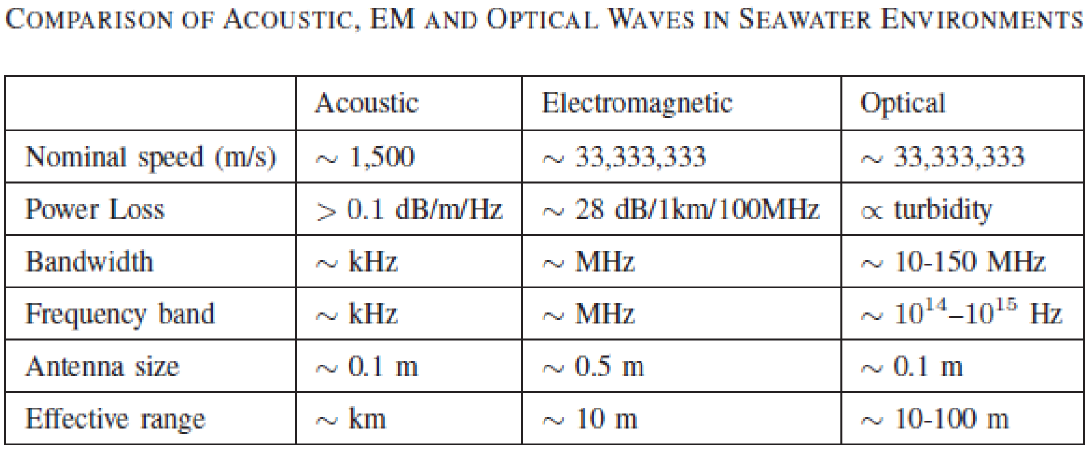
COMMUNICATION REQUIREMENTS OF UWSNS

Requirements	M-LT-UWSNs	S-LT-UWSNs	M-ST-UWSNs
Data Rate	Various	Various	Various
Transmission Range	Short (10m-1km)	Short (10m-1km)	Short (10m-1km)
Deployment Depth	Shallow Water	Shallow or Deep	Shallow Water
Energy Efficiency	Major Concern	Major Concern	Minor Concern
Antenna Size	Small	Small	Small
Real-time Delivery	Minor Concern	Minor Concern	Major Concern

Figure 1.6: Communication Requirements of WSN

1.4.3 Comparison of waves

The waves underwater vary in their characteristics. The acoustic waves is the slowest one among those three with limited bandwidth. Other characteristics of each waves are listed in the table below.



COMPARISON OF ACOUSTIC, EM AND OPTICAL WAVES IN SEAWATER ENVIRONMENTS

	Acoustic	Electromagnetic	Optical
Nominal speed (m/s)	$\sim$ 1,500	$\sim$ 33,333,333	$\sim$ 33,333,333
Power Loss	$>$ 0.1 dB/m/Hz	$\sim$ 28 dB/1km/100MHz	$\propto$ turbidity
Bandwidth	$\sim$ kHz	$\sim$ MHz	$\sim$ 10-150 MHz
Frequency band	$\sim$ kHz	$\sim$ MHz	$\sim 10^{14}$–10^{15} Hz
Antenna size	$\sim$ 0.1 m	$\sim$ 0.5 m	$\sim$ 0.1 m
Effective range	$\sim$ km	$\sim$ 10 m	$\sim$ 10-100 m

Figure 1.7: Communication Requirements of WSN

1.4.4 Routing in UWSN

Forwarding the data from source nodes to the sink node is very challenging in UWSNs. In mobile UWSNs routing is considered to be a critical issue for long-term applications. Thus, energy saving is a major concern in such networks. There exist various protocol, such as Directed Diffusion, and TTDD Dissemination. These protocols are generally designed for static networks. So as to discover data delivery paths, powerful method like query flooding usually employed. In mobile UWSNs, most sensor nodes are mobile, and the network topology changes very rapidly.

1.4.5 Threats to Security Goals

There are three types of security goals: first is Confidentiality, second is Integrity and third is Availability. But these goals are strongly affected by the malicious drivers. Confidentiality is affected by:

- Snooping: To Access the unauthorized information.
- Traffic Analysis: To Analyze the traffic (collection of information/transactions).

Integrity is affected by:

- Data Modification: To intercept and modify the data.
- Replay Attack means saving a copy of the data and later use it for replaying.
- Masquerading: means impersonating some other node by providing fake data and advertises itself as a legal node.
- Repudiation: Denial of message sending.
- Global Positioning System Attack: means providing fake and false position information by intercepting the message.
- Sybil Attack: means generating identities and cheating with fake identities.
- Message Tempering: means modification of messages.
- Position Cheating/Faking: means providing fake information about positions.
- Tunneling: creates a tunnel and inject the fake data.
- Message Alteration: means physical damage of inter-node

Availability is affected by:

- Black Hole Attack: means dropping of packets which creates disruption in the network.

- Denial of Service: means sending bogus requests by which the vehicles are overloaded and crashed.
- Spamming: increases the latency in the system.

1.5 Motivation and Research challenges

Since WSNs are deployed in human inaccessible and hostile environment, they should use the available energy efficiently. In recent years, the improvement in residual energy is an important parameter in the field of WSN. It is quite impossible to replace or recharge the battery of the sensor nodes. Less energy utilization leads to a longer lifetime. But due to the environment, improving the residual energy has become a challenging job for the researchers. Also, it needs the security of the data that the sensor nodes transmit. The major motivation that leads to study WSN are listed as:

- The residual energy of the sensor nodes in WSN can be improved.
- The sensed data are to be saved from the intruders by implementing data encryption mechanism.
- Selection of Cluster Head is an important parameter to be focused that leads to better energy utilization.

1.6 Problem Statement

The problem addressed in this thesis are the research challenges highlighted in the previous section. Sensor nodes are partitioned into groups called clusters. The cluster heads are selected depending upon the SNR value [3]. Single-hop communication is possible between the Base Station and the sensor nodes. However, due to transmission loss and noise, the quality of the signal degrades. To achieve better signal at the receiver side Cluster Heads are selected. The sensor nodes transmit the sensed data to their respective heads and then it is transmitted to the base station. The number of transmissions is reduced to reduce the energy utilization. The data sensed by the sensor nodes are encrypted to accomplish the security mechanism.

1.7 Thesis organization

The present thesis is organized into five chapters.

1. Chapter 1 presents introduction and the importance of residual energy problem in WSN. Furthermore, research challenges and the problem statements are included here.

2. Chapter 2 includes the literature review where we have described some existing works on clustering.

3. Chapter 3 presents model for SNR based clustering, with its various phases and algorithms. This chapter includes the Cluster Head selection process. An algorithmic approach to encrypt the sensed data is presented in this chapter. In this chapter various assumptions made for the system model and the simulated results are described.

4. Chapter 4 presents a reduced data transmission model for WSN and analyses the impact of the number of transmissions on residual energy. An algorithmic approach is considered for computing the energy consumption.

5. Chapter 5 concludes the work done, highlighting the contributions and suggests the directions for possible future work on efficient energy utilization and data security.

Chapter 2

Literature Review

2.1 Introduction

Wireless Sensor Network (WSN) is of three types. Such as i) Underwater Sensor Network (UWSN), ii) Terrestrial Sensor Network (TSN), and iii) Sky Sensor Network(SSN). UWSN explores the environmental condition underwater such as temperature, pressure, oil monitoring and many more. It is again categorized into three types [4] such as i) mobile UWSN for long term application, ii) static UWSN for short term application and iii) Mobile UWSN for short term application. First type of UWSN is deployed in shallow water with various data rate,small antenna size and short transmission range. The second one is suitable for both shallow as well as depth water. Rest of the requirements are same as the former one. The third type of UWSN is same as the first one but it is used for Short term application. TSN is deployed at the ground level.It uses radio signal as its communication media. The antenna size of such network is larger than that of UWSN. It is also implemented with high transmission range. SSN is suitable at extra low power,and high data rate sensor network application. It has integrated sensors, radio, antenna, microntroller, and capabilities.

Many techniques are developed to improve the lifetime of the WSN. Clustering is an important one of them. It is defined as a technique to partition the sensor nodes into different group called clusters [4]. In this group only one node is responsible for communicating with the base station (BS) and called as the cluster head (CH). The rest of the nodes in the clusters are called as the non-cluster head (NCH) or the followers. These nodes cannot directly transmit data to the base station so; they sense the data and transmit it to the corresponding CH. Since the NCHs are closer to CH as compared to the BS they take less energy to transmit the data as a result more energy conservation is possible and hence by improving the residual energy and network lifetime. Several clustering techniques have already been developed to achieve those above goals.

Yi et al. [5] have proposed a clustering technique based on the overhearing concept. It is named as PEACH, that stands for power efficient and adaptive clustering hierarchy.

Figure 1 describes the architecture of this protocol. When a packet is transmitted from a node its source and destination are recognized by the use of overhearing characteristic. No additional packet like an advertisement or announcement message is required here. The clusters are formed without overhead transmission. It is an adaptive multilevel clustering technique, which is operated on probabilistic routing. PEACH can work in both of the casees, whether the location information of the sensor node is available or not. It can be categorized in to two types. If the location information is available, it is said to be Location Aware PEACH otherwise it is called as Location Unaware PEACH. This technique minimizes the energy utilization of each node and extends the lifetime of the network. It suffers from the limitations such as: reception of unnecessary packets dissipates the residual

Chavda and Pareshkotak [6] have introduced Hybrid Energy Efficient Distributed clustering (HEED), which is based on the residual energy of the sensor nodes. In this technique, the CHs heads are periodically selected depending upon two parameters. The first parameter is the residual energy of the sensor nodes and

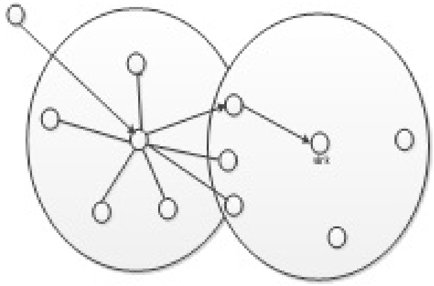


Figure 2.1: Architecture of PEACH [5]

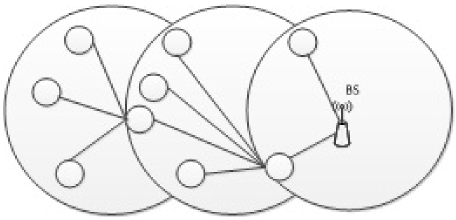


Figure 2.2: Architecture of HEED [6]

the second parameter is the node degree or the propinquity of a sensor node to its neighbour node. Figure 2 shows the architecture of this protocol. HEED uniformly distributes the CHs across the network and form the cluster. Due to this uniform distribution it balances the load and enhances the network lifetime by conserving more energy. But the periodic cluster head selection or rotation needs extra energy to rebuild the clusters. The nodes communicate with their corresponding cluster head, among them, or between a cluster head and a base station [6], which increases the communication overheads.

Lindsey and Raghabendra [7] have developed a chain based protocol, named as Power Efficient gathering in sensor information system (PEGASIS). The architecture of this protocol is shown in figure 3. In this protocol, data collected from one node to the neighbour node, gathered, fused and transmitted to the next neighbour node. One designated node called as the chain leader, will transmit the data to the sink. PEGASIS assumed that, the global information about the network is known to all

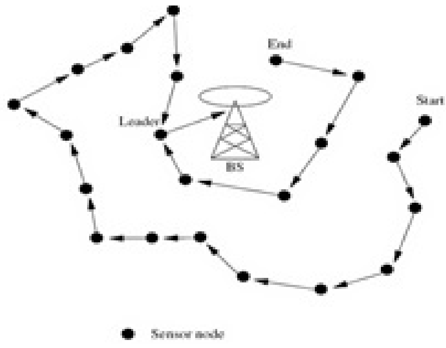


Figure 2.3: Architecture of PEGASIS [7]

the sensor nodes. As data is transmitted from one node to its neighbour node, transmitting distance is reduced. But due to the data fusion takes place at each node energy usage is more. The presence of one header node causes network delay. Redundant transmission is required in this technique as the data received by each header node are at most two.

Chavda and Pareshkotak [6] and Handy et al. [8] proposed a protocol, called as Low Energy Adaptive Clustering Hierarchy (LEACH). It is a cluster-based routing protocol that uses the distributed concept for cluster formation. A few sensor nodes are randomly selected as cluster heads (CHs) and this role is rotated to evenly distribute the load among the sensors nodes. CH receives data from other sensor nodes (the cluster members), compresses it and sends an aggregated packet to the BS. Therefore the amount of information transmitted to the BS is reduced. Figure 4 shows the architecture of Leach. It suffers from various limitations such as: as it uses single-hop routing, it is applicable to networks deployed in small regions only, it consumes more energy because of the overheads arises due to dynamic clustering. The complexity of the algorithm increases because of the two phases, the set up phase and the steady phase.

Ganesh and Amutha [3] have introduced ESRPSDC, that is efficient and secure routing protocol through SNR based dynamic clustering. In this technique, the CHs are selected based on the energy. The NCH nodes which are not able to communicate

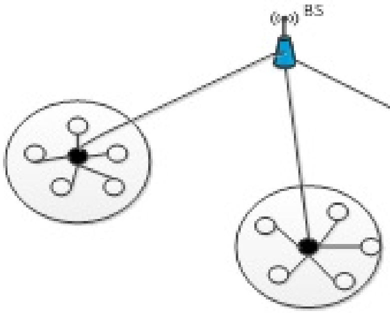


Figure 2.4: Architecture of LEACH [6][8]

with any of the CH due to its limited radio ranges, connected to a new CH that is selected depending upon the SNR value. Due to the dynamic clustering mechanism, more energy is consumed by the sensor nodes. In this technique, the complexity of the algorithm increases so as to execute two phases of CH selection such as energy based and SNR based. ESRPSDC has not been implemented with any encryption mechanism [2].

The following table compares various protocols.

Table 2.1: Protocol Comparison

Protocol	Energy Utilization	Designed for	Hop	Communication	Phases	Application
LEACH	moderate	homogeneous	single	CH	set up and steady phase	Continuous monitoring
HEED	less	heterogeneous	single	CH	initialization, setup, and steady	environmental monitoring
PEGASIS	less	homogeneous	multi	leader	chain formation and broadcasting	disaster management
PEACH	moderate	homogeneous	multi	CH	Cluster formation and data transmission	automation, robot control
ESRP	less	homogeneous	multi	CH	Initialization, CH selection,data transmission	environmental monitoring
EESCDE	very less	homogeneous	multi	CH	initialization,CH selection,data encryption, and data transmission	disaster management, submarine detection

Chapter 3

EESCDE Protocol

3.1 Introduction

One of the most important technologies, which is widely used in the 21st century is the UWSN, where each sensing device is called the sensor node[1][4][5]. The node senses the data from surrounding environment and converts them into the electrical signal. These nodes are responsible for gathering, processing and transmitting the data to the specified sensor node. A large number of applications are enabled by UWSN such as monitoring the environmental condition for scientific application, navigation assistance, oil monitoring disaster prevention and many more. Underwater Sensor Networks (UWSN) use acoustics signal as its communication media. The propagation delay of the acoustic signal is 1500 m/s that is higher than that of the radio signal. Due to attenuation and high absorption rate of acoustic signals the available bandwidth is limited [13].Since UWSNs are deployed in human inaccessible, hostile,and unpleasant underwater environment, replacement and recharging of the battery is not possible The proposed protocol is able to resolve various issues related to the characteristics of UWSN. In this work, we propose an energy efficient secured SNR based clustering protocol for UWSN for short term application to monitor the underwater environment. The basic task of this is to improve the residual energy of the nodes and the lifetime of the sensor network. Eficient energy utilization is implemented in this paper to improve the residual energy. For better energy utilization and improving the lifetime of the network, the following approaches are considered.

- i) The workloads of all the sensor nodes are equally divided among themselves in the route from source to destination,
- ii) Reducing the number of transmissions.

This chapter includes two contributions

- i) we propose an energy efficient clustering algorithm
- ii) we use HILL cipher for preventing the sensed data of different sensor nodes from the intruders.

3.2 System Model

The system model consists of three parts such as

- i) Model assumptions and notations
- ii) UWSN model
- iii) Energy and data model.

3.2.1 Model Assumptions and Notations

The system model notations are enlisted in Table 2. The sensor nodes are homogeneous in nature. All nodes are implemented with equal frequency, voltage, intensity, average capacitance switch per cycle, electronic energy dissipation, amplifier energy dissipation, processor constant, wind constant, leakage current, and weighing factor. However, the energy value supplied may vary from one sensor node to another sensor node. The location of the Base Station is assumed to be fixed. Each sensor node is responsible to transmit the sensed data to the corresponding Cluster Head. Fixed numbers of nonoverlapping clusters are formed. Each cluster has only one Cluster Head.

3.2.2 UWSN Model

A UWSN is modeled as a graph (G), consisting of a set of vertices (V), and a set of edges (E), where G= (V, E). The set of vertices V= V1, V2, V3, . . .Vn corresponds to sensor nodes in UWSN. Similarly, the set of edges E= E1, E2, E3, . . .EM correspond to set of communication links in UWSN. The following equalities hold such as$|V| = N$ and $|E| = M$. The sensor nodes sense the data from the underwater environment using sensing range (r). The sensed data are communicated to other sensor using the communication range (c). If a data d comes under the sensing range r of a sensor node S i, the data d can be sensed. The data which are beyond the sensing range of a sensor node can not be sensed. Similarly a node S i can communicate with another sensor node S j, if and only if, the $distance(Si, Sj) <= c$. The distance is the distance between the sensor node S i and S j. The sensor nodes can communicate to their one-hop neighbor only. In order to allow the communication between a pair of nodes which we referred as the one-hop neighbor, a set of sensor nodes are used as intermediate nodes, thereby forming a multi-hop communication network. We assume that UWSN form an arbitrary network topology with connectivity k. SNR is an important parameter to measure the signal quality. The SNR values of each sensor nodes are computed with respect to the Base station (BS). A fixed number of Cluster heads(CHS) are chosen depending on those values with the constraint that, only one CH in each cluster.

Table 3.1: Table 1:Notation Parameters

Symbols	Meaning
b	Packet size
b1	Packet size of the cluster head
BS	Base station
Cavg	Average capacitance switch/cycle
CH	Cluster Head
d	Euclidean distance
Eamp	Amplifier energy dissipation
Eelec	Electronic energy dissipation
f	Frequency
h	Weighing factor
H	Depth
I	Intensity
I0	Leakage current
Nc	Number of clock cycle
Np	Processor constant
NS	Noise due to shipment
NT	Noise due to turbulence
NTH	Thermal noise
NW	Noise due to wind
Psignal	Power signal at the sink
Pnoise	Noise Power
S	Shipment constant
SL	Power signal at the source level in db
SNR	Signal to Noise Ratio
TL	Signal loss during transmission in db
Vsup	Supply voltage to sensor node
Vt	Thermal voltage TP Transmission power
W	Wind constant

3.2.3 Energy And Data Model

After each transmission and reception of data, the residual energy of the sensor nodes are computed. The consumed energy is of three types such as transmission energy, reception energy, and processing energy. The sensor nodes process the data and the amount of energy consumed [3] is computed as in the following table. The parameter b1 is the total packet size of a cluster, which can be obtained as, $b1 = b * number\ of\ sensor\ nodes\ in\ that\ cluster$.

Table 3.2: Energy Consumption

Consumed Energy	CH	NCH
Transmission Energy	$E_{TXCH} = h*b*E_{elec} + b1*d*E_{amp}$	$E_{TX} = b*E_{elec} + b*d*E_{amp}$
Reception energy	$E_{RCCH} = h*b1*E_{elec}$	$E_{rc} = b*E_{elec}$
Processing Energy	$E_{procCH} = h*E_{procN}$	$E_{procN} = b*N_c*C_{avg}V_{sup}^2 + b*V_{sup}*(I_0*e^{V_{sup}/N_p*V_t})*N_c/f$

3.3 Proposed Algorithm

The proposed algorithm consists of two sections

- i) Algorithm descriptions
- ii) Algorithm analysis.

The first section describes the working of the designed algorithm and the second part gives the analysis of that algorithm.

3.3.1 Algorithm Description

It consists of four phases such as:

1. Initialization phase

2. CH selection phase

3. Data encryption phase

4. and Data transmission phase

The first phase describes, how the nodes are deployed and what are its parameter to be initialized. Similarly the second phase describes the method of forming the cluster and finds the CH. The third phase provides security to the sensed data using an encryption mechanism. The last phase describes how data are transmitted from the NCHs to CH and from CHs to BS.

Initialization Phase

In this phase, initially the sensor nodes are created and deployed in a planar region randomly. Those deployed nodes are assigned with some identification such as IP address. The function used for assigning address is address.Assign(). Address of the nodes are generated randomly. An address range is set in the system. Each address, which is assigned to the sensor nodes is within this range. The node parameters like initial energy, transmission power, frequency, depth etc. are initialized. The BS is deployed with more energy and its location is kept fixed. It broadcasts a request message to each sensor node.

The graphical presentation of the algorithm is as shown in the Figure: .

Cluster Head Selection Phase

Initially the variables numclust and clusterindex are initialized to zero. These two variables indicate that after initializing the network, no cluster has formed and all the sensor nodes are assumed as NCH. The Euclidean distance of each node from the BS is calculated and accordingly the SNR value of each node is computed with respect to BS. The SNR [8] value is computed as follows:

$$SNRdb = Psignaldb - Pnoisedb \tag{3.1}$$

Algorithm 1 Initialization Phase

```
1: Assign address to each node using the function address.Assign ()
2: Set i=1
3: Receive initialized information such as
4: Node[i].energy ← ienergy
5: Node[i].tpower ← tpower
6: Node[i].freq ← frequency
7: Node[i].depth ← depth
8: Repeat step 2 to 6 until $i$ ! = 50
9: BS sends request message to each node.
```

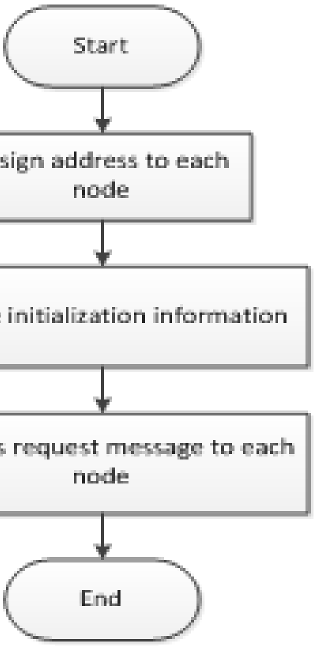

Start
Assign address to each node
Receive initialization information
BS sends request message to each node
End

Figure 3.1: Initilization phase

The meaningful information is represented as Psignal, which is the Power signal received at the sink or the receiver. This is the difference of the power signal generated at the source level [9] and signal loss during transmission and computed as follows:

$$P_{signal} = SL - TL \tag{3.2}$$

, where

$$SL = \frac{10\log I}{0.67 * 10^{-18}} \tag{3.3}$$

$$I = \frac{Tp}{4 * 3.141 * H} \tag{3.4}$$

TL (transmission loss) is dependent upon the distance. For calculating the TL in dB [10] we have taken the reference parameter at 1 m. As the distance of the node from the base station increases the signal level decreases. The loss is directly proportional to the Euclidean distance between the sensor node and the BS. TL in dB can be defined as follows

$$TL = 10\log(a^2 + b^2) \tag{3.5}$$

, where a = BS.xloc-node.xloc and b = BS.yloc - node.yloc

The background noise in the ocean has many sources, which vary with frequency and location. It can be of two types such as: i) man-made noise: caused by machinery and shipping activities and ii) Ambient noise: caused by the movement of water which includes tides, current, storms wind and rain [11]. The overall noise power for a given frequency is defined as :

$$Pnoise = Nt + Ns + Nth + Nw \tag{3.6}$$

, where

$$10\log Nt(f) = 17 - 30\log(f) \tag{3.7}$$

$$10\log Ns(f) = 40 + 20(S - 0.5) + 26\log(f) - 60\log(f + 0.03) \tag{3.8}$$

$$10\log Nw(f) = 50 + 7.5 * W0.5 + 20\log(f) - 40\log(f + 0.4) \tag{3.9}$$

$$10\log Nth(f) = -15 + 20\log(f) \tag{3.10}$$

After calculating the SNR value in this phase, nodes are chosen and their energy values are compared with the threshold energy. If the energy value is higher, then check for their SNR value. As in the flowchart the sensor nodes satisfying the energy and SNR criteria are assumed to be the CH. The nodes having energy less than the threshold value are said to be the non-cluster head (NCH). CH broadcast a hello message and the nodes within the range receive this. Then those nodes send a confirm message to the CH and become the cluster member. The graphical presentation of the algorithm is as shown in the Figure: .

Algorithm 2 Cluster Head Selection Phase

```
 1: Receive the initialized information as in Phase I
 2: Set numclust=0 and clusterindex = 0
 3: Get the location of the sensor node using getloc()
 4: Compute Euclidian distance from the BS
 5: Find the SNR value: Node[i].SNR = SL-TL-$P_{noise}$
 6: Select the Highest SNR value
 7: If ($nodeenergy > thresholdenergy$)
 8: Update the clusterindex to -1
 9: The node as assumed to be a CH and sends hello message
10: The node receives the confirm messages from NCH
11: Increment the numclust value by 1
12: If( numclust != 5)
13: Select the next highest snr value and repeat step 7
14: Else
15: Become the NCH
16: else assumed as a NCH
17: Receive hello message from CH
18: Sends confirm message to the CH
19: Proceed to Data sensing
```

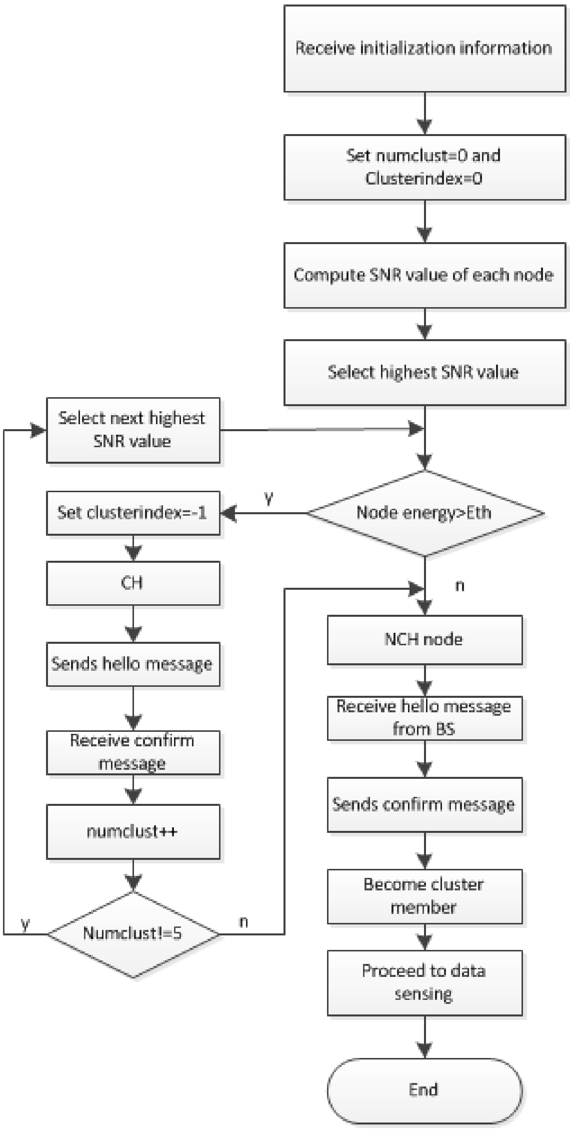


Figure 3.2: CH Selection phase

Data Encryption Phase

In this phase, the cluster index value of a node will be checked. Based on the value of the variable clusterindex the CHs and the NCHs are differentiated. The NCH senses the data and stores it in a buffer. After accessing the initialized key value, it performs encryption by applying the Hill Cipher [12] [20]. It provides data confidentiality as the security service. The cryptanalysis of this type of cipher is difficult because the key size is an m x m matrix. Each entry in the matrix can have values between 1 to 1499 (the chosen prime number). And as the size of the key domain became 1499 mxm, the brute-force attack is extremely difficult. The cryptanalysis of the known-plain text is also not so easy. The key domain is so large and the sender may change the key matrix. Even if the attacker has access to an original-encrypted data value pair, it is difficult to guess the key matrix. Rest two types of attacks those are chosen-plaintext and chosen cipher text, also less likely to happen. In these types of attack the attacker may choose an original data block or encrypted data block which may not be invertible and he does not know the key value which is embedded in the software used by the sender. The sensor node sends the encrypted data to the cluster head (CH). If the sensor node is a CH then it receives the data from all its members, decrypts the data, performs data integration and sends it to the BS.Similarly, the CH will receive the data from various sensor nodes, perform data integration and send it to the BS. Here it is assumed that all sensor nodes and their CH in a particular cluster will use the same key for encryption and decryption. If the residual energy of the CH becomes less than the threshold value, then that node cannot act as a CH for further transmission.

The graphical presentation of the algorithm is as shown in the Figure: .

Data Transmission Phase

Each cluster member is scheduled with a time division multiple access (TDMA) by the CH. This information is broadcast to the cluster members. The data transmission process starts after the cluster is created and the TDMA scheduled is derived. The cluster members are turned on during the allocated time. The NCH or the cluster members initiate data transmission to the corresponding cluster head (CH) with possible minimum transmission power. The energy consumed during the transmission is dependent on the dissipation of electronic energy to start up the transmitter. After receiving all the data from the cluster member the CH decrypt the data using the shared key value. Then the CH performs data integration and

Algorithm 3 Data Encryption Phase

```
1: Sensor nodes sense data
2: Check the clusterindex value
3:
4: If (clusterindex=-1)
5:
6: Assumed to be a CH and receive data
7: Perform data decryption
8: Integrate data
9: Send the data to BS
10:
11: If $(nodeenergy > energythreshold)$
12: go to step 1
13:
14: Else
15: assumed to be NCH
16: Perform data encryption
17: Sen$(nodeenergy > 0)$
18: go to step 1
19: Node dies
```

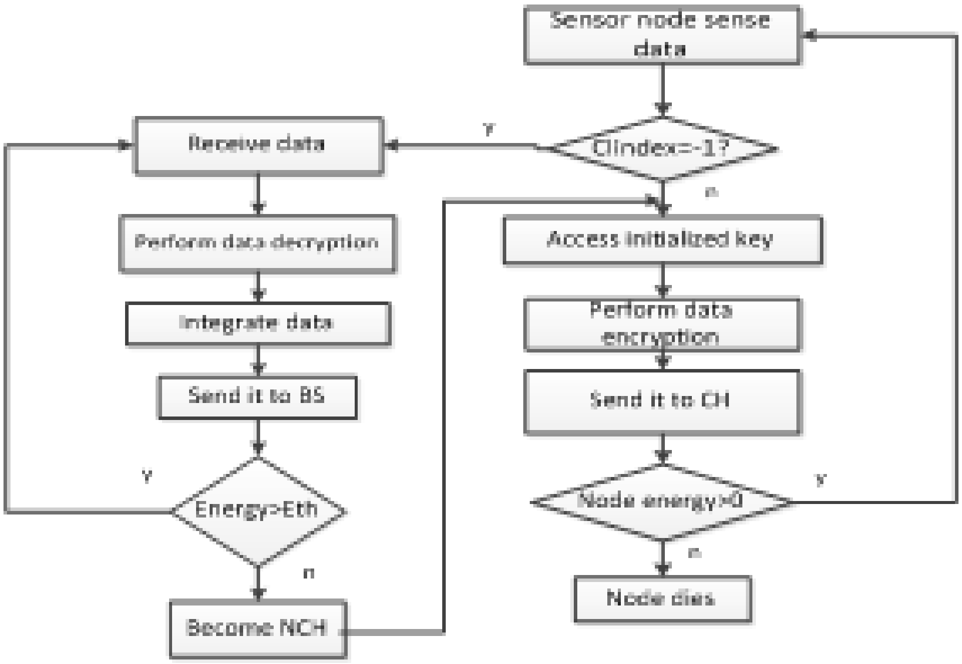


Figure 3.3: Data Encryption phase

compresses it into a single data. This single data will be transmitted to the BS.

Example 1:

Let us consider an example to measure the underwater temperature. The standard sound wave in underwater is 1500m/s. An increase in the wave velocity by 4m/Sec increases the temperature by 1^0c.

step1: Set a grid of 100mX100m and 50 nodes are deployed randomly. Each node is assigned with a unique address. the location of BS is fixed at (50,75) in the grid. Figure 1 shows therandom node deployment with a fixed BS.

step2: The SNR value of each node is computed and stored in sorted form. Let

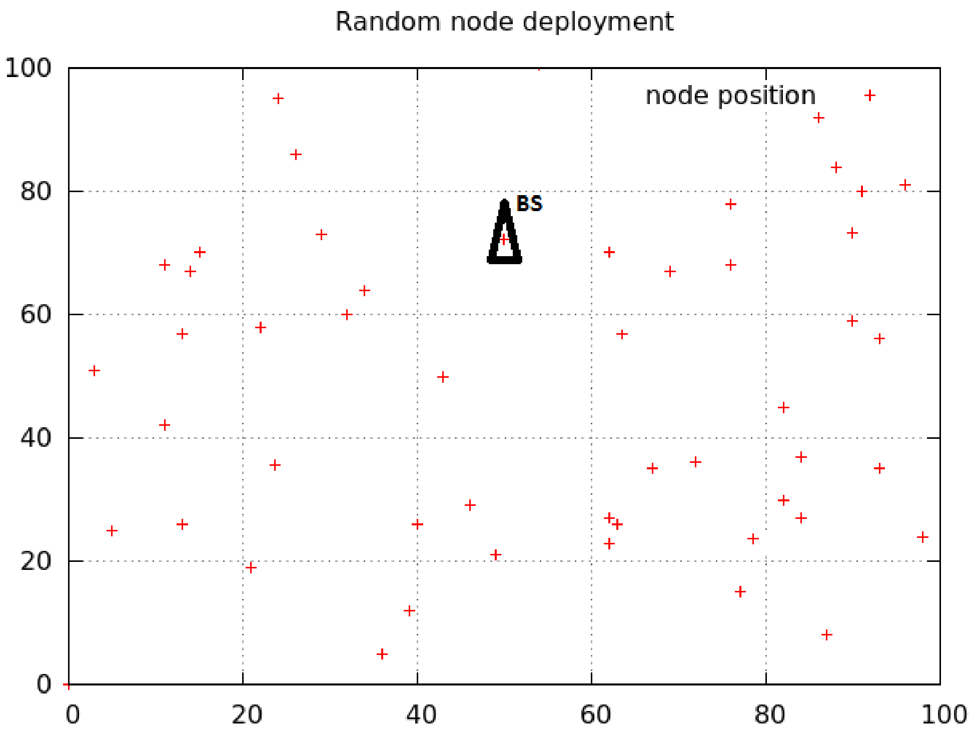


Figure 3.4: Random node deployment

the values are enlisted in table 4. The CHs are selected as . Now consider a communication between a pair of (CH,S_i).

Table 3.3: SNR value of Sensor nodes

Serial number	SNR value	Serial number	SNR value	Serial number	SNR value	Serial number	SNR value	Serial number	SNR value
1	17.770605	11	17.270308	21	17.152811	31	17.083771	41	16.985802
2	16.831207	12	16.823666	22	16.801319	32	16.653517	42	16.637484
3	16.608000	13	16.548714	23	16.355032	33	16.237606	43	16.144936
4	16.099493	14	15.892528	24	15.835801	34	15.443583	44	15.436481
5	15.374161	15	15.320229	25	15.304141	35	15.280247	45	15.052358
6	14.558638	16	14.551729	26	14.518232	36	14.126097	46	14.049298
7	13.948957	17	13.888174	27	13.738029	37	13.331367	47	13.331367
8	13.279752	18	12.888263	28	12.746639	38	12.726056	48	12.253738
9	11.710144	19	11.657891	29	11.646091	39	11.042922	49	10.440712
10	10.007893	20	8.999619	30	8.977273	440	8.608130	50	6.437752

In this step various clusters are formed and and the CHs are selected. Figure 2 shows the cluster, CH, and the NCH in that cluster step3: Let us assume the wave velocity sensed by the sensor node S_i are as following.

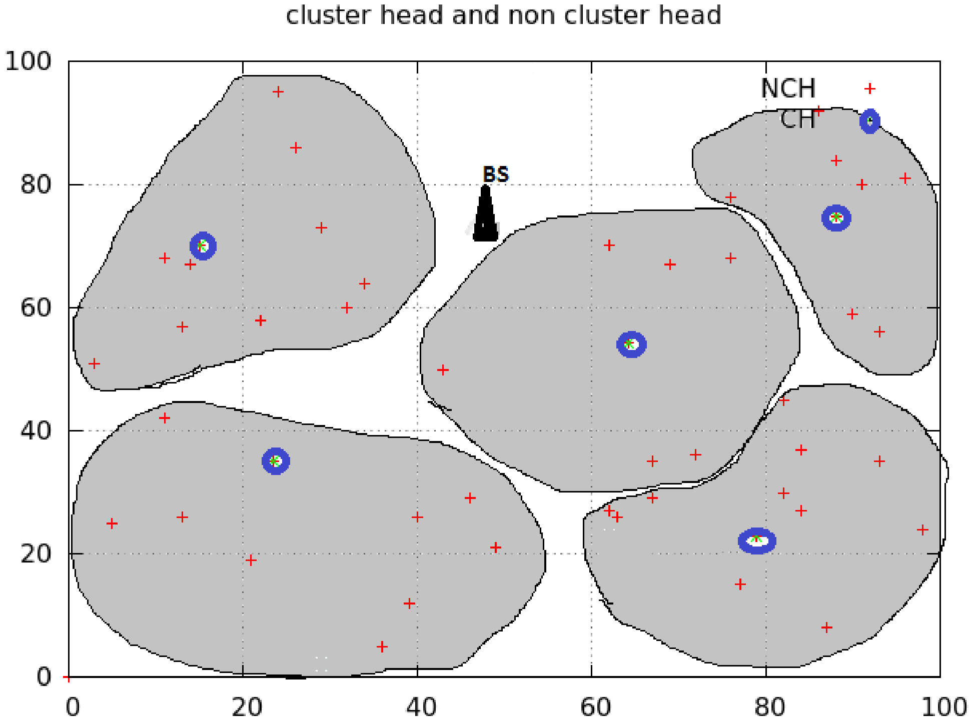


Figure 3.5: Cluster formation

$$\begin{bmatrix} 1500 & 1510 \\ 1520 & 1530 \end{bmatrix}$$

$$\begin{bmatrix} 1500 & 1500 \\ 1500 & 1500 \end{bmatrix}$$

$$\begin{bmatrix} 1510 & 1500 \\ 1510 & 1500 \end{bmatrix}$$

$$\begin{bmatrix} 1520 & 1010 \\ 1500 & 1500 \end{bmatrix}$$

The key value is chosen to be

$$K = \begin{bmatrix} 2 & 3 \\ 3 & 2 \end{bmatrix}$$

According to the hill cipher encryption method, a prime number is chosen to be 1499. Now, the sensor node instead of encoding all the 16 data, it will find out the average of them and then encrypt it.

$$Avg = \begin{bmatrix} 7 & 2 \\ 7 & 7 \end{bmatrix}$$

$$Avgmod1499 = \begin{bmatrix} 8 & 3 \\ 8 & 8 \end{bmatrix}$$

The encrypted value

$$C = \begin{bmatrix} 25 & 30 \\ 30 & 30 \end{bmatrix}$$

Now, the cluster head will get the encrypted data and decrypt it using the provided key values as follows

$$C * K^{-1} mod1499 = \begin{bmatrix} 25 & 30 \\ 30 & 30 \end{bmatrix}$$

$$DecryptedAvg = \begin{bmatrix} 1507 & 1502 \\ 1507 & 1507 \end{bmatrix}$$

Step4: The CH receives 4 data instead of 16. The number of transmission reduced here. The average value of the sensed data are computed as $sensedAvg = 1507 + 1502 + 1507 + 1507$, which is equal to 1506. Now, the CH sends the single data to the BS.

Result: The assumed standard value is 1500 and the value received at the BS is 1506. The difference is 6. Thus, the underwater temperature is increased by 1.5^0.

3.3.2 Algorithm Analysis

In this section, we analyzed the proposed algorithm for its operation in the underwater environment.

- Claim 1: The proposed clustering algorithm is energy efficient. The existing algorithm is a two-step process. The first step is energy based CH selection, and the second step is SNR based CH selection. The participating node consumes more energy due to this two phases. Whereas, the proposed algorithm is a single step process to select theCH. As a result, the participating nodes consumes less energy as compared to the existing one. Thus, it is more energy efficient.

- Claim 2: The Hill cipher algorithm for data security in the underwater environment is feasible. Sensing data in the underwater environment is a continuous process. Instead of sending a single data the sensor sends a block of data at a time. These data are to be protected from the unauthorized users or intruders. Using the HILL cipher algorithm, the block of sensed data are encrypted and sent to the corresponding CH. The HILL cipher is based on the modulus and the key matrix. It makes an adversary difficult to guess the prime number as well as the key value.

- Claim 3: The transmission loss of the proposed algorithm is minimum. While forming the cluster based on SNR values, the CH selects the nearest neighbor as its NCH. Thereby, the SNR values of the nodes increase. The distance between the CH and NCH is reduced. Thus, the transmission loss also decreases.

Table 3.4: Simulation Parameters

Parameter	Value	Parameter	Value
Area of sensing field	100m x 100 m	Packet size	2Kb
Number of sensor nodes	50	Average capacitance switch/cycle	22pF
Topology	Random	Electronic energy dissipation	50nj/bit
Sensor nodes type	Passive omnidirectional	Amplifier energy dissipation	100pj/bit/m2
Number of cluster	5	Leakage current	1.196mA
Network protocol	UDP	Number of clock cycle	0.97*106
Threshold energy	1.5j	Processor constant	21.26
Initial battery power	3.3volt	Thermal voltage	0.2v
Initial energy	2.4j	Depth	4m
Transmission power	2w	Shipment constant	0.5 (uwsn),0(wsn)
Frequency	2.4GHz	Wind constant	0 (uwsn), 0.5(wsn)
Data rate	6Kbps	Weighing factor	1.2
Sensing range	10m	Communication range	20m

3.4 Simulation And Results

In this section, we have evaluated the proposed model using network simulator NS3. In a 100m X 100m planar square region, 50 sensor nodes are deployed randomly. The sensor nodes are assumed to be passive omnidirectional. They do not send any active probe to the surrounding environment to sense data. The location of the BS is fixed at (50,75). The nodes are static in nature and deployed at a depth of 4m from the water surface level. The nodes are partitioned into 5 clusters. In each cluster, only one CH is chosen. All the sensor nodes are identical to each other. The key matrix is same for encryption and decryption. Each ordinary node sends the data packet to the CH independently and identically. The CHs deliver the packet to the BS. The simulation parameters listed in the following table are used for the evaluation purpose.

Observation -I

This observation is based on the comparison of the residual energy and the number of sensor nodes. When the number of nodes increase, the cluster member in each cluster also increases. The CH receives messages from each of its cluster members and hence the reception energy decreases for each message. However,

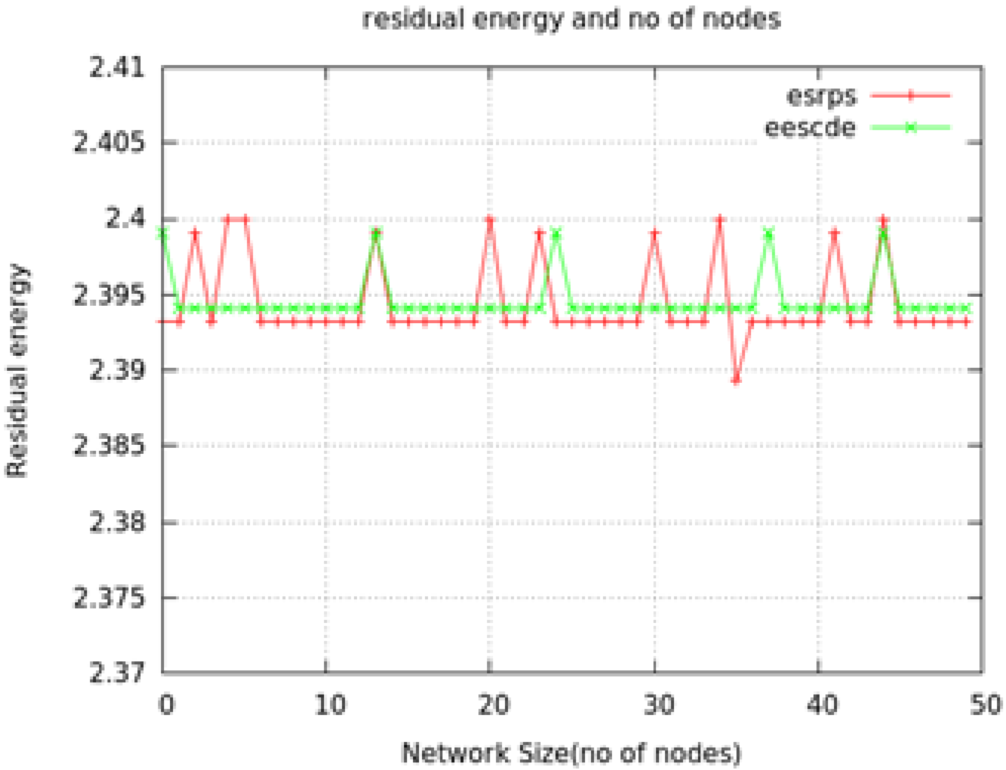


Figure 3.6: comparison of network size versus residual energy in UWSN

transmission energy will be same, as the CH broadcasts message to its cluster member. The nodes which are at the region end will be connected to the nearest CH. Using EESCDE, 10 percent improvement in residual energy is achieved. Figure 3.6 describes this.

Observation-II

Observation -II focuses on the comparison of residual energy and the message complexity. If the no of messages communicated among the sensor nodes increases, the no transmission also increases. Thereby increasing the no of receiving messages also. These two parameters, transmission and reception affect the residual energy of the sensor node. For each of these two activities the residual energy decreases. That is the residual energy of the nodes decreases by increasing the no of messages. In this investigation, the proposed protocol is proven better than ESRPS (Efficient

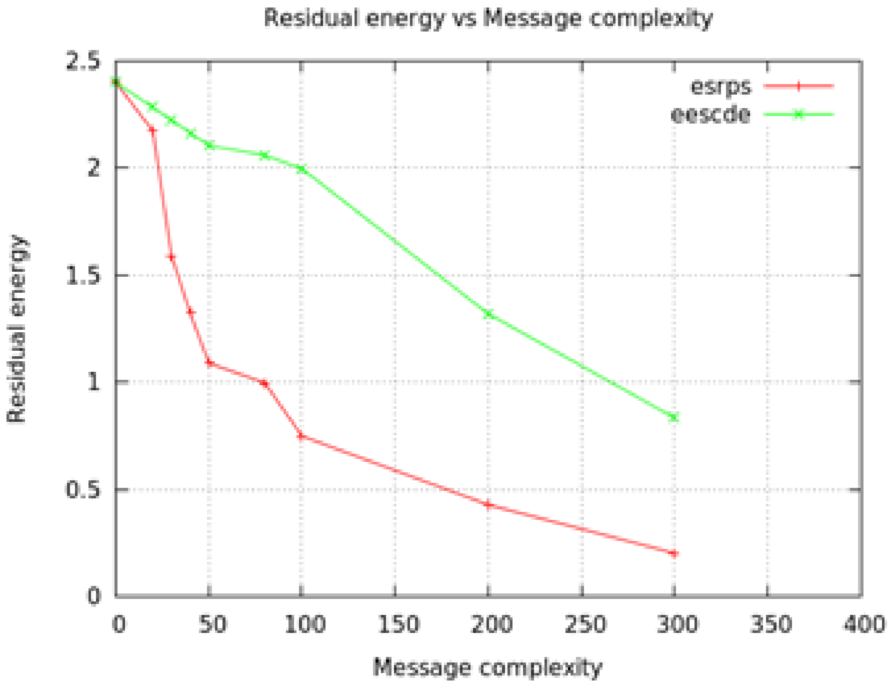


Figure 3.7: comparison of message complexity uwsn versus residual energy in UWSN

Secure Routing Protocol Based on SNR value). As we are choosing the CH as the nodes having a best SNR value the signal transmitted by the CH will be better, as compared to the existing protocol. And the amount of information loss as well as the no of retransmission will be least. This observation is described in figure 3.7.

Observation-III

As shown in Fig 3.8, the SNR values of the two types of WSN are compared. One is Underwater WSN and the second one is the Terrestrial WSN. If the proposed protocol is applied to the second one, then the some SNR values we are getting as negative, which should not be. That is if we represent it in DB then the noise power is more as compared to the power signal which indicates the noisy signal. But if the protocol applied to the UWSN, then all the SNR values generated are positive.

Observation-IV

This observation is done on the comparison of transmission loss versus distance.

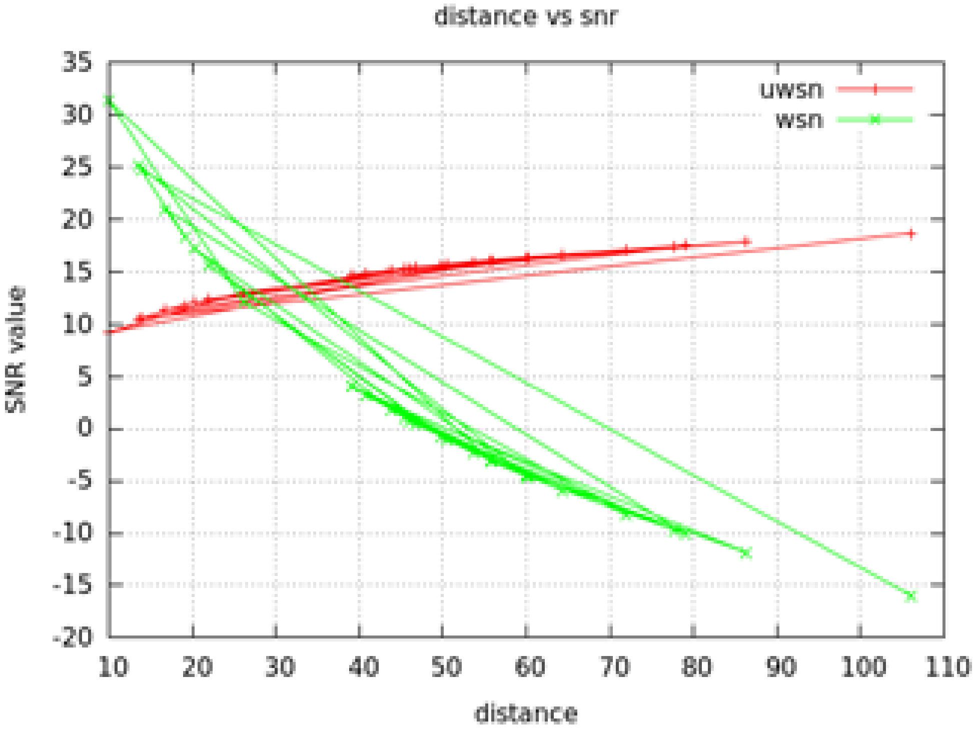


Figure 3.8: comparison of SNR value versus distance

The Transmission Loss (TL) is calculated using the following formula .

$$TL = 10\log(a^2 + b^2) \tag{3.11}$$

If the distance between the sender and the receiver node increases, the amount of transmission loss increases. Fig 3.9 shows the comparison of TL of the protocols esrps and eescde.

Observation-V

Observation-V is focused on comparing the position of the CH when the protocol EESCDE is applied to Underwater WSN and Terrestrial WSN. A total of 50 Sensor nodes are deployed in a 100x100 planar grid and their SNR values are computed. Depending on that value, the Cluster Heads are chosen. In our simulation, highest 5 SNR values are selected and the sensor nodes corresponding to those selected values are considered as the CH. They also satisfy one more criteria, that is the energy of

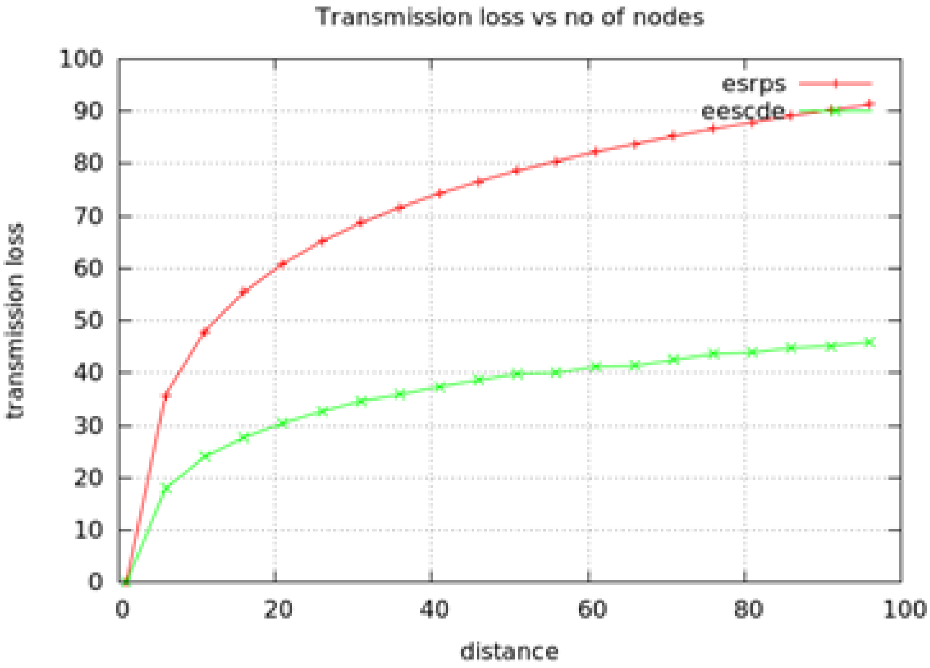


Figure 3.9: comparison of transmission loss versus distance

those nodes must be greater than or equal to the threshold value, initialized in the energy module. From figure 3.10 it is clear that, the position of CHs in Underwater WSN is more appropriate as compared to that of Terrestrial WSN.

3.5 Summary

The energy efficiency greatly affects the signal transmission and lifetime of the node. As the number of transmission and reception increases, the energy consumption also increases. Thus, the residual energy of the sensor nodes decreases. It has been observed in [13] that the network is a multi-hop network. For a single message transmission from source to sink, many nodes are taking part in this communication. Those participating nodes consume their energy. The second thing is the transmission of unencrypted raw data. It requires secure routing. The number of hop count increases in the isolation process of the malicious nodes or the intruders.

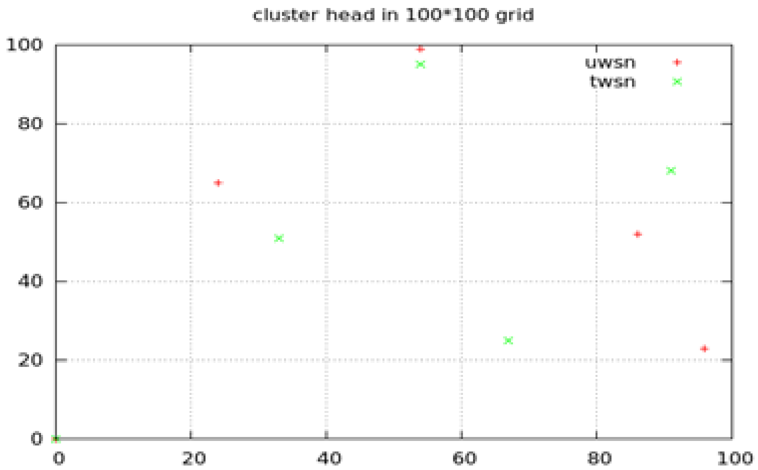


Figure 3.10: comparison of CH position in a 100x100 grid in UWSN and TWSN

Thus, the data delivery process will also be delayed. Therefore, the sink node will receive fewer messages. In this model, SNR based clustering is proposed which is incorporated with Data Encryption using HILL cipher. The proposed model is an energy-based model, which has been developed and simulated using the Network simulator NS3. Using this protocol, Energy Efficient SNR Based Clustering with Data Encryption (EESCDE), 10 percent improvement in residual energy has been achieved.

Chapter 4

Selective Data Transmission

4.1 Introduction

A Underwater Wireless Sensor Network (UWSN) is a network of sensing nodes, called the sensors[1-2]. These sensors are capable of monitoring surrounding environment. The sensor nodes are connected with wireless interfaces to communicate with each other. The UWSNs are deployed for sensing data over a spatially distributed environment. In sensors, Data gathered, pre-processed and send to a central node. The central node gathers the sensed information and provides a sensing map of the sorrounding environment [28]. As sensor networks are used in a hard to reach environment, they are battery operated. In such scenario, power consumption of WSN becomes a critical issue. The nodes must be designed in such a way that the available energy is used efficiently. Because, in certain circumstances, battery replacement is difficult or even impossible [25] [29]. Data transmission is a continuous process. The sensor nodes continuously sense the data and send it to the corresponding cluster head(CH).The nodes, participating in data communication utilize some amount of energy. Thus the residual energy decreases. To utilize less amount of energy, number of transmission should be reduced. Now A days, researchers are attracted towards Cluster-based data transmission in UWSNs. In a cluster-based UWSN (CUWSN), a leader sensor node is present. It is regarded as cluster-head (CH). A CH collects th data from the non-CH(NCH) in its cluster. It is responsible for sending the collected data to the base station (BS).In such network, lifetime is affected by the imbalanced energy consumption among the nodes [31]. Efficient data transmission is one of the most important issues for UWSNs. Recent work [25] has concerned a system construction modeling, in which the sensor nodes, furnished with transforming capacities and transmitting data to the CH. By selectively transmitting data, the number of transmissions in sensor nodes is controlled. In this chapter, we propose selective data transmission protocol in SNR based clustering protocol for UWSN.The proposed protocol concerned on reducing the number of transmissions. Thereby , the amount of energy utilization decreases and lifetime of the network increases.

sectionRelated Works Due to the reduced capabilities of the sensor nodes such as:

- limited bandwidth
- limited transmission range
- limited or no mobility
- limited battery power

The existing protocol may not work well.
The LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol exhibited by Heinzelman et al. [25], is generally a known and viable one to lessen and parity the total energy utilization for CUWSNs. In place to reduce the amount of energy utilization of the CHs, arbitrarily CHs are selected among all the sensor nodes in various rounds. Network lifetime is improved in LEACH (Low-Energy Adaptive Clustering Hi-erarchy) .

EADEEG [26] is a distributed clustering algorithm that elects cluster heads based on the ratio between the average residual energy of neigh-bor nodes and the residual energy of the node itself. Using this, a good cluster heads distribution is achieved. It also prolongs the lifetime of the sensor network.

An epidemic routing protocol proposed by Amit vahdat And David Beclet [28], where paths are set to all the nodes in the network and the messages are stored and forwarded to all the neighbor nodes blindly. It generates flood messages.

Arati Manjeshwar and Dharma P. Agrawal [29] proposed a hybrid routing protocol (APTEEN), suitable for retrieval of comprehensive infor-mation. In such networks, the sensor nodes are reactive to time-critical situations. At periodic intervals, they produce an overall picture of the network. The users are enable to request the network for the data of any time. That may be past, present, and future. However, the limited storage capability of the sensor nodes is a critical issue here.

4.1.1 Summary

Usually, the existing protocols requires more amount of buffer to store the data. However, the sensor nodes are equipped with a small memory chip.Thus, storing of all the sensed data is a critical issue. To overcome such shortcoming, we propose a selective forwarding clustered model.

4.2 Proposed Model

The proposed model is a two-step process. Those are as follows

- Design of clustered model
- Data and Energy model

The first step describes the designed step of a cluster and the second step shows, how energy is consumed during different operation.

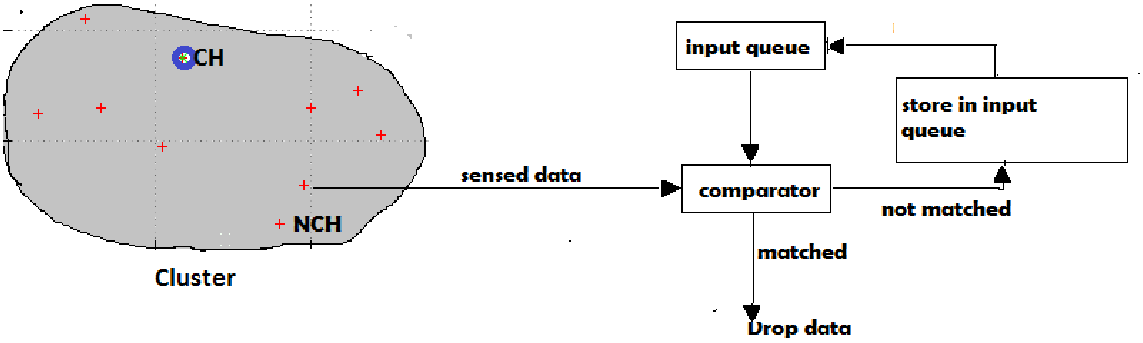


Figure 4.1: System model

4.2.1 Clustered Model

It is a model, that describes how the sensor nodes are partitioned in to cluster. As described in chapter 3,clusters are formed. The cluster heads are selected depending on the SNR of the sensor nodes. The nodes with higher SNR value and energy are selected as the CH. Only one CH is selected in each cluster. All other nodes coming within the communication range of the CH are included in that group and build a cluster. These nodes are called as the Non Cluster Head (NCH) or the followers.

4.2.2 Data and Energy model

We can catagorized the data transmission [27] into two types. Such as following

- Direct datatransmission
- Selective data transmission

In a sensor node, each time a data is transmitted directly, the residual energy of that node is decreased by a certain amount E_{Tx}. Only the transmission energy is required here. Whereas, when we selectively transmit the data, the sensor nodes require processing the data. Thus, the residual energy is decreased by the sum of transmission energy and the processing energy. This can be represented as

$$resenergy = resenergy - sum(E_{tx}, E_{proc}). \tag{4.1}$$

Similarly we can also compute the residual energy of the CH. However, the amount of residual energy is reduced by same amount whether the data is transmitted directly or selectively. The residual energy computed in a CH is

$$resenergy = resenergy - E_{rcch}. \tag{4.2}$$

The table describes the energy consumption[6] during different data transmission.

Table 4.1: Energy Consumption

Data transmission	CH	NCH
Direct	$resenergy = resenergy - E_{rcch}$	$resenergy = resenergy - E_{tx}$
Selective	$resenergy = resenergy - E_{rcch}$	$resenergy = resenergy - sum(E_{tx}, E_{proc})$

4.3 Proposed Algorithm

In this proposed algorithm, all the sensor nodes are initialized with initial energy, frequency, depth at which they are to be deployed, and transmission power. After the random deployment of the sensor nodes, clusters are formed by partitioning the sensor nodes into groups. Cluster Heads (CH) are selected, depending on the SNR value of the sensor node [5]. The sensor nodes in the network sense data. Before storing it into the input queue of the node, the sensed data is compared with the rear element of the queue. Initially, the input queue is empty, so the first sensed data is assumed to be 0. If the sensed data matched with the rear data element of the queue, it is dropped and no need to store it in the buffer. However, for a dissimilar data, that will be stored in the input queue of the sensor. This process continues until the queue is full. The sensor node encrypts the data using hill cipher [20] and sends it to the CH. The CH receives the encrypted data, decrypt it, find the average data value and sends it to the Base Station

Algorithm 4 selective data transmission

```
Build cluster depending on the SNR values of the sensor nodes.
Set $SensedData = 0.andQ[rear] = SensedData.$
Sensor node Sense data
State If ( $SensedData! = Q[rear]$)
Store it in the input queue as$Q[rear] = SensedData.$
State Else drop the data.
State If ($Q[rear]! = Qmax$)
Repeat step 3 to 6.
Else perform Data encryption
Send the encrypted data to the CH
```

4.4 Simulation and Results

Based on NS3 simulation model, the proposed protocol SCSD is evaluated. In a rectangular flat region of 100 X 100, the sensor nodes are deployed to form a CUWSN. The simulation parameters used for evauation are listed in table 2.

Figure 2 shows the comparison between the direct data transmission and selective data transmission. In direct data transmission, the number of data transmission same as the input queue size. However, in the second case, the number of transmissions is reduced depending on the sensed data value. Based on the number of transmissions, the residual energy is reduced. Figure 3 shows this reduction for direct and selective data transmission. In a CUWSN, if the number of nodes increases, then the number of member in a cluster increases. The residual energy of the CHS is reduced since it receives more number of messages from its members. Figure 4 shows the reduction in residual energy when the number of nodes increases.

Table 4.2: Simulation Parameters

Area of sensing field	100 X 100
Initial energy	2.4j
Frequency	2.4ghz
Packet size	2Kb
Number of Clusters	4
Sensing range	10m
Communication range	20m
Transmission power	2w
Average capacitance switch/cycle	22pF
Electronic energy dissipation	50nj/bit
Amplifier energy dissipation	100pj/bit/m2
Leakage current	1.196mA
Number of clock cycle	0.97*106
Processor constant	21.26
Thermal voltage	0.2v
Initial battery power	3.3volt

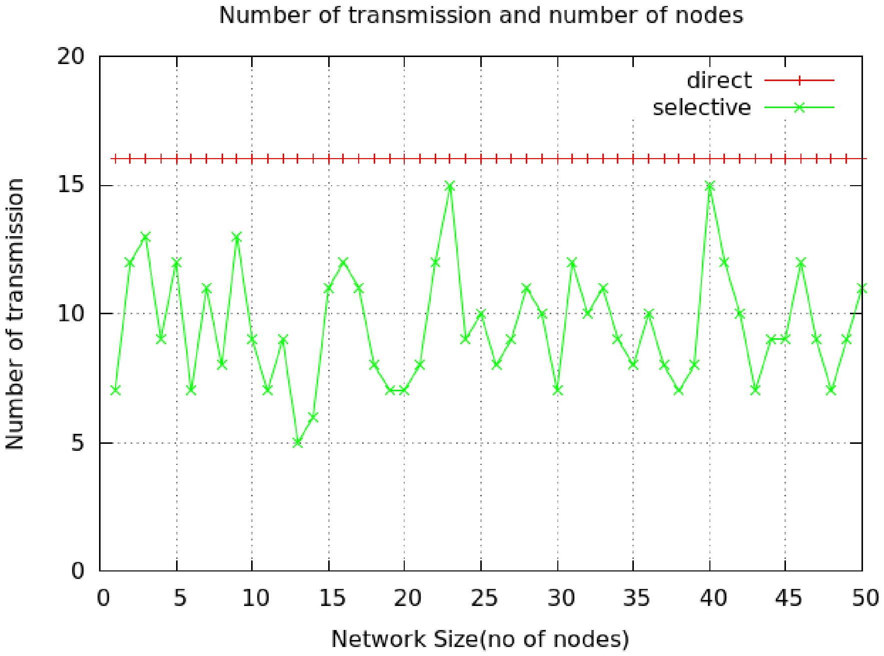


Figure 4.2: Comparison of Number of transmission versus Number of nodes

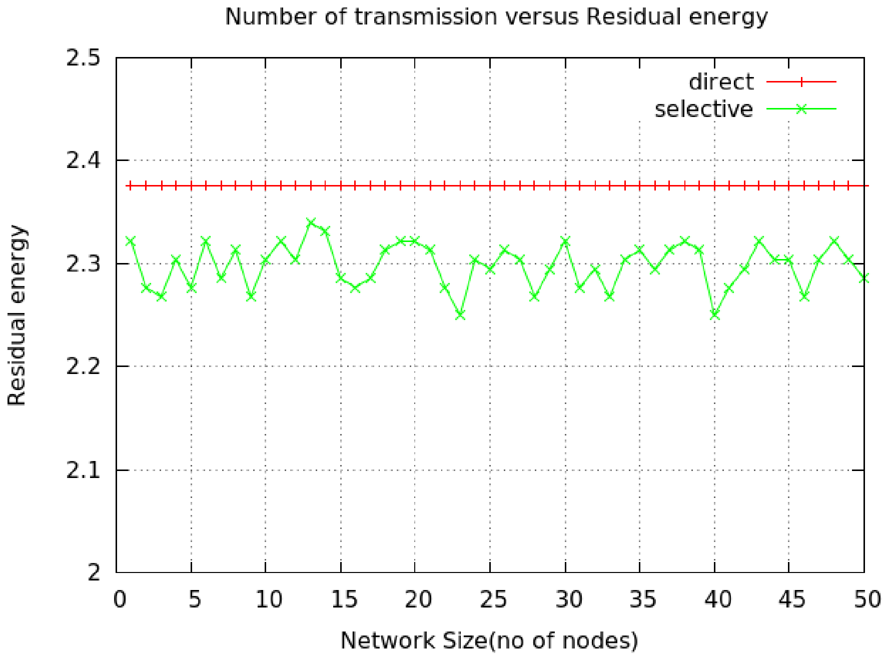


Figure 4.3: Comparison of Residual energy versus Number of nodes

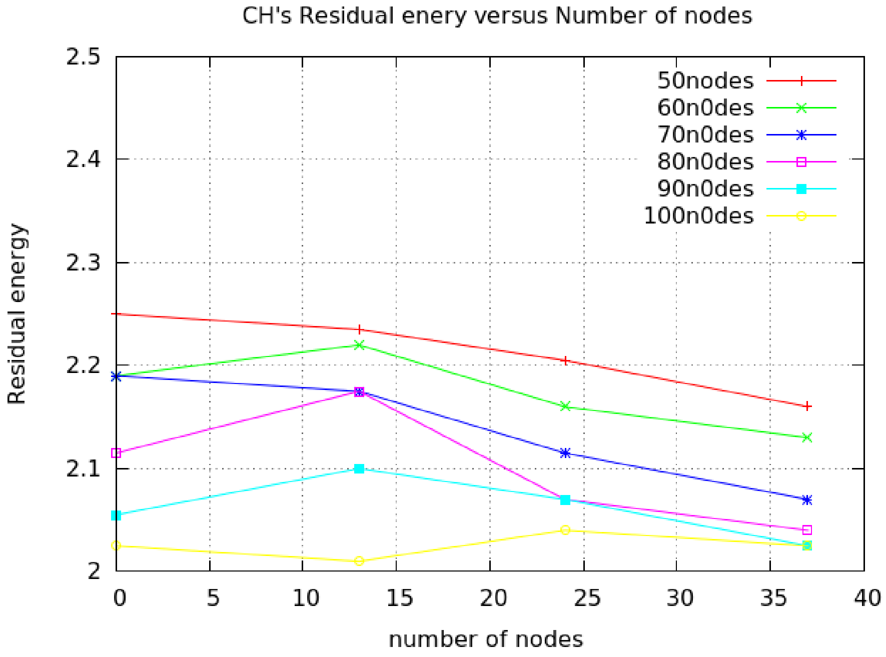


Figure 4.4: Comparison CHs residual energy versus Number of nodes

4.5 Summary

In this chapter, we reviewed the issues related to data transmission and data security in CUWSN. A protocol named, Selective Data Transmission In SNR based clustered (SDSC) is proposed. Using this protocol, only selected data are transmitted from the sensor nodes. If the sensed data is same as the previous one then the sensed data is dropped. The number of Data transmission is reduced. Thus, the amount of energy consumption is also reduced. For data security, HILL cipher is used as the data encryption mechanism. It is a block cipher and it makes the intruder difficult to guess the key matrix, it is considered to be suitable. In residual energy, 2 percent improvement has been achieved.

Chapter 5

Conclusion

EESCDE protocol consumes less amount of energy for processing, transmitting, and receiving the sensed data. This is energy efficient. The energy efficiency affects the node lifetime as well as the network lifetime. Energy consumption increases with the increase in number of transmissions and receptions operation. Thus, the residual energy of the sensor nodes decreases. It also provides security to the sensed data. In this model, SNR based clustering is proposed which is incorporated with Data Encryption using HILL cipher. Using this encryption mechanis, the sercurity service is achieved. The proposed model is an energy-based model, which has been developed and simulated using the Network simulator NS3. Using this protocol, Energy Efficient SNR Based Clustering with Data Encryption (EESCDE), 10 percent improvement in residual energy has been achieved.

A protocol named, Selective Data Transmission In SNR based clustered (SDSC) is also proposed in this work. It is suitable for CUWSNs. Using this protocol, only selected data are transmitted from the sensor nodes. If the sensed data is same as the previous one then the sensed data is dropped. The number of Data transmission is reduced. Thus, the amount of energy consumption is also reduced. For data security, HILL cipher is used as the data encryption mechanism. It is a block cipher and it makes the intruder difficult to guess the key matrix, it is considered to be suitable. In residual energy, 2 percent improvement has been achieved.

Scope for Further Research

In future, the research may be extended to a multi-hop network model with heterogeneous nodes.The secure routing mechanism has to be implemented in which the algorithm may be analyzed again. This work is concerned on single level clustering. Therefore, the work may be extended for multilevel clustering.

Bibliography

1. A.A. Abbasi, M. Y., Challenges for efficient communication in underwater acoustic sensor networks, vol. 30, 2007.

2. Akyildiz, I. Pompili, D. andMelodia, T., Challenges for efficient communication in underwater acoustic sensor networks, vol. 1, 2004.

3. Akyildiz, I. F., Pompili, D., and Melodia, T., Underwater acoustic sensor networks: research challenges, Ad hoc networks, vol. 3, no. 3, pp. 257279, 2005.

4. Babiker, A. and Zakarial, N., Energy efficiency in underwater wireless sensors networks, april 2012.

5. Ganesh, S. and Amutha, R., Efficient and secure routing protocol for wireless sensor networks through snr based dynamic clustering mechanisms,Journal of Communications and Networks, vol. 15, pp. 422 429, Aug 2013.

6. Halgamuge, M. N., Zukerman, M., Ramamohanarao, K., and Vu, H. L., An estimation of sensor energy consumption, Progress In Electromagnetics Research, 2009.

7. J. Heidemann, W. Ye, J. W. A. S. and Li, Y., Research challenges and applications for underwater sensor networking, Proceedings of the IEEEWireless Communications and Networking Conference, 2006.

8. J. Kamimura, N. W. and Muratai, M., Energy-efficient clustering method for data gathering in sensor networks, in Proc. BASENETS, April 2004.

9. J.H. Cui, J. Kong, M. G. and Zhou, S., Challenges: Building scalable mobile underwater wireless sensor networks for aquatic applications, IEEE Network, Special Issue on Wireless Sensor Networking, p. 12A S18, 2006.

10. L. Li, S. D. and Wenl, X., An energy efficient clustering routing algorithm for wireless sensor networks, J. China Univ. Posts Telecommun, vol. 13, pp. 7175, june 2006.

11. . Lanbo, L., Shengli, Z., and Jun-Hong, C., Prospects and problems of wireless communication for underwater sensor networks, Wireless Communications and Mobile Computing, vol. 8, no. 8, pp. 977994, 2008.

12. Liam Keliher, S. T., Slide attacks against iterated hill ciphers, Communications in Computer and Information Science, pp. 179190, 2013.

13. Lurton, X., An introduction to underwater acoustics: principles and applications. Springer Science Business Media, 2002.

14. M. J. Handy, M. Haase, D. T., Low energy adaptive clustering hierarchy with deterministic cluster-head selection, pp. 368372, september 2002.

15. Pratik R. Chavda, P. P. K., A comparison leach and heed cluster based protocol for wireless sensor network, IOSR Journal of Computer Engineering (IOSRJCE, vol. 7, pp. 5156, Nov-Dec 2012.

16. Preisig, J., Acoustic propagation considerations for underwater acoustic communications network development, vol. 11, pp. 210.

17. S Lindsey, C. S. R., Pegasis: Power-efficient gathering in sensor information system, IEEE conference, vol. 3, pp. 11251156, june 2002.

18. Sangho, Y., Junyoung, Yookun, and Jiman, Peach: Power-efficient and adaptive clustering hierarchy protocol for wireless sensor networks, Computer communications, vol. 30, no. 14, pp. 28422852, 2007.

19. Savitha M, S. D. P., A survey on clustering techniques in wireless sensor networks, International Journal of Emerging Technology and Advanced Engineering, vol. 4, April 2014.

20. Toorani, M. and Falahati, A., A secure variant of the hill cipher, in Computers and Communications, 2009. ISCC 2009. IEEE Symposium on, pp. 313316, IEEE, 2009.

21. Wahid, A. and Kim, D., An energy efficient localization-free routing protocol for underwater wireless sensor networks, International journal of distributed sensor networks, 2012.

22. Watfa, M. K., El-Ghali, M., and Halabi, H., A hybrid security protocol for sensor networks, International Journal of Communication Networks and Distributed Systems, vol. 3, no. 2, pp. 116145, 2009.

23. Xing, G., Wang, X., Yuanfang Zhang, a. C. L., and Robert Pless, A.C. G., Integrated coverage and connectivity configuration for energy conservation in sensor networks, ACM Transactions on Sensor Networks (TOSN, vol. 2, pp. 3672, August 2005.

24. Zahedi, Y. K., Ghafghazi, H., Ariffin, S., and Kassim, N. M., Feasibility of electromagnetic communication in underwater wireless sensor networks, in Informatics Engineering and Information Science, pp. 614623, Springer, 2011.

25. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, Energy -Efficient communication Protocols for Wireless Micro sensor Net-works (LEACH) in HICSS , vol. 8, Maui, Hawaii, January 2000, pp. 3005 3014

26. M. Liu, J.N. Cao, G. Chen, H. Eadeeg, An energy-aware data gathering protocol for wireless sensor networks, Journal of Software, 18 (2007), pp. 10921109

27. G. Battistelli, A. Benavoli, and L. Chisci, Data-driven communica-tion for state estimation with sensor networks, Automatica, vol. 48, no. 5, pp. 926935, 2012.

28. Amit vahdat, David Beclet, Epidemic Routing for partially-connected Adhoc networks, Department of Computer Science, Duke University, Durham, NC27708.

29. Arati Manjeshwar and Dharma P. Agrawal ,APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Re-trieval in Wireless Sensor Networks,Computer Society,IEEE,2002

30. Huanh Lu, Jie Li, Guizani. M. Secure and Efficient Data Transmis-sion for Cluster-Based Wireless Sensor Networks , IEEE transac-tion, Volume 25, Issue 3, Pages750-761, February 2013

31. Jiguo Yu, Yingying Qi, Guanghui Wang, Xin Gu, A cluster-based routing protocol for Wireless sensor networks with nonuniform node distribution.

Dissemination

Journal

1. Bandita Sahu and Pabitra Mohan Khilar, Energy Efficient SNR Based Clustering in Underwater Sensor Network (UWSN) with Data Encryption , *Frontiers of Computer Science (Springer)*, 2015 (Communicated)