A Novel Technique to Balance Trade Off between Energy Consumption and Security in WSN

By

Atiya Obaid

00000278698

Supervisor

Brig. Dr. Imran Rashid

A thesis submitted to the faculty of Information Security Department,
Military College of Signals, National University of Sciences and Technology,
Islamabad, Pakistan in partial fulfillment of the requirements for the degree of MS
in Information Security

September 2022

THESIS ACCEPTANCE CERTIFICATE

Certified that the final copy of MS/MPhil thesis written by **NS Atiya Obaid** Registration No. **00000278698** of **Military College of Signals** has been vetted by undersigned , found complete in all respect as per NUST Statutes / Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/MPhil degree. It is further certified that necessary amendments as pointed out by GEC members of the student have also been incorporated in the said thesis.

Signature: _____

Name of Supervisor: Brig. Dr. Imran Rashid

Date: _____

Signature (HOD): _____

Date: _____

Signature (Dean): _____

Date: _____

DECLARATION

I certify that this research work titled "**A Novel Technique to balance Trade Off between Energy Consumption and Security in WSN**" is my own work. No portion of this work presented in this dissertation has been submitted in support of another award or qualification either at this institution or elsewhere. The material that has been used from other sources has been properly acknowledged.

_____

Signature of Student

Atiya Obaid

00000278698

This page is left intentionally blank

ABSTRACT

Wireless Sensor Networks (WSN) refer to a group of sensors with the ability to network through wireless means in harsh environmental conditions capable of sensing temperature, humidity, and pressure, sound etc. These sensors are limited in terms of battery life affecting the networks performance and lifetime. These tiny devices transmit the data to the base station which is susceptible to be compromised if not encrypted. Therefore, the greatest challenge in wireless sensor networks is to balance the energy consumption and provide security simultaneously without degrading the lifetime or network performance. These limitations exist in WSN due to the large scale, open and resource constrained nature of the sensor networks. Several protocols exist for transmitting data to the base station but when these networks provide a secure data transmission they mostly suffer from key management, encryption time and many other limitations. Our algorithm uses a classical hierarchical routing technique to route the data from the nodes to the base station using a clustering technique. The cluster head selection has been performed using the modified LEACH protocol based on residual energy to increase the network lifetime. The data is then routed from the cluster heads to the base station using Particle Swarm Optimization (PSO) algorithm to minimize the energy consumption while providing encryption from the nodes to the base station. The encryption has been performed using a modified version of Flex Crypt algorithm with simple computations and the results are analyzed in terms of network performance and stability. After simulating the algorithm in MATLAB and comparing with the existing protocols such as LEACH, PSO and FlexCrypt the proposed algorithm revealed an improvement in the number of dead nodes, network energy consumption and the number of packets delivered to the base station while providing end to end data security. The encryption time was found to be better than the previous protocols. All the above factors reveal an improvement in the network throughput and enhanced lifetime while providing security.

COPYRIGHT STATEMENT

Copyright in text of this thesis rests with the student author. Copies (by any process) either in full, or of extracts, may be made only in accordance with instructions given by the author and lodged in the Library of NUST Military College of Signals (MCS).

Details may be obtained by the Librarian. This page must form part of any such copies made. Further copies (by any process) may not be made without the permission (in writing) of the author.

The ownership of any intellectual property rights which may be described in this thesis is vested in NUST Military College of Signals (MCS), subject to any prior agreement to the contrary, and may not be made available for use by third parties without the written permission of the MCS, which will prescribe the terms and conditions of any such agreement.

Further information on the conditions under which disclosures and exploitation may take place is available from the Library of NUST Military College of Signals (MCS), Rawalpindi.

DEDICATION

“In the name of Allah, the Most Beneficent, the Most Merciful”

Read in the name of your Lord who created. Created man from a clinging substance.

Read, and your Lord is the Most Generous.

Who taught by the pen.

Taught man that which he knew not (Al- ‘Alaq 1:5)

With the blessings of Allah, I dedicate this thesis to my parents for their untiring efforts, my siblings for their unrelenting support and my husband for believing in me and keeping me motivated throughout.

ACKNOWLEDGEMENT

First and foremost, I am grateful to Almighty Allah for His countless blessings and for the fortitude He bestowed upon me to complete what seemed to be a daunting task at times. I would like to express my deepest appreciation for Brig. Dr. Imran Rashid who not only supervised my work but mentored, encouraged, and supported me to complete my work. His knowledge and invaluable expertise are invaluable in the completion of this thesis. Sincere thanks are also due to Assoc Prof. Dr. Waseem Iqbal, Assoc. Prof. Dr. Mir Yasir Umair and Dr. Fawad Khan for their guidance and mentorship. I would like to thank and appreciate the enduring and never-ending support and encouragement of my friend Aimen Aakif who always helped me whenever needed.

This page is intentionally left blank

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS USED

Wireless Sensor Network	WSN
Cluster Head	CH
Time Division Multiple Access	TDMA
Received Signal Strength Indicator	RSSI
Media Access Control	MAC
Cipher Text	CT
Particle Swarm Optimization	PSO
Low Energy Adaptive Clustering Hierarchy	LEACH
Residual Energy	RE
Base Station	BS
Neighbor Numbers	NN
Rivest Shamir Adleman	RSA
Advanced Encryption Standard	AES
Micro Electromechanical Systems	MEMS
Adhoc On Demand Distance Vector	AODV
Modified LEACH	MODLEACH
Global Positioning System	GPS
Combined Cost Value	CCV
Exclusive OR	XOR

Chapter 1

Introduction

This chapter discusses the problem statement, objectives, goals along with the major contributions in the thesis. This is followed by a concise description of each chapter.

1.1 Problem Statement

Wireless sensor network refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. Wireless sensor networks can be used to measure environmental conditions like temperature, humidity, pollution etc. The data from these networks is transmitted wirelessly through sensors [1]. The growth and advancement of wireless sensor networks was motivated by military for surveillance purposes. Networks are used in many industrial applications, industrial process and control and machine health monitoring.

One of the key concerns in wireless sensor networks is the energy efficiency. The increased importance in energy efficiency can be accredited to several factors such as battery life, selection of nodes and clusters. These networks depend largely on tiny sensor nodes that consist of batteries which are usually the main source of power for these devices and are characterized by a limited battery life, after which they are exhausted. The deployment of these nodes in military environments where at times it is not possible to be physically present with their energy running out in a limited period is one of the major concerns. There are many different techniques available to manage this energy constraint and prolong the network usage.

The sensor nodes are responsible for relaying the data packets from the sensor nodes to the destination. These sensor networks are in the present day playing a very important role in military applications where apart from being able to reach inaccessible areas easily are also responsible for providing the much-needed confidentiality and data secrecy. The confidentiality of data is ensured through certain encryption algorithms which are very heavy and costly in terms of their complexity and calculations leading to increased energy consumption. To ensure confidentiality of data and

management of energy consumption of the nodes a balance needs to be achieved. Hence, the major focus is to minimize the consumption of energy while ensuring security of the transmitted data.

1.2 Goals

The chief goal of this research is to increase the network lifetime and longevity by improving the energy consumption of the sensor nodes in a wireless sensor network (WSN) while ensuring security of the data packets when stored in the sensor nodes / devices, during transmission and after reaching the destination / sink.

1.3 Thesis Objectives

The main objectives of the thesis are as follows:

a) Literature review and understanding of energy consumption protocols and security mechanisms in WSN.
b) Proposing a technique to reduce the tradeoff between energy consumption and security.
c) Simulating the proposed technique and comparing with existing techniques to show enhancements / improvements.

1.4 Thesis Contributions

The major contributions of this research are as listed below:

a) Analyzing existing clustering techniques, objectives and routing protocols with respect to energy to identify their strengths and limitations.
b) Analysis of existing light weight encryption techniques to understand their working and the execution time.
c) Investigate possible solutions for clustering and routing while encrypting the data.
d) Propose a novel technique for data clustering while minimizing energy and securing data.
e) Detailed analysis of the results using encryption and clustering to transmit the data while ensuring its security.

1.5 Thesis Organization

The thesis has been organized according to the following chapters as discussed below.

Chapter 1: The chapter discusses the preface, problem description, objectives, goals, thesis organization and contributions to the research.

Chapter 2: This chapter deals with the background information such as sensor networks, different types of routing protocols, objectives of clustering, different types of clustering techniques, fundamentals of network encryption and basic encryption techniques.

Chapter 3: A literature review of different techniques along with their limitations for clustering, routing and encryption are discussed in this chapter.

Chapter 4: This chapter discusses the design and methodology of the proposed technique which includes clustering, routing, and encryption.

Chapter 5: This chapter deals with the result and outcomes of the proposed technique.

Chapter 6: This chapter concludes the dissertation and suggests future recommendations.

Chapter 2

Background

Wireless sensor network is an upcoming technology that is gaining immense attention from researchers, particularly due to the recent explosion in Micro-Electro-Mechanical Systems (MEMS) technology which has enabled the development of smart sensors [1]. These sensors are small devices, with limited processing and computing resources. They can sense, measure, and gather information from the environment and, transmit the data to the destination. These devices are limited in terms of energy capacity and therefore, managing their energy is important for the longevity of the network. Simultaneously, while the data is being transmitted data security is also equally important. Therefore, the problem arises while trying to strike a balance between the energy consumption and security.

2.1 Architecture of a Wireless Network

A typical wireless sensor network consists of hundreds, or thousands of tiny devices called sensors which are responsible for continuous data sensing and communication. These nodes are randomly scattered in the monitoring area from where we intend to collect the data. They can either communicate with each other, forward the data to the base station directly or forward it to the cluster head from where it is transmitted to the base station. These nodes collect the data from the environment and forward it to the base station using a single or multi hop mechanism. The Base Station can either be fixed or mobile like the nodes which can also be mobile or static. The sensor nodes in the WSN are battery operated with limited energy resources and do not allow battery replacement [2]. Hence, creating energy efficient protocols is crucial for prolonging the lifetime of the network.

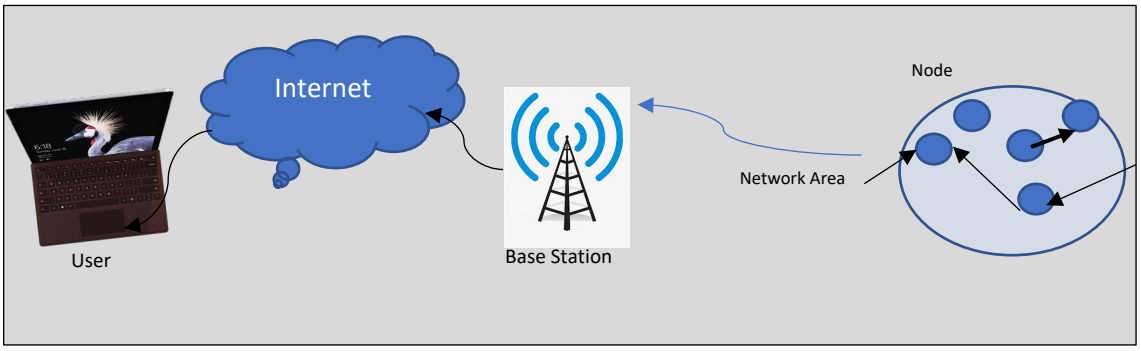

Figure 2. 1 Architecture of a Wireless Sensor Network

2.1.1 Characteristics of Wireless Network

The main characteristics of wireless sensor networks are listed below [3].

1. **Dynamic network topology**- The sensor nodes can either be static or mobile. The nodes travel in random directions at different speeds, and they may also fail to operate or be replaced therefore they can work with different network topologies.
2. **Scalable** – WSNs generally deal with a sizeable monitoring area therefore many nodes may be densely deployed in various applications.
3. **Communication Models** - WSNs use different communication models such as flat, hierarchical distributed WSNs, homogeneous or heterogeneous WSNs.
4. **Power consumption constraints for nodes** - WSN nodes are tiny devices powered by batteries. This justifies the service provided by nodes like communication and computation given the limited amount of memory.
5. **Error prone** – WSNs are prone to errors due to the harsh environment leading to instability, unpredictability, and node mobility.
6. **Application specific design** – The architecture of WSN is generally designed to be application specific.
7. **Communication paradigm** − The data centric feature of WSN explains its nature and justifies the restricted communication amongst the nodes.

2.1.2 Types of WSN

There exist several different types of wireless sensor networks which can be employed in different areas of applications [3].

1. **Terrestrial** – These networks consist of hundreds, or thousands of sensors deployed / dropped on the land. It has major applications in environmental and industrial monitoring as well as surface explorations.
2. **Underground** – The network of sensors deployed in caves, mines or under the ground to monitor different parameters. It finds great applications in the areas of landscape management, agricultural monitoring, underground monitoring of soil, rock, water, or mineral.
3. **Underwater** – Network consisting of sensor nodes which collect data from under the water from which special vehicles deployed in deep water later collect the data. This finds major application in seismic monitoring and underwater robotics as well as undersea surveillance and pollution monitoring.
4. **Multimedia** – Network consisting of wireless sensor devices equipped with cameras and microphones with the ability to store, process, and retrieve multimedia data which includes images, videos, and audios to provide enhancement in existing applications.
5. **Mobile**- Network consisting of mobile sensor nodes that can move around and interact with the surroundings. They can be used in the environment, underwater, habitat, military, search and rescue and target tracking and monitoring.

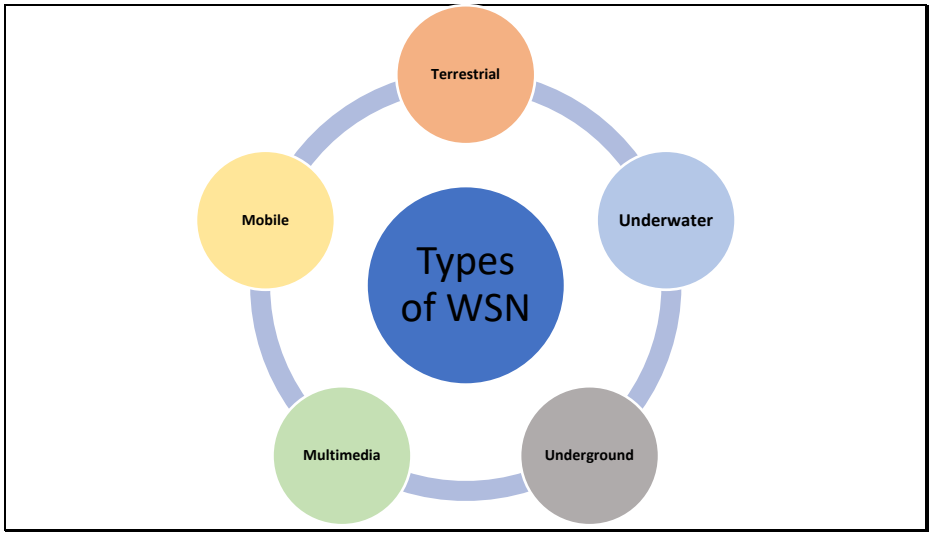

Figure 2. 2 Types of Wireless Sensor Network

.

2.1.3 WSN Applications

The popularity of wireless sensor networks can be attributed to the various and diverse areas of applications where it is applicable. Some major areas of application include but are not limited to the ones given below.[4]

1. **Military applications**

   Nowadays, military has started relying extensively on wireless sensor networks. They are considered a vital part of the military command and control systems, communications, intelligence, surveillance, reconnaissance, self-healing land mines, soldier detection, soldier tracking, early attack reaction sensor, sniper detection, training systems and so on.

2. **Environmental applications**

   Environment has nothing to do with wireless sensor networks but, nowadays they are being used to find out about the movement of birds, insects, and other animals as well as monitor the environmental situations having an impact on the cattle. In agriculture these WSNs are used extensively to divert animal intrusions in the fields to manage pest control to increase the crop yield, smart irrigation, fertilization, greenhouse and so on [5].

3. **Health applications**

   Sensor networks also find extensive applications by providing different interfaces for those who are challenged, patients telemonitoring especially elderly, patients' biological data, patients' diagnostics, and drug administration in hospitals.

4. **Smart Home applications**

   WSN has gained immense popularity in smart home automation. With the rapid advancement in technology, smart sensor nodes and actuators are being embedded in our everyday appliances like microwaves, mobile phones, air conditioners, refrigerators, and different appliances to manage them remotely making life easier and convenient for us.

5. **Commercial / Industrial applications**

   Wireless sensor networks increasingly play an important part in the construction of smart office spaces, inventory management, vehicle tracking, product manufacturing and monitoring and robotic management in manufacturing environments. WSNs are not limited to the above only but they are also quite important in equipment, structure, and workers' status monitoring. Over a period, the industrial equipment may worsen over time making WSNs monitor machines to

identify the machines that start deviating from the ideal solution. They can also be used to make life comfortable for the employees or workers working in unsafe or hazardous conditions to reduce the number of casualties and damage for workers like coal miners and firemen who always face constant dangers in line of their work [6].

6. **Disaster Management Applications**

   Disaster management refers to hazardous environment sensing which includes fire, flood, landslide, debris flow, and gas leakage. WSNs are employed for continuous monitoring of these hazardous environments to minimize or eradicate any threat to human life or property.

Figure 2. 3 Applications of WSN

2.2 Sensors

A sensor refers to a tiny device that receives a signal which could be physical, chemical, or biological and responds with an electrical signal which could be a voltage or current. These sensors can be classified based on the parameters such as applications, input signal, and conversion mechanism, sensor material, and additional criteria such as cost, accuracy, or range.

These nodes are limited in terms of computing power, bandwidth, memory, communication range and most importantly energy. They have limited power and batteries which are irreplaceable therefore they are referred to as single-use devices [7].

There are two main types of sensors: passive and active sensor. A passive sensor is one that does not require an extra energy source to produce an electric signal directly [8]. Examples

include chemical, photographic, thermal, and seismic. On the contrary, active sensors are ones that need an external source of energy to respond and are used widely by the meteorology department.

The presence of sensors and its applications can be seen everywhere in our homes, offices, cars, appliances, malls etc. There are different kinds of sensors available around us, in our offices, gardens, shopping malls, homes, cars, toys etc. They make our lives easy and comfortable, starting from applications such as switching on consoles, lights, air conditioners, fire alarm etc.

2.2.1 Types of sensors

Various types of sensors based on their detection properties include the ones listed below[9].

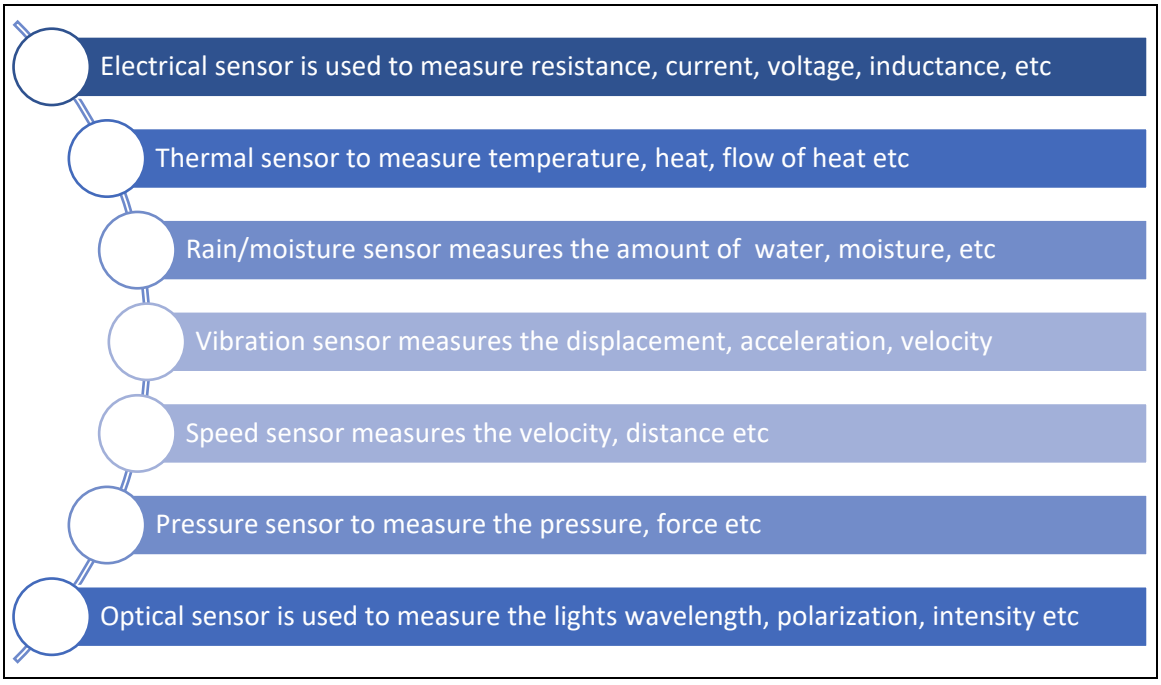

Figure 2. 4 Sensor types based on detection

2.2.2 Components of a sensor

The main components of a sensor node include the: Sensing unit, Processing unit, Power unit and a transceiver [8].

1. **Sensing Unit -** consists of a group of sensors responsible for measuring the physical characteristics around the environment.
2. **Processing unit -** consists of both the processor and storage. The processor in the sensor node is used for data processing and coordination among all the other components. The storage depends on the type of application.
3. **Transceiver -** is used to both send and receive messages wirelessly.
4. **Power Unit -** is an essential component for providing energy to all the components of a WSN.

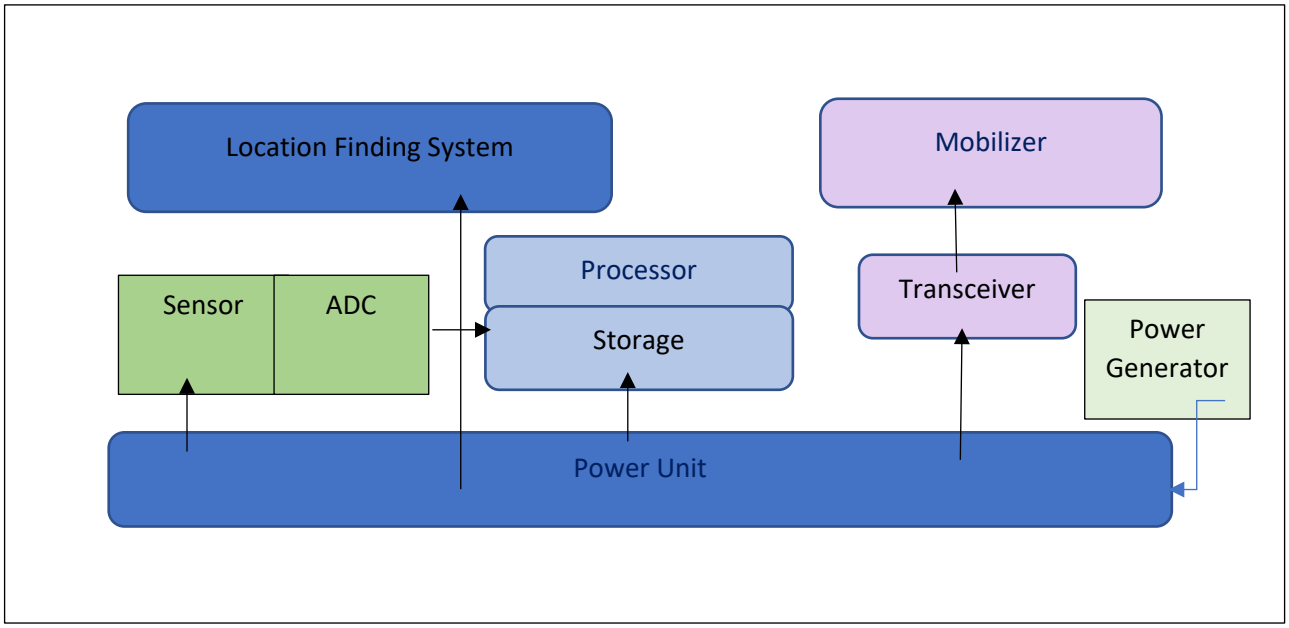

Figure 2. 5 Components of a sensor node [10]

2.3 Clustering

Clustering is a method of organizing the sensor nodes in a network in the form of a hierarchical structure [11]. This helps them to use their resources like energy, battery, and other radio resources in an efficient manner. In a cluster the data is aggregated at the cluster head to reduce the amount of data transmission to the sink. Cluster Heads are selected based on several parameters after which the member nodes tend to transmit their data to them. The data is then aggregated at the cluster heads before its forwarded to the sink resulting in higher energy drainage, thereby degrading the performance of the network.

2.3.1 Clustering Objectives

Wireless sensor network is made up of hundreds or thousands of sensor nodes all of which are connected by some means to form a network. Clustering is an important technique of increasing the networks lifetime in wireless sensor networks (WSNs). Although clustering is mainly associated with reducing the networks energy consumption, but there are many other objectives that are also achieved. The table below sheds light upon the objectives of clustering along with the techniques to achieve these [12].

Table 2. 1 Objectives of Clustering

Objectives of Clustering	Techniques to achieve
Energy Consumption	To balance energy consumption and improve network lifetime. • CH Duty Rotation • Hierarchical Clustering • Balanced Clusters
Load balancing	Some packets transfer higher amounts of data than other. • More layers, more CH • Balanced Clusters • Congestion Control • Balanced Energy Consumption
QoS	QoS is important to optimize jitter, throughput as well as minimizing the delay. It improves the rate of successful data transmission to avoid node death. • Reliability- Increases by improving PDR • Delay- Reduced by decreasing hops and optimizing routing • Throughput-improved by pre-determining no of CH, data aggregation and compression
Packet Delivery Improvement	PDR can increase QoS and reduce energy usage and network overhead by decreasing the number of re-transferred packets and data loss etc. • Structures • Splitting unbalanced traffic streams
Connectivity	Improving connectivity helps increase network reliability and transfer a large volume of sensed data to the BS. Clustering improves connectivity as each node has at least one connection to other nodes and BS. • Improve coverage • Improve connectivity
.Fault Tolerance	Clustering should tolerate defective nodes to keep the network linked. Node failure can occur due to battery depletion, hardware failure and physical or environmental factors. • Detect failure • Spare nodes • Re-clustering
N/W Topology Management	WSNs need to be connected, reliable, and stable. Each CH is responsible for managing a network area.

	• Stability- makes network reliable in terms of connectivity, QoS, fault tolerance, etc. SEP and ACHTH-LEACH provide stability in a network. • Scalability
Support Multi-Sink	Allow the network to have several gateways which improve network efficiency during data gathering and transferring. • Multiple sinks to improve success rate • Multiple sinks to reduce number of hops
Mobility Management	Mobility though an advantage can cause several issues like connectivity, reliability, stability. • Use mobile sinks • Create service zones by performing neighbor discovery
Security	Clustering can improve security by reducing attacks and detecting malicious nodes. • Key Verification • Authentication • Intelligent Transport System
Physical Layer Support	Clustering techniques belong to the network layer, but they can make other layers efficient as well like the physical layer. • Group nodes • Adaptive clustering for bandwidth allocation

2.4 WSN Routing Protocols

Routing protocols refer to a defined set of rules to route data from source to destination moving from node to node across the different avenues available. In wireless sensor networks it refers to the way data is collected and routed from the network field to the base station [13].

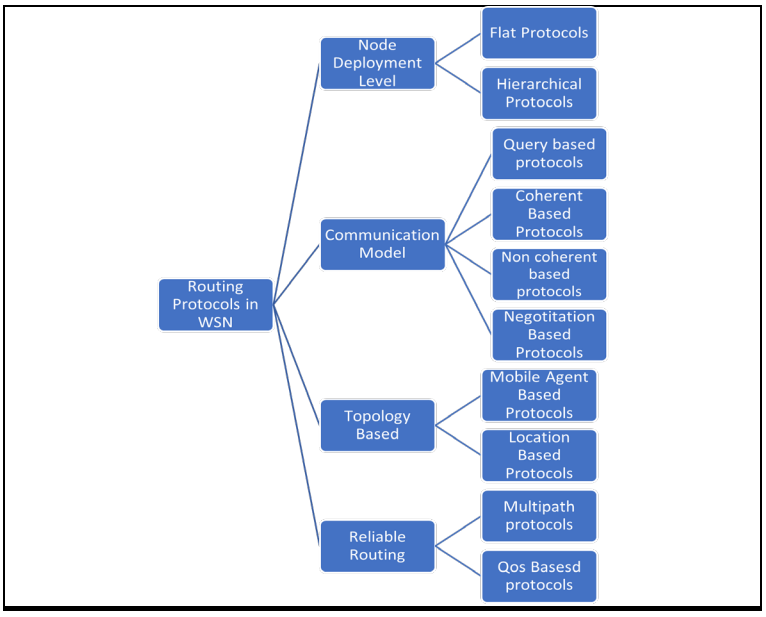

Figure 2. 6 Routing Protocols in WSN

[14] has further classified hierarchical protocols as classical or intelligent algorithms. Routing protocols can also be classified into three main categories namely location, data-centric and hierarchical. Each category is divided into classical and computational intelligence. Classical routing protocols are conventional protocols like AODV (Ad hoc On-Demand Distance Vector), LEACH (Low Energy Adaptive Clustering Hierarchy), SPIN (Sensor Protocol for Information via Negotiation), etc. Classical protocols are ones which are based on the forming of clusters using basic algorithms while the intelligent algorithms are the ones which are considered self-organized or biologically inspired, and both tend to provide flexibility, dynamic network topology, clustering, security, and data aggregation.

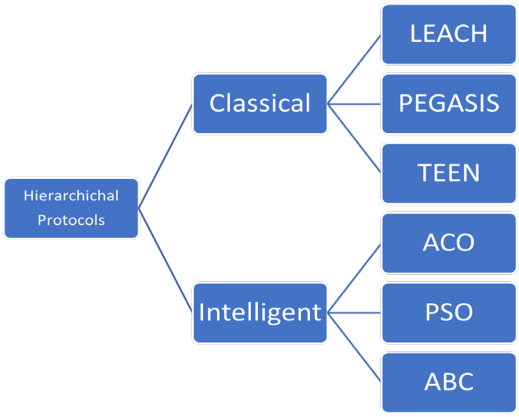

Figure 2. 7 Hierarchical Protocols classification

2.4.1 Hierarchical Protocols

The aim of hierarchical routing is to maintain or reduce energy consumption by involving the nodes within a cluster, transmit the data using a single or multi hop communication and performing data aggregation at the cluster heads to manage the energy consumption by reducing the number of packets. Hierarchical approaches can either be cluster based or intelligence based. They use a two-layer approach where one layer is used for physical data sensing and the other for data routing. Low energy nodes are used for data sensing while high energy nodes are reserved for data aggregation, collection and forwarding purposes [15].

The advantage of cluster based hierarchical approach includes increased scalability, efficient data aggregation and efficient channel bandwidth utilization. On the other hand,

unbalanced clusters lead to high energy dissipation, increased total energy consumption, and network connectivity not being guaranteed. /

The different hierarchical routing protocols consists of several different routing protocols such as TEEN, APTEEN, LEACH, ACO, PSO and PEGASIS of which the most important classical based protocol LEACH and intelligence based PSO have been discussed briefly below. LEACH (Low Energy Adaptive Clustering Hierarchy) is one of the first hierarchical routing approaches in WSN. The idea presented in LEACH has served as a basis for all the other hierarchical protocols.

2.4.1.1 LEACH Algorithm

Low-energy adaptive clustering hierarchy – LEACH is an extremely popular algorithm for routing in sensor networks. The idea is to form clusters based on the RSSI to use the cluster heads to forward the aggregated data to the sink to save up on energy. The cluster heads change randomly to manage the energy dissipation of the nodes. In case of LEACH algorithm, the cluster heads are decided based on randomly generated value. The random value is later compared with the threshold value and if it is less than the threshold value it ends up being the cluster head [16].

2.4.1.2 PSO Algorithm

Particle Swarm optimization algorithm (PSO) is a biological population-based algorithm that simulates the behavior of animal, birds, and fish which they exhibit socially. It is an intelligence-based protocol which is strongly inspired by the swarm behavior as observed in the nature [17]. All the particles are retained throughout the search process since there is no selection procedure in this case. After each iteration both the velocity and the position of each particle is updated with the particles own and groups best position attained.

2.5 Security

Security is a very important aspect for any real time application. It is a critical aspect for securing the data when it is transferred from the source to the destination. The data must be protected from hackers, attacks, or rogue nodes while it is in transit from source to the destination. In case of WSNs security the routing protocol should fulfil as many objectives as it can.

2.5.1 Security Objectives

WSNs are prone to several different types of attacks when the data is being transmitted in air and is prone to eavesdropping during transit. Listed below are the security objectives which need to be taken into account while designing any routing protocols for wireless sensor networks [18].

a) **Authentication-** This means that the nodes involved in the network should be the one they claim to be. The process of authentication fails after an adversary node injects malicious packets in the data while being transmitted ending up modifying or altering the data packets.
b) **Confidentiality-** It is imperative to ensure that the data is only accessible for whom it was intended. Confidentiality ensures that the data should not be revealed to any one for whom it is not intended during the transition phase.
c) **Integrity –** Refers to data corruption and data loss during transmission. Integrity check ensures that the message cannot be modified by attackers while it is transmitting from the source to destination.
d) **Availability-** This is important to guarantee the working of the network in case of node failure or in case of attacks.
e) **Freshness-** As the name implies it means the data is always the most recent one and that no adversary can replay old messages. It is extremely vital when shared keys come into play for transferring data, and an adversary can launch an attack.

2.6 Cryptography

Online communication, transactions, and e-commerce play an important role in transferring large amounts of data. The data transmitted from the sender might be transmitted through an insecure medium. This data might be sensitive or classified data in certain industries and therefore it needs a different level of protection to secure it from unintended users. Different techniques and algorithms are being employed to guard and prevent data breaches.

Cryptography is one of the popular techniques used to secure the data from intruders using two sub-processes known as encryption and decryption. Encryption refers to the process of converting

data in a form which makes it impossible for hackers from being able to access the original data. It converts the plain text to an unreadable form known as cipher text which is scrambled data. After the data reaches the destination then it is decrypted by an authorized individual or entity to recreate its original form. Cryptographers tend to divide encryption algorithms based on the type of transformation and the keys [19]. Some of these require prior agreement on secret key irrespective of the normal communication protocol. A list of such algorithms / techniques used for encryption and decryption of data is discussed in the figure below.

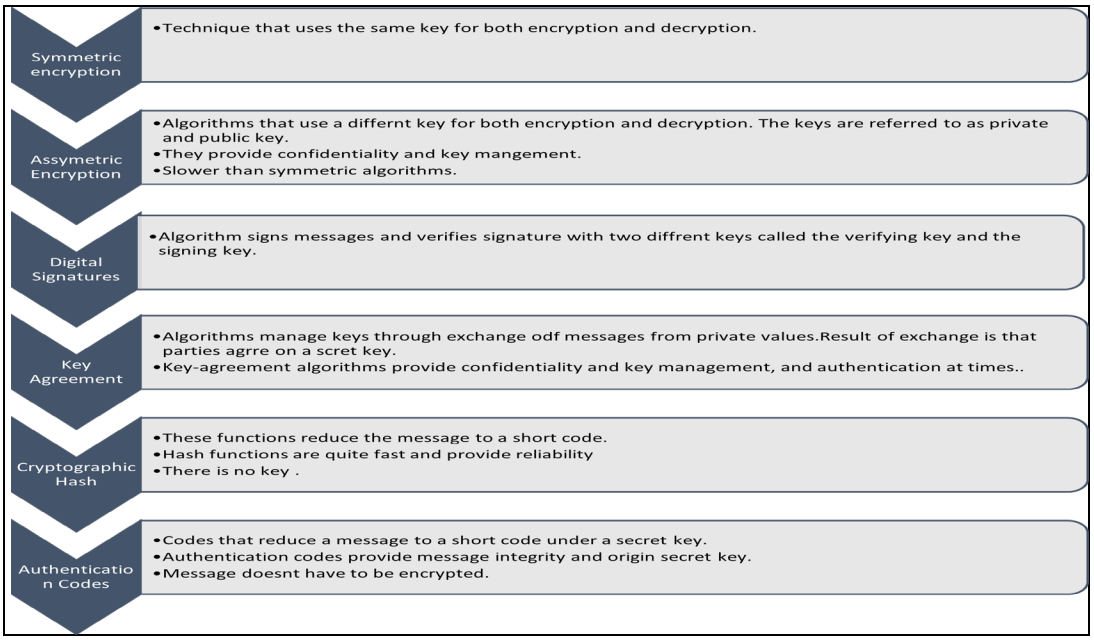

Figure 2. 8 Encryption Techniques

2.6.1 AES Algorithm

AES is an iterative cipher, which relies on the expansion of key to encrypt and decrypt using the same key for both the processes as well as mathematical calculations. It usually operates in rounds where each one has a new key.

The algorithm is divided into three different types i.e., AES-128, AES-192 and AES-256. This classification is based on the size of the key in bits for both encryption and decryption process.[20] The key size is responsible for determining the level of security hence, greater the key size greater the security.

The AES algorithm uses a round function consisting of four byte-oriented transformations for encryption as listed below.

Substitute byte
Shift row
Mix columns
Add round key

2.6.2 RSA

RSA public key cryptography is also known as asymmetric encryption which uses two keys for execution. The receiver generates both the public and the private key. The public key is then used by the sender to encrypt the message and send it to the sender. The data after encryption as a cipher text is then forwarded to the receiver where it is decrypted using the private key. The private key is not obtained from the public key thereby keeping the data safe even if the public key is compromised. This algorithm works well for data encryption and digital signatures.

This technique is known for authentication, non-repudiation, and key exchange purposes. The algorithm relies heavily on the breakup of two large prime numbers used for creating the public and private key [21].

Wireless sensor networks refer to a group of sensor nodes that are randomly placed in a monitoring area where that area might be huge, difficult to access, prone to danger and so. Sensor nodes form the basis of these networks and are responsible for continuous data sensing and then transmitting them to the sink. The data may be aggregated using several different techniques and similarly forwarded to the base station based on a particular criterion using many classical or intelligent based protocols. Nonetheless, any technique used would always suffer from energy loss since the data is transmitted from a certain distance and once the sensor runs out of battery it is difficult to replace it. At the same time data can always be compromised when transmitted as plain text so secure transmission is also an important factor. This security can again be achieved through several different algorithms, but the objective is to transmit the data with security while saving on energy.

Chapter 3

Literature Review

This chapter discusses the existing techniques in wireless sensor networks for clustering, as well as protocols for routing the data using minimal energy. It also discusses the different techniques available for encrypting the data each with its own advantages and disadvantages leading to creation of a proposed algorithm that balances both the energy consumption and security.

Routing is essential in WSNs to support reliable data transfer, achieve low latency and provide energy-efficient operation. Wireless communications consume significant amount of power for transmitting sensed data from sensor nodes to sink nodes. However, the power consumption has become a limiting factor because most sensor nodes are powered by batteries. Sensor nodes in wireless networks have limited computational capability and cannot have full information about networks hence it is very difficult for nodes to calculate the optimum route to the destination quickly. Even when a node can obtain the optimum routing path, the path may not remain optimum over time owing to various types of changes in the sensing environment, for example, the node movement, unstable wireless channel conditions and dynamic energy status of sensor nodes.

While the data is being transmitted from the nodes to the sink certain applications require the data to be secure all the way from the nodes till the end. This requires the use of encryption algorithms which vary in terms of their strength and the energy consumed for securing the data.

3.1 Existing Techniques for clustering and routing

Kamaljot Singh [22] discusses the variants of leach-based protocols in terms of their advantages and disadvantages. According to the writer the energy consumption in the wireless sensor networks is an important factor that enhances the lifetime of the network. Many protocols are available for routing and energy conservation of which LEACH is one of the best for energy conservation. It is one of the most important clustering based hierarchal routing protocols due to its scalability. Since LEACH is associated with several advantages and disadvantages therefore,

several variants were developed to overcome the weaknesses.: LEACH-A, LEACH-B, LEACH-C, LEACH-Cell, LEACH-E, LEACH-EEE, LEACH-F, LEACH-K, LEACH-M, LEACH-S, LEACH-TL, LEACH-V are compared in the paper. The paper concludes that although several variants of LEACH exist that prolong the lifetime of the wireless sensor network each with its own pros and cons nonetheless, there is always going to be room for a better, more efficient, and scalable clustering scheme since none of these existing ones are perfect in all aspects.

Shiv Ashish Dhondiyal et al. [23], proposed the SM-MODLEACH protocol which is an enhancement to the existing MODLEACH protocol. It focusses on enhancing the network lifetime by implementing the square measure algorithm. It focuses on a specific kind of sleeping method for sensors inside a cluster to augment the existence of sensors. The two main parameters which have been optimized in this algorithm include the network soundness and the network period time.

Mortaza Fahimi Khaton Abad et al. [24], proposes modifications in the LEACH protocol to reduce the energy loss if two cluster heads are in proximity which then leads to an increased energy consumption. The energy loss is proportional to the number of cluster heads in the area. An important precondition for this algorithm though, is that when the cluster heads are close then the distance between them becomes negligible. The algorithm modifies the equation for T(n) such that the cluster heads are produced progressively during the CH generation phase, after which a node decides if it is a suitable cluster head based on its existing location as well as the location of other cluster heads. If the sensor node is near an existing cluster head, then this node gives up being a cluster head. The algorithm operates by dividing the network into three parts. The nodes in a specific region example G1 compete to become a cluster head and after its selection broadcasts the information to all the nearby nodes. When nodes in region G2 receive the message, the position of the cluster head in G1 is considered. When a node in G2 is close to the cluster head in G1, the node will be discarded to ensure that the CHs are not in proximity. When certain nodes stop competing to become a CH, it reduces the total number of cluster heads, but doesn't affect the network energy. When any node is excluded from becoming a CH it broadcasts a message to the network, modifying the value of T(n) and increasing the probability of other nodes to be selected as a cluster head.

Saiful Islam et al. [25] proposes a centralized protocol where the base station is responsible for selecting the cluster head after the sensor deployment and network formation. Firstly, the base

station calculates the radius for calculating node neighbors and optimum number of clusters. The main factors identified for CH selection include the following: Firstly, the Residual Energy (RE) with its' major drawback that if there are a greater number of contestant nodes for CH with the same or higher energy this could lead to an unstable situation in the network. Secondly, neighbor numbers (NN) with a one hop neighbor information restricting more than one CH in a cluster reducing back transmission and saving energy. The distance from the BS to CHs to select the nodes closer to BS as possible and save energy while transmitting the data to the BS and increasing the networks lifetime. The energy saving mechanism relies upon energy information, neighbor CH, neighbor information and status and distance from base station through clustering and data transmission to identify the improvement.

Li XingGuo et al. [26] shows that the LEACH protocol selects cluster heads according to the random number generated by the node along with a threshold value, which does not take energy into account and therefore may result in the low energy node becoming a cluster head and bringing untimely death to the CHs while affecting the network lifetime. The modified algorithm considers the residual energy of nodes enabling those with higher energy to be cluster heads and prolonging the network lifetime by avoiding low energy nodes to be cluster heads. The modified algorithm shows an improvement over the LEACH protocol in terms of network lifetime, stability period, amount of data and energy utilization.

Riham S. Elhabyan et al. [27] proposes an algorithm where the set up begins with neighbor discovery when each sensor node in the network broadcasts its ID along with other information. The receiving node updates its neighbor table with the ID and Received Signal Strength Indicator (RSSI). The protocol uses flooding to transmit data to the BS. Each node broadcasts its ID, residual energy, and neighbor table data. Node receiving this packet will rebroadcast the information till it reaches the BS which executes the PSO algorithm to identify the best CHs. Nodes with above average energy are eligible to be a CH for a round to ensure it has sufficient energy. The best CHs adjust the combined effect of energy, link quality, and network coverage. For balancing the energy, the role of the CHs is rotated amongst all nodes. After the BS wraps up the configuration of the network, it repeats flooding to transfer the configuration to all the nodes and the other nodes employ TDMA to communicate data to its relevant CH. Non-CH nodes enter the sleep state to

save up on energy after they have transmitted the data. The modified protocol enhances the energy efficiency of WSN while maintaining an appropriate data throughput.

Muhammed Tay and Arafat Senturk discuss "A New Energy-Aware Cluster Head Selection Algorithm for Wireless Sensor Networks" [28] for selecting the most appropriate node as a cluster head (CH) according to clustered sensors to minimize the energy consumption. They propose a new type of clustering algorithm for WSNs to reduce energy consumption and extend the life of the network. The Cluster Centered Cluster Head Selection Algorithm (C3HA) gives a new outlook to the CH selection while creating a more efficient WSN than LEACH, and PEGASIS. The technique selects CH near the cluster centers to minimize energy usage while transferring data from the nodes to BS. After the sensors in CC and OCC are identified for each cluster, priority is given to the sensors for becoming a CH in the central cluster. The sensors in the central cluster are prioritized to reduce total energy consumption by sending sensed data at the receiving end over a shorter distance. The technique ensures that the cluster heads accepting packets from the sensors will be closer to the cluster center and the energy consumed by the sensors can be reduce based on the distance.

Akhilesh Panchal et al. [29] RCH-LEACH in the paper titled "Residual Energy based Cluster Head Selection in LEACH for Wireless Sensor Networks" based the cluster head selection on various parameters e.g., node's energy, Euclidean distance, and randomness. The paper discusses a Residual Energy based Cluster Head Selection in LEACH (RCH-LEACH) for stabilizing the formation of clusters in the network. Additional parameters including threshold energy, residual energy of the nodes, and the optimum number of clusters are additionally considered for the cluster head selection. The RCH-LEACH algorithm improves the FND value and simultaneously stabilizes the number of clusters formed in the network compared to other algorithms.

Xu-Xing Ding [30] in the paper "An Optimized Cluster Structure Routing Method Based on LEACH in Wireless Sensor Networks" proposes an improvement in the K-Nearest-Neighbor (KNN) algorithm to determine the most apt initial center and number of clusters of K-Means in the algorithm (ICD-KNN). The two main stages in the algorithm include the clustering and position estimation stage. The clustering stage employs K-Means based on Canopy to improve the efficiency and clustering accuracy of K-Means algorithm. The position estimation stage sets the

threshold according to the dispersion in reference points to improve positioning accuracy. When the proposed algorithm of ICD-KNN is compared with previous algorithms such as DH-KNN. ICD-KNN optimizes K-Means algorithm using the Canopy algorithm and helps improvise both the clustering partition speed and accuracy. The dynamically set threshold coefficient for each cluster set by dispersion improves the positioning accuracy and the real-time performance. The K-means algorithm has been modified to preprocess the data offline, and in the online stage the positioning accuracy is improved through the dynamic threshold. The main setback with this algorithm happens to be the larger positioning error in the location of cluster boundary.

Sina Einavi Pour [31] in the paper titled "A new energy aware cluster head selection for LEACH in wireless sensor networks" suggests a new CH selection algorithm based on the residual energy, position, and centrality of the nodes for an energy balanced network. Before the selection of the cluster heads the algorithm considers the distance between nodes and sink, network density and residual energy of nodes. When the nodes start to give up that decreases the network connectivity along with a decrease in the number of direct transmissions between the nodes and sink. It is based on single hop communication to manage the energy consumption. If some CHs act as relay nodes and transmit their data to the sink through them, the network energy usage will be decreased. Routing tables in WSNs need constant updating since routes are constantly changing. Results clearly prove that the algorithm outperforms LEACH, Multi-hop Routing with LEACH (MR-LEACH) and Enhanced Multi-hop LEACH (EM-LEACH) with respect to multiple parameters which include the energy consumption, increased network lifetime and reliability.

In [32] Turki Ali Alghamdi presents an optimized cluster head selection model. The sensors in the network are fueled by batteries which tend to die down after a certain time. In th process of clustering, the selection of cluster head (CH) is one of the most important aspect responsible for energy efficient routing to minimize transmission delays in WSN. The proposed algorithm has suggested a new clustering model with optimal cluster head selection by considering four major criteria like energy, delay, distance, and security. The algorithm is a blend of the well-known dragon fly and firefly algorithms. The proposed work has been carried out in comparison with the normal working models with respect to the count of alive nodes, network energy, delay and risk probability. It has been analyzed with respect to convergence analysis, alive node analysis, normalized network energy, delay analysis, risk probability analysis and algorithmic analysis. The

FPU-DA model-based cluster head selection in wireless sensor networks proved to be the best among all the others compared. The objective function considers the distance and delay, as well as other restraints for improved performance.

Trupti Mayee Behera et al. [33] in "Residual Energy Based Cluster-head Selection in WSNs for IoT Application", discuss an efficient cluster head scheme where the cluster head rotates amongst the higher energy nodes. The algorithm considers residual and initial energy values to identify the cluster heads for the network. The main aim of the algorithm is extending the lifetime of the network by monitoring the networks energy dissipation and is useful in real life scenarios such as environmental monitoring using IoT since it works well for homogeneous networks as compared to the classical algorithms like LEACH.

Edla et al. [34] in the research have employed the particle swarm optimization algorithm for effective routing in wireless sensor networks for extending the sensors lifetime. The routing has been achieved through a novel fitness function keeping the relay load factor and the number of relay nodes between the gateways to base station. The proposed algorithm is evaluated in terms of network lifetime, number of hops and average relay load under two different WSN topologies. The results revealed that the proposed PSO-based routing algorithm increased the lifetime of the network and reduced the average relay load by increasing the number of hops when compared with other routing protocols like GA. The proposed algorithms fitness function outperformed the basic algorithm in terms of the performance.

Sundar et al. [35] has floated the idea of clustering revolving around CPSO with one additional dimension as well as a new initialization algorithm referred to as MPSO. Each modification to CPSO was introduced individually, and the clustering was tested on ten datasets. The performance for each change is compared with the CPSO through external validity indices while the performance is determined using z – test. The SIL index is used as a fitness function for each of the cases. The solutions were handled through velocity clamping and saturation correction strategies. The limitation of this technique requires prior knowledge of the total count of clusters. The three main performance factors considered for MPSO are TRC, FR, and TCss. MPSO proved its cost-effectiveness and outperformed in terms of TRC and TCss.

Kulkarni et al.[36] in their research discuss that WSNs are faced with a set of challenges which include the size and density of monitoring, environmental conditions, and resource constraints

such as energy, memory, bandwidth, and processing. Optimization problems include node deployment issues, localization, energy-aware clustering, and data aggregation. PSO is a popular technique used to speed up optimization problems in WSNs because of its simplicity, best possible solution, fast convergence, and insignificant computation cost. PSOs iterative nature prohibits the use of the algorithm for high-speed real-time applications. It also suffers from the large memory requirement which limits its implementation. Data aggregation needs frequent distributed optimization and fast solutions. PSO is highly suited to an environment where issues of static deployment, localization, and clustering are resolved only once at the sink.

Sumit et al. [37] in the research have worked on an efficient clustering technique to enhance the lifetime of the network and make the communication process efficient and reliable. Their focus is a PSO based technique for detection of malicious nodes and cluster head selection. The technique is based on three main parameters which include the residual node energy, sponsored coverage, and the link quality to decide the best node for each WSN. The proposed algorithm (PSO-NMDC) suggests a spatially distributed technique for the cluster head selection, minimizing the clusters overlapping and increasing the energy efficiency. It identifies the nodes which are malicious and does not allow them to become a cluster head leading to a fault tolerant network.

3.2 Existing techniques for data security and encryption

Joseph Raphael et al. [38] proposes a simple and light encryption algorithm to convert plain text to cipher text through the generation of Fibonacci numbers where each character is extracted from the message and swapped with a different character. The message is converted from plain text to cipher text, followed by Unicode symbols and later transmitted as a text file making the decryption process difficult. The ASCII code of each of the cipher text character, original character, and the next character are all summed up together. The process of encryption uses four ASCII characters as a security key to encrypt the cipher text characters to Unicode symbols whereas, decryption works with two keys. Each text file symbol is mapped to determine the hexadecimal value, to determine its equivalent plain text. At the recipient end, Unicode symbols are converted to hexadecimal and decimal values using the same key and encryption algorithm. The suggested algorithm jumbles up the plain text using swapping and other operations to enhance security. Unicode symbols are quite difficult to decode therefore, making it difficult to retrieve

from the text file and making it impossible for an unknown individual to be able to decode that information. They reduce the chances of snooping while data transmission is taking place. Even if the information is captured and converted to hexadecimal values, nothing can be accomplished until the key is known.

V. Elamurugu et al.[39] in the paper presents a lightweight, energy-efficient, encryption technique using a dynamic salt key. The encryption technique is both reliable as well as low power consuming. The three main steps involved in the algorithm are salt generation, followed by the format-preserving encryption based on the salt key and lastly decryption. The salt value is randomly generated based on alphabets and digits, converted to ASCII and then its corresponding hexadecimal value. The salt value and its corresponding hash is also generated. The message is then converted into a matrix to which the salt is added. The matrix generated is then converted to a message, which after converting to a binary value is then applied FPE to generate the cipher text. Decryption is simply the reverse of encryption. The algorithm achieved both a reduction in energy consumption and time complexity.

Thiruppathy Kesavan Venkatasamy et al. [40] suggested a Cluster Based Dynamic Keying Technique for wireless sensor networks (WSN). The cluster head is enabled with a global positioning system (GPS) to determine a combined cost value (CCV) stored in the memory table for each sensor node consisting of three main parameters which include the node degree, its location, and virtual battery power. The encryption key changes dynamically thru the sensors' CCV, hence eliminating the need to re-enter the key and thereby saving energy. Separate dynamic keys are generated by each cluster head using RC5 encryption mechanism. It is followed by the source cluster head forwarding data through different clusters to the sink to verify the authenticity, data integrity and nonrepudiation as well. When the aggregated data needs to reach the sink, it is divided into segments according to the threshold secret sharing algorithm. The routing mechanism is a multi-path dispersal technique which considers the nodes location and its degree therefore it is equally applicable for mobile nodes as well. The main advantage of this algorithm over others is that because the keys are dynamic hence the approach is resistant to node capture attacks and secondly since the key is not updated regularly hence it helps in cutting down the cost of energy consumption.

ChunHua Cao et al. [41] proposes an improved identity-based encryption algorithm for wireless sensor network security. The proposed algorithm executes by dividing the user's private key into two parts one controlled by the PKG while the other is controlled by the users themselves. The technique is different from others in that it does not require the public key certificates nor the management of those certificates. This technique helps not only in encryption but also resolves the two main challenges of key escrow as well as its revocation. The proposed IIBE algorithm simulation seems highly suitable for deploying in WSN environments involved with high security.

Daniela and Giovanni [42] improved the application of AES in WSN. The algorithm suggested seven rounds of encryption along with the table lookup to optimize each round of operation. The algorithm results revealed the algorithm to be 13 times more efficient than the AES algorithm and takes up less than 1 KB for storage. When the proposed algorithm is compared to AES it turned out to be slightly weaker in terms of security but works well for WSN with limited energy.

Rachkidy et al. [43] suggests a technique for data storage with homomorphic encryption for wireless networks with real time data referred to as DIOS. In case of the underwater sensor networks researchers are concerned with the whole data rather than data at a particular time. Networks generally deal with large amounts of data and data loss is also bound to happen if the data is transmitted over longer distances. In the proposed algorithm the data is stored in a relay node in advance and processed in advance to keep it from scattering and interrupted data transmission. Homomorphic encryption is used to secure the algorithm. The technique is effective for saving energy and data securely in most cases. However, it is not suitable for most net laying environments.

Huda A. Babaeer et al.[44] in their research focus on a secure sinkhole detection and transmission model using homomorphic encryption and watermarking especially for time-critical applications. Sensor nodes are limited in terms of their battery and other resources and are ideal for use in harsh and tactical environments. TEEN is a very important protocol known for applications dealing with energy and time critical applications although it is not well known with respect to security and is prone to hacking. The paper suggests several measures which include cryptography based on identification and authentication. Public key encryption is an effective technique but computationally expensive. The algorithm proposes a lightweight secure technique

based on Threshold Sensitive Energy Efficient Sensor Network protocol and watermarking technique to guarantee data integrity during transmission relying on the communication techniques present in TEEN. Homomorphic encryption provides speedy and effective encryption while minimizing the energy usage while identifying nodes for the sinkhole detection as well as prevention. Each packet is stamped with watermark for data authentication, which is produced by a combination of message authentication function and a pseudo-random number generator. The data is secured during the transmission by encrypting the ids of the sensor nodes. The algorithm has increased the level of security by detecting the attacker node before the attack and attempting to identify any data tampering.

LongTeng Yi et al.[45] suggests usage of chaotic and stream block ciphers in WSN based on their low energy consumption. Chaos is gaining popularity in cryptography research and is moving towards novel chaotic ciphers for WSN. A lightweight encryption technique has been recommended based on S-box focusing on the memory in terms of its cost and efficiency while keeping in mind the limited power of computation and communication capability of WSN. The algorithm focuses on designing a new S-box based on the compound chaotic map, sinusoidal chaotic map, Baker map, and linear congruence generator. It is followed by a unique method of generating circle subkeys and F functions based on the S-box. The simulation results show that it performs well in terms of high security and low resource consumption ideal for WSN.

Bander A. Alzahran et al. [46] proposes an efficient cryptographic technique using modified Diffie–Hellman in wireless sensor networks. In WSN sensor nodes are used to sense different environmental conditions such as temperature, rain, humidity, sound, vibration, and position. Data security is a major issue when the data travels over wireless channel and attackers may gain access to critical information. Secure efficient encryption algorithms like the DH is quite vulnerable to the man-in-the-middle attack. The proposed modified Diffie–Hellman has been modified by generating a hash of each value that is transmitted over the network.

In the study by Elhoseny et al. [47] proposes an algorithm which is built up on GASONeC based on genetic algorithm to build the network structure in the form of clusters. ECC is used for exchange of public and private keys because of its ability to provide high security with a small key size. The proposed 176-bit key is produced with a combination of ECC key, node id, and distance from cluster head (CH). The proposed algorithm works well not only for data but for images as

well. This technique is also helpful in preventing passive attack, CH compromised attack, as well as brute force attack.

Osama A. Khashan et al. [48] proposes an automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. The authors propose a FlexCrypt, automated lightweight cryptographic scheme for WSNs. It is based on a dynamic technique that supports node mobility and rotation of the CH. It also presents a flexible lightweight cryptographic method to control the encryption complexity by automating the selection of encryption parameters based on the current resources of each node to encrypt the data. The security analysis demonstrates that ta resistance to the brute-force attack, eavesdropping, man-in-the-middle and replay attacks.

Haythem Hayouni et al. [49] in the paper proposes a novel energy-efficient encryption algorithm for secure data in WSNs. In this paper, the major focus is the encryption algorithm complexity. Most of the encryption algorithms provide security but suffer from a high cost of computation, require large storage. The research is based on a Feistel structure with an ultra-light encryption algorithm, named ULEA. It is based on simple transformations, diffusion, and confusion of data and functions to form the cipher text. The ULEA algorithm proves to be a low storage space and energy-efficient encryption process with high security for WSN.

After a thorough reading and understanding of the different techniques and algorithms used for clustering, routing, and encryption along with their advantages and limitations the proposed algorithm was formulated.

Chapter 4

Design and Methodology

This chapter discusses the proposed algorithms for cluster head selection based on the residual energy, followed by routing of the data from cluster heads using PSO algorithm and data encryption using a lightweight technique have been discussed. Various parameters used in the algorithms along with their values have also been discussed.

Data security and information secrecy is one of the most important research areas in the world of wireless communication due to the increasing use of data transmission through wireless means. The sensor nodes are responsible for communicating critical and sensitive data hence, it's important to ensure that no hackers or eavesdroppers intercept the information in transit and thereby gain access to the critical and valuable information. Data encryption using a preexisting shared key is a common way of ensuring data confidentiality which ensures that information is only accessible to the receiver for whom the information is intended. Most of the methodologies used for encryption / decryption increase the cryptographic security but an increase in the computations leads to an increase in the resource consumption such as energy.

The sensor nodes in a wireless sensor network are typically resource-constrained, hence are limited by energy, storage, and processing power. They are powered by tiny devices which can neither be replaced nor recharged and hence die after a certain time. Therefore, the focus of this research is to ensure that the energy consumption is reduced to a minimum and the network kept alive for a longer time while managing the security to ensure that data is not compromised.

4.1 Proposed Algorithm

The proposed algorithm starts with the selection of the cluster head using the well-known LEACH algorithm. The LEACH algorithm is well suited for energy conservation hence, a modified version of LEACH focusing on one of the most important parameters namely residual energy has been used for the selection of cluster heads. After the selection of the cluster heads the data is then routed from the cluster heads to the base station using the Particle Swarm Optimization Algorithm (PSO) . The data from the nodes is encrypted and then communicated to the cluster

head. The data from multiple nodes is then aggregated at the cluster head. Data is then routed from the cluster head nearest to the base station using the PSO algorithm. Encryption is carried out using a light encryption scheme supported by a light-weight key management scheme. This technique ensures that the data is transmitted securely, using a data encryption mechanism that is both secure and low power to minimize energy consumption. Data is decrypted at the sink.

The main phases of data transmission along with encryption can be summarized as listed below .

Step 1: Cluster head selection

Selection of cluster head can be made based on several factors, but our algorithm focuses on the cluster head selection based on residual energy. The cluster heads are selected based on the threshold value that is calculated. The first cluster head is determined on the basis of the probability/ random value whereas the repeated iterations determine the cluster head by calculating the threshold value where the residual and initial energy are considered.

Step 2: Cluster Formation

After selection of the cluster heads, the clusters are formed based on the value of the received signal strength indicator.

Step 3: Data Transmission using PSO

After the clusters are formed the data is aggregated at the cluster heads and then transmitted from there to the base station using Particle Swarm Optimization (PSO) Algorithm.

Step 4: Encryption and Key Management

The data is transmitted from the nodes to the cluster head, and onwards to the base station using a lightweight key management mechanism, encrypted throughout the transmission.

Flowchart of the Proposed Algorithm

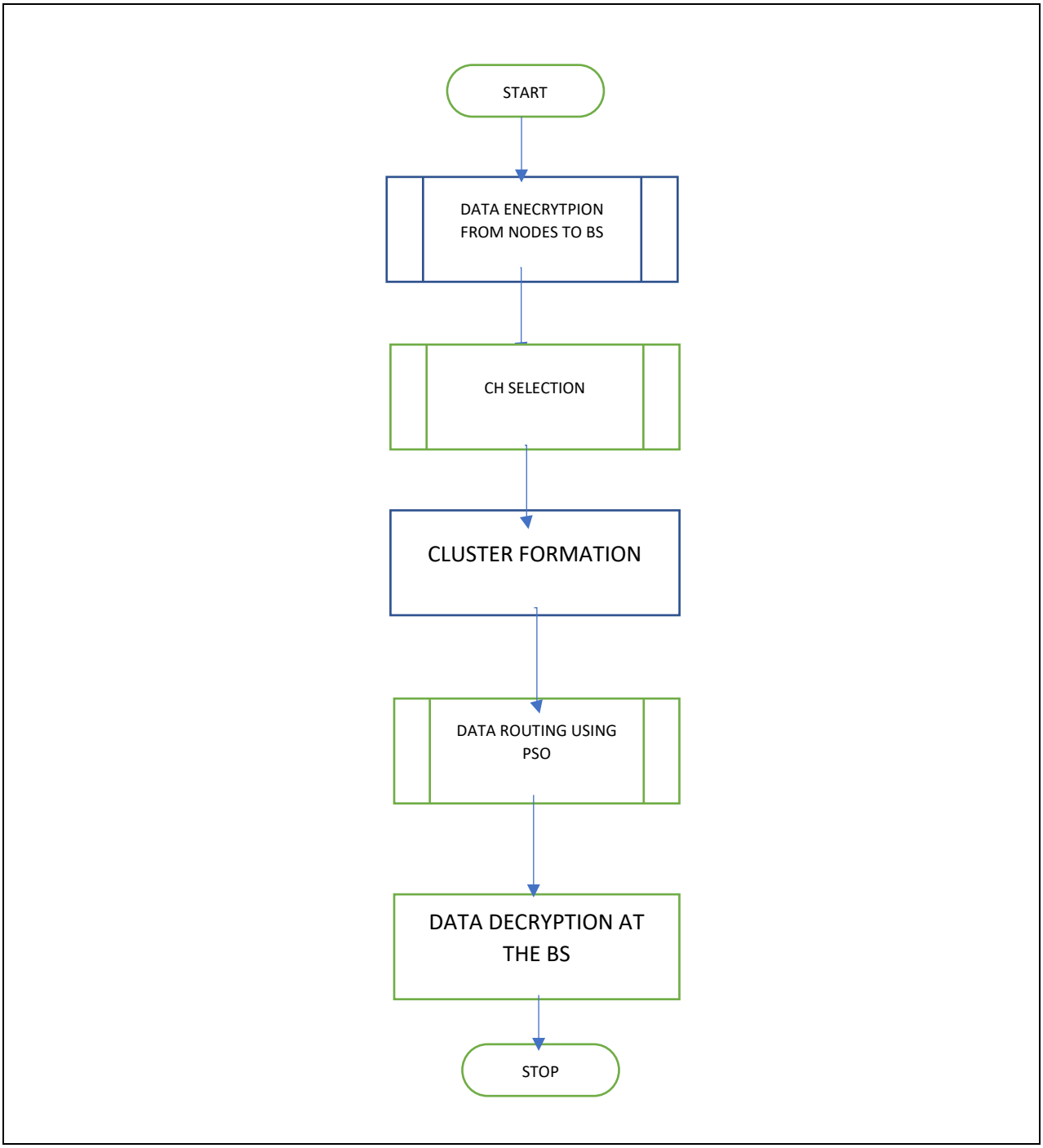

Figure 4. 1 Flowchart of the Proposed Algorithm

Table 4. 1 Symbols and their description

Symbol	Description
CT	Cipher text
PT	Plain text
CH	Cluster head
CH_{id}	Cluster Head ID
H_{id}	Hashed cluster head ID
K	Key pool
d_0	Threshold distance
P	Probability
S_k	Session key
M_k	Master key
Sym_k	Symmetric Encryption key
T(n)	Threshold value
C_{opt}	Optimal number of clusters
ε_{fs}	Energy consumed in free space
ε_{mp}	Energy consumed by
E_{Tx}	Energy consumed by transmitter
E_{Rx}	Energy consumed by receiver
M	Network Area
N_a	Number of alive nodes
E_{Res}	Residual energy
E_{Ini}	Initial energy
B	Block size in bits
K	Key selected from the key pool
Pty	Parity bit
R	Number of rounds
Enc_{Paras}	Encryption parameters
Stb_r	Rotation start bit
C_b	Cipher Block

4.2 Wireless energy transmission mode

The radios energy consumption model for data transmission in wireless sensor networks for k-bit data is shown below in figure 4-2. The figure depicts a simple model for the energy dissipation where the transmitter is responsible for dissipating energy to run the electronics and amplifier whereas, the receiver consumes energy to run the electronics.

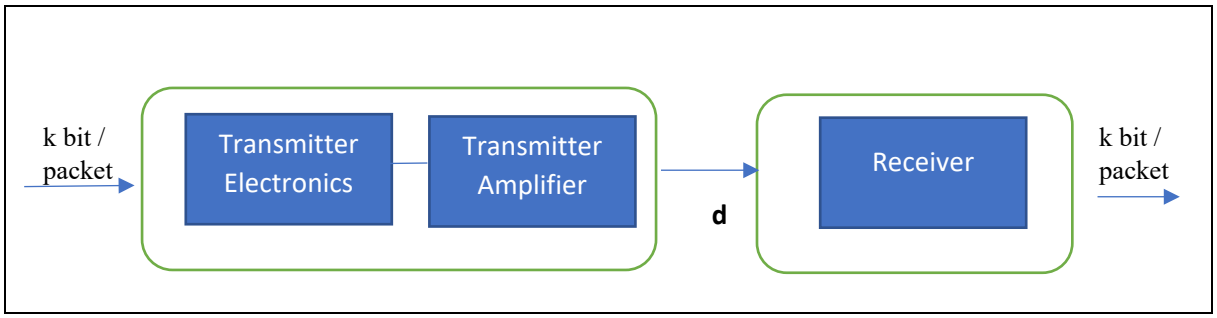

Figure 4. 2 Wireless Energy Transmission Model

The energy consumption of the transmitter consists of two distinct components each responsible for its own job which include the transmitting circuit and the power amplifier circuit. At the receiving end the receiver is responsible for receiving the data at a distance **d** from the transmitter circuit. We can therefore summarize the total energy consumption as shown below in eqn (1).

$$E_{Total} = E_{Send} + E_{Receive} \qquad (1)$$

The energy required to transmit the data at a distance d from the transmitter to receiver circuit is given below in eq.(2)

$$E_{Tx}(k,d) = E_{Tx_{elec}} * k + E_{Tx_{amp}}(k,d) \qquad (2)$$

$E_{Tx}(k,d)$ represents the energy consumed when transmitting k bits of data over a distance d . $E_{Tx_{elec}}$ represents the energy consumed by the transmitter and $E_{Tx_{amp}}(k,d)$represents the energy consumed by the power amplifier. Equation (3) and (4) below represent two additional parameters which are referred to as Ɛfs and $Ɛ_{mp}$ which correspond to the amplification energy. They represent the energy consumed by the amplifier for short and long distance respectively. The

propagation loss for short distance is given as d^2 and the propagation loss for longer distance is given by d^4. If the distance d is less than the threshold distance d_0 then the free space model equation (3) is used; otherwise, equation (4) for multi path model is used.

Now the value of $E_{Tx_{amp}}(k, d)$ can be substituted by one of the equations below depending on the kind of the model being used. $E_{Tx_{Elec}}$ represents the energy consumption by the radiating circuit for processing 1-bit of data.

$$E_{Tx}(k, d) = E_{Tx_{elec}} * k + \varepsilon_{fs} * k * d^2 \quad \text{if } d >= 0 \text{ and } d < d_0 \quad (3)$$

$$E_{Tx}(k, d) = E_{Tx_{elec}} * k + \varepsilon_{mp} * k * d^4 \quad \text{if } d >= d_0 \quad (4)$$

The equation below calculates the threshold distance which happens to be the ratio between the free space and amplification factor.

$$d_0 = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}} \quad (5)$$

The equation below represents the energy consumed at the receiving end of the circuit by the receiver for processing *k*- bit data.

$$E_{Rx} = E_{Tx_{elec}} * k + E_{Rx_{elec}}(k) \quad (6)$$

The aim of clustering is to group the scattered sensors of the network into groups each headed by a cluster head. Cluster heads are ordinary nodes with additional responsibility of aggregating the data from the nodes belonging to its cluster, and then forwarding it to the base station or sink. The cluster heads are employed so that instead of hundreds or thousands of sensors forwarding data to the sink directly, making it difficult for the sink to manage the data along with the security, it's better to handover the job to a single node having more energy as compared to the other nodes in the cluster. This helps in reducing the energy consumption and increasing the networks lifetime.

4.3 Cluster Head selection

The aim of clustering is to group the scattered sensors of the network into groups, each headed by a cluster head. Cluster heads are ordinary notes with additional responsibility of aggregating data from the nodes belonging to its cluster, and then forwarding it to the base station. The cluster heads are employed so that instead of hundreds of thousands of sensors forwarding data to the sink directly and creating congestion, it is better to hand over the job to a single node with higher energy as compared to the other nodes in the cluster. This helps in managing the energy consumption and increasing the network lifetime.

The wireless sensor nodes sense the data from their surroundings and transmit their IDs along with the encryption parameters to the sink/ base station.

The selection of a cluster head is dependent on several factors which include but are not limited to the residual energy, nearest neighbors, initial energy, radius of network, and proximity from the sink. According to the literature review conducted [24],[25][,[29],[33] strongly recommend and through their results clarify that cluster head selection based on residual energy greatly reduces the energy consumption and increases the lifetime of the network.

The cluster head is selected on the first iteration based on the equation (7) given below. Initially for the first iteration a node randomly chooses a number between 0 to 1, if the number is greater than the threshold T(n) then the node remains a normal node, else if the value is less than the threshold T(n) then the node becomes a cluster head.

In the equation below T(n) represents the threshold value, P refers to the desired percentage of nodes to become a cluster-head, r refers to the current round and G is the set of nodes that have not been selected as a cluster head in the last 1/ P rounds. After the cluster head has been selected it advertises to all the normal nodes as the new cluster head in the network.

$$T(n) = \begin{cases} \frac{P}{1-P*\left(r*mod\left(\frac{1}{P}\right)\right)}, & n \in G \\ 0, & otherwise \end{cases} \qquad (7)$$

Multiple rounds are needed for data transfer to occur therefore, every node ends up saving some of its energy which would be used to transfer its data to the cluster head. The number of rounds run from 4, 8, 16 , 32, 64 and 128 . The choice of rounds affects both the encryption speed and security. The amount of energy expended to transmit the data depends on the distance between the sender and receiver node. The cluster heads for subsequent rounds is determined using equation (9). The optimal number of clusters C_{opt} can be written as in [33] where the value depends on the amplification factor, number of alive nodes, network diameter and the distance from nodes to the base station.

The value of the optimal number of clusters is important since it is used for the calculation of the threshold value. The equation considers the two amplification factors, symbol N_a represents the total number of alive nodes, M refers to the network area and d_{BS} refers to the average distance from the BS to a node.

$$C_{opt} = \sqrt{\frac{N_a}{2\pi}} * \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}} * \frac{M}{d_{BS}^2} \qquad (8)$$

Our proposed algorithm then uses the modified version of equation (7) to determine the threshold value responsible for finding the cluster heads in the sensor network. The symbols E_{Res} and E_{Ini} below refer to the residual energy and initial energy of the nodes respectively.

$$T(n) = \begin{cases} \frac{P}{1-P*\left(r*mod\left(\frac{1}{P}\right)\right)} * \frac{E_{Res}}{E_{Ini}} * C_{opt} & , n \in G \\ 0 & ,otherwise \end{cases} \qquad (9)$$

The data transmission from nodes to the CHs occurs during the time allocated to each node. Only the transmitting node remains active during the allocated time slot while other nodes turn-off their radios to conserve energy.

After normal nodes receive the announcement of becoming the cluster head, they determine the cluster to be associated with based on the RSSI. They inform the appropriate cluster-heads as a new member in the cluster. The cluster heads follow a TDMA approach based on which they assign a time to the normal nodes on which they can send their data. This approach helps in reducing the congestion on the network since all the nodes cannot transmit the data at the same time and therefore reduce the number of collisions as well.

After all the nodes in the cluster finish data transfer, the CH then starts data aggregation to remove data redundancy and compress the information for proper bandwidth utilization. The cluster-heads aggregate data from the nodes in their cluster before sending it to the base station. The CHs then forward the data from the cluster heads to the base station through multi-hop communication. After a certain time the network restarts with another round of cluster-heads selection.

The cluster head nearest to the base station communicates directly with the base station through a single hop communication mode. If the base station is far from the cluster head nodes, then approximately 80% of the nodes' energy is dissipated because of the long-distance data communication [4]. The amplifier energy consumption to total energy consumption ratio for the free space channel model is about 80% when the distance d ≈141 m whereas, under the multipath fading channel, the same ratio is about 80% when d ≈ 112 m.

Considering real life applications, it is necessary to develop an energy-efficient protocol to decrease the energy loss in wireless sensor networks. [50]

4.4 Cluster formation

After the CHs for existing rounds are selected, they send an announcement to member nodes in the respective clusters. Normal nodes decide the cluster to join based on the Received Signal Strength Indicator (RSSI) which represents the strength of the received signal. The sensing nodes check the signal strength of the request message and decide the cluster head to join. The cluster head is then made responsible for broadcasting the member nodes TDMA schedules so that each one of them transmits the data in their allotted slots to avoid data collision. After the nodes are associated with a particular cluster, a confirmation message is sent to the respective cluster heads. This finalizes the cluster formation. After receiving all the data, the cluster head then starts its job of data aggregation to remove redundancy. This process continues until all the nodes in the network exhaust their energy completely in the rest of the rounds.

4.5 Data Routing Through PSO

Particle Swarm optimization (PSO) is a nature inspired algorithm that draws stimulation from the natural behavior of living things like birds flocking or fish schooling basically dealing

with a crowd or group of things. The individual elements of the group are referred to as particles, and the group of particles is referred to as the swarm. The algorithm basically focusses on determining the global best which represents the best solution using an objective function responsible for determining the minima.

In the proposed algorithm every individual sensor acts like a particle and the clusters form the swarms each headed by a cluster head. Since, multiple cluster heads exist in the overall network, each one can either transmit the data directly to the base station or amongst these cluster heads the one nearest the base station can be determined that can transmit the aggregated data to the base station or sink. This job of identifying the cluster head nearest to the sink is managed by the PSO algorithm and then the data is routed to the base station through the nominated cluster head. If all the cluster heads start transmitting the data to the base station it will create a congestion and increase chances of data collision and deplete energy of the network much quicker since several cluster heads would be forwarding data to the base station. In comparison, if the data is sent to one CH and forwarded it would help retain the energy of so many nodes and extend the lifetime of the network.

There are four important factors which are associated with this function to identify the cluster head responsible for data transmission which include:

1. Velocity of the particle
2. Position of the particle
3. Local best referred to as *lbest*
4. Global best referred to as *gbest*

If we have a total of P particles in all. At any one instance assume a particle i is at location

$$X^i(t) = \left(x^i(t), y^i(t)\right) \qquad (10)$$

where x and y denote the coordinates of the particle i at time t. Apart from the position of each particle each one is also associated with a velocity. Therefore, at any given time the velocity of any particle i at time t is denoted by:

$$V^i(t) = \left(v_x^i(t), v_y^i(t)\right) \qquad (11)$$

After one iteration the position of each particle is updated as follows:

$$X^i(t+1) = \left(X^i(t) + V^i(t+1)\right) \qquad (12)$$

At the same time the velocity of the particles is also updated after each iteration as shown in the equation below.

$$V^i(t+1) = \left(wV^i(t) + c_1 r_1 \left(pbest^i - X^i(t)\right) + c_2 r_2 \left(gbest - X^i(t)\right)\right) \qquad (13)$$

The symbols c_1, c_2, w represent the constants in the PSO algorithm, whereas r_1, r_2 denote random numbers in the range 0 and 1 and $lbest^i$ represents the best position leading to the best function value explored by the particle *i* and *gbest* refers to the best particle in the swarm. The values of *gbest* and $lbest^i$ are updated in each iteration to reflect the best value. The complete process of data routing described above has been clarified using both an algorithm and a flowchart on the next page .

```
Identify the swarm size S according to the count of CH
    for each particle i ∈ [1..no of CH]
            Randomly generate Xi and Vi
        Calculate the fitness of Xi through the fitness function denoting it as f (Xi)
        Set lbesti = Xi and f (lbesti) = f (Xi)
    end for
Set gbest = lbest1
Set f (gbest) = f (lbest1)
    for each particle i ∈ [1..no of CH]
        if f (lbesti) < f (gbest) then
            f (Gbest) = f (lbesti)
        end if  end for
    while t < maximum number of iterations
    for each particle i ∈ [1..no of CH]
        Evaluate its velocity vid (t + 1) using Equation (1)
        Update the position xid (t + 1) of the particle using Equation (2)
        if f (xi (t + 1)) < f (lbesti) then
            lbesti = xi (t + 1)
            f (lbesti) = f (xi (t + 1)
        end if
        if f (lbesti) < f (Gbest) then
            Gbest = lbesti
            f (Gbest) = f (lbesti)
        end if
    end for
    t = t + 1
 end while
return gbest
```

FLOWCHART FOR DATA ROUTING

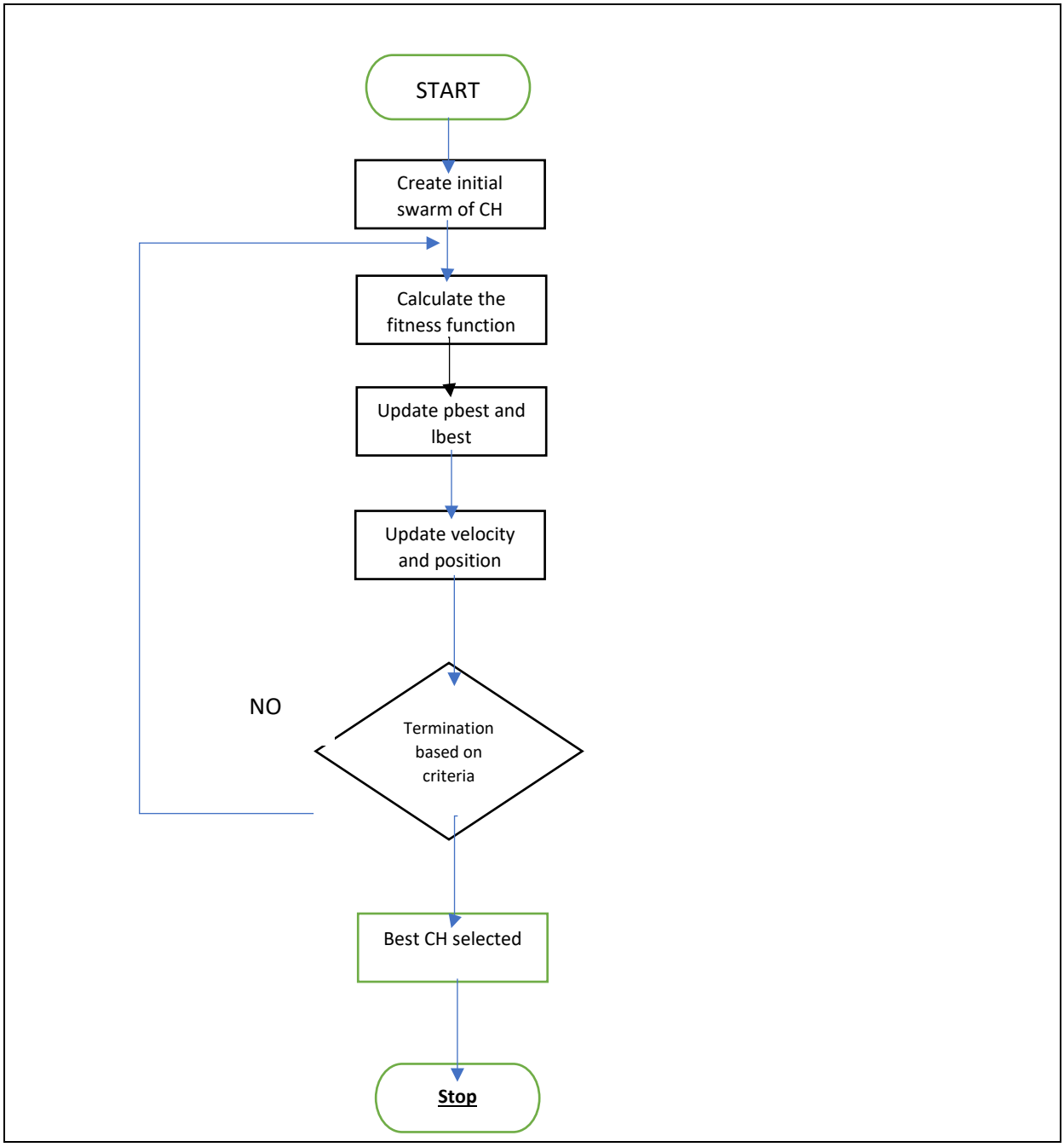

Figure 4. 3 Flowchart for Data Routing through PSO

4.6 Proposed Algorithm

The overall proposed algorithm for transmitting data securely using minimum energy is given below.

1. BEGIN
2. Set the network area and randomly spread the sensor nodes.
3. Select the probability.
4. Calculate the energy using equations.
5. Calculate the optimal number of clusters.
6. Compute the threshold value using P where it decides the percentage of cluster head to be selected in each round.
7. Identify the cluster heads based on the threshold value calculated.
8. Cluster head aggregates the data from non-cluster head nodes.
9. Apply the PSO (Particle swarm optimization) Algorithm.
10. Find the global best path from cluster head to the base station.
11. The data aggregated at the cluster heads is sent to the base station using global best path.
12. Dissipate the energy from cluster head and non-cluster head nodes.
13. When the energy of a node becomes less than the minimum probability value then it is identified as dead.
14. Plot the required results and start a new round.
15. END

4.7 Encryption Process

The balance between security and power consumption is important to increase the lifetime of the network. This balance can be maintained by managing the parameters in different ways. The technique discussed below for the purposes of encryption is a modification of the Flexen Tech algorithm.

Two immensely important factors include residual power (P_{res}) and the distance (d) between the cluster head and the node. Consumption of energy can lead to quick network downtime or unintended delay while processing or transmitting the data. In fact, when we apply security algorithms the calculations and operations involved tend to consume a large amount of energy. Two additionally important parameters for encryption include number of rounds and the block size. Higher the number of rounds more the operations and greater the security of the algorithm. Similarly, greater the block size, more the randomness making it more secure, but []

shows that a block size of 128 is an ideal size to maximize security. Both the above listed parameters can be kept flexible nonetheless that means added computations which can additionally slow down the encryption.

4.7.1 Encryption scheme

Most of the cryptographic algorithm's efficacy focuses on algebraic forms which rely strongly on factors such as: parameter size, memory-time tradeoffs, software/ hardware optimization and mathematical rules. Hence, while designing encryption techniques it is important to consider the parameters listed above and use simple but efficient mathematical operations to carry out the operations in least amount of time using minimal resources and capacity available.

The algorithm revolves around a block-based encryption technique where the data /plain text (PT) is broken down into fixed blocks of b-bit, which means the algorithm takes b-bits as plain text and provides b-bits of corresponding cipher text (CT). We break our data into blocks of max 127 bits. The key (k) is selected by each node from a randomly generated key pool (K) each time data is transmitted. This technique provides improved results when b > 0 and block size is large. Although, the variables b and k have no maximum or minimum limit value nonetheless it is still required to ensure that gcd(k,b) =1.

The technique focuses on two important private parameters: firstly, the key and secondly the plain text /sensor data that needs to be encrypted. An encryption table responsible for random permutations is created consisting of three rows and B columns, where B refers to the number of bits. The first row consists of the values of L_i which are calculated using eq (14) to perform random permutations at the bit level in a block consisting of b-bits. The second row consists of the values of i namely 0, 1, 2 representing the original bit positions whereas the last row consists of the new bit positions after sorting the values of L_i using an appropriate sorting technique of minimum order.

$$L_i = \big(b * (k - i)\big) mod\ k \qquad (14)$$

In each round r, random rotations are applied at the bit-level where the start bit of rotation (Stb_r) is determined using eq (15) and all bits are rotated from the starting value of Stb_r , generated for each round for irregular rotation. The value of Stb_r offers a random permutation in each round, ensures the bit substitutions. The value of nonce added to each round guarantees data uniqueness

and freshness eliminating any additional overhead. For each value of round (r) the same permutations and rotations operations will be applied to the output from each round before the final encrypted information C_b is obtained for each block of size b. After the random rotation based on the value of Stb_r right rotation is carried out for the block.

$$Stb_r = (k * (r + nonce) mod\ b) \qquad (15)$$

The algorithm basically focuses on two types of permutation: the first is by sorting / ordering the values of L_i and the second is achieved through right or left rotation. However, our encryption technique still needs a substitution function to reduce the occurrence of frequency analysis attacks. Therefore, an XOR operation has also been incorporated such that the existing cipher block is XOR-ed with the previously generated cipher block.

$$C_b = C_b \oplus C_{b-1} \qquad (16)$$

After the XOR operation once a cipher block has been created, a parity bit is then generated for each block to further enhance the security. The parity bit is always appended as the last bit in each encrypted block C_b . If each block has less data, the parity bit would always go as the last bit in the block. It is important to note that the selected block size would always hold one less data bit since that 1-bit would always be dedicated for the parity bit (Pty) of the block.

Decryption works in the reverse order of the encryption process to convert the cipher text (CT) to plaintext (PT).

Encryption Algorithm

BEGIN

for each n ϵ (1, N) do

Assign b, nonce, k, r

Input M

if (k > b) then

for each b ϵ M do

for ∀ i ϵ(1, b)do

$L_i \leftarrow (b * k - 1) mod\ k$

$L := (L_1, L_2 \ldots L_b) \leftarrow L_i$

end for

for ∀ r_i ϵ (1, r)do

$Stb_r = (k * (r + nonce) mod\ b)$

$C_b \leftarrow$ RightRotate (C_b , Stb_r)

$C_b \leftarrow C_b \oplus C_{b-1}$

end for

Pty ← GenParityBit(C_b)

$C_b \leftarrow$ Append (C_{Pty})

return C_b, Pty

CT← ConcatAllCipherBlocks(C_b)

end for

end if

return C

end for

END

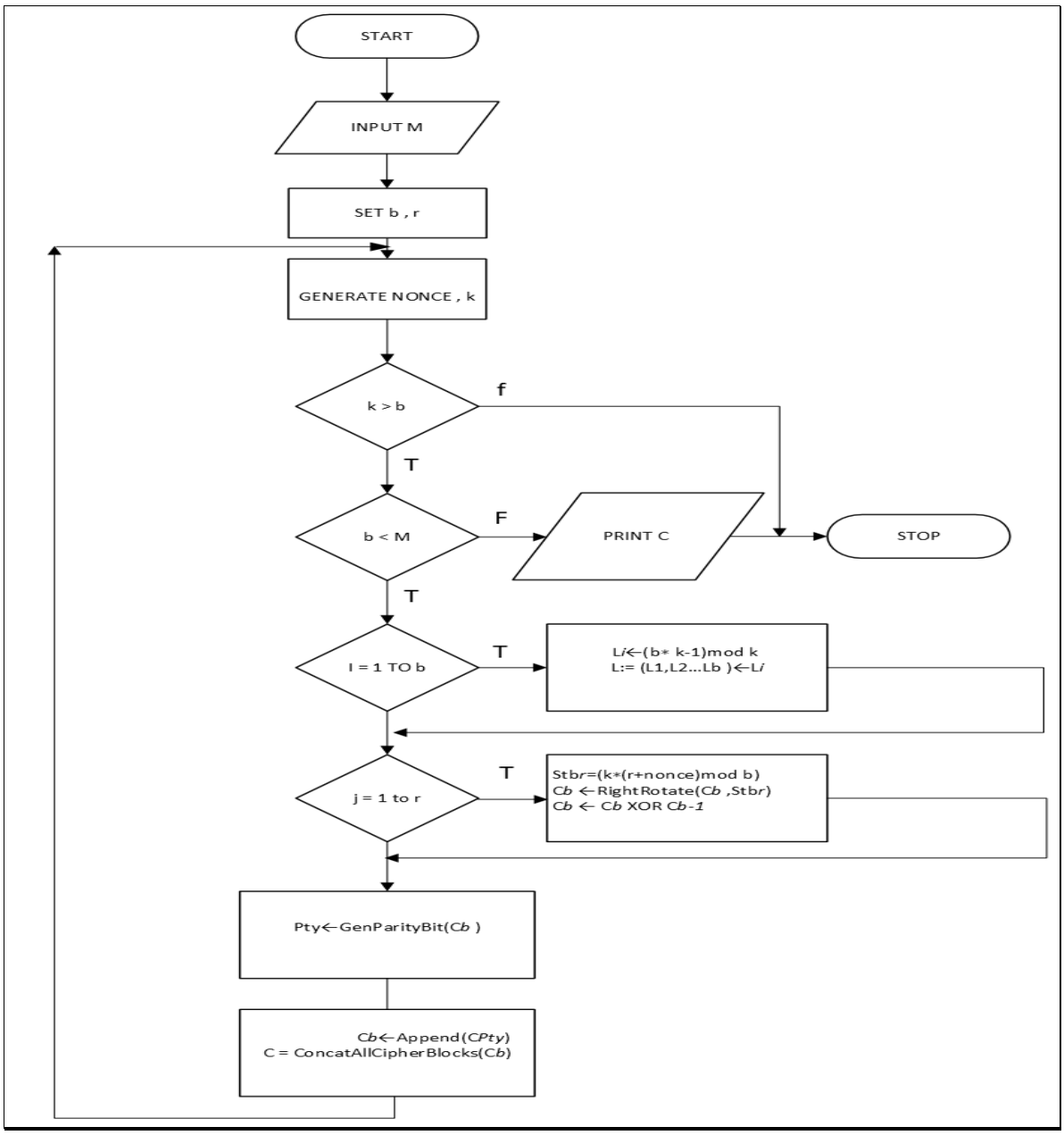

Figure 4. 4 Flowchart for Encryption

4.7.2 Key management scheme

The key management scheme in any communication is generally responsible for keeping the overheads low for the key generation, agreement, and distribution of the key in the networks. The prime focus of this phase is to minimize the energy consumption and transmission delay.

The first phase of key management is responsible for establishing the symmetric encryption key while the second phase is responsible for creation of a session key and distributing it to all the nodes to safeguard their symmetric encryption keys.

The key pre-distribution phase is responsible for reducing complex calculations and nodes power while generating and exchanging the encryption keys. A large key pool (K) is generated using a pseudo random function from where a random subset of keys (k) is then assigned to each of the sensor nodes before their placement. The keys are stored in the nodes in plain text therefore to secure them each key selected from the key pool is XOR-ed with a nonce to produce the symmetric encryption key Sym_k.This key will then be used to encrypt the plaintext data of the nodes.

$$Sym_k = k \oplus nonce \qquad (17)$$

The second phase is responsible for the creation of session keys and encoding of the key and encryption parameters (Enc_{Paras}) before forwarding them to the cluster head. Every sensor node has an ID or MAC which is physically secured, also known, and registered with the base station as well as the cluster head. These IDs are also forwarded to all the related nodes and updated whenever the cluster head changes.

Before the start of data transmission each cluster head computes its own session key S_k which does not involve any computations and simply considers the transmission time as its session key. This key is distributed to all the nodes associated with the cluster. This uniquely generated session key is used by the node that intends to communicate with the CH to generate the master key M_k. The cluster head ID value is encrypted using SHA-3 to produce the corresponding hashed ID (H_{id}). The node then computes its master key by XOR-ing the S_k and H_{id}. This master key is then used for encrypting the encryption parameters (Enc_{paras}) k and r. These encrypted parameters are then concatenated with the payload and transmitted to the cluster head.

The cluster head then transmits the data and session key to the other cluster heads or the sink using Particle Swarm Optimization Algorithm (PSO) until they are finally delivered to the base station.

On the base station side, the H_{id} is calculated by comparing the ID value held with the base station. The Master key M_k is then calculated using equation below:

$$M_k = H_{id} \oplus S_k \quad (18)$$

The master key thus created is used to decrypt the encryption parameters (Enc_{paras}) which are further used to decipher cipher text (CT) of the nodes to be able to retrieve the plain text (PT). This process is repeated for all the nodes to retrieve the corresponding data.

The data is validated at two levels which involve the sender that is the cluster head and receiver that is the base station. The authentication of nodes is carried out at the CH side by calculating the master key, which is used to decrypt the ciphered parameters in the payload. At the base station the authentication is carried out by checking the generated master key M_k , and verifying if it can decrypt the encryption parameters. If the authentication is not carried out it signifies that the cluster head is not registered with the base station and hence it would not accept the data.

The different cluster head IDs, nonce values as well as unique session times provides security against different attacks since it's almost impossible to know or access each of the values correctly. For each session the data for each node is encrypted using a unique session key. If the data is captured by hackers while in transit they cannot get hold of any meaningful information, nor gain access to the encryption key since that requires the session time which is a unique value generated at the beginning of every session.

Algorithm for key management

for ∀N ϵ CH do

Input M
$S_k \leftarrow$ GetSessionTime( );
$Sym_k \leftarrow$ k⊕ nonce
C← Encrypt (M || k , r)
$H_{id} \leftarrow$ SHA3(CH_{id})
$M_k \leftarrow S_k \oplus H_{id}$
$Enc_{paras} \leftarrow M_k Encrypt(k, r)$
C←**AddToPayload(** Enc_{Paras})
ForwardToCH(C)
end for

for ∀ *CH* ϵ BS do
GetFromCH(C , S_k)
HID←SHA3(CH_{id})
$M_k \leftarrow S_k \oplus$ HID

for ∀ *N* ϵ CH do

(k, r) ← Decrypt (Enc_{Paras} ||M_k)
PT ← Decrypt (C || k , r)
end for
end for

There are so many different techniques and options available for cluster head selection, routing as well as encryption. Nonetheless, the options selected are based on balancing the energy consumption along with encryption. The encryption technique has been chosen carefully keeping in view a minimal number of computations to minimize the energy consumption and prolong the lifetime of the network.

Chapter 5

Results And Discussions

This chapter discusses the parameters and the simulation environment for the proposed algorithm. This is followed by a detailed analysis and discussion based on the results of the algorithm, encryption parameters involved in the encryption process.

5.1 The simulation environment

We have simulated our algorithm using MATLAB to determine the performance of our algorithm. The default parameters used for the simulation of the code are summarized in the table below.

Table 5. 1 Default parameters used for simulation

Parameter	Value
Sensor Network Area	100 m x 100 m
Base Station (BS)	(50, 50)
Total number of Nodes (N)	100
Initial energy of Node	0.005J
Dissipation energy E_{elec}	5E-08 J/ bit
(ε_{amp})	1.3E-15 J/bit/m^2
(ε_{fs})	1E-08 J/bit/m^2
Data aggregation energy (E_{da})	5E-09 J/ bit
Packet size	4000 bits
Block size	128 bits
Probability (P)	0.1
E_{Tx}	5E-08 J/ bit
E_{Rx}	5E-08 J/ bit

5.2 Assumptions

In the proposed algorithm which has been simulated using MATLAB several assumptions have been made of which the important ones have been listed below.

1. All nodes are homogeneous, stationary and have the same capacity.

2. Each node has a unique identifier.
3. All nodes transmit at the same power level.
4. Base station is placed at the center of the network.
5. Network topology remains unchanged over time.
6. All nodes are randomly placed in the monitoring area.
7. All the nodes can send and receive the data.
8. When the node energy is used up, the node no longer exists and is classified as a dead node.

5.3 Performance Factors

The main parameters evaluated in this algorithm to balance the tradeoff between security and energy include the following:

1. Total Energy: This factor focuses on the overall energy available in a network. The greater the energy the more data that can be transmitted and longer the lifetime of the network.
2. Throughput: This parameter evaluates and determines the number of data packets that leave the cluster head and reach the receiving end in a specific number of rounds.
3. Dead Nodes: This factor determines the count of nodes whose energy falls below a defined threshold and contribute to the decrease in the lifetime of the network.
4. Encryption Time: Another important factor considered here is the encryption time required for data transmission

5.4 Network Creation

Network area is the area formed with sensor nodes. In our algorithm the simulated network area is 100x100 m. It consists of a network of 100 sensor nodes placed randomly in the area, with the base station statically located in the center at location (50, 50). After the deployment of the network the data transmission then starts according to the number of rounds. The figure below depicts a snapshot of 100 x 100 area with 100 sensor nodes randomly deployed.

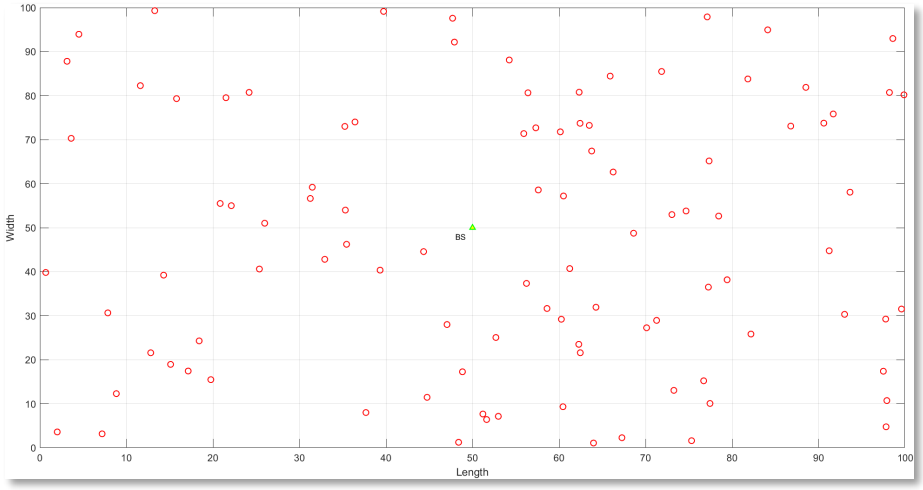

Figure 5. 1 Network Area

5.5 Simulated Results for The Proposed Algorithm

The three parameters discussed in our algorithm are the total energy consumption, the number of dead nodes and the number of packets delivered to the base station.

5.5.1 Total Energy

The total energy of the network is defined as the overall energy of all the nodes in the network. Hence, greater the energy the better its' considered to be since that means the longer the network time. According to the parameters defined the initial node energy is 0.0050J. The total count of the nodes is 100 therefore it would lead to a total energy of 0.50J. The graph below shows that the total network energy is reducing slowly as the number of rounds increase. The total energy of the network is initially 0.50J and after first 20 rounds the total energy reduces to approximately 0.3654 J , after another 20 rounds the total energy becomes 0.2875 , after 80 rounds it reduces to 0.1125 and after 100 rounds the energy came down to 0.0498. Hence , we can conclude that as the number of rounds increase the energy slowly declines. The reduced energy consumption can be attributed to the additional parameter of residual energy that is considered when selecting the cluster heads and putting nodes to sleep after they have transmitted their data.

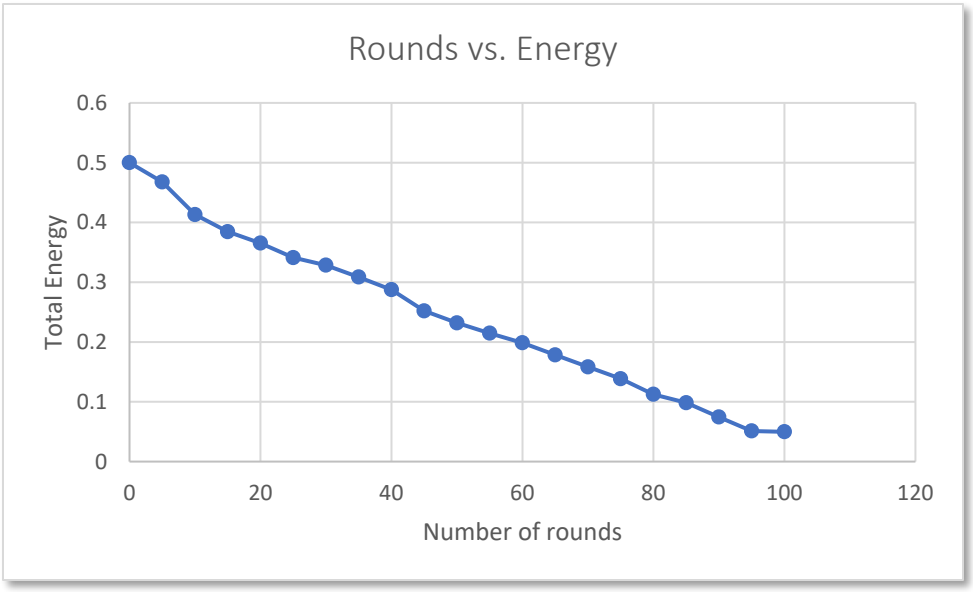

Figure 5. 2 Comparison of Rounds versus Total Energy

5.5.2 Throughput

Throughput refers to the number of packets successfully transmitted from the source to the destination. Therefore, the greater the number of packets transmitted in a particular timeframe the better it is, since that reflects a larger amount of data packets being transmitted. The graph below depicts that the number of packets transmitted increases as the number of rounds tends to increase. The analysis of the graph shows that approximately 1546 packets are transmitted from the cluster head to the base station after the first 25 rounds, increasing the number of rounds to 50 increases the transmission packets to 2552, after 75 rounds it reaches 3170 and after 100 rounds manages to transmit approximately 3300 packets to the base station. So, basically an increase in the number of transmissions as the rounds increase is a positive indicator representing a better network performance.

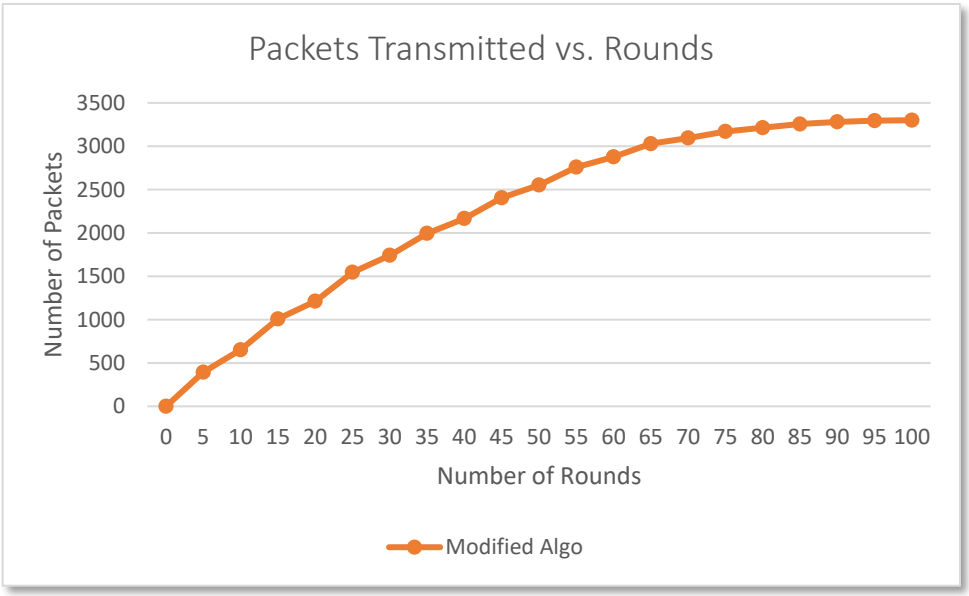

Figure 5. 3 Comparison of Rounds versus Number of Packets Transmitted

5.5.3 Dead Nodes

The dead nodes are defined as those nodes which have zero energy. In other words, if a node consumes .005 J of its energy it is referred to as a dead node. Here we have initialized the count of the dead nodes initially with 0. As the rounds keep increasing with time, the energy starts decreasing and the number of dead nodes keeps increasing. The graph below illustrates that the relation between the dead nodes and the number of rounds seems to be almost a direct relationship. For a network consisting of 100 nodes, we can see that after 50 rounds almost 35 nodes have died, after 75 rounds the value increases to almost 54 and after 100 rounds reaches almost 73 nodes. Hence, when the number of rounds start increasing the network lifetime starts reducing slowly. Greater number of dead nodes shows that the lifetime of the network starts going down and the moment the number of dead nodes reaches100 that means all the data transmission comes to a halt since the nodes have all reached zero energy value. This could also be the case if the battery is dead, network has malfunctioned or some device issue.

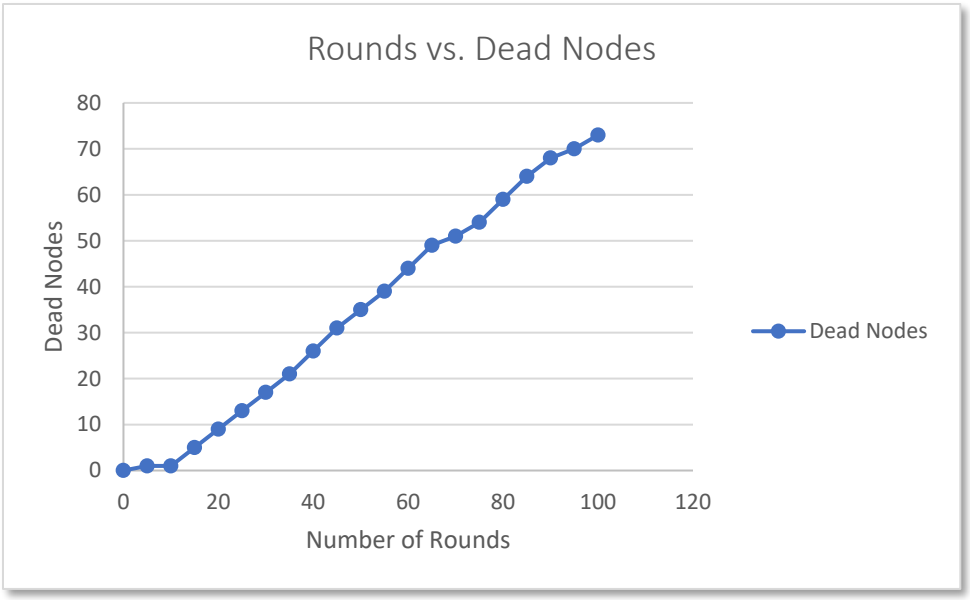

Figure 5. 4 Comparison of Rounds versus Number of Dead Nodes

5.6 Comparison of Different Algorithms

The modified algorithm is a blend of different algorithms consisting of LEACH and PSO for clustering and routing with encryption. The figures below give an idea about the difference in the values when executed under the same conditions for different algorithms.

The results tabulated in Figure 5-5 reveal that the initial network energy for all the algorithms is same. The count of nodes is 100 and the total energy for the network is approximately 0.5 J. The graph below depicts that PSO seems to be the worse in terms of energy consumption, followed by LEACH and the modified algorithm has approximately .0498 J even after 100 rounds which can be attributed to the routing algorithm selected only transmits the data through the cluster head which is near to the base station instead of all cluster heads transmitting the data to the base station like it is for the LEACH algorithm , while the PSO algorithm is suffering from the issue that greater the number of the particles greater is the number of iterations and the longer it would take to converge to the best possible solution for transmitting the data from the cluster heads.

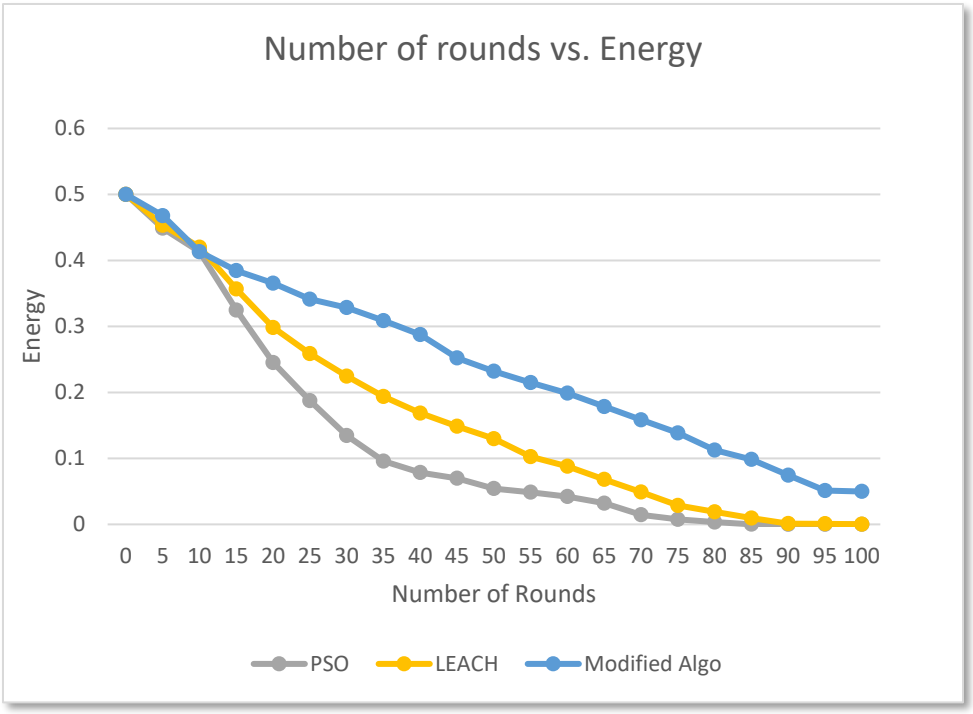

Figure 5. 5 Comparison of Algorithms with respect to Energy Consumption

The graph below reveals the results for the count of dead nodes after 100 rounds. It is an important parameter to determine the network lifetime and gauge about the performance of the network. Our modified algorithm shows approximately 70% of dead nodes after 100 rounds so that shows 30% nodes are still alive for transmitting the data, while almost all the nodes had died for both the LEACH and PSO algorithms which shows that the network lifetime for these two algorithms was approximately 30% less than our algorithm. The reason for the reduced number of dead nodes in the modified algorithm can be attributed to the fact that the nodes sleep after they transmit their data so they can retain their energy for a longer time. Similarly, cluster heads are also transmitting the data to the CH closest to the base station and therefore that's how all the CHs also save their energies whereas in case of LEACH the selection of CH is done in a random fashion and all the cluster heads forward the data to the base station directly.

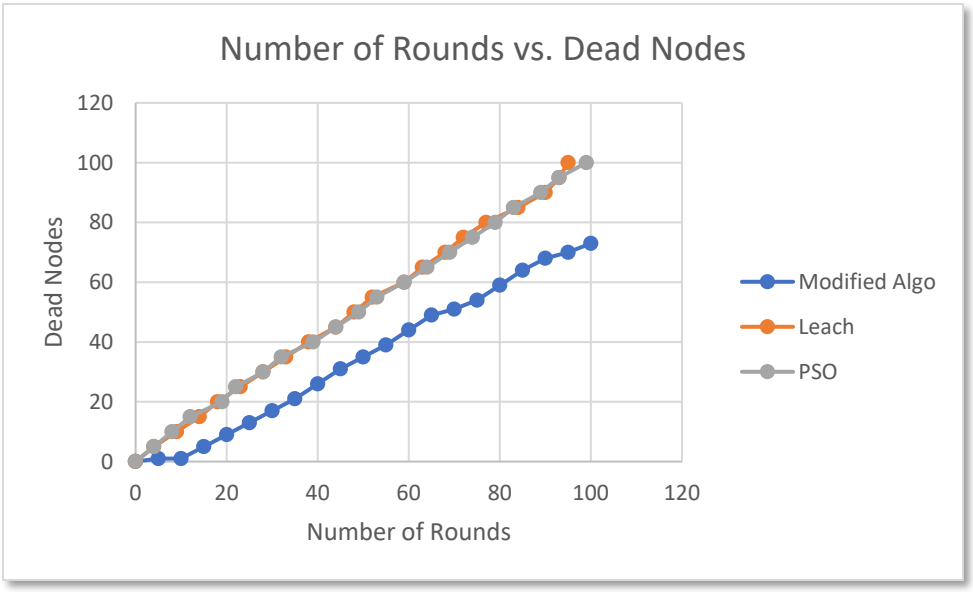

Figure 5. 6 Comparison of Algorithms Based on Dead Nodes

The aim of any algorithm / protocol is to maximize the delivery of data packets to the BS. The number of data packets delivered to the base station is an important means of determining the network performance. The greater the number of packets delivered, the better the performance. Fig. 5-7 shows the results of comparing our proposed algorithm with LEACH and PSO. It is evident from the results that the largest number of packets are delivered for the proposed algorithm as compared to LEACH or PSO. The reason our algorithm outperforms the others is based on the reason that unlike LEACH where cluster heads are randomly selected or the PSO algorithm where the focus is simply convergence our algorithm selects the cluster heads based on the residual energy which reduces the loss in energy for nodes that transmit frequently and therefore deliver greater amount of data with reduction in energy loss.

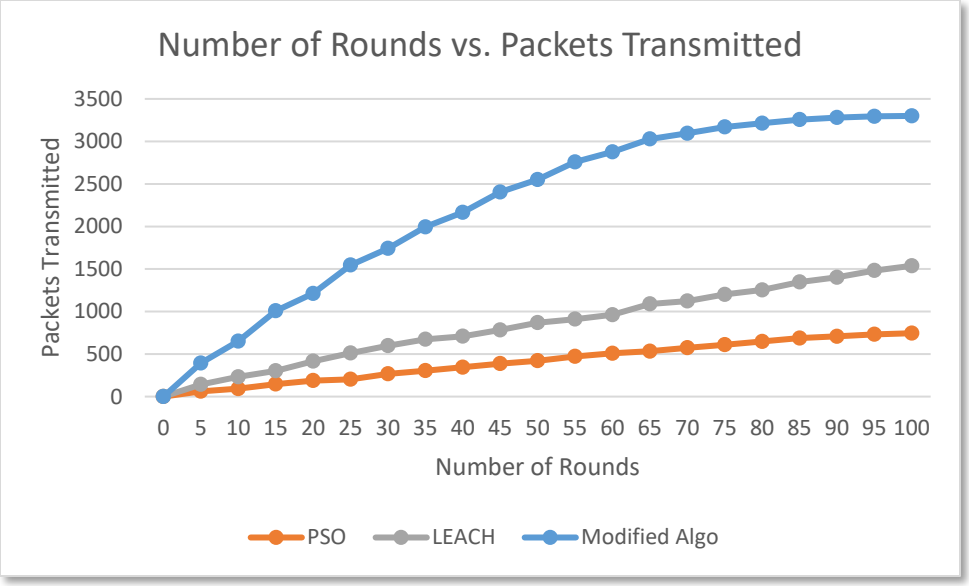

Figure 5. 7 Comparison of Algorithms Based on Packets Transmitted

5.7 Analysis of Encryption

Different algorithms exist for data security purposes. The proposed algorithm is a modified version of FlexCrypt algorithm which provides lightweight encryption to reduce energy consumption without compromising on security. The major focus of our algorithm is ensuring that the data is transmitted to the base station securely with minimal energy usage.

Our encryption algorithm is a modified light version of the FlexCrypt algorithm consisting of basic math operations, substitutions, and rotations to save data transmission energy and prolong the network lifetime while securing the data during transmission. The simulation times for AES, RSA algorithms along with our modified FlexCrypt algorithm are given below in Table 5- 2 for a block size of 128 bit.

Table 5. 2 Algorithm execution time

Algorithm	Time Elapsed
AES	0.024297
RSA	0.110243
Proposed Algorithm	0.001024

5.7.1 Data Freshness

Data freshness is a very important characteristic which focuses on the speed of data transfer without additional overhead. It won't be wrong to say that in the field of wireless networks one cannot forget the concept of data freshness which helps in reducing attacks especially replay attacks. Our algorithm implements data freshness using a nonce during the encryption. This nonce has been implemented as a counter but can be implemented as a randomly generated value. It has been incorporated without additional overhead and generated every time the encryption key is generated.

5.7.2 Data integrity

Data integrity is an important element in cryptography. It aims to attempt whether the data has been altered in transit when it reaches the base station. Even a single bit of alteration changes the meaning of the whole data. At the decode stage the integrity is authenticated or validated. The calculation of parity bit (i.e. even parity) at the block level and incorporation of that with the cipher block serves the purpose. In the decryption phase, the authorized entity has to check a possible alternation by computing the parity bit of the bits that are listed on the right side of str, then compare it with the originally received bit in each block. Furthermore, it is possible to detect a data alteration before obtaining the plain text.

The validation of the data is carried out at two levels. Firstly, authentication is carried out between the sensor nodes and their cluster head at the CH. The cluster head tends to verify the associated nodes with its cluster based on the value of the master key and its ability to decode the individual nodes encryption parameters. Secondly, the base station compares the session key values and the hashed id of each of the cluster heads and the capability of the BS to compute master key for decoding the encryption parameters for each of the node. The cluster head IDs are stored in the encrypted form in the base station to ensure the data security and thwart any possible attacks.

A parity bit is calculated for each individual block and a separate parity block is created for these bits. This block is appended at the base station once all the data blocks have been ciphered. At the BS when the blocks are deciphered the parity bit is checked for each block and if there is any difference that would indicate a compromise in the integrity.

5.7.3 Confidentiality

Our modified version of the Flex Crypt algorithm is responsible for converting the sensed data into ciphered data of same size. The random permutations and substitutions in the algorithm minimize and thwart frequency attacks. It requires basic calculations for data encryption with the key value by calculating the values of L_i.It also employs rotation starting from Str_b to further enhance security by increasing the diffusion. All these operations combined create transformations making it difficult to gain access to the plain text or data. At the end once all these calculations are done the cipher blocks created are also exclusive or-ed with the previous cipher block creating even more randomization. This XOR operation is very important because though simple in nature it is in itself an encryption algorithm as well as an additive cipher. Hence, it adds more complexity in any algorithm. The main restriction for this encryption algorithm is to ensure that the value of k (key) selected from the key pool , and b which is 128 bit in our case should always ensure that k > b .

The data confidentiality is ensured if the data is transmitted securely over the sensor network and is not disclosed to random entities.

Our algorithm can be modified to incorporate the concept of flexible parameters but that would lead to an increase in the number of computations and expend the node energy earlier bringing down the whole network. The number of rounds is an important parameter that tends to affect both the speed of encryption and security. While selecting the number of rounds a smaller value for them tends to provide some security probably within a given speed frame. However, an increase in the number of rounds tends to affect the speed of data transfer and the packet loss due to an increased number of data collisions.

The proposed algorithm outperforms other algorithms with respect to the network performance and network lifetime, along with the provision of data security. The light encryption algorithm provided the much-needed data security while conserving the network energy at the same time.

Chapter 6

Conclusion and Future Recommendations

6.1 Conclusion

This chapter summarizes the overall aspect of wireless sensor networks with respect to the security and energy perspective and provides some enhancements and future work recommendations for the research provided in the previous chapters.

These days we are all aware of the fact that sensor networks are an upcoming technology designed for time critical applications especially for hard-to-reach areas requiring continuous monitoring with major implications. Rapid advancement in the field of WSN and its support in the challenging application areas ranging from basic to healthcare to military has forced and motivated researchers to perform extensive work in critical areas of WSN such as energy efficiency, data security, efficient routing, scalability, and reliability.

Sensor networks strongly rely upon these tiny devices known as sensors which have limited resources and battery utilized for data transmission purposes. These networks are made up of not one or two but hundreds or thousands of these nodes which are unfortunately limited in battery power and are both difficult to recharge and replace. Therefore, a critical issue facing researchers is increasing the lifetime of the network by saving the energy of these tiny devices. These nodes are randomly deployed in sensitive or hard to reach areas and their data is going around in the form of plain text making it open to eavesdropping so secure transmission of this data is a huge challenge. Securing this data comes with a cost since encryption requires computations that strain the nodes for additional resources. Some application areas like the military require a very high level of data secrecy and cannot afford eavesdropping hence encryption and energy consumption require a balance.

Selection of an algorithm that is both energy efficient and secure is a huge challenge these days. LEACH is a TDMA based protocol which is an excellent choice for energy saving aimed at improving the lifetime of sensor networks by reducing the energy consumption, nonetheless, it has

its own limitations such as no count of the number of CHs, uneven distribution of clusters and lastly when any cluster head dies the cluster becomes useless. Similarly, the second protocol considered in the suggested algorithm is the Particle Swarm Optimization Algorithm (PSO) which is an ideal choice for optimizing a problem by repetitively improving a possible solution keeping a certain goal in mind, it certainly does come with its own restraints such as lower local optimum search capability, slower convergence rate and increased memory consumption to update the velocity parameter.

Our algorithm has been developed using a hybrid technique based on modified LEACH and PSO algorithms to initially form clusters, followed by identification cluster heads where data aggregation takes place, and then routing the data from the cluster heads to the base station appropriately. A modified cluster head selection algorithm has therefore been proposed as the initial step to extend the networks lifetime by managing the energy parameter. The enhanced routing process can be used effectively in scenarios like smart homes using IoT. The data is transmitted from the nodes all the way to the base station and should be secured with minimal loss of energy. The data can generally be secured through several different techniques like AES, DES encryption or multiple hashing techniques like SHA256, SHA3. The data in our algorithm is encrypted using a lightweight modified version of the Flex Crypt technique to attain a balance between energy and. security.

The proposed algorithm performs better than the previous techniques of LEACH and PSO in terms of energy consumption and extended lifetime since the cluster formation is based on residual energy combined with PSO leading to an increased network lifetime. The data is being routed from the cluster heads through the PSO algorithm by identifying the cluster head nearest to the sink to save up on the energy of the rest of the cluster heads as well which could be utilized for transmitting the data across more distance. The security implemented thru the modified Flex Crypt algorithm uses basic mathematical operations along with some rotation and substitution operations to transmit the data securely. The use of simple operations keeps the algorithm light and saves up on energy by cutting down on the cost of heavy computations. Simulation results reveal improved network performance for parameters such as residual energy, number of packets sent to BS, throughput, and energy.

The increased throughput and energy consumption of the modified algorithm is approximately X% more than the LEACH and PSO algorithms. It is evident that the marked improvement in result compared to other algorithms is attributed to the cluster head selection based on the residual energy in wireless sensor network combined with PSO based routing along with the modified Flex Crypt algorithm for encryption. Results reveal that the throughput and energy are greatly improved compared to LEACH and PSO while providing security, and the algorithm is well suited for majority applications in wireless sensor networks which need security while minimizing the energy expense while routing the data thereby keeping the network alive for a longer time. The algorithm is suitable for implementation in large scale network for energy efficiency.

6.2 Future Recommendations

The proposed algorithm has shown great performance compared to the LEACH and PSO algorithms while providing security through a lightweight encryption technique. Nonetheless, there is always room for improvement in any algorithm. Firstly, an efficient cluster formation mechanism considering multiple or different parameters can be incorporated to optimize energy consumption. Similarly, a different set of parameters can be chosen for cluster head selection. The suggested algorithm can be verified against multiple attacks possible to enhance the security. The existing algorithm is only simulating the code for static nodes and a fixed sink which can be modified for mobile nodes or sink to see the effect. Nonetheless, the existing algorithm for encryption lacks extensive testing against different attacks so a thorough testing can be carried out. The suggested algorithm currently works well for homogeneous networks but can be improvised to work for other kinds of networks. The proposed algorithm can be tested in a real time scenario for wireless sensor networks based on IoT system.

REFERENCES

[1] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, (2008). Wireless sensor network survey. *Computer Networks*, 52(12), 2292-2330.

[2] Aditya Sharma, Garima Tripathi, Md Sohail Khan, Kakelli Anil Kumar (Nov 2015). A Survey Paper on Security Protocols of Wireless Sensor Networks.2(8)

[3] Aditya Sharma, Garima Tripathi, Md Sohail Khan, Kakelli Anil Kumar. (Nov 2015). A Survey Paper on Security Protocols of Wireless Sensor Networks. 2(8)

[4] Ajaz Ahmed Khan 1, Mrs Himani Agrawal. (Jan 2016). A Survey Paper on Applications and Challenges in Wireless Sensor Network.5(1).

[5] Othman, Fauzi & Shazali, Khairunnisa. (2012). Wireless Sensor Network Applications: A Study in Environment Monitoring System. In *Journal of Procedia Engineering,* (pp. 1204 – 1210).

[6] Zhang, Zeyu & Mehmood, Amjad & Shu, Lei & Huo, Zhiqiang & Zhang, Yu & Mukherjee, Mithun. (2018). A Survey on Fault Diagnosis in Wireless Sensor Networks. IEEE Access.

[7] Yousefpoor, E., Barati, H. & Barati, A. A hierarchical secure data aggregation method using the dragonfly algorithm in wireless sensor networks. (2021). *Peer-to-Peer Network*, (pp. 1917–1942)

[8] Patel, B.C., Sinha, G.R., & Goel, N. (2020). Introduction to sensors. *Advances in Modern Sensors*.

[9] Hina Tandel Prof. Rakesh Shah. (2017). A Survey Paper on Wireless Sensor Network. In *IJSRD - International Journal for Scientific Research & Development*, 5(10).

[10] Singh, Preetkamal, Dr. OP Gupta and Sita Saini. (2017). A Brief Research Study of Wireless Sensor Network. *Advances in Computational Sciences and Technology*,10(5).

[11] Afsar, M. Mehdi, and Mohammad-H. Tayarani-N. (2014). Clustering in sensor networks: A literature survey. *Journal of Network and Computer applications ,*198-226.

[12] Amin Shahraki, Amir Taherkordi, Øystein Haugen, Frank Eliassen (2020). Clustering objectives in wireless sensor networks: A survey and research direction analysis. *Computer Networks*. 180:107376.

[13] Daanoune, Ikram, Baghdad Abdennaceur, and Abdelhakim Ballouk. (2021). A comprehensive survey on LEACH-based clustering routing protocols in Wireless Sensor Networks. *Ad Hoc Networks*.114:102409.

[14] I. Daanoune, A. Baghdad and A. Balllouk. (2019). A comparative study between ACO-based protocols and PSO-based protocols in WSN. *In 7th Mediterranean Congress of Telecommunications (CMT*), pp. 1-4.

[15] Bilal Jan, Haleem Farman, Huma Javed, Bartolomeo Montrucchio, Murad Khan, Shaukat Ali. (2017). Energy Efficient Hierarchical Clustering Approaches in Wireless Sensor Networks: A Survey. *Wireless Communications and Mobile Computing*.2017

[16] Ben Salah, M., & Boulouz, A. (2016). Energy efficient clustering based on LEACH. *International Conference on Engineering & MIS (ICEMIS)*, pp. 1-3.

[17] Juneja, M., & Nagar, S.K. (2016). Particle swarm optimization algorithm and its parameters: A review. *International Conference on Control, Computing, Communication and Materials (ICCCCM)*, pp. 1-5.

[18] Shazana Md Zin, Nor Badrul Anuar, Miss Laiha Mat Kiah, Al-Sakib Khan Pathan. (2018). Routing protocol design for secure WSN: Review and open research issues. *Journal of Network and Computer Applications*.41 (pp. 517-530).

[19] Ms. Ankita P. Baheti, Prof. Lokesh Singh, Prof. Asif Ullah Khan. (2018).A Comparative Literature Survey On Various Image Encryption Standards. *International Journal Of Engineering Research and Technology (IJERT)*. 2(4)

[20] Zodpe, Harshali, and Arbaz Shaikh. (2021). A Survey on Various Cryptanalytic Attacks on the AES Algorithm. *International Journal of Next-Generation Computing*. (pp.115-123).

[21] Sandeshi, Sachithi & Priyanjana, W & Bandara, Hansi & Sajindra, Hirushan. (2020). RSA in Communication IEEE.

[22] Singh, K. (2015). WSN LEACH based protocols: A structural analysis. *International Conference and Workshop on Computing and Communication (IEMCON)*, 1-7.

[23] Dhondiyal, S.A., & Rana, D.S. (2018). Sleeping Mode MODLEACH Protocol for WSN. *IJARCCE*. pp.112-116

[24] Fahimi, Mortaza & Abad, Khaton & Jabraeil Jamali, Mohammad & Jamalip, Jabraeil. (2015). Modify LEACH Algorithm for Wireless Sensor Network. *International Journal of Computer Science Issues*. 8.(pp.219-224).

[25] Islam, S.M., Khan, M.N., Islam, S.M., & Akhtar, M.J. (2019). Cluster Head Selection Technique Using Four Parameters of Wireless Sensor Networks. *2019 International Conference on Computer Communication and Informatics (ICCCI)*, 1-4.

[26] Xingguo, L., Junfeng, W., & Lin-lin, B. (2016). LEACH Protocol and Its Improved Algorithm in Wireless Sensor Network. In *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 418-422.

[27] R. S. Elhabyan and M. C. E. Yagoub. (2014). Energy efficient clustering protocol for WSN using PSO. In *Global Information Infrastructure and Networking Symposium (GIIS)*, pp. 1-3.

[28] Tay, M., & Sentürk, A. (2022). A New Energy-Aware Cluster Head Selection Algorithm for Wireless Sensor Networks. *Wireless Pers. Communications,* 122, 2235-2251.

[29] Panchal, A., Singh, L., & Singh, R.K. (2020). RCH-LEACH: Residual Energy based Cluster Head Selection in LEACH for Wireless Sensor Networks. *2020 International Conference on Electrical and Electronics Engineering (ICE3)*, 322-325.

[30] Ding, X., Liu, Y., & Yang, L. (2021). An Optimized Cluster Structure Routing Method Based on LEACH in Wireless Sensor Networks. *Wireless Personal Communications*.121, 2719–2733.

[31] Pour, S.E., & Javidan, R. (2021). A new energy aware cluster head selection for LEACH in wireless sensor networks. *IET Wireless Sensor Systems. 11*, 45-53.

[32] Alghamdi, T.A. (2020). Energy efficient protocol in wireless sensor network: optimized cluster head selection model. *Telecommunication Systems, 74*, 331-345.

[33] Behera, T.M., Mohapatra, S.K., Samal, U.C., Khan, M.S., Daneshmand, M., & Gandomi, A.H. (2019). Residual Energy-Based Cluster-Head Selection in WSNs for IoT Application. *IEEE Internet of Things Journal,* 6, 5132-5139.

[34] Edla, D.R., Kongara, M.C. & Cheruku, R. (2019). A PSO Based Routing with Novel Fitness Function for Improving Lifetime of WSNs. *Wireless Pers Commun*ication. (pp. 73–89).

[35] Sundar Rengasamy, Punniyamoorthy Murugesan, (2021). PSO based data clustering with a different perception, Swarm and Evolutionary Computation, 64.

[36] Kulkarni, R.V., & Venayagamoorthy, G.K. (2011). Particle Swarm Optimization in Wireless-Sensor Networks: A Brief Survey. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 41(2)*, 262-267.

[37] S. Kumar and S. Mehfuz. (2019). A PSO Based Malicious Node Detection and Energy Efficient Clustering in Wireless Sensor Network. *International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 859-863.

[38] Liu, Y., Wu, Q., Zhao, T., Tie, Y., Bai, F., & Jin, M. (2019). An Improved Energy-Efficient Routing Protocol for Wireless Sensor Networks. *Sensors (Basel, Switzerland), 19*.

[39] Raphael, A. Joseph and V. Sundaram. (2012). Secured Communication through Fibonacci Numbers and Unicode Symbols. *International Journal of Scientific & Engineering Research*.3(4)

[40] Elamurugu, V., and D. J. Evanjaline. (2021). An Efficient and Secure Text Encryption Scheme for Wireless Sensor Network (WSN) Using Dynamic Key Approach. *International Journal of Computer Networks and Applications.*

[41] Venkatasamy, T.K., & Shanmugasundaram, R. (2016). Authentication in Wireless Sensor Networks Using Dynamic Keying Technique. *International Journal of Intelligent Engineering and Systems, 9*, 146-155.

[42] Cao, C., Tang, Y., Huang, D., Gan, W., & Zhang, C. (2021). IIBE: An Improved Identity-Based Encryption Algorithm for WSN Security. *Secure Communication Networks, 2021*, 8527068:1-8527068:8.

[43] Venuto, D.D., & Mezzina, G. (2018). Spatio-Temporal Optimization of Perishable Goods' Shelf Life by a Pro-Active WSN-Based Architecture. *Sensors (Basel, Switzerland), 18*(7), p. 2126, 2018

[44] N. E. Rachkidy, A. Guitton, and M. Mission.(2018). Avoiding routing loops in a multi-stack *WSN.Journal of Communications.*8(3) pp. 151–160.

[45] H. A. Babaeer and S. A. Al-Ahmadi. (2020). Efficient and Secure Data Transmission and Sinkhole Detection in a Multi-Clustering Wireless Sensor Network Based on Homomorphic Encryption and Watermarking. IEEE. 8, (pp. 92098-92109).

[46] Yi, L., Tong, X., Wang, Z., Zhang, M., Zhu, H., & Liu, J. (2019). A Novel Block Encryption Algorithm Based on Chaotic S-Box for Wireless Sensor Network. IEEE,*7*, 53079-53090.

[47] Hayouni, H., & Hamdi, M. (2021). A novel energy-efficient encryption algorithm for secure data in WSNs. *Journal of Supercomputing, 77*, 4754-4777.

[48] Elhoseny, M., Elminir, H.K., Riad, A.M., & Yuan, X. (2016). A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic encryption. *J. King Saud Univ. Computing Inf. Sci., 28 (3)*, 262-275.

[49] Khashan, O.A., Ahmad, R., & Khafajah, N.M. (2021). An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. *Ad Hoc Networks, 115*, 102448.

[50] Hayouni, H., & Hamdi, M. (2021). A novel energy-efficient encryption algorithm for secure data in WSNs. *Journal of Supercomputing, 77*, 4754-4777.