AN ENERGY EFFICIENT PROTOCOL FOR OPTIMAL CLUSTER HEAD SELECTION IN WIRELESS SENSOR NETWORK

A Thesis Submitted
In Partial Fulfillment of the Requirements
for the Degree of

DOCTOR OF PHILOSOPHY
In
COMPUTER SCIENCE & ENGINEERING

By

RAKESH KUMAR SINGH
(Enrolment No.: MUIT0117038029)

Under the Supervision of
Dr. Ajay Kumar Bharti
MUIT

To the
Faculty School of Engineering

MAHARISHI UNIVERSITY OF INFORMATION TECHNOLOGY
LUCKNOW, U.P.

SEPTEMBER, 2021

DECLARATION

I hereby declare that the work presented in this report entitled "**AN ENERGY EFFICIENT PROTOCOL FOR OPTIMAL CLUSTER HEAD SELECTION IN WIRELESS SENSOR NETWORK**", was carried out by me. I have not submitted the matter embodied in this report for the award of any other degree or diploma of any other University or Institute.

I have given due credit to the original authors/sources for all the words, ideas, diagrams, graphics, computer programs, experiments, results, that are not my original contribution.

I have used quotation marks to identify verbatim sentences and given credit to the original authors/sources.

I affirm that no portion of my work is plagiarized, and the experiments and results reported in the report are not manipulated. In the event of a complaint of plagiarism and the manipulation of the experiments and results, I shall be fully responsible and answerable.

Name: RAKESH KUMAR SINGH

Enroll. No. : MUIT0117038029

Field: Computer Science and Engineering

(*Signature of the Research Scholar)*

Date:

CERTIFICATE

Certified that **RALESH KUMAR SINGH** (Enrollment no.:MUIT0117038029) has carried out the research work presented in this thesis entitled **"AN ENERGY EFFICIENT PROTOCOL FOR OPTIMAL CLUSTER HEAD SELECTION IN WIRELESS SENSOR NETWORK"** for the award of **Doctor of Philosophy** from Maharishi University of Information Technology, Lucknow under my/our supervision. The thesis embodies results of original work, and studies are carried out by the student himself/herself and the contents of the thesis do not form the basis for the award of any other degree to the candidate or to anybody else from this or any other University/Institution.

Signature:
(Dr. Ajay Kumar Bharti)
Professor
Maharishi University of Information Technology, Lucknow
Date:

Note: In case of only one supervisor, the sole supervisor will sign on the right side and the details on the left will not be printed. In case of three supervisors, the third one along with his/her name, designation, address will sign in the centre of the page underneath the details of the two other supervisors. The date, however, will be common to all.

ACKNOWLEDGEMENT

I would like to thank my supervisor Prof. (Dr.) Ajay Kumar Bharti for his support, help and constant guidance with this PhD. I am also extremely grateful to the management of Maharishi University of Information Technology for rendering me this wonderful opportunity. I also appreciate all the support I received from the officials and faculty members of the Maharishi University Lucknow, specially Computer Science & Engineering Department. I extend my sincere gratitude to Dr J.P. Pandey,Vice Chancellor Madan Mohan Malviya University of Technologogy Gorakhpur, for his constant motivation and support. I cannot forget the technical help and support of Dr Karan (JNU) and Dr Pawan Mishra (NIT Raipur). I extend thanks to Mr Kalamuddin Ahmad, associate professor Integral University Lucknow for his valuable conversation, suggestion and motivation. I have often looked towards my colleagues at KNIT Sultanpur, specially Mr B.P. Chaurasia and Mr Samir Srivastava for their valuable suggestions.

I am truly grateful to my parents for their immeasurable love and care. They have always encouraged me to explore my potential and pursue my dreams. I would like to thank my wife Suman for all the support and motivation throughout this work. Sweet thank to my children Abhinav, Astha, Dr Komal and Rishabh for their tremendous understanding and encouragement in the past few years.

At last I wish to thank many other people whose names are not mentioned here but this does not mean that I have forgotten their help and support.

(RAKESH KUMAR SINGH)

ABSTRACT

Due to the incorporation of sensors into embedded systems, Wireless Sensor Networks now have a greater range of applications (WSNs). Recent years have seen the emergence of a new field of research, fueled by this new challenge: vision sensor networks. Indeed, numerous applications demand reliable detection of objects that are outside the range of view of the WSN. Multimedia data is necessary for validating a wide number of applications, including object identification, location, and tracking. However, multimedia processing is energy intensive, emphasising the importance of a custom solution for the nodes in a network of multimodal sensing. This chapter begins by providing an overview of WSNs and then examines and justifies the development toward networking of vision sensors, which are now being appraised premature from an industrial aspect. Before developing any unique algorithm for WSNs, a thorough examination of the literature is required. A study of routing protocols is presented, with protocols categorized according to their topologies: flat and hierarchical, with hierarchical protocols classified according to their security and energy efficiency. The majority of protocols described in the literature employ a hierarchical or clustered topology (SK & KC, 2013). Flat topology is distinct from hierarchical topology in several ways, and it comes with several advantages and downsides. LEACH was the first and most often used WSN hierarchical clustering technique (Heinzelman et al., 2000). As the name implies, it is based on the dispersed construction of clusters, a sort of cluster formation that distributes nodes. Randomly, LEACH selects some sensor nodes as CHs and causes every node to spin as CHs, employing a randomized rotation strategy, which equally divides energy demand throughout the node's network. To minimize the amount of information transmitted throughout the communications network, the CH node compresses data collected from its members and provides the aggregated data/package for the BS. During data transmission, collisions may occur as a result of an external disruption within the network. Collisions generally happen in two ways: inter-cluster or intra-cluster crashes. Consequently, LEACH uses TDMA/CDMA MAC protocols to minimize such collisions (Ye et al., 2002). This protocol is appropriate for applications requiring continuous sensor network monitoring. Data collection in LEACH is centralized and can be performed periodically (Yadav & Sunitha, 2014). PEGASIS was developed as a LEACH protocol improvement (Lindsey & Raghavendra, 2002). PEGASIS was an optimally functioning chain-based protocol. Unlike

LEACH, it uses a chain-based technique to improve the energy efficiency of the sensor network. Each node in a chain receives and transfers data to the nearest neighbor, but only one node transmits aggregated data to the BS. Nodes will turn to be the leader of the chain to transfer data to the sink node. Due to the consistent load distribution, a remarkable increase in load was seen over the lifetime. Chain formation can be performed through the BS or the nodes themselves. If nodes organize a chain themselves, they have to be aware of their places. This chapter reviews the literature to comprehend the various previous flat and hierarchical protocols and the current problem. The primary issue discovered is that energy-efficient CH selection is required in WSNs. This research primarily focuses on performance analysis and designing mechanisms for optimizing the selection of energy-efficient CHs in WSNs.

Wireless Security and trust are inextricably linked concepts. Safety cannot be felt without prior faith assumptions, and confidence metrics must be created in a safe setting. The use of encryption, for example, often ensures confidentiality. In this case, authorised nodes share an encryption key. Adverse nodes are not decipherable since the key is not encrypted/decoded. As a result, node-node communication is secure. However, the message will be confidential only if the initial assumption of confidence is correct. It is unambiguous that encryption/decryption keys must only be passed to trustworthy nodes to ensure safety. Acceptable levels of security cannot be reached without this basis of reasonable trust. Wireless sensor nodes are probably affected. Tamper-proof WSN commodity solutions which are not necessary are not cost-effective. As a consequence, they are susceptible to security breaches involving the physical removal of encrypted material. WSNs bring new safety issues that impede the easy use of existing security procedures. In this research work, simulations are presented for the first trust-based cluster and secure routing programme (TCSRS). Because of its inherent energy-saving properties and scalability for high scalable networks, clustering is among the most acceptable alternatives for sensor networks. Clustering enhances data aggregation, a low-energy strategy in which nodes submit data to a CH for treatment and merger before they are transmitted to BS. It is instrumental in clustering in multicast, unicast and broadcast communications. However, the whole protocol and technique for establishing clusters as explained so far require the confidence of wireless sensor nodes. Naturally, this assumption may lead to a compromise or malicious node for CH. A malicious CH significantly weakens the network's security and usability. Sensor nodes in terms of power, calculation capability, bandwidth and

memory are constrained to be economically viable. Because of memory restrictions and processing capabilities, public cryptography and digital signatures are unworkable. Furthermore, because of the limited power available for these small sensor nodes, overhead communication associated with typical security approaches is unsatisfactory. Especially symmetrical encryption is beneficial for WSNs, which are inherently vulnerable to eavesdropping. However, the cryptographic algorithms do not adequately protect the network in the event of compromised nodes. Because the afflicted nodes are already connected to the web, all the cryptographic material is necessary. This requires a trust mechanism that enables WSN to function effectively even in the face of compromised nodes. It is then essential to focus on CHs, as they are more significant to the proper operation of the network than average. The primary objective is to develop a reliable architecture for clustered WSNs and a technique that minimises the potential to choose compromised or malicious nodes as CHs. The following assumptions are utilised in this suggested TCSRS: First of all, we presume that a protocol and a mechanism for cluster creation are reliable. Once formed, the clusters keep their members except for blocked nodes, deaths or new nodes. The TCSRS approach was simulated and examined using the network simulator, and the findings demonstrated that it is more efficient than T-AODV.

Securing data transfer is critical for WSNs. WSNs can benefit from clustering, which is an effective and practical technique to improve network performance. Since there are so many nodes in WSNs, it is easy for an adversary to infiltrate and breach the sensor nodes, allowing them to obtain the sensor nodes' private keys. To lengthen the lifespan of the network, we can use clustering. while arranging the sensors into clusters, the authors neglected to account for security. Credence is a big deal in this section of the research. One big advantage of this approach is that malevolent or selfish nodes are excluded from emerging as a dominant cluster in a cluster group. The overall performance of the network is improved with the addition of QoS. Clustering techniques for WSN did not take security into account while combining sensors into clusters. The Trust-based Cluster Head Election (TCHE) in WSN was susceptible to dominating cluster selection. There is a chance that the malicious or selfish node will be chosen as the dominant cluster. As a result of the CH's data collection role, it may have an effect on the entire network. The DCSC method was simulated and studied using the network simulator, and the findings demonstrated that the DCSC mechanism is more

efficient than TCHE.A WSN is composed of several dispersed sensor nodes. These sensor nodes are power-constrained. Recharging the sensor node's battery is considered a challenging process. To accomplish this goal, the main focus is on improving the energy efficiency of WSNs. This section proposes the Energy Efficient Cluster Head Selection and Data Convening (EECHDC) technique for WSNs. The CH is determined by the residual energy, the connection density, the node capabilities, and the node degree. Most clustering methods rely on a single measure, and that is power. The following influences may come into play in cluster algorithms that use weights: mobility, degree, and node stability. The approaches above do not account for how all essential measurements are interrelated. ECSHA results are given as a combination of four elements: how many neighbours the node has, how much residual energy remains, and how far away the node is from the cluster's centre. Only nodes near the cluster's centre can be selected. The network is affected by it. For these reasons, WSNS has designed an algorithm to choose a CH based on the variables above: Remaining Energy (Eres), Connection Density (CD), a node's capability (Cn), and degree of the node (D). The EECHDC method was simulated and examined using the network simulator, and the findings demonstrated that the EECHDC mechanism is more efficient than ECSHA.

Extending the lifetime of WSN networks necessitates using clustering mechanisms. Clustering Sensor Nodes (SNs) and choosing CHS for each cluster make up the solution. This enables CHs to receive information from consonant clusters and then pass it on to the BS. Clustered WSNs are commonly assumed to have no obstruction. This research effort proposes the Energy Efficient Clustering Scheme for Obstacles (EECSO), which uses the CH value as the clustering criterion. Three different parameters are used to evaluate the quality of a connection: the quality of the connection, the amount of residual energy, and the node degree. In the presence of an obstruction, the POT determines the shortest path through the WSN. Decreasing the number of forwarders and reducing packet delay are accomplished by using POT. CHs collect and transmit data to the BS on a regular basis. For WSNs, an EECSO, a clustering technique, was devised. WSN entails a large number of sensors spread across a large area, as well as a BS located far from the SN. These sensors monitor the surroundings and provide data to the BS on a regular basis. The use of energy for information transmission should be minimized by splitting the network into clusters. The EECSO method was

simulated and examined using the network simulator, and the findings demonstrated that the EECSO mechanism is more efficient than ADRC.

In Wireless Sensor Networks, Energy Efficient Cluster Head Selection is proposed and investigated in order to maximise throughput and packet delivery, which are critical components of effective communication. To accomplish the research objectives, four protocols have been devised and simulated in the NS2 tool for Wireless Sensor Networks. The protocols are as follows. I Trusted Clustering and Secure Routing (TCSRS) ii) Dominant Cluster Selection based on Credence (DCSC) iii) Energy Efficient Cluster Head Selection and Data Convening (EECHDC) iv) Energy Efficient Clustering Scheme Among Obstacles (EECSO) technique for wireless sensor networks (WSNs). The simulation and analysis of the initial protocol TCSRS established the mechanism's superiority to the T-AODV. At each node, this scheme calculates the direct trust rating normalised to a fuzzy value between zero and one using a trust evaluation algorithm. The DCSC technique was simulated and examined, and the findings demonstrated that the suggested DCSC method is more efficient than the TCHE approach. The foundation for selecting trustworthy CHs is outlined in this section using a credence-based approach. The EECHDC method was simulated, and the findings demonstrated that the EECHDC mechanism is more efficient than the ECSHA mechanism. We performed the simulation of EECSO approach using NS2, and the findings demonstrated the EECSO mechanism's superiority to the ADRC mechanism. The CH is chosen based on the quality factor determined by the link robustness, the node degree, and the energy. The suggested EECSO mechanism increases total packet delivery by 22.65 percent, reduces packet loss by 43.11 percent, reduces average delay by 69.35 percent, increases throughput by 22.65 percent, and saves residual energy by 98.98 percent. While the offered strategies are capable of adapting to dynamic changes, predicting the sensor network's life time boundaries is challenging.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS & ABBREVIATION

Ns2	Network Simulator2
N	Total number of sensor nodes
CBR	Constant Bit Rate
PDR	Packet Delivery Rate
PLR	Packet Loss Rate
RE	Residual Energy
CM	Cluster Member
CH	Cluster Head
QoS	Quality of Service
CD	Connection Density

CHAPTER 1

INTRODUCTION TO WIRELESS SENSOR NETWORKS

Due to the incorporation of sensors into embedded systems, Wireless Sensor Networks now have a greater range of applications (WSNs). Recent years have seen the emergence of a new field of research, fueled by this new challenge: vision sensor networks. Indeed, numerous applications demand reliable detection of objects that are outside the range of view of the WSN. Multimedia data is necessary for validating a wide number of applications, including object identification, location, and tracking. However, multimedia processing is energy intensive, emphasising the importance of a custom solution for the nodes in a network of multimodal sensing. This chapter begins by providing an overview of WSNs and then examines and justifies the development toward networking of vision sensors, which are now being appraised premature from an industrial aspect.

1.1 WIRELESS SENSOR NETWORKS:

WSNs are ad-hoc networks comprised of miniature autonomous entities referred to as sensor nodes that communicate through radio link. The WSN has generated considerable interest in scientific study, owing to novel routing challenges that arise as a result of present network lifetime limits and low node capacity. Numerous technological advancements in disciplines of Micro Opto Electro Mechanical Systems (MOEMS) and wireless communication technologies have enabled the development of inexpensive miniature communicative objects outfitted with sensors. These objects, referred to as nodes, sensors, or hosts, incorporate a computing unit (microcontroller or microprocessor), one or more data collection devices (temperature, humidity, pressure, smoke, motion sensor, etc.), memory, a wireless communication unit, and a power battery or a system for recovering energy from the environment.

The network of wireless sensors depicted in Figure 1.1 is a typical one. The sensor or host nodes are distributed randomly around the monitored zone. The Base Station (BS) is located at the monitored region's far end and is responsible for collecting information from various sensors and transmitting it to a processor interface for analysis.

When an event happens (such as a sudden change in temperature or pressure), an alert is routed through a multi-hop communication network. As such, it is the gathering of information in the aftermath of an incident. There are two additional methods for collecting network data: on-demand and periodic. The first technique entails the sink node broadcasting a request to all nodes in the network, requesting that they deliver their most recent reports. The sensors take measures (temperature, pressure, etc.) at regular time intervals during the periodic collection.

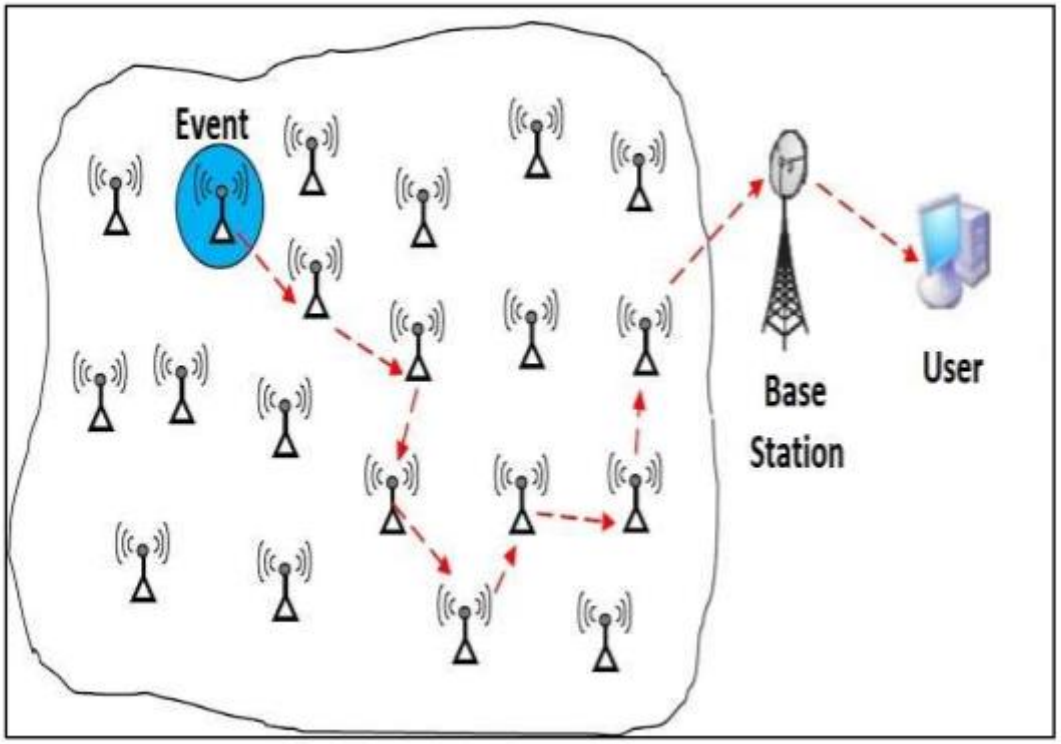


Figure 1.1 Wireless Sensor Network

1.2 WIRELESS SENSOR NETWORKS DESIGN CHALLENGES:

Sensor network features and application requirements have a significant impact on the network design objectives and issues associated with network capabilities and performance. The following are the issues addressed by WSNs:

1.2.1 Flexible and scalable architecture:

The connection should be scalable and expandable. The routing protocols must be designed so that adding nodes has no impact on routing and clustering. To match the additional topology, protocols must be updated. Information transmission messages will be issued to integrate new nodes into the existing network as they are added to the network. This must be done in such a way that the sensor networks exchange as few messages as feasible and hence consume the minimum amount of resources.

1.2.2 Tolerance for errors and adaptation:

If a sensor node fails to operate normally owing to a technical issue or excessive energy consumption, the remainder of the network must function properly normally. Researchers must create adaptive protocols that enable the formation of new links in the event of node failure or link congestion (Mishra et al, 2012). Appropriate methods should be developed to synchronise topological information in response to environmental factors, hence reducing unnecessary energy consumption.

1.2.3 Error prone wireless medium:

Due to the range of settings in which sensor networks can be used, the demands for each operation may vary significantly. Researchers must keep in mind that noise has a substantial

effect on the wireless medium, and therefore the signal attenuates in response to the noise. Bear in mind that an adversary can interfere purposefully and produce enough noise to disrupt communication. It is vital to maintain rapid communication in a setting such as healthcare in order to respond to situations.

1.2.4 Heterogeneity:

Sensor networks are collaborative and highly specialised in their use. Each sort of implementation requires an environment-specific set of safety procedures. Numerous sensors of various types, from a variety of suppliers, are already in use in a variety of applications. Currently, the sensor data is processed in broad application detail. Each application requires its own set of sensors and processing algorithms.

1.2.5 Scaling:

The number of sensors installed might be in the thousands or even millions, and most likely more in the near future. Additionally, the sensor arrays are constructed without regard for any predefined architecture. As a result, the dependability mechanisms specialised to sensor arrays must be capable of efficiently operating with a large number of sensors. These mechanisms must be capable of processing a high volume of events without becoming saturated. Nodes frequently emit additional packets in addition to their data packets in order to undertake monitoring, diagnostic, or debugging tasks.

1.3 Platforms for the Construction of WSN:

Several different sensor categories exist, each with a unique size, computing capacity, memory size, and bandwidth. Depending on the sensor features, the network's size, and the communication protocols used, an RCSF is structured into four distinct types of platforms:

1.3.1 Platform of miniaturized sensors:

The tiny sensor platform is intended for sensors with a small volume (a few mm3) and a low bandwidth (50Kbps). Spec is an example of this type of platform. With a small footprint (2mmx2.5mm), Spec is one of the world's smallest sensors.

1.3.2 Gateway platform:

Gateway platform devices are used to connect the sensor network's data to a more standard network (Ethernet, 802.11), such as Stargate.

1.3.3 General sensor platform:

A general sensor platform is being created to collect and route data from the surrounding environment. A number of platforms in this family have been created, the most recent of which is based on MicaZ, a 10cm3 size sensor with IEEE 802.15.4 communication protocols. Today, MicaZ has established itself as the gold standard for research in the field of sensor networks.

1.3.4 High bandwidth sensor platform:

Sensor platforms with high bandwidth are designed to handle enormous amounts of recorded data (video, sound, vibration). Imote is an example of this family, as its communication is based on the Bluetooth 1.1 standard.

1.4 Operating Systems for Wireless Sensor Networks:

Current solutions for energy conservation at nodes can be classified as microcontroller energy management (calculating the minimal wake state) and peripheral energy management (single- A device when not in use). Numerous specialised operating systems exist, including the following:

1.4.1 Mantis:

Mantis is a multithreaded system written in the C programming language, which was chosen due to its efficiency and portability. It has a minimal memory footprint: 500 bytes in RAM and 14 KB in flash. Mantis conserves energy by enabling a standby mode that removes the sensor when all active processes are completed.

1.4.2 LiteOS:

LiteOS provides a Unix-like environment optimised for network sensors. To construct applications and enable their deployment of the sensors, a C++ object-oriented programming language is offered. LiteOS is memory efficient, requiring only 4 KB of RAM and 128 KB of flash memory to run.

1.4.3 TinyOS:

TinyOS is a component-based operating system that is event-driven in its execution. It is small (less than 400 bytes of RAM), adaptable, and suited for low power consumption performance due to its fundamental concept. TinyOS offers network protocols, distribution services, sensor drivers, and data collecting tools in its library. TinyOS is mostly developed in C, although bespoke apps written in C, NesC, or Java are fairly straightforward to produce.

1.4.4 Contiki:

The code for Contiki is written in C. The entire system is expected to work flawlessly with 2 KB of RAM and 40 KB of memory chips.

1.5 WSNs Routing Challenges

WSN is composed of multiple routing protocols, each of which poses its own set of communication challenges. These impediments must be overcome before WSNs may achieve efficient communication (Romer & Mattern, 2004). WSNs include a number of the routing difficulties and design concerns that impact the packet forwarding (Wang, 2008).

1.5.1 Deployment of Nodes:

The placement of nodes has an effect on the performance of the routing protocol. Node deployment is application-specific and can be either deterministic or random. Sensors are physically integrated into the deterministic implementation, and data is sent through

specified paths. As the name implies, random node deployment distributes sensor nodes randomly, resulting in an ad-hoc architecture. If the exact solution of nodes is not homogeneous, effective clustering is essential to ensure network connectivity and energy efficiency during operation. Inter-sensor communication is often confined to short transmission ranges due to resource and bandwidth constraints. As a result, it is quite likely that a pathway will have a significant number of wireless hops.

1.5.2 Consumption of energy:

By executing computations and transferring data wirelessly, sensor nodes might drain their limited energy supply (Duarte-Melo & Liu, 2002). The lifetime of the sensor node is strongly dependent on the battery. Each node in a multi-hop WSN acts as both a sender and a router of data. When specific sensor nodes fail as a result of a power failure, significant topological changes might occur, necessitating packet rerouting and network redesign.

1.5.3 Model for Data Reporting:

Sensing and reporting data is programs have focused and time-dependent in WSNs. Data reporting is classified into four categories: time-driven (continuous) analysis, event-driven trying to report, query-driven going to report, and hybrid reporting (Yao & Gehrke, 2002). The time-based delivery technique is ideal for applications that require regular data monitoring. As such, sensor nodes will periodically activate their sensors and transmitters, observe their surroundings, and broadcast pertinent data at consistent periodic time intervals.

1.5.4 Tolerance for Errors:

Certain sensor networks may fail or become blocked as a result of a power outage, physical damage, or environmental interference. Sensor node failures should have no influence on the overall purpose of the sensor network. When a high number of nodes fail, the MAC and routing protocols must enable the construction of new links and routes to the data gathering base station (BS). This may involve actively adjusting the transmit energies and signalling rates of existing lines in order to reduce energy consumption, or reconfiguring packets through areas of the network with more energy available.

1.5.5 Scalability:

There can be hundreds, thousands or more sensor nodes in the sensing region. Any routing design must be able to support so many sensor nodes. In addition, network sensor routing techniques should be sufficiently scalable to react to environmental events. The majority of sensors may remain in sleep until an event happens, with data from the few remaining sensors that provide coarse grain information.

1.5.6 Media transmission:

A multi-hop network of sensors connects communication nodes via a wireless connection. Traditional wireless channels problems (e.g. fading, high error rate) may potentially affect the performance of the sensor network. Sensor data often requires a low bandwidth of 1-100

kb/s. The design of the MAC is linked to the media. One technique of creating MACs for sensor networks is to use multiple access (TDMA) time division protocols that cost less energy than dispute-based protocols, such as multiple access carriers (CSMA).

1.5.7 Quality of Service:

In many applications, data must be delivered within a specific length of time following perception; (Tilak et al, 2002).

However, energy saving, which is directly related to network durability, is considered more important than data transmission quality in many applications. When the energy supply expires, the system may have to degrade the quality of the results so that the energy dissipation of the nodes reduces and so extends the life of the network.

1.5.8 Connectivity:

Due to their high node density, sensor networks cannot be completely separated from one another. The sensor nodes should therefore be tightly linked. However, this cannot prevent the design of the network from altering and its size from contracting due to sensor node errors. Connectivity also depends on the distribution of the nodes, which can be random.

1.5.9 Network Dynamics:

The majority of network topologies are supposed to have stationary sensor nodes. However, for various applications, mobility of either BSs or sensor nodes is occasionally necessary (Ye et al, 2002). It becomes more difficult to route messages from or to moving nodes as the stability of the route adds to the energy, bandwidth and other aspects.

1.5.10 Data Aggregation:

Due to the chance that sensor nodes create significant volumes of duplicated data, the number of transfers can be reduced by adding comparable packets from several nodes. The process of aggregating data from various sources is based on a preset aggregation function, for example, double deletion, minimal, maximum, and average data (Krishnamachari et al, 2002). This method has been used for improved energy efficiency and data throughput in several routing protocols.

1.5.11 Node/Link Heterogeneity:

All sensor nodes were more often than not deemed homogenous, i.e. equivalent to the computing, communication and power capacity. The presence of a heterogeneous set of sensors offers a host of technological data flow issues. For example, a vast array of sensors may be necessary to monitor the temperature, pressure and humidity of the surrounding environment, identify movement by means of acoustic signatures and record images or video tracking of moving subjects.

1.6 WSN Applications:

WSNs are used in a variety of multidisciplinary fields because they combine the advantages of distributed computing, sensing, and communication. The following are the principal applications for WSNs:

1.6.1 Military applications:

The civilian realm is critical, as WSNs are designed for surveillance and military purposes. Figure 1.2 illustrates a military application (Shen et al, 2001).

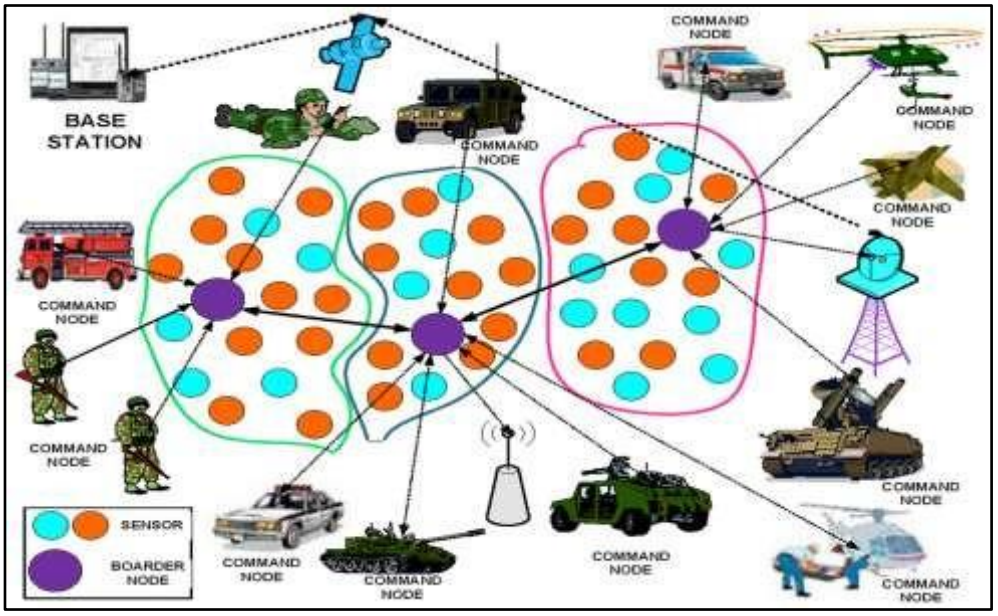


Figure 1.2 Military application (Razaque & Elleithy, 2014)

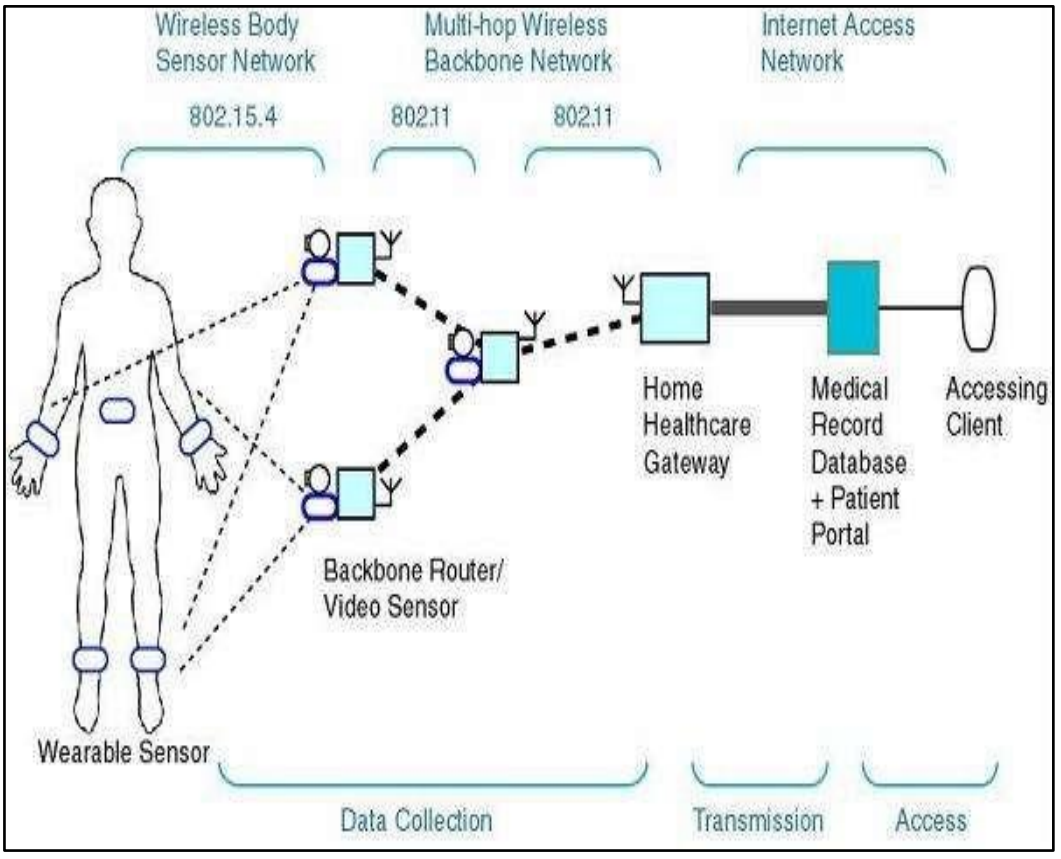


Figure 1.3 Healthcare monitoring (Jimenez & Torres, 2015)

1.6.2 Healthcare monitoring:

This includes emergency medical response, specifically through the use of biosensor technologies to body sensor networks. A person wears biosensors to collect data while performing daily activities on a wireless body sensor network (Heinzelman et al, 2004). Figure 1.3 illustrates a sample healthcare monitoring representation.

1.6.3 Environmental Monitoring:

WSNs have been used to monitor the environment, such as detecting forest fires and monitoring agriculture (Ituen & Sohn, 2007). The sample monitoring of the environment by WSNs is depicted in Figure 1.4.

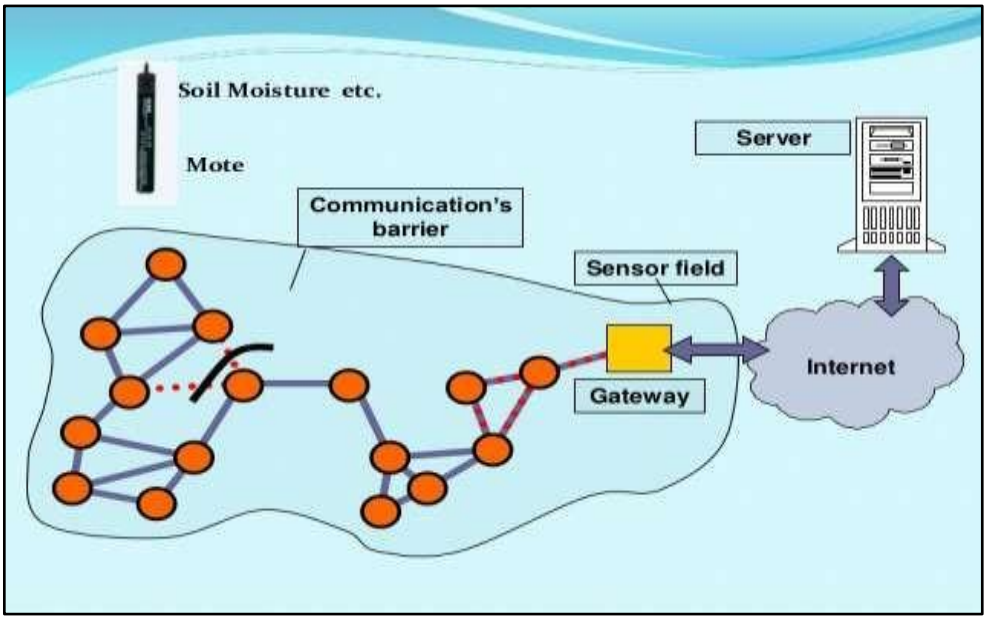


Figure 1.4 Environmental monitoring (Dixit & Smol, 1994)

1.6.4 Water/Wastewater monitoring

Water quality and quantity monitoring encompasses a variety of operations, including assessing the quality of subterranean or surface water and ensuring a country's water infrastructure benefits both humans and animals.

Cluster-based algorithms could be used to subdivide sensor nodes for task subdivision or energy management. Figure 1.5 illustrates a waste water monitoring system.

1.6.5 Rail temperature monitoring:

Evopro is a wireless sensor network (WSN) designed to monitor the temperature distribution in train cars. Temperature measuring modules powered by batteries are connected through ISM radio channels. Communication is organised through the use of repeater and gateway units. The gateway units gather network data and send it to the central processing server. Browser and smartphone applications are used to view monitoring data records. According to the temperature limit settings, alarm messages are sent to selected customers. Figure 1.6 illustrates a temperature monitoring system for rails.

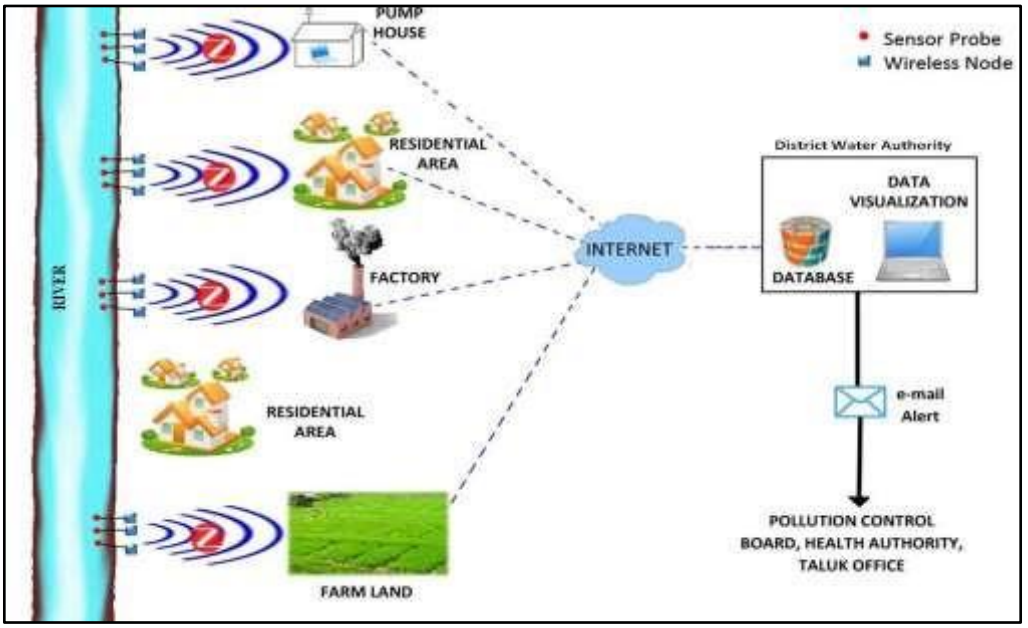


Figure 1.5 Wastewater monitoring (Langergraber et al, 2004)

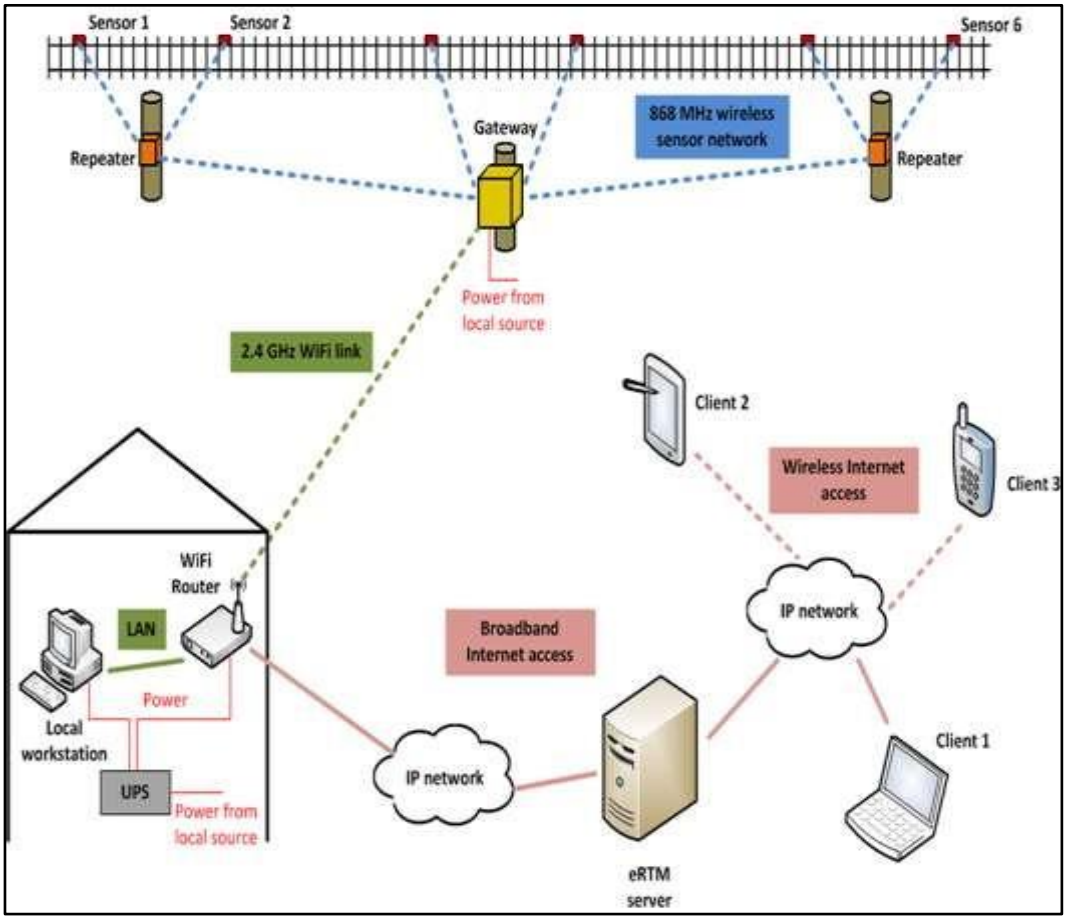


Figure 1.6 Rail temperature monitoring (Hodge et al, 2015)

1.7 Need for the Study:

Although hierarchical routing has a number of advantages, WSNs are still distrusted for their energy efficiency. Group heads/Cluster Heads (CHs) are particularly vulnerable to attacks due to their positions of responsibility within the WSN. Expensive cryptographic solutions are unaffordable to all small and medium-sized businesses while yet maintaining security. Keeping this in mind, the research was conducted to develop unique approaches for selecting energy-efficient CHs in WSN.

1.8 Problem Statement:

WSNs have attracted increased interest in recent years, both from the research community and from actual users. Due to the fact that a large number of nodes in WSNs run on finite batteries, energy resources are a significant bottleneck. A long communication distance between sensors and a sink can significantly drain sensor energy and limit the network's lifetime. Energy is a critical factor to consider with WSNs. It is critical to maximise the lifetime of wireless sensors. Numerous strategies are utilised to optimise the energy consumption of WSN sensor nodes.

1.9 Objectives of the Study:

The fundamental goal of this project is to evaluate and develop acceptable approaches for energy-efficient cluster head selection in wireless sensor networks (WSNs).

- To develop a Dominant Cluster Selection algorithm for WSNs based on Credibility.
- To present an Energy-Efficient Cluster Head Selection and Data Convergence Methodology for Wireless Sensor Networks.
- To design an Energy-Efficient Clustering Scheme for Wireless Sensor Network (WSN) Obstacles.

1.10 Methodology of the Study:

The primary goal of this research is to compare Energy Efficient Clustering to established techniques. The first of the three protocols is Dominant Cluster Selection in Wireless Sensor Networks Based on Credence. Second, we present an energy-efficient method for cluster head selection and data convergence in wireless sensor networks. Finally, we demonstrate an Energy Efficient Clustering Scheme with Obstacles that combines the advantages of the first and second techniques while routing more efficiently than either. The complete study effort demonstrates the efficacy of the proposed mechanism through simulation analysis.

1.11 Limitations of the Study:

While their small size makes them attractive for usage in particular scenarios, their size has an effect on available resources such as energy, computational power, and storage.

1.11.1 Power restrictions:

Due to the sensor nodes' small physical size and lack of wires, they have increased power requirements. Due to the scarcity of cables, there are limited available power sources.

Battery-powered sensor nodes are frequently used. However, because sensor networks have a huge number of nodes and WSNs are typically put in remote or hazardous locations, it is difficult to repair or recharge batteries.

1.11.2 Storage restrictions:

The main limitation of the developer is the available memory and the WSN operating system needs to fit in this memory. The system software, such as the OS, the virtual machine, middleware and application algorithms must be supported in this memory. This RAM should start to be used optimally at a modest level. Furthermore, sensor nodes have a non-volatile external data storage system (e.g. flash memory).

1.11.3 Computational power limited:

For computing power, calculations are proportional to the quantity of power available. Since a small amount of electricity is available, calculations are equally constrained. Whilst it is recognised, that sensors are never able to compute workstations or even mobile handheld computers, researchers and developers are particularly concerned about this problem (Kim et al, 2010).

1.12 Organization of the Thesis:

Chapter 1 introduces WSNs, their design issues, the many platforms on which they can be built, their operating systems, and their routing challenges. The routing problems encompass a variety of routing techniques in two distinct topologies: flat and hierarchical. This section also discusses the limits of sensor nodes and their applications. In general, this chapter discusses the usage and applications of WSN in today's society. The objectives of the research, the motivation for the research, the description of the problem, and the organisation of the thesis complete chapter 1.

Chapter 2 presents a comprehensive review of the literature on Wireless Sensor Networks research. Routing topologies are classed as flat or hierarchical. Routing in a hierarchical topology is further divided into protocols that prioritise security and energy efficiency. Numerous protocols are examined under each area to have a better grasp of the protocols and their applications in the current environment.

Chapter 3 discusses trust-based clustering and secure routing in wireless sensor networks. The major objective is to build a trust-based architecture for clustered WSNs and a mechanism that minimises the possibility of compromised or malicious nodes being chosen as CHs. This technique calculates two critical metrics: cluster head selection and trust. The simulation analysis is carried out in two scenarios involving the deployment of 50 and 70 nodes in the communication network.

Chapter 4 discusses the creation of a WSN-based Dominant Cluster Selection algorithm based on Credence. The credibility value is determined by aggregating data from the node's

neighbours. The credibility function is used to assess the nodes in the network for malicious behaviour. The proposed dominant cluster selection technique evaluates four critical metrics: neighbour node recommendation, node communication, node quality of service, and node residual energy. The simulation analysis is carried out in two scenarios involving the deployment of 50 and 70 nodes in the communication network.

Chapter 5 provides the design of the WSN Head Selection and Data Convening energy-efficient cluster. The selection of CH is limited to nodes only around the centre of the cluster. It affects network performance. The proposed selection and data collecting of energy-efficient cluster heads at WSN comprises the following phases: installation phase, cluster head selection stage, data collection phase and data transmission phase. In two situations, the simulation study involves 50 and 70 nodes in the communication network.

Chapter 6 presents the Energy Efficient Clustering Scheme among Obstacles. Separation phase, election phase, obstacle estimation phase and transmission phase depicts the proposed energy efficient scheme among obstacles. The data transmission phase contains three main activities: collecting the information, aggregating it and sending the collected data to the destination. The simulation analysis is carried in two cases with 50 and 70 nodes deployed in the communication network.

Chapter 7 provides the comparison analysis of all the four methods proposed in this research work against each other. Animation window is shown for the research work for 50 and 100 node scenarios. Four methods are compared with five metrics including packet delivery rate, packet loss rate, average delay, throughput and residual energy.

Chapter 8 provides the Conclusion of investigation work and the future scope.

CHAPTER 2

LITERATURE REVIEW

Before developing any unique algorithm for WSNs, a thorough examination of the literature is required. A study of routing protocols is presented, with protocols categorized according to their topologies: flat and hierarchical, with hierarchical protocols classified according to their security and energy efficiency. Figure 2.1 illustrates the routing protocol types studied in this survey for WSNs with flat and hierarchical topologies.

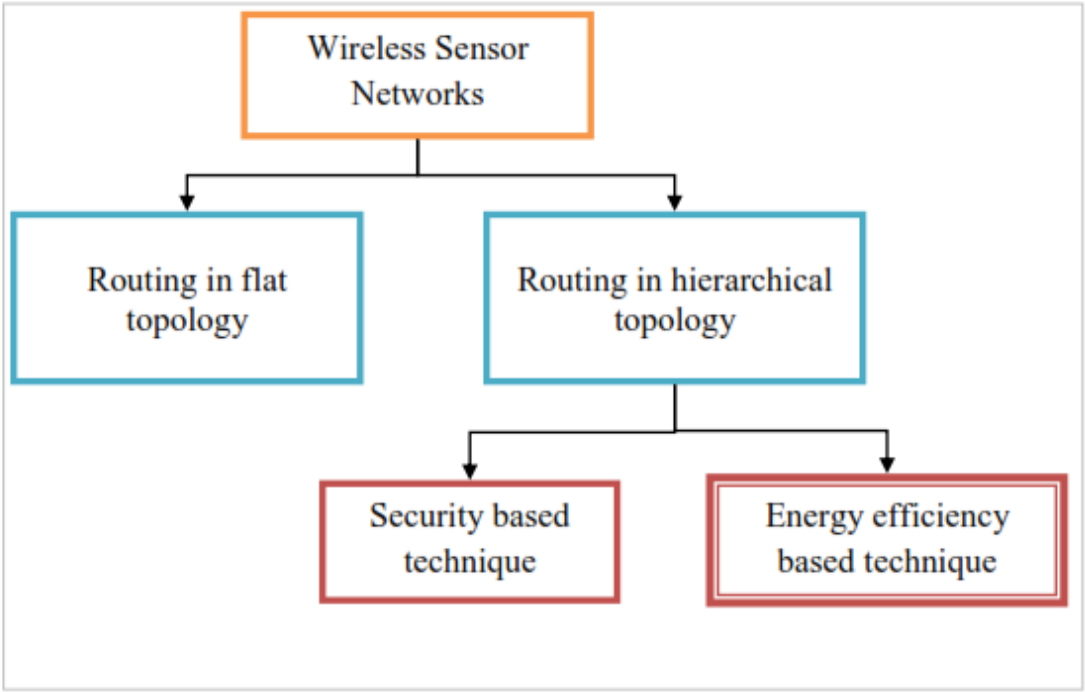


Figure 2.1 Routing strategies for WSNs classified

The majority of protocols described in the literature employ a hierarchical or clustered topology (SK & KC, 2013). Flat topology is distinct from hierarchical topology in several ways, and it comes with several advantages and downsides.

- Routing in a spherical topology
- Routing in a nested topology

This chapter describes in depth the various routing protocols proposed for a WSN, both flat and hierarchical.

2.1 Routing in a spherical topology:

Routing is the process of determining which relay nodes in the WSN are suitable for transmitting data from source to destination.

2.1.1 Flooding and Gossiping:

Flooding and gossiping require no knowledge of the topology or protocols of the network (Heinzelman et al., 1999). Each sensor gets a data packet and then distributes it through the flooding process to all surrounding nodes. The communication is terminated when the required hop number is achieved or the package is received. Gossiping is a more advanced type of flood

where the receipt or destination node dispenses the packet to randomly selected neighboring nodes, subsequently forwarding it to another randomly selected neighbor, and so forth (Kumar & Pahuja, 2014). Overlap, resource blindness, and implosion restrict flooding. Implosion is averted by sending data to a random neighbor instead of utilizing the usual broadcast strategy that transmits packets to all neighbors (Dutta et al., 2016). Gossip causes a delay in data transmission in a communication network between sensor nodes.

2.1.2 SPIN: Sensor Protocols for Information via Negotiation:

SPIN is a mechanism for disseminating information effectively across the sensors in a low-energy WSN system (Kulik et al., 2002). Nodes utilizing the SPIN communication protocol name their data with meta-data, high-level data descriptors (Heinzelman et al., 2009). You use metadata negotiation, which removes needless network-wide data transfer. SPIN nodes may make decisions depending on the availability of knowledge of resources and application-specific data. This allows sensors to spread data efficiently in the face of a restricted energy supply (Xiao et al., 2006). For point-to-point transmission (Point Point Transmission) and Energy Conservation (Energy Conservation) networks, SpinPP and SPIN-RL are meant for broadcast networks, while SPIN-BC is intended for broadcasting networks.

2.1.3 Directed diffusion: a scalable and robust communication paradigm:

Directed diffusion is a data-centered strategy where any communication is intended to identify specific data (Intanagonwiwat et al., 2000). The application is known to each node in a directed distribution network. This permits diffusion in empirically optimized paths and caching and data processing in the network to save energy. The four main features of direct dissemination are interests, gradients, data, and strengthening (Sohrabi et al., 2000). Environmental monitoring is considered a guided application for dissemination.

2.1.4 Gradient-Based Routing:

Generic GBR (GBR-G) and Competing GBR (GBR-C) techniques have already been proven to be energy efficient in single platform WSNs (Migabo et al., 2015). These approaches rely on the premise that each sensor node creates a different BS gradient. The advantage of this technique is that the energy consumption of sensor nodes is often higher due to the proximity of the sink than the energy consumption of another sensor node in the network. Enhanced routing algorithms GBR-G and GBR-C consider the design of a new gradient to extend network life (Faruque & Helmy, 2003). The GB-GBR and CB-GBR algorithms select the highest gradient connections and the link that avoids the most congested sensor nodes when packets are transmitted.

2.1.5 Rumor routing algorithm:

Rumor Routing enables the delivery of inquiries to network events (Braginsky & Estrin, 2002). Rumor Routing is a programmable system that allows trade-offs between setup time and delivery reliability. Rumor Routing is intended for situations in which geographic routing rules

are inapplicable due to the absence of a coordinate system or a geographically related event of interest (Messina et al., 2007). Directed diffusion is thought to have several uses, including habit/environmental monitoring.

2.2 Routing in a nested topology:

In hierarchical WSNs, there are several data transfer techniques available. WSNs have widely used hierarchical topology for several protocols, including data gathering (Ye et al., 2005), target tracking (Chen et al., 2004), one-to-many, multiple-to-one, one-to-many or one-to-all communication, and routing (Yuan et al., 2008). (Al-Karaki, 2004). Khamal. This can be done upon request or on a recurrent basis to keep the BS up to date on the monitoring scenario. Routing protocols can be classed as proactive or reactive depending on how routes in each WSN node have been adjusted (Haas & Tabrizi, 2008). Typically, proactive protocols are used in big networks.

2.2.1 Proactive Protocols

The main proactive protocols are:

2.2.1.1 Destination Sequenced Distance Vector (DSDV):

Each node maintains a routing table and transmits packets to other nodes inside the network via the table (Perkins & Bhagwat, 2004).

2.2.1.2 Topology Broadcast based on Reverse Path Forwarding (TBRPF):

The nodes regularly communicate information about the network topology to create their routing tables (Ogier et al., 2004).

2.2.1.3 Optimized Link State Routing (OLSR):

It dynamically determines the routing tables by using a form of routing link-state (Clausen & Jacquet, 2006).

2.2.1.4 Fisheye State Routing (FSR):

Each node transmits its routing table at a frequency dictated by the number of hops needed to pass through a packet (Pei et al., 2000).

Routing tables of nodes are not sent periodically in reactive protocols but only if user traffic has to be routed to a place for which no path is currently known. In this circumstance, a request for such a path is spread across the network. Examples of reactive protocols are ad hoc on-demand distance vehicle routing (AODV) (Perkins et al., 2003) and dynamic source routing (DSR) (Johnson et al., 2001).

The routing tables of nodes are not supplied periodically in reactive protocols, but only if the user traffic is routed to a place where the path is not currently known. In this circumstance, a request to build such a path is broadcast throughout the network. Examples of reactive protocols are ad-hoc on-demand vector routing (AODV) (Perkins et al., 2003) and dynamic source routing (DSR) (Johnson et al., 2001).

Hybrid protocols constitute a subset of proactive and reactive protocols for routing. These protocols include proactive and reactive principles of protocols. They use an aggressive protocol to determine the next neighbor (for instance, the neighborhood 2 or 3 hops away) and have trails right instantly. The hybrid protocol searches for routes utilizing a reactive protocol beyond the nearby area. The zone routing protocol is an application of a mixed protocol (Lakhtaria, 2010).

2.2.2 Security based hierarchical routing protocols:

Hierarchical routing issues involve a safe environment where the network is devoid of attackers in all sensor nodes. Many techniques for Security in large-scale hierarchical routing systems are being developed.

2.2.2.1 An authentication framework for hierarchical ad hoc sensor networks:

TESLA certificates are used as an authentication mechanism (Bohge & Trappe, 2003). The use of the message authentication code by the framework protects all data against fraudulent modification and manufacture. It introduced an authentication architecture for a hierarchical ad hoc sensor network driven by application and explored how compromised nodes were treated (Sadananda et al., 2013). It cannot prevent intruders from entering, sending, or safeguarding them against eavesdropping on the network.

2.2.2.2 Secure Routing Protocol for Sensor Networks:

SRPSN was a hierarchical routing technique for energy efficiency (Tubaishat et al., 2004). You have devised a secure WSN routing protocol that protects you from other assaults by setting a safe path from the source to the sink node (Perrig et al., 2002). They used symmetric-key cryptography to construct a secure group management scheme that comprises group communications policies, an algorithm, and group membership requirements when producing the distributed group key (Zhang et al., 2008). The absence of an authentication technique was a shortcoming of this protocol. SRPSN is vulnerable to certain attacks, including spoofing, modification, and replay.

2.2.2.3 LHA-SP: Secure Protocols for Hierarchical. Wireless Sensor Networks:

LHA-SP aims to secure arbitrary levels of heterogeneous Wireless Sensor Networks (WSNs) (Oliveira et al., 2005). It adopts a symmetric key approach and assumes that an adversary trying to compromise the group key requires patience with a communication network node. It prevents intruders from intercepting, changing, or adding messages to the networks and prohibits the eavesdropping of communication between genuine nodes (Karlof & Wagner, 2003). The common key guarantees authentication and confidentiality. It addresses the problem of the orphan node.

2.2.2.4 Efficiency Security Model of Routing:

The Efficient Routing Security Model (ESMR) protocol uses only public-key encryption (Chen et al., 2008). Although ESMR works better in a non-attacking environment, it is useful if the

number of attacker nodes in the communication network increases. This protocol is designed to protect against external threats and is highly computerized using public-key encryption (Rabin, 2009).

2.2.2.5 Secure Routing Protocol Cluster Gene-Based for WSNs:

Secure Routing Protocol Gene-Based Cluster (SRPBCG) was developed for WSN's to manage local trust and reputation and authenticate a node identity with a low overhead and time delays (Zhou & Li, 2009). The biological "gene" as an encryption key is a very safe and efficient key distribution strategy requiring minimum overhead memory and transmission. This technique is limited to tackling the attack and compromising the nodes of the opponent.

2.2.2.6 REACH:

REACH is a safe LEACH solution for clusters' dynamic and periodic production (Wu et al., 2008). REACH introduces the problem of the orphan node due to its random parallel key system. A random pair-wise key technique was used to avoid the orphan node problem. REACH uses one-way hash chains, symmetric and asymmetric encryption to ensure LEACH safety. In REACH, too many attacks, for example, fraudulent, altered, and replayed information, sinkhole, wormhole, selective transfers, HELLO flooding, and the Sybil attack, have been rejected.

2.2.2.7 F-LEACH:

F-LEACH was a communication protocol between nodes in a LEACH network (Oliveira et al., 2006). It strengthened LEACH's Security by integrating a random key pre-distribution process with symmetrical key encryption. FLETCH offers authenticity, integrity, confidentiality, and freshness node-to-node communication. However, it is susceptible to attacks by nodes.

2.2.2.8 Secure Hierarchical Energy Efficient Routing:

The Secure Hierarchical Energy Efficient Routing (SHEER) protocol provides safe communication on the network layer (Ibriq & Mahgoub, 2006). It enhances the network's energy performance and life by using a three-level cluster design with a probabilistic broadcast mechanism. The HIKES asymmetric key encryption technology and a secure key transfer protocol were designed in the SHEER protocol to secure routing.

2.2.2.9 A Novel Hierarchical Routing Protocol Algorithm:

A Novel Hierarchical Routing Protocol (NHRPA) Algorithm was a routing protocol that employed the best routing technology for nodes depending on their distance from the base station (BS), their distributed node density, and their residual energy (Cheng et al., 2008). Its energy consumption, packet latency, and Security were compared against Directed Diffusion (DD), LEACH, and PEGASIS in the event of compromise assaults by nodes (Fang et al., 2005). Since this routing protocol does not use encryption mechanisms, its overhead is negligible. It only stops node compromise attacks, however.

2.2.2.10 Authentication Confidentiality cluster-based secure routing:

Authentication, The secure cluster-based confidentiality routing system employs both public-key (digital signature form) and private-key encryption (Srinath et al., 2007). This protocol is used to connect with an opponent or compromised node inside. Due to high computing needs, it is inefficient for WSNs (usage of public-key cryptography).

2.2.2.11 SS-LEACH:

A secure hierarchical protocol is known as SS-LEACH; a certain LEACH variant enhances the selection process for CHs and generates dynamic stochastic CH multipaths to communicate with the BS. This boosts energy efficiency and, therefore, the lifetime of the network. It secured the LEACH protocol by using the key mechanisms for pre-distribution and self-location. It forbids the participation of a compromised node in a network and maintains the confidentiality of the packet over the communication network. It reduces the effects of selective transmission, HELLO flooding, and Sybil attack.

2.2.3 Energy efficiency based hierarchical routing protocols:

Either "useful" or "wasteful" operations generate energy consumption in a node. The benefits include data transfer and processing of requests while wasteful consumption occurs during the construction of the routing tree, data transmission owing to an improbable environment, redundant broadcasting via heading messages, and idle media listening (Liu, 2012). (Kaur et al., 2013).

2.2.3.1 Low Energy Adaptive Clustering Hierarchy:

LEACH was the first and most often used WSN hierarchical clustering technique (Heinzelman et al., 2000). As the name implies, it is based on the dispersed construction of clusters, a sort of cluster formation that distributes nodes. Randomly, LEACH selects some sensor nodes as CHs and causes every node to spin as CHs, employing a randomized rotation strategy, which equally divides energy demand throughout the node's network. To minimize the amount of information transmitted throughout the communications network, the CH node compresses data collected from its members and provides the aggregated data/package for the BS. During data transmission, collisions may occur as a result of an external disruption within the network. Collisions generally happen in two ways: inter-cluster or intra-cluster crashes.

Consequently, LEACH uses TDMA/CDMA MAC protocols to minimize such collisions (Ye et al., 2002). This protocol is appropriate for applications requiring continuous sensor network monitoring. Data collection in LEACH is centralized and can be performed periodically (Yadav & Sunitha, 2014).

2.2.3.2 Power-Efficient Gathering in Sensor Information System:

PEGASIS was developed as a LEACH protocol improvement (Lindsey & Raghavendra, 2002). PEGASIS was an optimally functioning chain-based protocol. Unlike LEACH, it uses a chain-based technique to improve the energy efficiency of the sensor network. Each node in a chain

receives and transfers data to the nearest neighbor, but only one node transmits aggregated data to the BS. Nodes will turn to be the leader of the chain to transfer data to the sink node. Due to the consistent load distribution, a remarkable increase in load was seen over the lifetime. Chain formation can be performed through the BS or the nodes themselves. If nodes organize a chain themselves, they have to be aware of their places.

2.2.3.3 Threshold sensitive Energy Efficient Protocol:

A reactive protocol specifically developed for reactive networks was the Threshold Sensitive Energy Efficient Protocol (TEen) (Manjeshwar & Agrawal, 2001). Reactive networks require nodes to react to sudden network changes such as auditory, thermal, or magnetic modifications. TEEN uses a hierarchical cluster-based technique as well as a data-centered approach. Each cluster will have a CH that collects, aggregates, and sends data from its members to the BS or the top CH node. This protocol sets up the cluster hierarchy and directly reports the full cluster nodes to the BS. The BS is the center of the order, which directs the entire network.

2.2.3.4 Adaptive Threshold-sensitive Energy Efficient Protocol:

An improvement to the TEEN Protocol is provided by the Adaptive Threshold Sensitive Energy Efficient Protocol (APTEEN). The TEEN threshold value is a hybrid protocol dependent on application type and user requirements (Manjeshwar & Agrawal, 2002). The aim is not just to achieve a holistic network perspective but also to execute time-critical data sensing. The CHS will broadcast the following messages following the network clustering: characteristics, thresholds, schedules, and count time (CT). The features define the number of physical factors the user is curious about. The entry refers to the hard and soft thresholds. The program parameter sets the TDMA schedule, assigning time slots to each node, while the count-time parameter specifies the maximum period between two consecutive node reports.

2.2.3.5 Group based Sensor Network:

GSEN may be divided into two phases: group training and transmission (Tabassum et al., 2006). (Song 2005). Song, 2005. GSEN prefers to rebuild groups after an interval of rounding. Therefore, the groups established remain unchanged for the next (R-1) rounds, but the duty of the group leaders rotates randomly between the other nodes inside each cycle. The geographical definition of each GSEN group is that each group leader is a representative of that region. Each leader collects data from its group members' nodes at the data collection and transmission phase.

2.2.3.6 Power Efficient and Adaptive Clustering Hierarchy:

Cluster generation is performed using overheard information through Power Efficient and Adaptive Clustering Hierarchy (PEACH) (Yi et al., 2007). Overhearing is a phrase that refers to the dialogue between two neighboring nodes. PEACH has the advantage that no additional overhead packet transmission is required. In conventional clustering algorithms, PEACH is aimed at alleviating the difficulties associated with fixed-level clustering. It is scalable and

more efficient than other currently used protocols. It can also be employed in position-conscious and position-insensitive WSNs.

2.2.3.7 Hybrid Energy Efficiency Protocol:

The Hybrid Energy Efficient Protocol (HEEP) is an upgrade protocol that extends network life by minimizing energy use (Boubiche & Bilami, 2011). It was designed by merging LEACH and PEGASIS, the two most widely used protocols. It exploits the weaknesses of both protocols to optimize data routing by using their features. HEEP is built on the principle of LEACH clustering and the direction of PEGASIS chain building.

The construction of the PEGASIS chain is inside the LEACH clustering, therefore minimizing chain formation. Furthermore, HEEP avoids the CH overhead in LEACH by aggregating data down a chain of nodes rather than via a CH node. This reduces the amount of data transmitted between the CH and its members and saves energy.

2.2.3.8 HEED: Hybrid Energy-Efficient Distributed:

Hybrid Energy-Efficient Distributed (HEED) clusterings collect CHs periodically based on a node residual energy combination and a secondary criterion, for example, the proximity of the node to neighbors or grade (Younis & Fahmy, 2004). HEED completes iterations in O(1), has a low overhead messaging, and distributes CH fairly evenly around the network. HEED can assure clustered network connectivity asymptotically with proper node density limitations and transmission inter-cluster and intra-cluster ranges.

2.2.3.9 Distributed Weight based Energy-efficient Hierarchical Clustering:

The DWEHC protocol was a distributed hierarchical clustering system, similar to the HEED protocol, The distributed energy-efficient hierarchical clustering system (Ding et al., 2005). The main purpose of the DWEHC method was to improve HEEDs by balancing the cluster structure and maximizing communication within clusters through sensor node position sensing. To allow communication between nodes (i.e., multi-Hop communication inside the group), the DWEHC Protocol creates a multilevel routing structure within the cluster and restricts the number of children in a parent node. In addition, each node is assigned a weight in the DWEHC protocol for the CH election.

2.2.3.10 Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks:

Span, the power-saving solution for ad-hoc multi-hop networks, significantly reduces energy consumption without compromising network capacity or connection (Chen et al., 2002). Span is based on the notion that just a small number of nodes must be active to transmit traffic for active connections if the area of a shared channel WiFi network has a suitably dense population of nodes. Spain is a distributed, randomized system in which nodes select whether to sleep or join a transmission backbone as a per-node coordinator. Each node decides based on evaluating how many of its neighbors will benefit from their presence and the energy available. A

randomly selected technique demonstrates how localized node decisions produce a related global design that preserves capabilities. The system's lifetime is increased due to the expanded span as the ratio of idle to sleep energy use has improved substantially.

2.2.3.11 Geographical Energy-Aware Routing:

A low-energy routing system used to route requests to specified places within a sensor field was geographical energy ware routing (Yu et al., 2001). In GEAR, sensors should be fitted with location hardware such as a GPS unit or localization system to detect their position at the moment (Bulusu et al., 2000). Furthermore, the sensors are aware of their remainder of energy and their neighbors' positions and residual energy. GEAR uses energy-aware algorithms based on geographic information to pick the sensors for a packet to its destination area. The package is subsequently distributed by a recursive geographical transmission method in the target region.

2.2.3.12 Scalable Energy Efficient Clustering Hierarchy:

CH and relays are allocated via the Scalable Energy Efficient Clustering Hierarchy (SEECH) approach (Tarhani, M., 2014). SEARCH was used primarily to minimize the CH energy load. The Data Aggregation Efficient Cluster Head Selection Scheme (ECHSSDA) uses n clusters (Varalakshmi et al., 2014). (Delgado et al., 2011). CH received data from cluster members, aggregated data, and communicated with the BS at last.

2.2.3.13 Secure and Efficient data Transmission:

Secure and efficient Data Transmission (SET) protocols have included Identity-Based digital Signature (IBS) and Identity-Based Online and Offline (IBOoS) systems for Cluster-based Wireless Sensor Networks (CWSNs) (Lu et al., 2014). SET-IBS security depends on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS minimizes the computing costs necessary to secure a protocol crucial for WSNs, based on the discrete hardness of the logarithm issue. A simple and effective CH-selection strategy called Smart Cluster Head Selection (SCHS) was designed using the distributed clustering technique (Pal et al., 2012). In this arrangement, the network area is separated into two parts: the border area and the inner area. Only internal nodes are qualified for the job of CH. This selection approach minimizes communication intra-cluster distances, thus boosting the energy efficiency of a cluster.

2.2.3.14 LAMAR: Landmark routing for large-scale wireless ad hoc networks with group mobility:

LAMAR is a routing protocol that combines FSR and landmark routing properties (Pei et al., 2000). The use of landmarks for each node group minimizes the overhead routing (e.g., a team of coworkers at a convention or a tank unit on the battlefield). As with FSR, nodes only exchange connections with their neighbors (Ni et al., 2011). Within the Fisheye range, routes are right, while corresponding network landmarks sum up ways to faraway node groups. The

first target for a packet sent to a remote destination is the landmark; while approaching the goal, it gradually changes to the correct path provided by Fisheye.

2.2.3.15 Node Behavioural Strategies Banding Belief Theory of the Trust Evaluation Algorithm:

Behavioral Nodes Strategies, The method of trust assessment (NBBTE) integrates behavioral nodes and updated evidence theory (Feng et al., 2011). To calculate the weighted average trust factors, coefficients, and behavior of sensor nodes related to the network application, direct and indirect trust values are obtained. The fuzzy set approach was employed to construct the fundamental input vector of evidence throughout this period. The value of evidence is determined between indirect and direct trust values and is used to connect the revised combination rule to the integrated trust value of communication nodes.

The Regional Energy-Aware Clustering technology (REAC) has been developed to extend the lives of wireless sensor networks (Leu, J.S. 2015). The CH was determined by the weight of the sensor nodes in this method. The importance of each sensor node and region is calculated using all sensor nodes in each cluster's average energy. This strategy improves the longevity and stability of the network.

WSN clustering-based data monitoring is a process driven by events, which only reports data when an event occurs (Adulyasas et al., 2013). This approach sets a threshold and communicates any sensor data that shows substantial changes above the point to the BS. When an event is recognized, the sensors are grouped, and one sensor is referred to as CH, transmitting data to the BS of the network. The drawback is that it is incompatible with continuous monitoring applications (Feng et al., 2013).

2.2.3.16 Load Balanced Clustering Algorithm with Distributed Self- organization:

The Load Balanced Clustering Technique with DSBCA is a load-balanced clustering algorithm that takes the stochastic distribution of the sensor node into consideration. This technique builds balanced clusters (Sebastian et al., 2014). The cluster radius can be estimated by the density and distance of the group from the BS. The radius of the clusters rises with increasing distance from the BS and reduced connection density. Each individual selects their weight (Liao et al., 2013). The highest weight node decides the CH. The weight is defined by the remaining energy and the proximity of certain neighbors, and the number of times the node is chosen as CH (Syed & Kumaran, 2008). The biggest disadvantage is that it demands more transmission energy and takes more time during the selection of CH to compute weight.

2.2.3.17 Hierarchical Power-Aware Routing:

HPAR divides the network into groups of sensors (Li et al., 2001). Each sensor cluster is referred to as an area in the immediate vicinity, and each zone is treated independently. Each site is free to select how communications are hierarchically routed across the other places to maximize the system node battery life. The message is routed so that the minimum residual

capacity splits the maximum remaining power, called the ultimate minute path (Abdullah & Hua, 2009). High residual power consumption nodes can be more costly than those with the lowest energy consumption.

2.2.3.18 Virtual Grid Architecture routing:

A power-efficient routing paradigm using data aggregation and network processing is the virtual grid architectural path that maximizes the network's lifetime (Al-Karaki et al., 2004). Due to the static nature of nodes and their relatively limited mobility in many WSN applications, nodes in fixed topology should be organized (Xu et al., 2001). A GPS-free strategy was used to build clusters with fixed, similar, adjacent and non-overlapping symmetrical morphologies.

2.2.3.19 Self Organizing Protocol:

The infrastructure supporting heterogeneous sensors was constructed utilizing an SOP and a taxonomic application (Subramanian & Katz, 2000). The sensors could be portable or stationary. Some sensors perform environmental scanning and transfer data to a preset group of routers (Bandyopadhyay & Coyle, 2003). The router nodes are static and function as the backbone of communication. The routers route the data acquired to the stronger BS nodes. To be included in the network, each sensor node must interact with a router (Doumit & Agrawal, 2002).

2.2.3.20 Sensor Aggregates Routing:

Three approaches were developed in Sensor Aggregates Routing (SAR) (Fang et al., 2003). To begin with, to aggregating sensor data for a given monitoring task, a lightweight protocol called DAM is presented. Second, the Energy-based Activity Monitoring (EBAM) technique calculates the power level of each node by calculating the signal effect area and aggregating the detected target energy with a weighted form at each affected sensor, provided that each sensor has the same or consistent energy level. The third approach, Expectation-Maximization Similar to Activity Monitoring (EMLAM), eliminates the assumption that the target energy level is continuous and uniform.

2.3 SUMMARY:

This chapter reviews the literature to comprehend the various previous flat and hierarchical protocols and the current problem. The primary issue discovered is that energy-efficient CH selection is required in WSNs. The subsequent chapters propose novel techniques for resolving this issue in WSNs. This research primarily focuses on performance analysis and designing mechanisms for optimizing the selection of energy-efficient CHs in WSNs.

CHAPTER 3

WIRELESS SENSOR NETWORK WITH A TRUST-BASED CLUSTER AND SECURE ROUTING SCHEME

Wireless Security and trust are inextricably linked concepts. Safety cannot be felt without prior faith assumptions, and confidence metrics must be created in a safe setting. The use of encryption, for example, often ensures confidentiality. In this case, authorised nodes share an encryption key. Adverse nodes are not decipherable since the key is not encrypted/decoded. As a result, node-node communication is secure. However, the message will be confidential only if the initial assumption of confidence is correct. It is unambiguous that encryption/decryption keys must only be passed to trustworthy nodes to ensure safety. Acceptable levels of security cannot be reached without this basis of reasonable trust. Wireless sensor nodes are probably affected. Tamper-proof WSN commodity solutions which are not necessary are not cost-effective.

As a consequence, they are susceptible to security breaches involving the physical removal of encrypted material. WSNs bring new safety issues that impede the easy use of existing security procedures. In this research work, simulations are presented for the first trust-based cluster and secure routing programme (TCSRS).

3.1 Background work for the proposed TCSRS:

Because of its inherent energy-saving properties and scalability for high scalable networks, clustering is among the most acceptable alternatives for sensor networks. Clustering enhances data aggregation, a low-energy strategy in which nodes submit data to a CH for treatment and merger before they are transmitted to BS. It is instrumental in clustering in multicast, unicast and broadcast communications. However, the whole protocol and technique for establishing clusters as explained so far require the confidence of wireless sensor nodes. Naturally, this assumption may lead to a compromise or malicious node for CH. A malicious CH significantly weakens the network's security and usability.

3.2 Depiction of the proposed TCSRS:

Wireless Security and trust are inextricably linked concepts. Safety cannot be experienced without trust and trust measurement presumptions. The use of encryption, for example, often ensures confidentiality. In this case, authorised nodes share an encryption key. Adverse nodes are not decipherable since the key is not encrypted/decoded. As a result, node-node communication is secure. However, the message will be confidential only if the initial assumption of confidence is correct. It is explicitly stated that encryption/decoding keys must be passed on to credible nodes for security purposes alone. Acceptable levels of security cannot be reached without this basis of reasonable trust. Wireless nodes are a physical compromise. Tamper-proof methods are not cost-effective for commodity WSNs (Anderson et al., 2004). As a consequence, they are susceptible to security breaches involving the physical

removal of encrypted material. WSNs provide new issues that prohibit standard security measures from being implemented easily (Slijepcevic et al., 2002).

Sensor nodes in terms of power, calculation capability, bandwidth and memory are constrained to be economically viable. Because of memory restrictions and processing capabilities, public cryptography and digital signatures are unworkable. Furthermore, because of the limited power available for these small sensor nodes, overhead communication associated with typical security approaches is unsatisfactory. Especially symmetrical encryption is beneficial for WSNs, which are inherently vulnerable to eavesdropping.

However, the cryptographic algorithms do not adequately protect the network in the event of compromised nodes. Because the afflicted nodes are already connected to the web, all the cryptographic material is necessary. This requires a trust mechanism that enables WSN to function effectively even in the face of compromised nodes. It is then essential to focus on CHs, as they are more significant to the proper operation of the network than average.

The primary objective is to develop a reliable architecture for clustered WSNs and a technique that minimises the potential to choose compromised or malicious nodes as CHs. The following assumptions are utilised in this suggested TCSRS: First of all, we presume that a protocol and a mechanism for cluster creation are reliable. Once formed, the clusters keep their members except for blocked nodes, deaths or new nodes.

3.2.1 Cluster Head selection mechanism:

The CH performs conventional functions for the TCSRS system for data gathering, fusion and transmission to the BS at a higher level. CHS are initially self-elected. Self-selection for the initial set of CHs is permitted originally. This is congruent with the underlying idea that no hostile nodes exist during setup. The CH schedules transmission of each member in TDM format and notifies all members when the clusters are established.

If the current CH battery level goes below or after a predefined service life, a new message is sent (inside the cluster). Then all the nodes vote a secret ballot for a new CH. This is done by answering the preference of your candidate for the new electoral message. The CH key is used to encrypt the answer or vote. Neighbours, therefore, have no information concerning each other's political affiliations since the key is secret and unique to each node-CH pair. The node candidate is chosen from the list of trusted neighbours. The current CH after that summarises the results by a simple majority. Vice-CH is the second-largest voting node. Vice-goal CH's is to carry out CH responsibilities. Before its successor is handed over, the newly elected CH shall be deposed. When the process is finished, CH will forward the winner and runner to all cluster members.

The CH sometimes sends a message that is not credible. Nodes chose their less confident neighbour and reacted to the CH in the same manner. The CH provides a list of messages

from non-trust and selects the node with the lowest trust. The CH presents this node as a challenge. If it doesn't look successful, it's blocked. If accepted, the cluster members will be alerted. However, they are not essential to improve the node's confidence.

3.2.2 TRUST CALCULATION:

Confidence parameters can be observed, and network occurrences can be measured. Each node has a monitoring mechanism to keep an eye on other nodes' network behaviour. It allows nodes to calculate and preserve confidence levels for neighbours by using monitoring information. A node can learn about the successful delivery of any packet that it transmits using passive recognition. In passive recognition, the sender node enters the promiscuous mode after delivering any package to hear the retransmission of the recipient node. In addition, when one node is transmitted, all other neighbourhood nodes listen to check whether the message has been delivered correctly. When messages are sent, neighbourhood nodes can determine if the notice is updated before the broadcast by comparing it with the message stored in your buffer. This requires nodes to cache neighbouring messages for at least one TDMA framework. Passive recognition involves the following:

- Dumped data packets are not re-transmitted.
- The data's contents have been fraudulently altered.
- Spoofing of unique addresses has occurred.

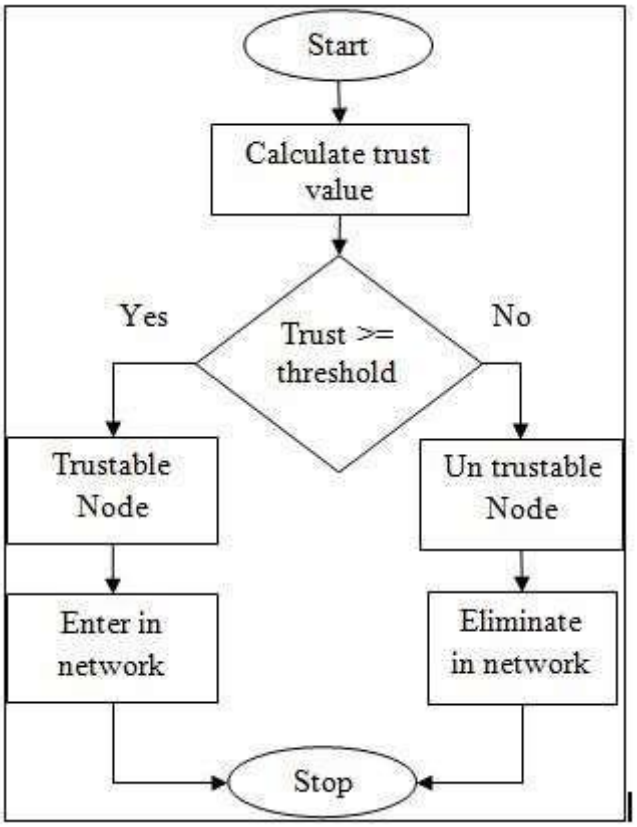


Figure 3.1 Flow of trust model

The flow of the trust model is shown in Figure 3.1. The threshold is initially set to a standard value. If the value exceeds a preset threshold, the node flag shall be set to 1. Otherwise, it

shall be set to 0. Otherwise, the flag of one node from the network is removed. TCSRS is compared with the Trusted-AODV (T-AODV) approach presently available.

3.3 SIMULATION ANALYSIS:

The TCSRS scheme's performance is evaluated using Network Simulator2 (NS2). The NS2 programming language is an open-source project built in C++ and Object-oriented Tool Command Language (OTCL).

Table 3.1 Simulation Parameters of TCSRS

Parameter	Value
Type of Channel	Wireless Channel
Simulation Time	100 s
# Nodes	50, 70
MAC Type	802.11
Traffic Model	CBR
Simulation Area	700×700
Transmission Range	250m
Radio Propagation Model	TwoRayGround
Type of Network Interface	WirelessPhy
Mobility Model	Random Way Point
Antenna Model	Omni Antenna

NS2 is a discreet event-based network protocol emulator. The nodes must be configured with NS2 node-config as mobile nodes. The two-ray soil model is used for spreading radio waves. There are nodes in the simulation environment. Table 3.1 lists the settings used to simulate the TCSRS system and installed in the simulated region of 700700, TCSRS simulation with 50 and 70 nodes. The nodes are communicated through the User Datagram Protocol (UDP). The nodes are moved randomly within the simulation range using the mobility model Random waypoint. Every node's omnidirectional antenna receives signals from every direction. Traffic is controlled using the Constant Bit Rate model (CBR).

The performance of the TCSRS scheme is measured using the Packet Delivery (PDR), Packet Loss Rate (PLR), output, average delay and residual energy properties.

3.3.1 Case 1: N = 50 nodes

The TCSRS system is first simulated using a 50-node scenario.

3.3.1.1 Packet Delivery Rate

The PDR is the ratio of the number of data packets supplied by the source node to the number of packages delivered to all destinations. Equation 3.1 is used to calculate PDR.

$$PDR = \frac{\sum_0^n Packets\ Received}{Time} \qquad (3.1)$$

WHERE N= NUMBER OF NODES

T-AODV and TCSRS PDR values for 50 nodes are shown in Table 3.2. In Figure 3.2, the PDRs for T-AODV and TCSRS are plotted. It demonstrates that the planned TCSRS scheme has a 21.27 percent higher PDR than the existing T-AODV scheme.

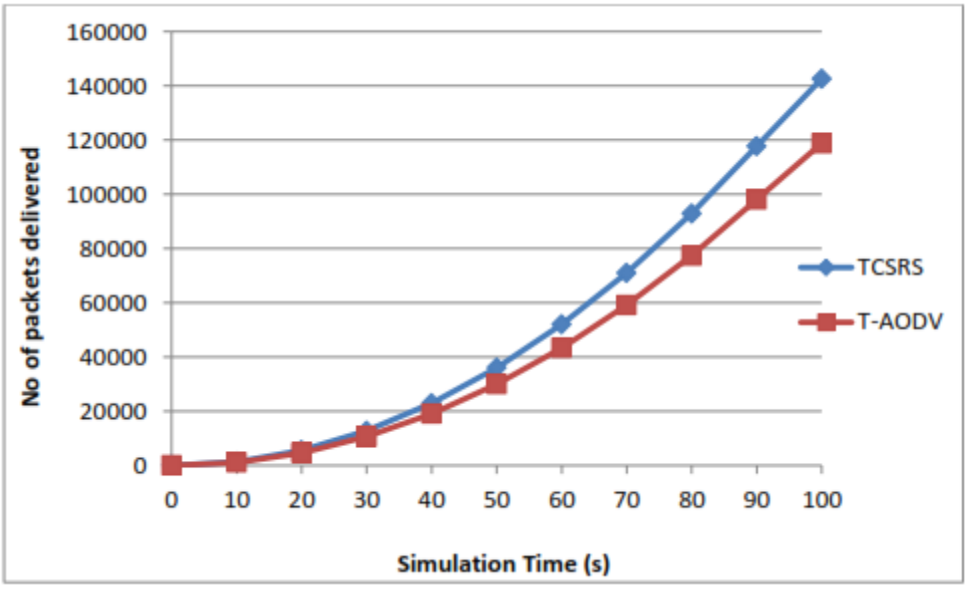


Figure 3.2 Packet Delivery Rate of T-AODV and TCSRS for 50 nodes

3.3.1.2 Packet Loss Rate:

The PLR is defined as the difference of packets received per unit time in the network, in Equation 3.2, where n is the number of nodes.

$$PLR = \frac{\sum_0^n Sent\ Pkts - Rcvd\ Pkts}{Time} \qquad (3.2)$$

Table 3.2 PDR values of T-AODV and TCSRS for 50 Nodes

Simulation Time (s)	PDR of T-AODV	PDR of TCSRS
0	0	0
10	1084	1310
20	4636	5573
30	10639	12776
40	19091	22919
50	29994	36002
60	43346	52025
70	59149	70988
80	77401	92891
90	98104	117734
100	118831	142606

Table 3.3 PLR values of T-AODV and TCSRS for 50 nodes

Simulation Time (s)	PLR of T-AODV	PLR of TCSRS
0	0	0
10	88	61
20	186	130
30	284	198
40	382	267
50	480	336
60	578	404
70	676	473
80	774	541
90	872	610
100	960	672

The PLR values resulting from the T-AODV and TCSRS simulation studies are provided in Table 3.3. In Figure 3.3, the T-AODV PLR is 30 percent higher than the TCSRS PLR.

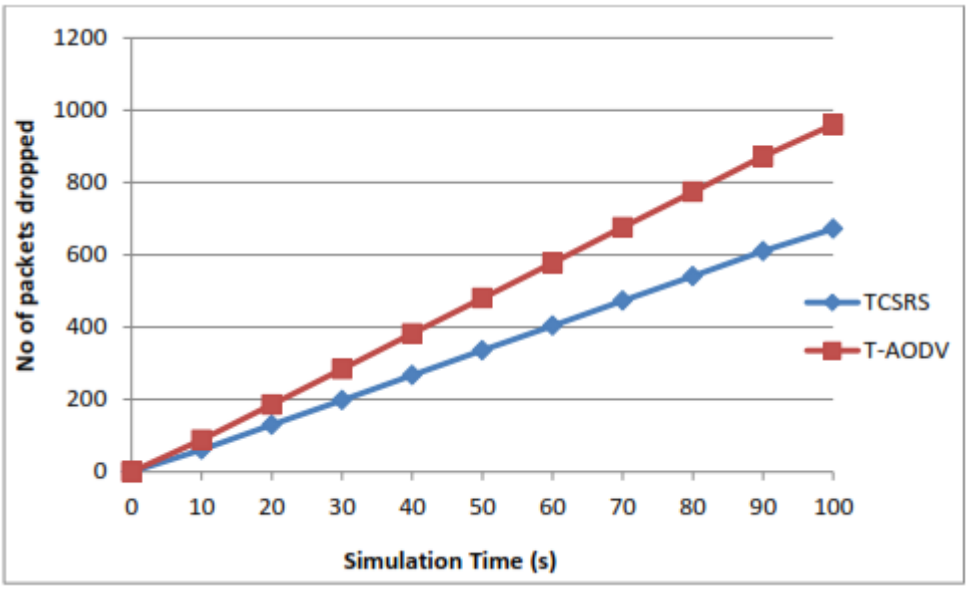


Figure 3.3 Packet Loss Rate of T-AODV and TCSRS for 50 nodes

3.3.1.3 Throughput:

The term "throughput" refers to the total number of packets delivered successfully through a network for every 1000 packets sent. Equation 3.3 is used to calculate throughput.

$$Throughput = \frac{\sum_{0}^{n} Packets\ Received(n) * Packet\ size}{1000} \qquad (4.5)$$

Where n = number of nodes

Table 3.4 represent the throughput values obtained during the simulation study for the T-AODV and TCSRS mechanisms. As illustrated in Figure 3.4, the number of packets successfully received for every 1000 packets using TCSRS is more excellent than 16.67 per cent when compared to the T-AODV method.

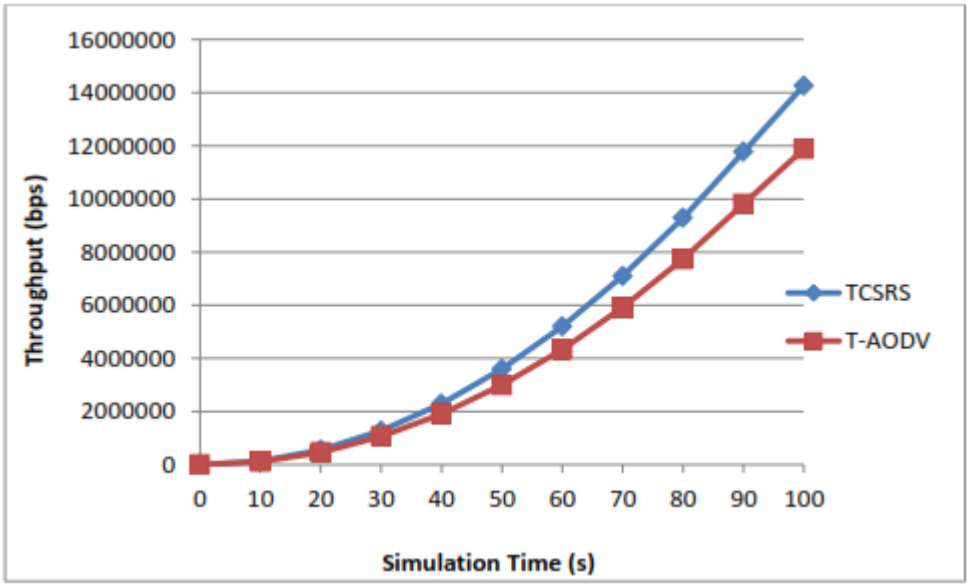


Figure 3.4 Throughput of T-AODV and TCSRS for 50 nodes

Table 3.4 Throughput values of T-AODV and TCSRS for 50 nodes

Simulation Time (s)	Throughput of T-AODV (bps)	Throughput of TCSRS (bps)
0	0	0
10	108437	131050
20	463687	557350
30	1063937	1277650
40	1909187	2291950
50	2999437	3600250
60	4334687	5202550
70	5914937	7098850
80	7740187	9289150
90	9810437	11773450
100	11883137	14260690

3.3.1.4 Average Delay:

The average period between the packets currently received and the packets previously received is defined. For calculating it, Equation 3.4 is utilised.

$$Avg\ Delay = \frac{\sum_0^n (Packet\ \text{Re}ceived\ Time - Packet\ Sent\ Time)}{n} \quad (3.4)$$

Table 3.5 shows the average time spent on T-AODV and TCSRS simulation experiments for 50 nodes. Figure 3.5 shows a 28 percent reduction in the node delay in the TCSRS system compared to the T-AODV scheme.

Table 3.5 Average Delay values of T-AODV and TCSRS for 50 nodes

Simulation Time (s)	Delay of T-AODV (ms)	Delay of TCSRS (ms)
0	0	0
10	0.263971	0.184654
20	1.022732	0.715626
30	2.271494	1.589586
40	4.010256	2.806546
50	6.239015	4.366508
60	8.957778	6.269468
70	12.16654	8.51543
80	15.8653	11.10439
90	20.05406	14.03635
100	24.2429	16.96838

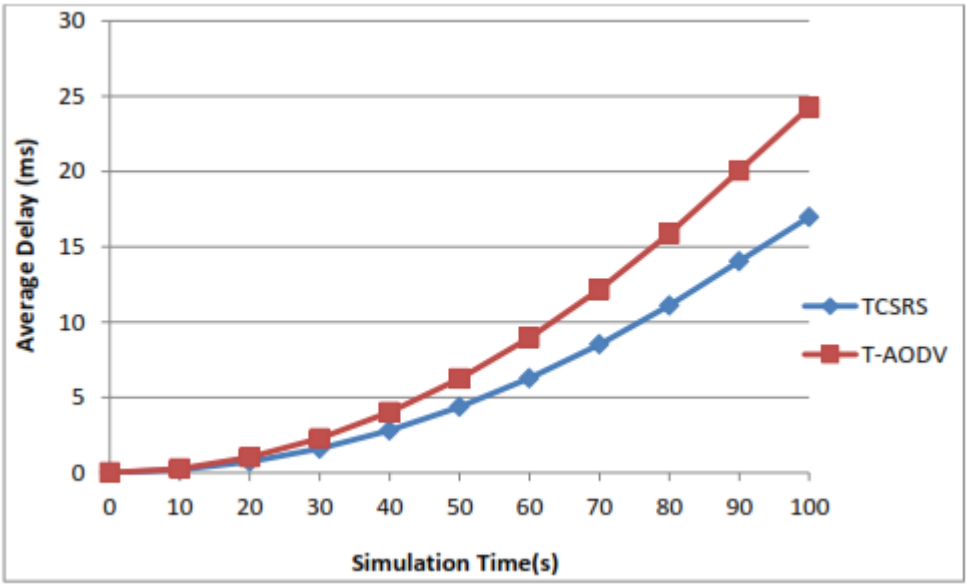


Figure 3.5 Average Delay of T-AODV and TCSRS for 50 nodes

3.3.1.5 Residual Energy:

RE indicates the amount of energy in the node at the moment. The RE is an electricity consumption unit that shows the rate of operation of the network.

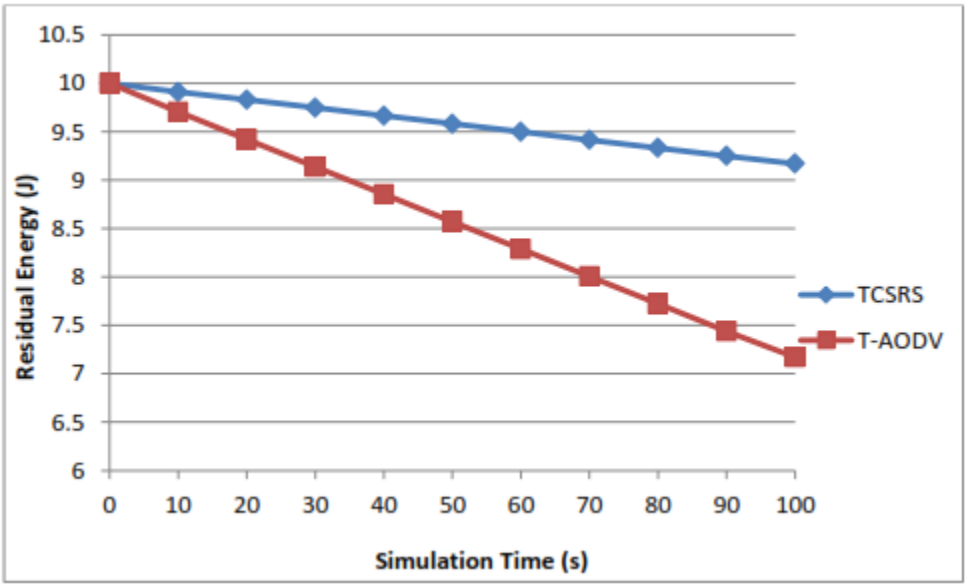


Figure 3.6 Residual Energy of T-AODV and TCSRS for 50 nodes

Table 3.6 shows the RE values acquired during the simulation analysis. According to Figure 3.6, the proposed TCSRS scheme has a higher RE than the current T-AODV scheme. TCSRS routing system saves around 15.4% of the energy per node.

Table 3.6 RE values of T-AODV and TCSRS for 50 nodes

Simulation Time (s)	RE of T-AODV (J)	RE of TCSRS (J)
0	10	10
10	9.70285	9.9087
20	9.41985	9.82985
30	9.13685	9.74685
40	8.85385	9.66385
50	8.57085	9.58085
60	8.28785	9.49785
70	8.00485	9.41485
80	7.72185	9.33185
90	7.43885	9.24885
100	7.17	9.17

3.3.2 Case 2: N = 70 nodes:

N is increased to 70 to explore how performance changes as the number of nodes rise. The following diagrams exhibit the same parameters as 50 nodes:

3.3.2.1 Packet Delivery Rate:

The values are derived using Equation 3.1 during T-AODV and TCSRS protocol simulations with the PDR of 50 nodes. These statistics are shown in Table 3.7, which is also shown Fig. 3.7

Table 3.7 PLR values of T-AODV and TCSRS for 70 nodes

Simulation Time (s)	PDR of T-AODV	PDR of TCSRS
0	0	0
10	191	5
20	1778	1000
30	6658	6153
40	14320	16728
50	22500	32181
60	32573	51872
70	44949	76174
80	59580	105308
90	76643	140325
100	94148	176918

This shows that TCSRS has a PDR 46.78% higher than the T-AODV mechanism. The number of nodes increases the PDR values, which shows the efficiency of TCSRS.

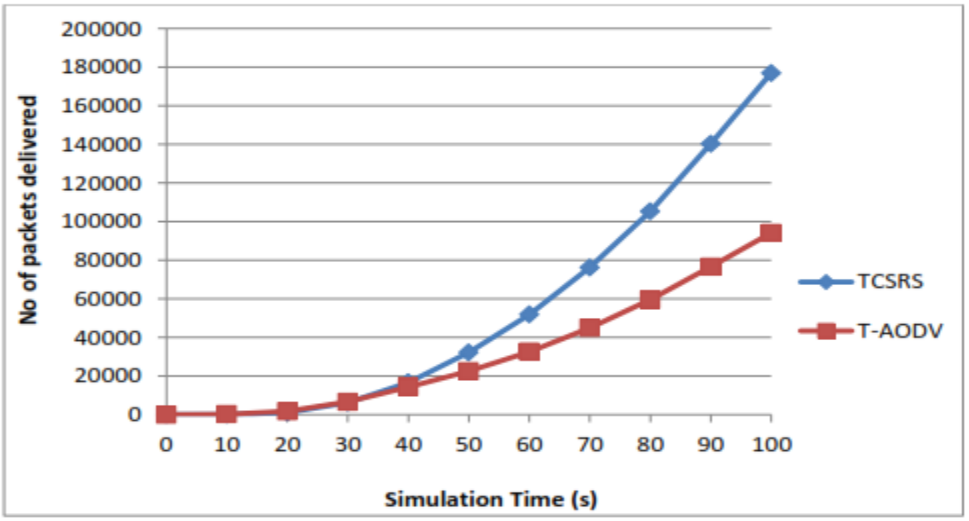


Figure 3.7 Packet Delivery Rate of T-AODV and TCSRS for 70 nodes

3.3.2.2 Packet Loss Rate:

The PLR is likewise estimated similarly to the situation of 50 nodes using equation 3.2 for 70 nodes. Table 3.8 shows the 70 nodes PLR of T-AODV and TCSRS.

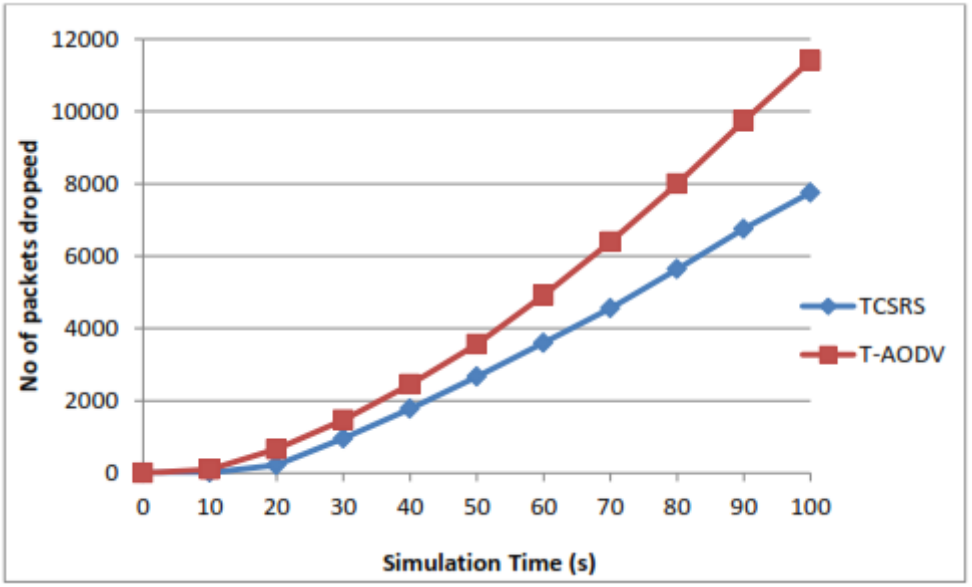


Figure 3.8 Packet Loss Rate of T-AODV and TCSRS for 70 nodes

T-PLR AODV is 32.03% higher than the mechanism of the TCSRS. The T-AODV and TCSRS PLR for 70 nodes are illustrated in Figure 3.8.

Table 3.8 PLR values of T-AODV and TCSRS for 70 nodes

Simulation Time (s)	PLR of T-AODV	PLR of TCSRS
0	0	0
10	98	11
20	665	221
30	1465	958
40	2450	1777
50	3560	2667
60	4914	3602
70	6393	4557
80	8001	5641
90	9739	6754
100	11411	7756

3.3.2.3 Throughput:

The mechanisms T-AODV and TCSRS are both measured by the use of equation 3.3. Table 3.9 shows data in a 70-node situation for both of these devices.

The current and proposed mechanisms are shown in Figure 3.9 to illustrate the change graphically. TCSRS improves by 44.4% compared to T-AODV in a setting of 70 nodes.

Table 3.9 Throughput values of T-AODV and TCSRS for 70 nodes

Simulation Time (s)	Throughput of T-AODV (bps)	Throughput of TCSRS (bps)
0	0	0
10	19107	594
20	177804	100088
30	665874	615383
40	1432035	1672852
50	2250072	3218143
60	3257397	5187253
70	4494996	7617455
80	5958017	10530877
90	7664381	14032507
100	9414899	17691844

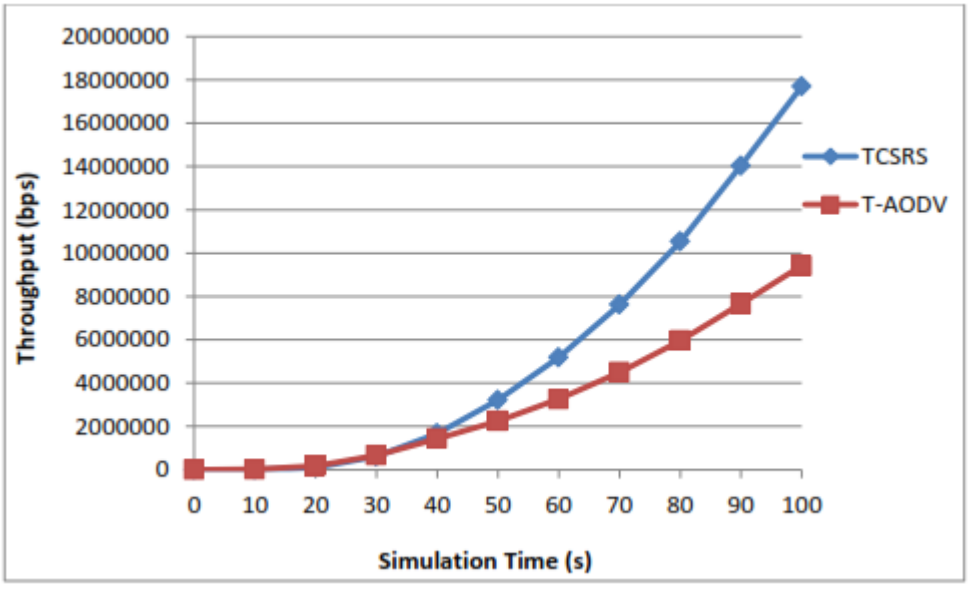


Figure 3.9 Throughput of T-AODV and TCSRS for 70 nodes

3.3.2.4 Average Delay:

The average delay is calculated as the difference between the time a packet is sent and received for all nodes, represented in equation 3.4.

Table 3.10 Average Delay values of T-AODV and TCSRS for 70 nodes

Simulation Time (s)	Delay of T-AODV (ms)	Delay of TCSRS (ms)
0	0	0
10	0.201731	0.059223
20	0.964428	0.590174
30	2.225964	1.4724
40	3.923626	2.701847
50	5.884543	4.277942
60	8.630785	6.197664
70	11.86946	8.466482
80	15.60541	11.08189
90	19.83655	14.04379
100	24.06763	17.00577

The acquired numbers are the average network delay values for one node. Table 3.10 and Figure 3.10 demonstrate an average delay difference for T-AODV and TCSRS techniques in 70 node MANET. The T-AODV, as can be seen, is 32% longer than the TCSRS. The short latency of the TCSRS mechanism makes it more usable than the previous basic protocol.

3.3.2.5 Residual Energy

The amount of energy remaining in a node at any time is called residual energy. A residual energy measurement shows how quickly energy is wasted through network processes. Table 3.11 shows the residual energy values acquired by the simulation analysis.

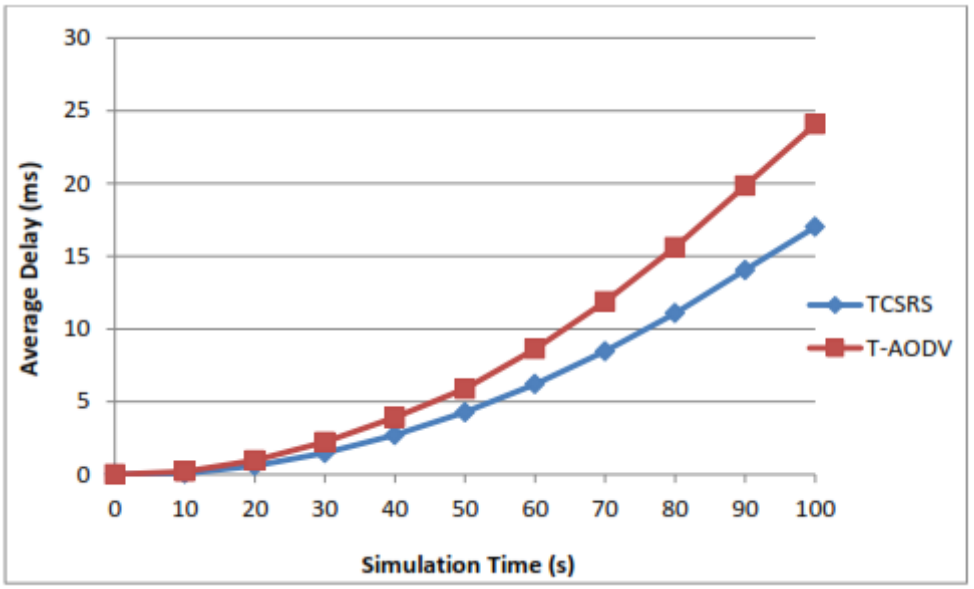


Figure 3.10 Average Delay of T-AODV and TCSRS for 70 node

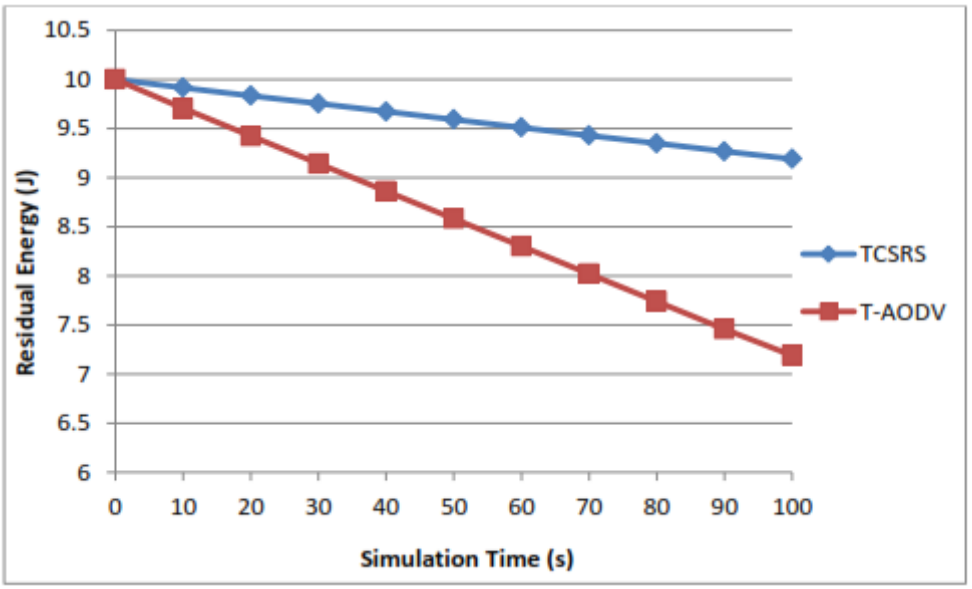


Figure 3.11 Residual Energy of T-AODV and TCSRS for 70 nodes

Figure 3.11 shows that the proposed TCSRS scheme has a lower residual energy content than the current T-AODV system. By using the TCSRS protocol for routing, around 21.67% of energy per node is saved.

Table 3.11 RE values of T-AODV and TCSRS for 70 nodes

Simulation Time (s)	RE of T-AODV (J)	RE of TCSRS (J)
0	10	10
10	9.70495	9.91495
20	9.42395	9.83395
30	9.14295	9.75295
40	8.86195	9.67195
50	8.58095	9.59095
60	8.29995	9.50995
70	8.01895	9.42895
80	7.73795	9.34795
90	7.45695	9.26695
100	7.19	9.19

3.4 SUMMARY:

The TCSRS approach was simulated and examined using the network simulator, and the findings demonstrated that it is more efficient than T-AODV. The suggested TCSRS mechanism increases total packet delivery by 33.72 percent, decreases packet loss by 31.01 percent, decreases average delay by 29.67 percent, increases throughput by 31.72 percent, and saves residual energy by 18.78 percent. As a result, the TCSRS method is used by the clustering topology in the WSN, which boosts the communication network's efficiency.

CHAPTER 4

WIRELESS SENSOR NETWORK INTEGRATION DOMINANT CLUSTER SELECTION

Securing data transfer is critical for WSNs. WSNs can benefit from clustering, which is an effective and practical technique to improve network performance. Since there are so many nodes in WSNs, it is easy for an adversary to infiltrate and breach the sensor nodes, allowing them to obtain the sensor nodes' private keys. To lengthen the lifespan of the network, we can use clustering. while arranging the sensors into clusters, the authors neglected to account for security. Credence is a big deal in this section of the research. One big advantage of this approach is that malevolent or selfish nodes are excluded from emerging as a dominant cluster in a cluster group. The overall performance of the network is improved with the addition of QoS.

4.1 RESEARCH FOR THE PROPOSED DCSC

A wireless sensor network (WSN) is a network system made up of spatially distributed devices that utilise wireless sensor nodes to monitor physical or environmental factors such as sound, temperature, and motion. Each node in a WSN is capable of sensing its environment, processing the data locally, and transmitting it to one or more collecting points. A WSN is used to collectively perceive, gather, and process information about recognised objects and deliver it to a monitor. Due to the fact that sensors are battery-powered and deployed in an unsupervised environment, WSNs face far more issues than traditional networks. As a result, energy efficiency and security are becoming prominent study topics.

When considering the entire network design challenge in WSN, several critical factors must be considered, including the node's lifetime, the sensor node's reduced size, its hardware complexity, and ultra-low energy consumption. Among them, maximising longevity should be the primary design target, as a sensor node can only be outfitted with a certain amount of energy. Sensor nodes persist until their energy is depleted. In some application circumstances, it is impossible to replace the energy supplies, and so sensor node lifetime is inextricably linked to battery life.

The network's frequent topology changes as a result of sensor failures make it highly unstable. As a result, a true dominant cluster selection procedure is necessary that can extend the system's life and optimise data transfer. There are few established protocols for selecting CHs in WSNs. Several recent works employ a random selection of CHs. As a result, the current round may select the same node as the prior round. The cluster may or may not be equally divided.

There are several more efforts in the area of CH selection that do not take load balancing amongst CHs into account. As a result, it increases the pressure on the CHs for data

regeneration and processing. Due to this unbalanced balancing, a few heads perish soon due to increased energy use. Existing efforts, which rely on direct communication between sensor nodes, use more energy to relay data to the base station, and so the nodes die quickly. As a result, research on efficient CH selection becomes critical to extending the life of the system and optimising data communication in WSNs.

4.2 DETAILS ABOUT THE PROPOSED DCSC

Clustering techniques for WSN did not take security into account while combining sensors into clusters. The Trust-based Cluster Head Election (TCHE) in WSN was susceptible to dominating cluster selection. There is a chance that the malicious or selfish node will be chosen as the dominant cluster.

As a result of the CH's data collection role, it may have an effect on the entire network. Figure 4.1 illustrates the clustering operation in WSNs.

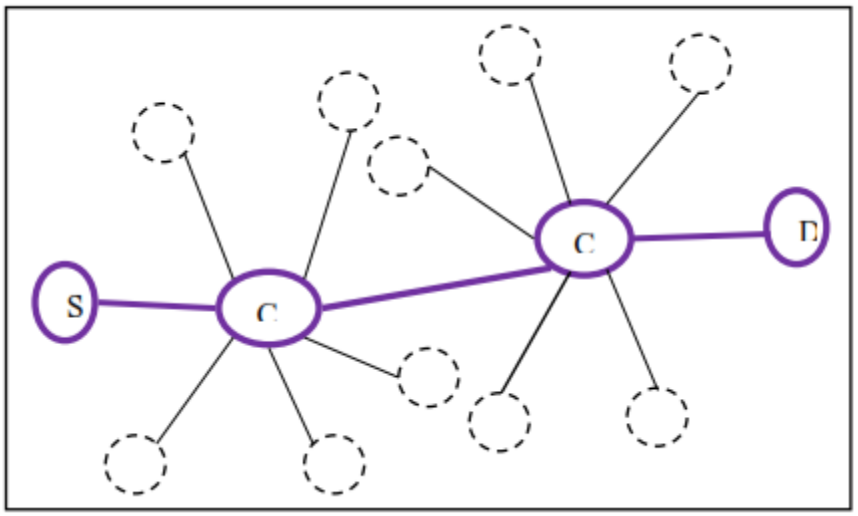


Figure 4.1 Cluster operation in WSN

To address this issue, a parameter called credibility is included during the dominant cluster selection process. The credibility value is determined by aggregating data from the node's neighbours. The credibility function is used to assess the nodes in the network for malicious behaviour. The node with the highest credibility value and the greatest energy is chosen as the dominating cluster. The primary advantage of this strategy is that it prevents malevolent or self-centered nodes from establishing a dominant cluster. Because the credibility function includes QoS as a parameter, the network's overall performance is improved.

The credence value of each sensor node in the network is derived using this approach. The credibility value will be dynamically adjusted. The credibility value of each node is determined by its neighbours. The ratio of the value collected from a neighbour sensor is used to determine the node's credibility value. For the duration of the specified period, the setup server shall update the credibility value based on the vote of its neighbours.

4.2.1 RECOMMENDATION FOR A NEIGHBOR NODE

The primary criterion for determining the credibility value is obtaining values from neighbouring nodes. The values assigned to neighbouring nodes indicate that the nodes are chosen as the dominant cluster in each cluster group. Additionally, the neighbourhood value is computed based on the interactions between the dominating cluster node and its group nodes. Equation 4.1 is used to calculate the neighbour node recommendation value.

$$Node_{rmdn} = \left(\frac{CM_{elect}}{CM_{total}}\right) * 100 \qquad (4.1)$$

Where CM_{elect}= Elected Cluster Number

CM_{total}=Total Cluster Number

4.2.2 COMMUNICATION BETWEEN NODES:

The proposed work calculates the node communication C_{ij}. The node communication ratio is determined by the number of successful and unsuccessful interaction messages sent throughout the communication network. Each node keeps track of its neighbours' interactive and non-interactive behaviours. If the count value exceeds the system threshold (say 70%), the node is considered completely interactive. Otherwise, it is treated as an inactive node. The communication between two nodes I and j, indicated by C_{ij}, is calculated for each node in the network using the equation 4.2.

$$C_{i,j} = \left[\left(\frac{X_{i,j}}{X_{(i,j)} + Y_{i,j}}\right)\left(\frac{1}{\sqrt{Y_{i,j}}}\right)\right] * 100 \qquad (4.2)$$

Where $X_{i,j}$ = total number of successful interactions of i with j.

$Y_{i,j}$ = total number of unsuccessful interactions of i with j.

4.2.3 Node QOS

The Quality of Service (QoS) is a critical measure for determining the network's quality. The PDR, PLR, and delay time parameters are utilised to calculate the QoS value. Node N's PDR indicates the number of packets transmitted to all of its neighbours per unit time t. PLR denotes the packet loss ratio over time t. The term "delay" refers to the time interval between the current and previous packets received.

4.2.4 RESIDUAL ENERGY AT THE NODE

The network's nodes are all homogenous and energy limited. Sensors randomly chose to be local CHs at any given time. These CH nodes transmit their status to the network's other sensor nodes. Each sensor node chooses which cluster to join by selecting the CH that requires the least communication energy.

A credence management method can be used to any WSN composed of heterogeneous WSNs with widely varied initial energy levels and varying degrees of malice or selfish behaviour. The credential management protocol is implemented in a clustered WSN in which source nodes can dynamically adapt their behaviour to their operational status and environmental conditions. When a source node is low on energy or has a large number of unselfish neighbour nodes nearby, it is more likely to become selfish. When a source node is surrounded by compromised neighbours, it is more likely to become compromised. Energy is consumed more efficiently by a dominant cluster than by source nodes. Once the dominant cluster has been hacked, it may consume additional energy to conduct attacks. On the other side, a selfish node consumes less energy than an unselfish node since it demonstrates its selfish behaviour by suspending sensing operations and arbitrarily dropping messages.

4.3 SIMULATION ANALYSIS

NS2 is used to examine the DCSC scheme's performance. The NS2 programming language is an open source project built in C++ and OTCL. NS2 is a discrete event time-based simulator that is mostly used to mimic network protocols. The simulation environment is spread with nodes. The nodes must be configured as mobile nodes using the NS2 command node-config. Table 4.1 summarises the parameters used to simulate the DCSC scheme. The suggested system is simulated using 50 and 70 nodes distributed in the simulation region 700mX700m. Using the mobility model Random waypoint, the nodes are moved randomly within the simulation area. The nodes communicate with one another via the UDP protocol. The CBR traffic model is used to manage the traffic. Radio waves are propagated using the two-ray ground model. The Omnidirectional antenna on each node receives signals from all directions. The parameters PDR, PLR, throughput, average latency, and residual energy are used to evaluate the DCSC scheme's performance.

Table 4.1 Simulation Parameters of DCSC

Parameter	Value
Type of Channel	Wireless Channel
Simulation Time	100 s
# Nodes	50, 70
MAC Type	802.11
Traffic Model	CBR
Simulation Area	700×700
Transmission Range	250m
Radio Propagation Model	TwoRayGround
Type of Network Interface	WirelessPhy
Mobility Model	Random Way Point
Antenna Model	Omni Antenna

4.3.1 CASE 1: N = 50 NODES

The DCSC method is initially simulated using a 50-node scenario.

4.3.1.1 Packet Delivery Rate:

The PDR is the ratio of the number of data packets supplied by the source node to the number of packets delivered to all destinations. PDR is calculated using Equation 4.3.

$$PDR = \frac{\sum_0^n Packets\ Received}{Time} \tag{4.3}$$

TCHE and DCSC PDR values for 50 nodes are shown in Table 4.2. In Figure 4.2, the PDRs of TCHE and DCSC are plotted. It demonstrates that the planned DCSC scheme has a 54.95 percent higher PDR than the existing TCHE method.

Table 4.2 PDR values of TCHE and DCSC for 50 nodes

Simulation Time (s)	PDR of TCHE	PDR of DCSC
0	0	0
10	4586	9153
20	14273	28136
30	24482	49129
40	36935	81068
50	48356	106604
60	57525	126735
70	65065	143670
80	71547	158489
90	77016	171004
100	81719	181426

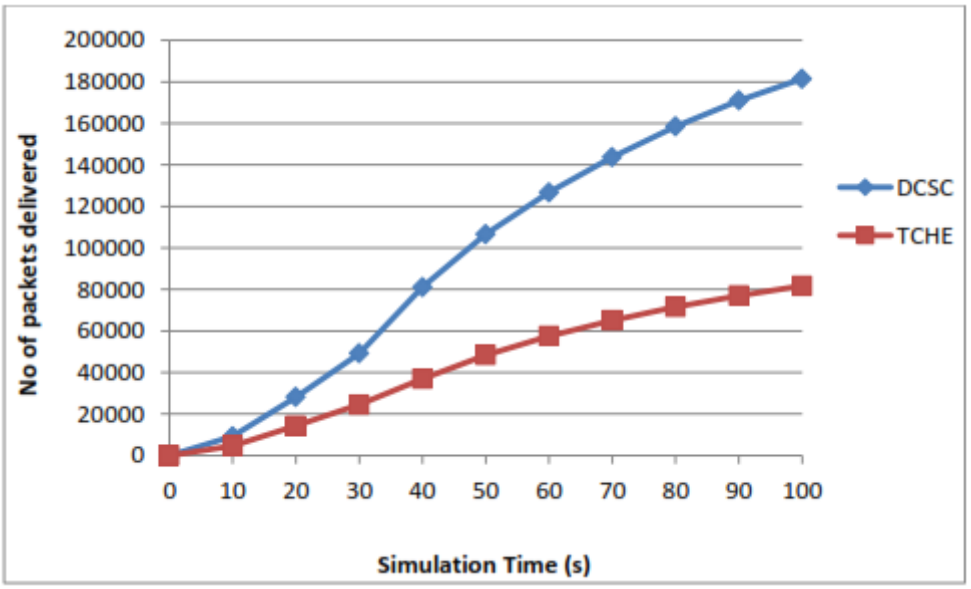


Figure 4.2 Packet Delivery Rate of TCHE and DCSC for 50 nodes

4.3.1.2 Packet Loss Rate:

As specified in Equation 4.4, the PLR is defined as the difference between the number of packets transmitted and received in the network per unit time.

$$PLR = \frac{\sum_{0}^{n} Sent\ Pkts - Rcvd\ Pkts}{Time} \qquad (4.4)$$

Table 4.3 PLR values of TCHE and DCSC for 50 nodes

Simulation Time (s)	PLR of TCHE	PLR of DCSC
0	0	0
10	0	0
20	0	0
30	0	11
40	596	548
50	1472	1121
60	2394	1694
70	3316	2267
80	4238	2840
90	5160	3412
100	6036	3957

The PLR values derived from the simulation analysis of TCHE and DCSC are shown in Table 4.3. According to Figure 4.3, the PLR of TCHE is 34.44 percent more than that of DCSC.

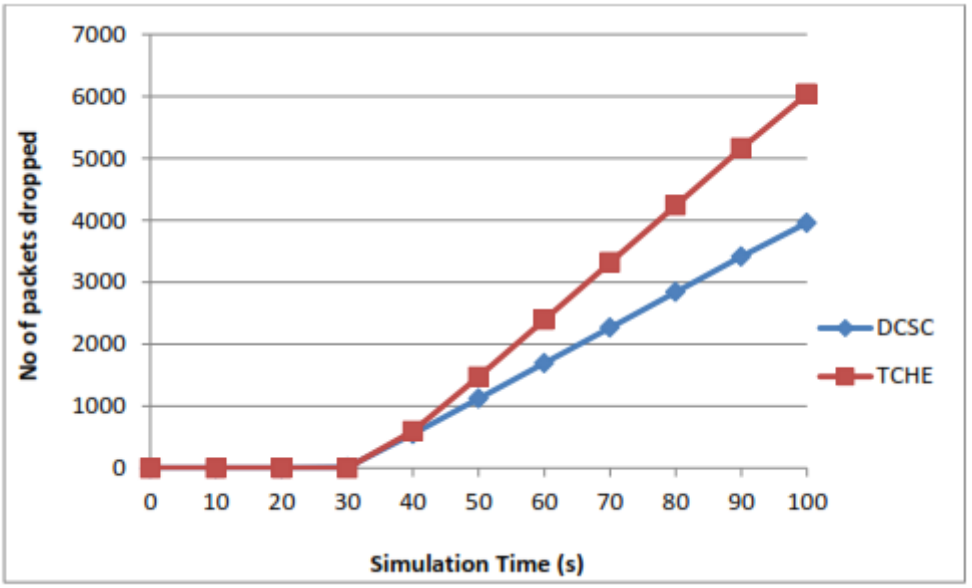


Figure 4.3 Packet Loss Rate of TCHE and DCSC for 50 nodes

4.3.1.3 THROUGHPUT:

The term "throughput" refers to the total number of packets delivered successfully through a network for every 1000 packets sent. Equation 4.5 is used to determine the throughput.

$$Throughput = \frac{\sum_{0}^{n} Packets\ Received(n) * Packet\ size}{1000} \quad (4.5)$$

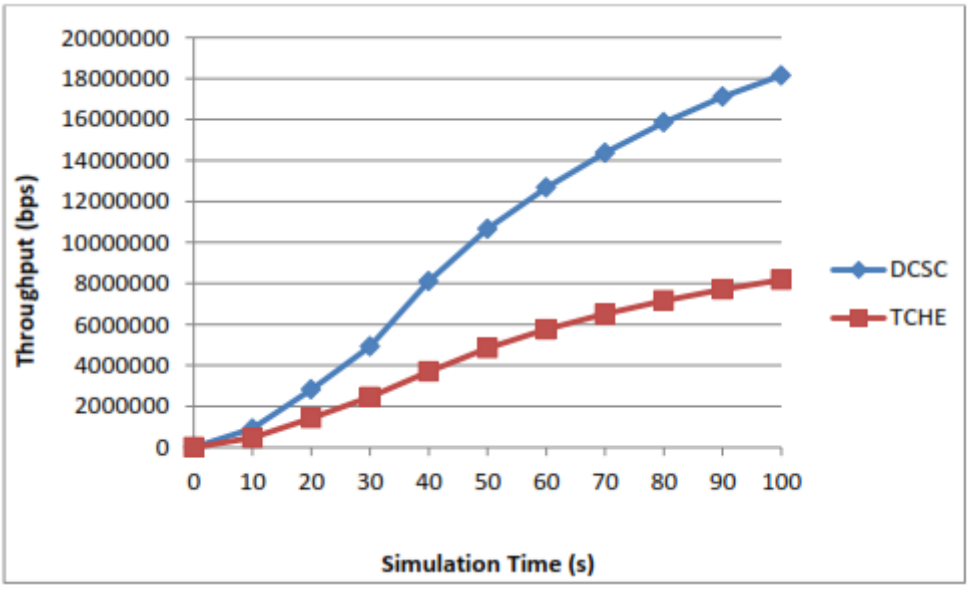


Figure 4.4 Throughput of TCHE and DCSC for 50 nodes

Table 4.4 Throughput values of TCHE and DCSC for 50 nodes

Simulation Time (s)	Throughput of TCHE (bps)	Throughput of DCSC (bps)
0	0	0
10	458604	915389
20	1427310	2813671
30	2448293	4912950
40	3693533	8106818
50	4835663	10660414
60	5752585	12673593
70	6506550	14367055
80	7154794	15848972
90	7701661	17100419
100	8171945	18142613

The values in Table 4.4 represent the throughput values obtained during simulation analysis for the TCHE and DCSC systems. As illustrated in Figure 4.4, the DCSC mechanism

successfully receives more than 51.24 percent of packets for every 1000 packets, compared to the TCHE method.

4.3.1.4 Average Delay:

The average delay is defined as the time interval between the currently received packets and the previously received packets. It is calculated using the equation 4.6, where n denotes the number of nodes, which in this case is 50.

$$Avg\ Delay = \frac{\sum_0^n (Packet\ Received\ Time - Packet\ Sent\ Time)}{n} \quad (4.6)$$

Table 4.5 Average Delay values of TCHE and DCSC for 50 nodes

Simulation time (s)	Delay of TCHE (ms)	Delay of DCSC (ms)
0	0	0
10	0.018108	0.007969
20	0.009943	0.010739
30	0.118187	0.096358
40	1.052363	0.622673
50	2.163474	1.148989
60	3.274585	1.675305
70	4.385696	2.201621
80	5.496807	2.727937
90	6.607919	3.254252
100	7.663474	3.754252

The average delay derived from simulation studies of TCHE and DCSC mechanisms for 50 nodes is shown in Table 4.5. According to Figure 4.5, the DCSC method has a 51.01 percent lower delay per node than the TCHE design.

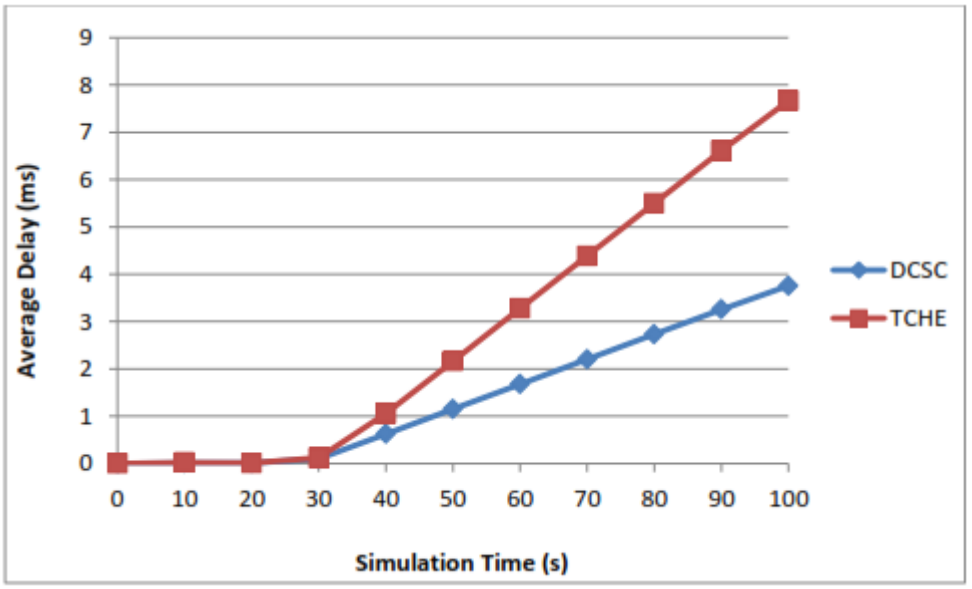
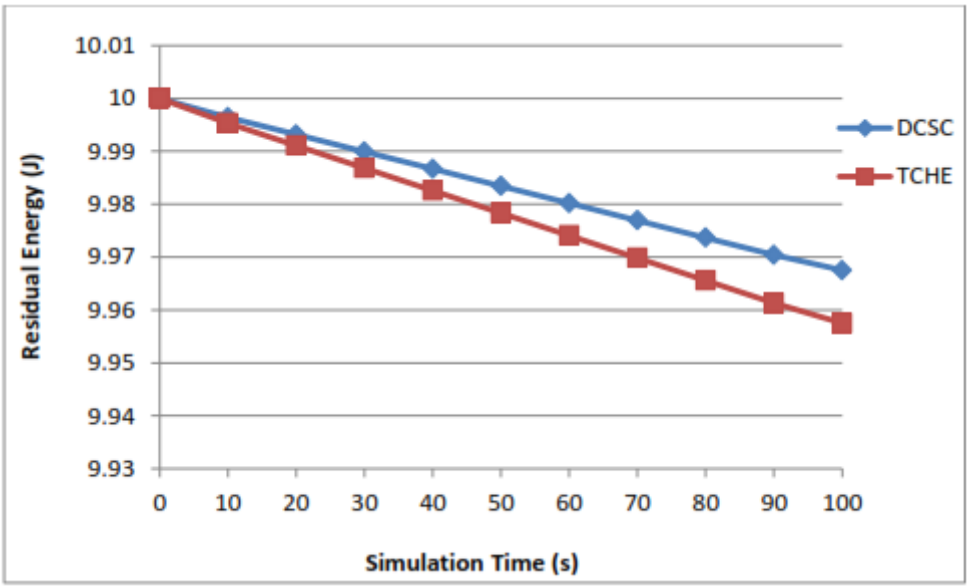


Figure 4.5 Average Delay of TCHE and DCSC for 50 nodes

4.3.1.5 RESIDUAL ENERGY:

RE denotes the amount of energy remaining in a node at the present instant of time. The RE is a unit of energy consumption that indicates the rate at which the network operates.

Figure 4.6 Residual Energy of TCHE and DCSC for 50 nodes



The RE values obtained during the simulation analysis are shown in Table 4.6. According to Figure 4.6, the proposed scheme DCSC has a higher RE than the present scheme TCHE. By employing the DCSC protocol for routing, approximately 1.0 percent of energy is saved per node.

Table 4.6 RE values of TCHE and DCSC for 50 nodes

Simulation Time (s)	RE of TCHE (J)	RE of DCSC (J)
0	10	10
10	9.995325	9.996425
20	9.991075	9.993175
30	9.986825	9.989925
40	9.982575	9.986675
50	9.978325	9.983425
60	9.974075	9.980175
70	9.969825	9.976925
80	9.965575	9.973675
90	9.961325	9.970425
100	9.9575	9.9675

4.3.2 CASE 2: N = 70 NODES:

To investigate how performance changes as the number of nodes increases, N is increased to 70. The charts below show the same parameters as those for 50 nodes:

4.3.2.1 Packet Delivery Rate:

Similar to the PDR of 50 nodes, the values are determined using equation 4.3 during TCHE and DCSC protocol simulations. Table 4.7 contains these results, which are also depicted in picture 4.7. This indicates that DCSC has a PDR of 40.48 percent more than the TCHE mechanism. The number of nodes increases the PDR values, demonstrating DCSC's efficiency.

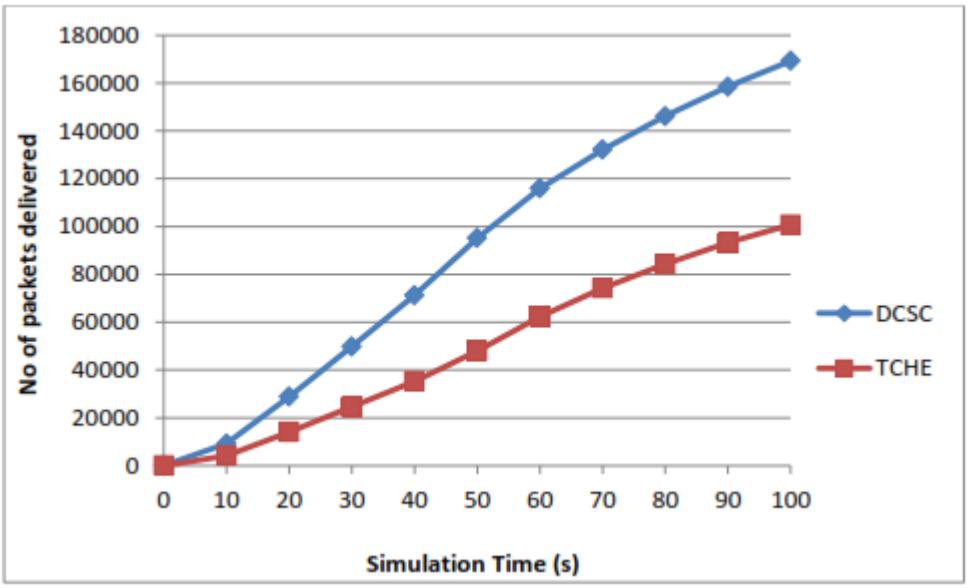


Figure 4.7 Packet Delivery Rate of TCHE and DCSC for 70 nodes

Table 4.7 PDR values of TCHE and DCSC for 70 nodes

Simulation Time (s)	PDR of TCHE	PDR of DCSC
0	0	0
10	4191	9172
20	14075	28849
30	24588	49830
40	35279	71261
50	48015	95149
60	62327	115908
70	74282	132111
80	84254	146130
90	93201	158468
100	100716	169232

4.3.2.2 Packet Loss Rate:

For 70 nodes, the PLR is likewise determined similarly to the 50 nodes situation using equation 4.4. Table 4.8 illustrates the PLR of TCHE and DCSC for 70 nodes.

TCHE has a higher PLR than the DCSC mechanism by 85.34 percent. Figure 4.8 illustrates the PLR of TCHE and DCSC for 70 nodes.

Table 4.8 PLR values of TCHE and DCSC for 70 nodes

Simulation Time (s)	PLR of TCHE	PLR of DCSC
0	0	0
10	0	0
20	0	0
30	5	0
40	5	0
50	700	175
60	2445	415
70	4195	660
80	5940	900
90	7690	1140
100	9350	1370

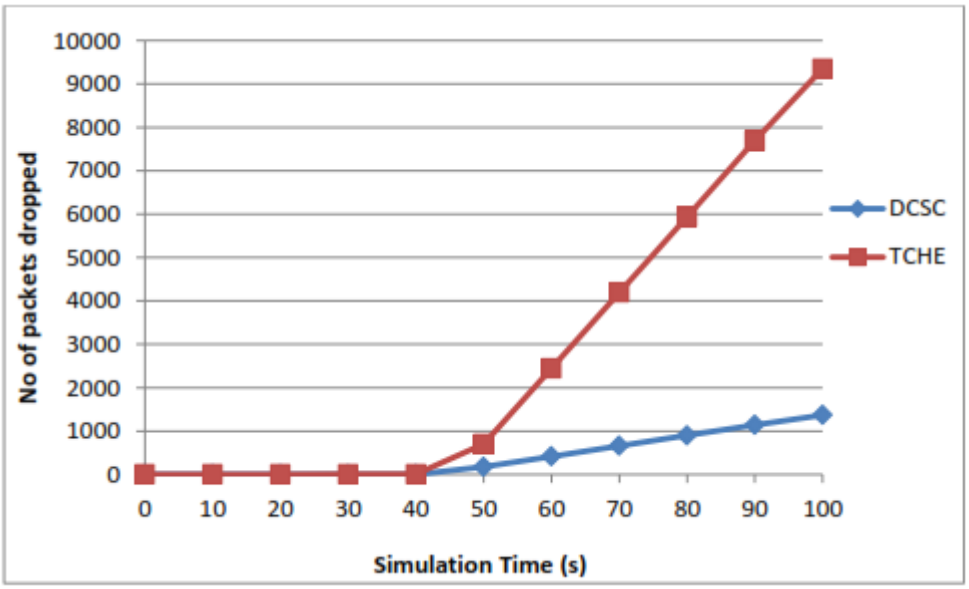


Figure 4.8 Packet Loss Rate of TCHE and DCSC for 70 nodes

4.3.2.3 Throughput:

For both the TCHE and DCSC methods, throughput is calculated using equation 4.5. Table 4.9 contains the values for both of these devices working in a 70-node scenario.

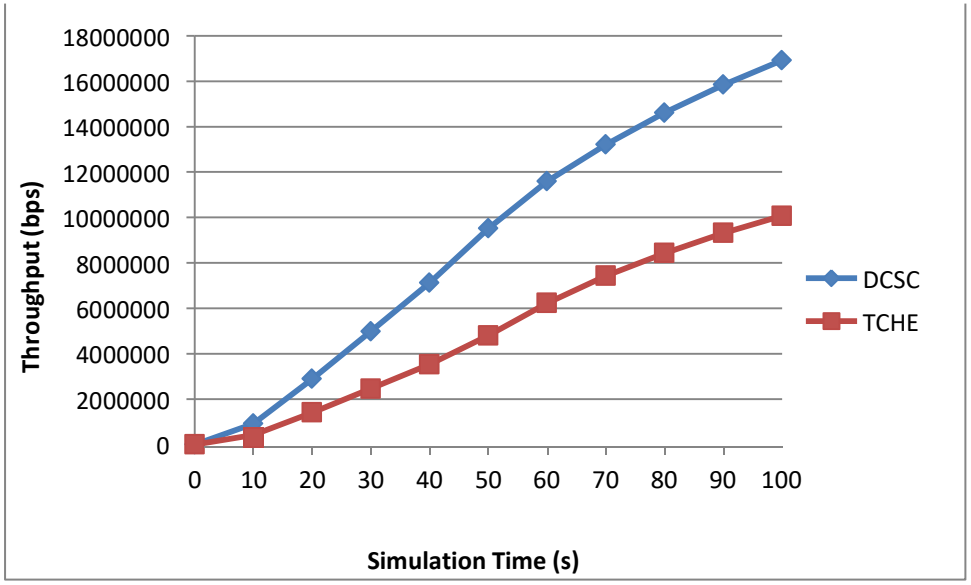


Figure 4.9 Throughput of TCHE and DCSC for 70 nodes

Figure 4.9 plots the throughput values for both the existing and proposed mechanisms to illustrate the differences visually. For a 70 node situation, there is a 40.48 percent improvement in DCSC as compared to the TCHE.

Simulation Time (s)	Throughput of TCHE (bps)	Throughput of DCSC (bps)
0	0	0
10	419126	917208
20	1407504	2884918
30	2458839	4983055
40	3527907	7126193
50	4801534	9514989
60	6232757	11590821
70	7428280	13211160
80	8425453	14613048
90	9320148	15846828
100	10071614	16923218

Table 4.9 Throughput values of TCHE and DCSC for 70 nodes

4.3.2.4 Average Delay:

The average delay is calculated as the difference between the timings required to send and receive a packet across all nodes, as shown in equation 4.6. The numbers obtained are the network's average delay values for a single node. The difference in the average delay values for TCHE and DCSC methods in a 70-node MANET is shown in table 4.10 and picture 4.10.

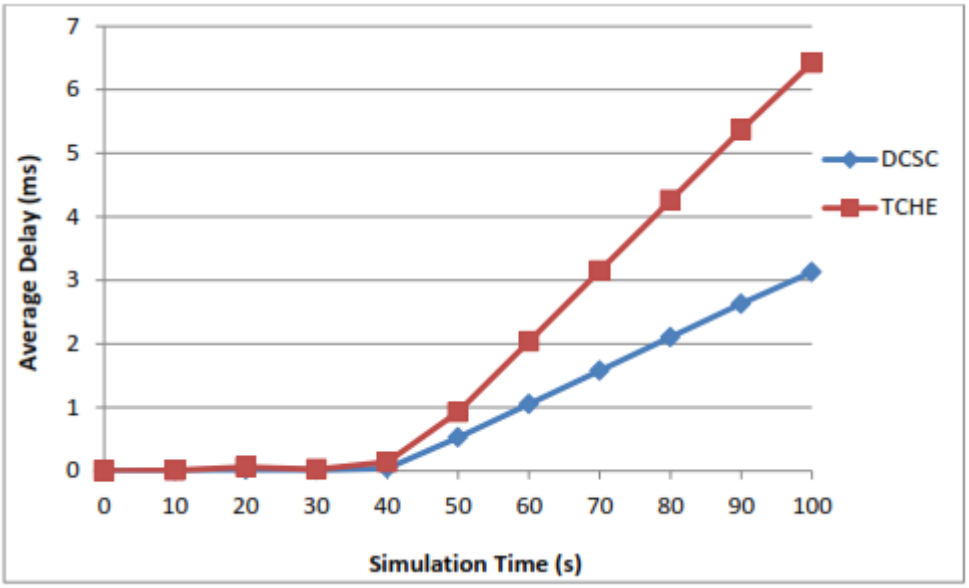


Figure 4.10 Average Delay of TCHE and DCSC for 70 nodes

Table 4.10 Average Delay values of TCHE and DCSC for 70 nodes

Simulation time (s)	Delay of TCHE (ms)	Delay of DCSC (ms)
0	0	0
10	0.007038	0.003882
20	0.059118	0.01868
30	0.024312	0.012109
40	0.139178	0.040421
50	0.925681	0.524366
60	2.036786	1.050682
70	3.147898	1.576998
80	4.259009	2.103314
90	5.37012	2.629629
100	6.425675	3.129629

As can be seen, the TCHE has a delay of 51.29 percent more than the DCSC. Due to the DCSC mechanism's low latency, it is more useable than the present baseline protocol.

4.3.2.5 Residual Energy:

The quantity of energy that remains in a node at any point in time is referred to as residual energy.

Table 4.11 RE values of TCHE and DCSC for 70 nodes

Simulation Time (s)	RE of TCHE (J)	RE of DCSC (J)
0	10	10
10	9.997525	9.998625
20	9.995275	9.997375
30	9.993025	9.996125
40	9.990775	9.994875
50	9.988525	9.993625
60	9.986275	9.992375
70	9.984025	9.991125
80	9.981775	9.989875
90	9.979525	9.988625
100	9.9775	9.9875

A residual energy measurement indicates the pace at which energy is consumed by network processes. The residual energy values acquired from the simulation analysis are shown in Table 4.11. According to Figure 4.11, the proposed method DCSC has a lower residual energy than the present scheme TCHE. By employing the DCSC protocol for routing, approximately 1.0 percent of energy is saved per node.

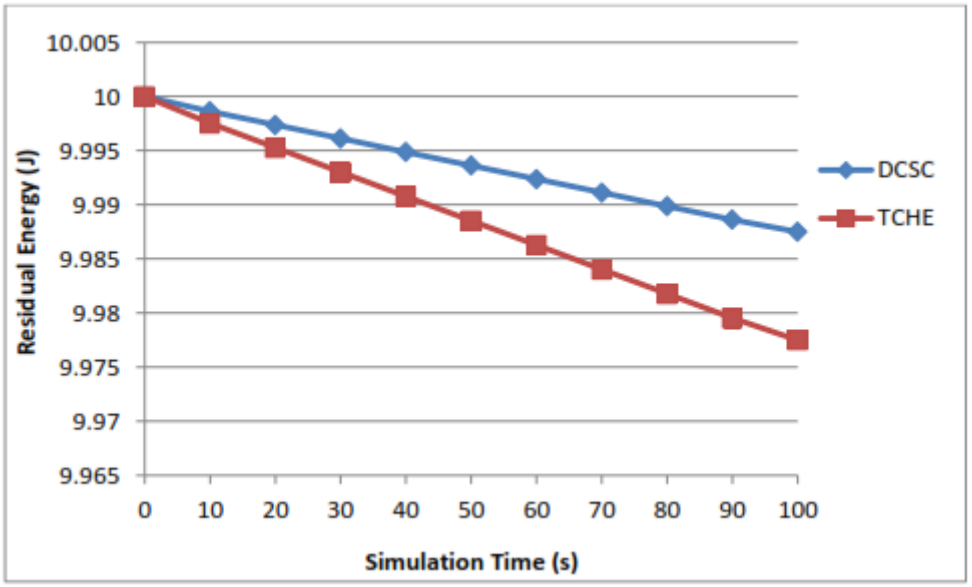


Figure 4.11 Residual Energy of TCHE and DCSC for 70 nodes

4.4 SUMMARY:

The DCSC method was simulated and studied using the network simulator, and the findings demonstrated that the DCSC mechanism is more efficient than TCHE. The suggested DCSC mechanism increases total packet delivery by 47.72 percent, decreases packet loss by 59.89 percent, decreases average latency by 51.15 percent, increases throughput by 50.38 percent, and saves residual energy by 1.0 percent. As a result, the DCSC scheme is used by the clustering topology in the WSN, which boosts the communication network's efficiency.

CHAPTER 5

CLUSTER HEAD SELECTION AND DATA CONVERGENCE IN WIRELESS SENSOR NETWORKS IN AN ENERGY-EFFICIENT MANNER

A WSN is composed of several dispersed sensor nodes. These sensor nodes are power-constrained. Recharging the sensor node's battery is considered a challenging process. To accomplish this goal, the main focus is on improving the energy efficiency of WSNs. This section proposes the Energy Efficient Cluster Head Selection and Data Convening (EECHDC) technique for WSNs. The CH is determined by the residual energy, the connection density, the node capabilities, and the node degree.

5.1 RESEARCH FOR THE PROPOSED EECHDC

WSNs are groups of mobile or stationary nodes that may communicate to transport data more quickly and independently. Due to the rapid growth of the industry, there are several uses. In addition to being used in many environmental applications, it is also utilised in the military and health sectors. The advantage of WSNs is that they can operate automatically in harsh environments, which human operators may not or may choose not to monitor. These sensors are used to construct an ad-hoc network through uncontrolled means, such as by helicopter delivery.

The mechanism through which a network is subdivided into interconnected subnetworks is known as clustering. Each cluster has a unique CH, such as identity, degree, mobility, weight, and density, which is picked based on a single parameter or a combination of metrics such as that metric. Within the substructure, the CH serves as the network's coordinator. Every CH is an ES and interacts with other CHs inside the cluster. CH must be aware of the cluster information within the network. This dataset includes a list of the cluster's nodes and each node's route to the next. The CH has a network connection with all cluster nodes and acts as the communications hub. But, it must be able to communicate with the other clusters' nodes. This can be done either by directly connecting to them or by using a gateway. The three steps involved in communication are: understand, accept, and interact. Once CH members submit data, the CH begins to process it. Once that has happened, the data is compressed and transferred to the BS or another CH. Using appropriate CH will assist in minimising energy usage and network life.

5.2 DEPICTION OF THE PROPOSED EECHDC

Most clustering methods rely on a single measure, and that is power. The following influences may come into play in cluster algorithms that use weights: mobility, degree, and node stability. The approaches above do not account for how all essential measurements are interrelated. ECSHA results are given as a combination of four elements: how many

neighbours the node has, how much residual energy remains, and how far away the node is from the cluster's centre. Only nodes near the cluster's centre can be selected. The network is affected by it. For these reasons, WSNS has designed an algorithm to choose a CH based on the variables above: Remaining Energy (Eres), Connection Density (CD), a node's capability (Cn), and degree of the node (D). The following assumptions are made in this research:

- The sensor nodes and BS are fixed in their positions.
- The connections are symmetrical.
- The nodes are scattered randomly.
- All sensor nodes are capable of sensing the surroundings and transmitting data to BS.
- The Received Signal Strength Indicator is used to calculate the distance between two nodes (RSSI).

A network with a graph of vertices (a V) and edges (an E) is shown. The diagram in Figure 5.1 displays the EECHDC process flow. To simplify things, we can describe the algorithm for CH selection as follows:

5.2.1 PREPARATION PHASE:

During the setup phase, BS broadcasts a message to the sensor nodes. When receiving the broadcast message, sensor nodes will send a reply message to their local nodes, along with their position, node ID, and the distance between them.

5.2.2 CLUSTER FORMATION PHASE

All sensor nodes will keep their receivers turned on during the CH selection phase. A CH represents every sensor node in the communication network. When selecting the CH, residual energy, connection density, node capabilities, and node degree are critical considerations.

5.2.2.1 Remaining Energy:

The quantity of energy that remains in a node at any time is referred to as remaining energy (Eres). To become a CH, a node must have a higher residual energy value than its nearby nodes. Consider Ei to be the node's initial energy. Equation 5.1 gives the power spent by the node (E(t)) after the t period.

$$E(t) = (n_{tpkts} * \alpha) + (n_{rpkts} * \beta) \quad (5.1)$$

where

n_{tpkts} = number of data packets transmitted

n_{rpkts} = number of data packets received

α, β = constants in the range (0, 1)

$$E_{res} = E_i - E(t) \quad (5.2)$$

5.2.2.2 Connection Density:

To calculate the Connection Density (CD(x)) of a node, divide the average distance between it and all of its neighbours by the inter-node length. Equation 5.3 indicates the connectivity density.

$$CD(\mathrm{x}) = \sum_{1}^{N(\mathrm{x})} [(x, y) \in E \,/\, \mathrm{y} \in N(x)] / |N(x)| \qquad (5.3)$$

where

$|N(x)|$ = number of neighbors of node x.

y= node

5.2.2.3 Node performance:

The capabilities of a node are determined by the node's capacity to transition from a sensor group to a CH. Capability significance says that a node is more likely to become a CH. The node qualifies to be a challenger node if it has more capacity than or equal to the threshold (T) percentage (1 to 100). To ensure there are enough challenges to produce high-quality CH selection, the threshold value must be established to have a significant number of challenger nodes.

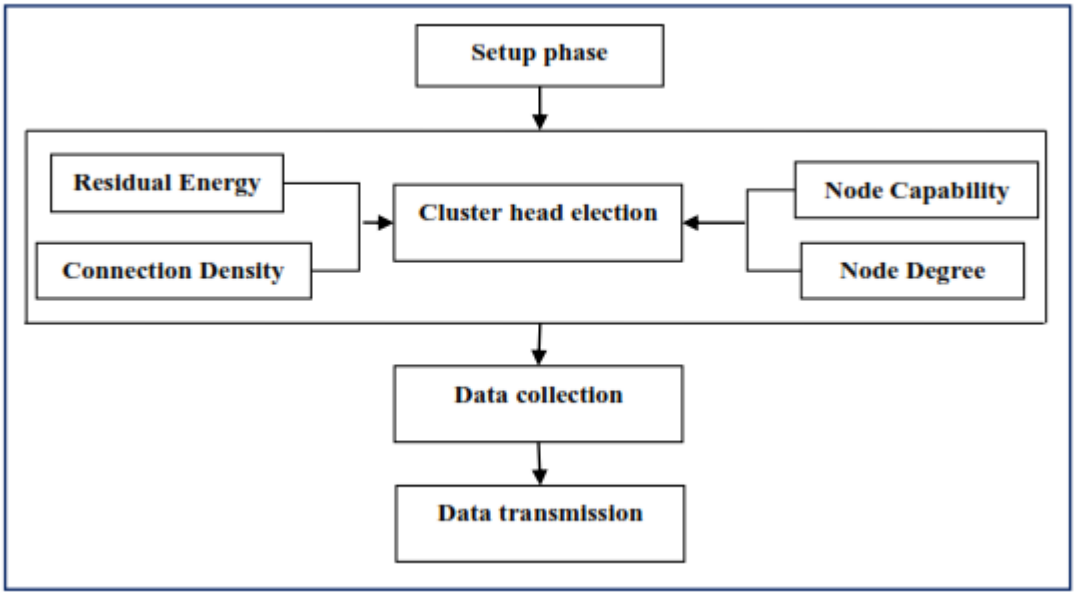


Figure 5.1 EECHDC strategy

5.2.2.4 The node's degree:

When x is a node, the degree of x is indicated by the symbol d(x). D(x) is equal to the number of links x has. If a node has the most neighbours, then it is said to be "CH." Isolating a node of the polynomial equation of x equals zero (no neighbours). The formula in Equation 5.4 depicts the degree of the graph shown.

$$d(G) = \{d(x)\} \qquad (5.4)$$

5.2.3 Data Collection phase:

The cluster members send data packets to individual CHs once a CH has been selected and made known to all cluster members. The CH collects network packets that it receives from members of the cluster.

5.2.4 Data transmission phase:

In some cases, if the sink is outside of the communication range, the aggregated data packets are conveyed to the BS via several CHs. Alternatively, the aggregated data packets are immediately transmitted to the sink if the sink is within communication range.

5.3 Simulation Analysis:

EECHDC is used to evaluate the NS2 performance. This open-source project is built in C++ and OTCL and is known as NS2. Although it is usually used to simulate network protocols, NS2 is a discrete event time-based simulator. Each node contains a simulation environment. You will need to use the NS2 command node-config to set up the nodes as mobile nodes.

Table 5.1 EECHDC Simulation Parameters

Parameter	Value
Type of Channel	Wireless Channel
Simulation Time	100 s
# Nodes	50, 70
MAC Type	802.11
Traffic Model	CBR
Simulation Area	700×700
Transmission Range	250m
Radio Propagation Model	TwoRayGround
Type of Network Interface	WirelessPhy
Mobility Model	Random Way Point
Antenna Model	Omni Antenna

This table summarises the EECHDC system parameters as they are summarised in the figure below. We have implemented the suggested strategy on 50 and 70 nodes evenly distributed in the simulation region 700mX700m. Using the Random Waypoint mobility model, the nodes are moved around in a simulation region in a random manner. To talk to one another, the nodes use the UDP protocol. CBR traffic model is employed to regulate traffic flow. The

two-ray ground model is used to propagate radio waves. Every node is equipped with an Omni-directional antenna that receives signals from all directions.

The PDR, PLR, throughput, average delay, and residual energy measure the EECHDC scheme's performance.

5.3.1 Case 1: N = 50 nodes:

The EECHDC scheme is first simulated using a 50-node scenario.

5.3.1.1 Packet Delivery Rate:

The PDR is the ratio of the number of data packets supplied by the source node to the number of packages delivered to all destinations. Predictive Delivery Rate Equation 5.5 is used to determine PDR.

$$PDR = \frac{\sum_0^n Packets\ Received}{Time} \tag{5.5}$$

The PDR values for ECSHA and EECHDC during the simulation analysis for 50 nodes are shown in Table 5.2. In Figure 5.2, the PDRs of ECSHA and EECHDC are displayed. It demonstrates that the proposed scheme EECHDC has an 9.2 per cent higher PDR than the present ECSHA.

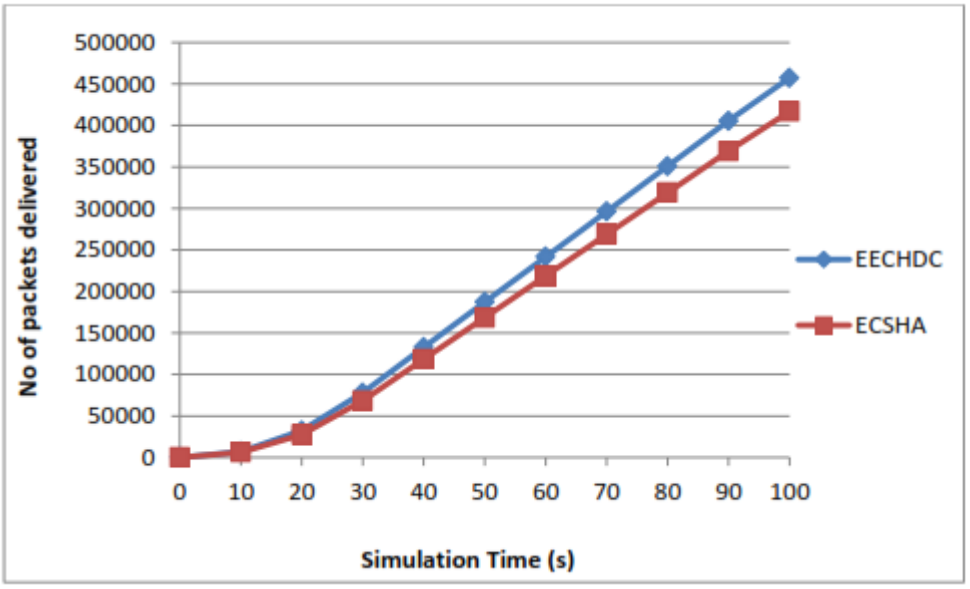


Figure 5.2 ECSHA and EECHDC Packet Delivery Rates for 50 nodes

5.3.1.2 Packet Loss Rate:

The PLR is defined in Equation 5.6 as the difference between the number of packets delivered and received in the network per unit time.

$$PLR = \frac{\sum_{0}^{n} Sent\ Pkts - Rcvd\ Pkts}{Time} \quad (5.6)$$

Table 5.2 PDR values of ECSHA and EECHDC for 50 nodes

Simulation Time (s)	PDR of ECSHA	PDR of EECHDC
0	0	0
10	6324	7089
20	27472	32297
30	68296	78042
40	118314	132602
50	168474	187162
60	218634	241722
70	268794	296282
80	318954	350842
90	369114	405402
100	416766	457234

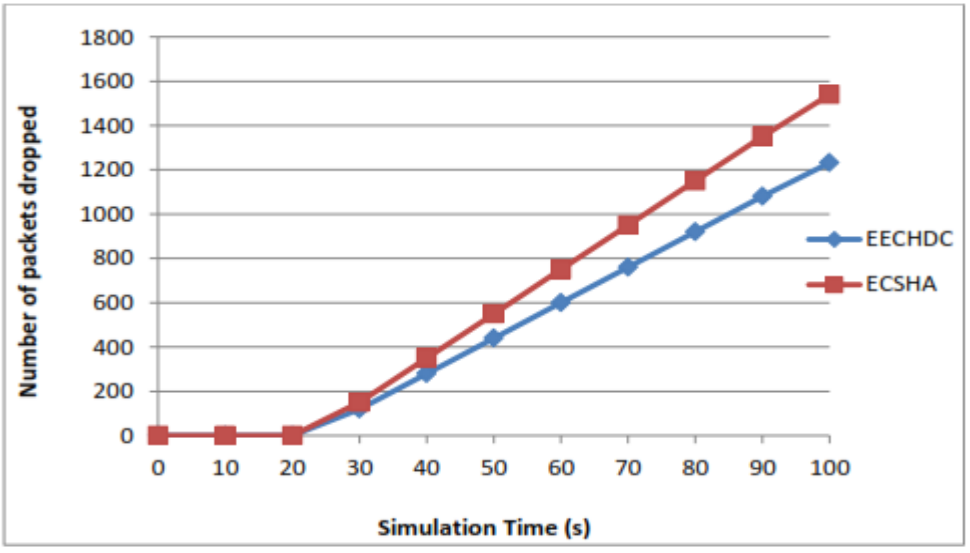


Figure 5.3 ECSHA and EECHDC Packet Loss Rates for 50 nodes

Table 5.3 PLR values of ECSHA and EECHDC for 50 nodes

Simulation Time (s)	PLR of ECSHA	PLR of EECHDC
0	0	0
10	0	0
20	0	0
30	150	120
40	350	280
50	550	440
60	750	600
70	950	760
80	1150	920
90	1350	1080
100	1540	1232

The PLR values derived from the simulation analysis of ECSHA and EECHDC are shown in Table 5.3. According to Figure 5.3, the PLR of ECSHA is19% more than that of EECHDC.

5.3.1.3 Throughput:

The term "throughput" refers to the total number of packets delivered successfully over the network per 1000 packets submitted. Equation 5.7 is used to calculate throughput.

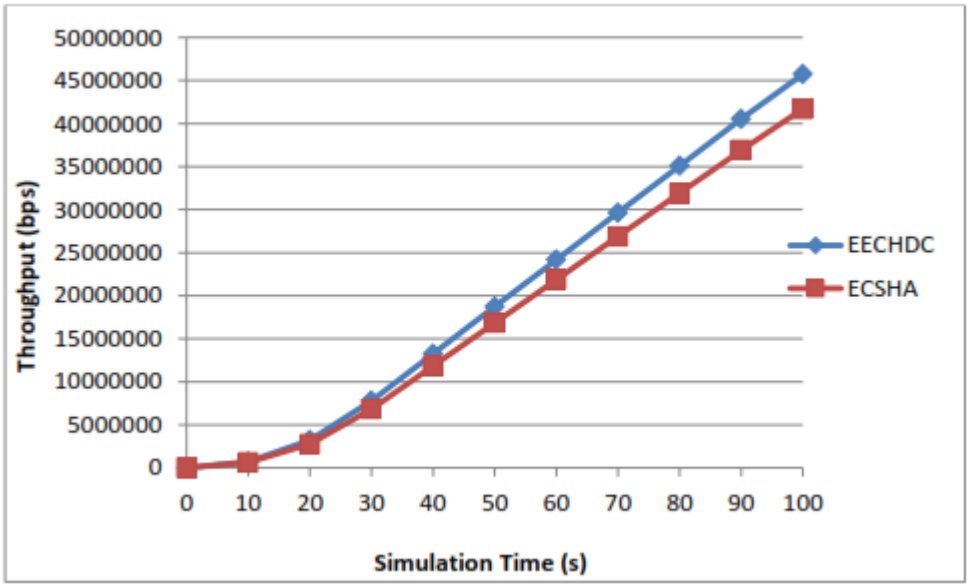


Figure 5.4 ECSHA and EECHDC throughput for 50 nodes

$$Throughput = \frac{\sum_0^n Packets\ Received(n) * Packet\ size}{1000} \quad (5.7)$$

Table 5.4 ECSHA and EECHDC throughput values for 50 nodes

Simulation Time (s)	Throughput of ECSHA (bps)	Throughput of EECHDC (bps)
0	0	0
10	632400	708900
20	2747200	3229700
30	6829600	7804200
40	11831400	13260200
50	16847400	18716200
60	21863400	24172200
70	26879400	29628200
80	31895400	35084200
90	36911400	40540200
100	41676600	45723400

Table 5.4 represent the throughput values obtained during the simulation study for the ECSHA and EECHDC mechanisms. As illustrated in Figure 5.4, the number of packets successfully received for every 1000 packets using EECHDC is more significant than 8.5 per cent when compared to the ECSHA technique.

5.3.1.4 Average Delay:

The average delay is calculated as the time that elapses between the current packets that have been received and the preceding boxes that were previously received. n, the number of nodes, which is 50, is computed using equation 5.8.

$$Avg\ Delay = \frac{\sum_0^n (Packet\ Received\ Time - Packet\ Sent\ Time)}{n} \quad (5.8)$$

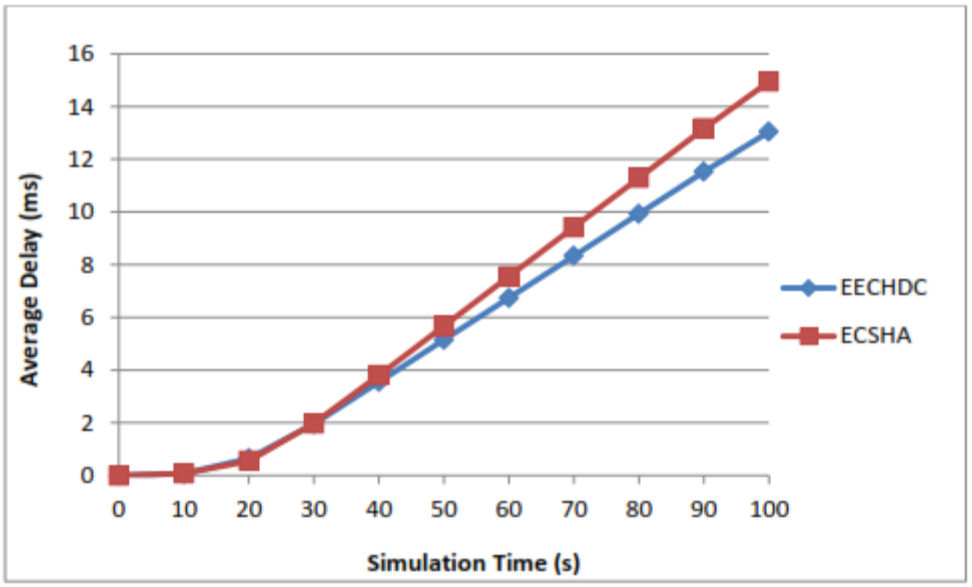


Figure 5.5 ECSHA and EECHDC Average Delay for 50 nodes

Table 5.5 Average ECSHA and EECHDC delay values for 50 nodes

Simulation time (s)	Delay of ECSHA (ms)	Delay of EECHDC (ms)
0	0	0
10	0.081209	0.08146
20	0.555346	0.651599
30	1.979768	1.953923
40	3.804926	3.548755
50	5.676853	5.143587
60	7.548779	6.738419
70	9.420706	8.333252
80	11.29263	9.928084
90	13.16456	11.52292
100	14.94289	13.03801

The average delay achieved from simulation studies of the ECSHA and EECHDC mechanisms for 50 nodes is shown in Table 5.5. According to Figure 5.5, the EECHDC scheme has a 11.94 percent lower node delay than the ECSHA system.

5.3.1.5 Residual Energy:

The quantity of energy that remains in a node is referred to as RE. The RE represents the amount of energy used to power the network and indicates how quickly the network functions.

Table 5.6 ECSHA and EECHDC RE values for 50 nodes

Simulation Time (s)	RE of ECSHA (J)	RE of EECHDC (J)
0	10	10
10	9.57	9.64
20	9.475	9.58
30	9.38	9.52
40	9.285	9.46
50	9.19	9.4
60	9.095	9.34
70	9	9.28
80	8.905	9.22
90	8.81	9.16
100	8.71975	9.1

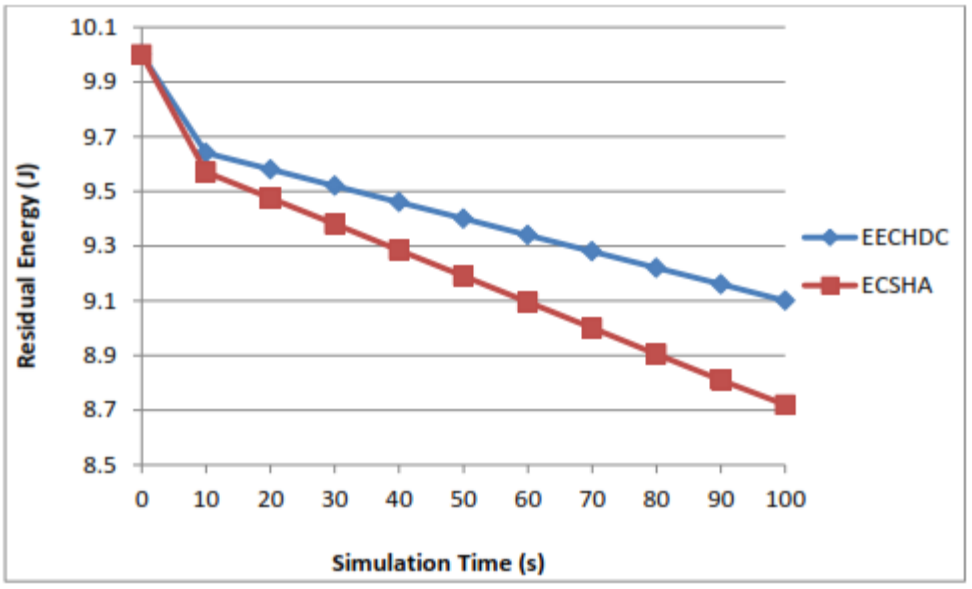


Figure 5.6 ECSHA and EECHDC Residual Energy for 50 nodes

The RE values obtained during the simulation analysis are shown in Table 5.6. According to Figure 5.6, the proposed scheme EECHDC has a higher RE than the present schemeECSHA.

By adopting the EECHDC protocol for routing, approximately 4.47 percent of energy is saved per node.

5.3.2 Case 2: N = 70 nodes:

To investigate how performance changes as the number of nodes increases, N is increased to 70. The charts below show the same parameters as those for 50 nodes.

5.3.2.1 Packet Delivery Rate:

As with the PDR of 50 nodes, the values are derived by simulating the ECSHA and EECHDC protocols using equation 5.5. Table 5.7 contains these data, which are also depicted in picture 5.7.

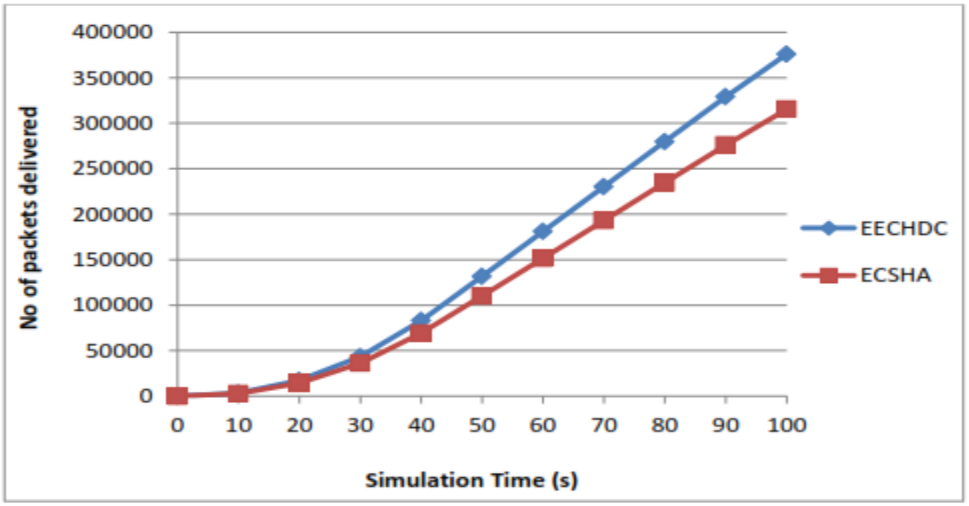


Figure 5.7 ECSHA and EECHDC Packet Delivery Rates for 70 nodes

Table 5.7 ECSHA and EECHDC PDR values for 70 nodes

Simulation Time (s)	PDR of ECSHA	PDR of EECHDC
0	0	0
10	2748	3298
20	14419	17276
30	36246	43338
40	69150	82925
50	110184	131623
60	151624	180982
70	193064	230340
80	234504	279698
90	275944	329057
100	315312	375947

This indicates that the PDR of the EECHDC mechanism is 16.12 percent bigger than the ECSHA method. The number of nodes increases the PDR values, demonstrating EECHDC's efficiency.

5.3.2.2 Packet Loss Rate:

For 70 nodes, the PLR is likewise determined similarly to the 50 nodes situation using equation 5.6. Table 5.8 illustrates the PLR of ECSHA and EECHDC for 70 nodes.

ECSHA's PLR is 28.57 percent bigger than that of the EECHDC mechanism. The PLRs of ECSHA and EECHDC are presented in Figure 5.8 for 70 nodes.

Table 5.8 ECSHA and EECHDC PLR values for 70 nodes

Simulation Time (s)	PLR of ECSHA	PLR of EECHDC
0	0	0
10	0	0
20	56	55
30	211	202
40	543	452
50	937	722
60	1331	993
70	1725	1264
80	2119	1534
90	2513	1805
100	2887	2062

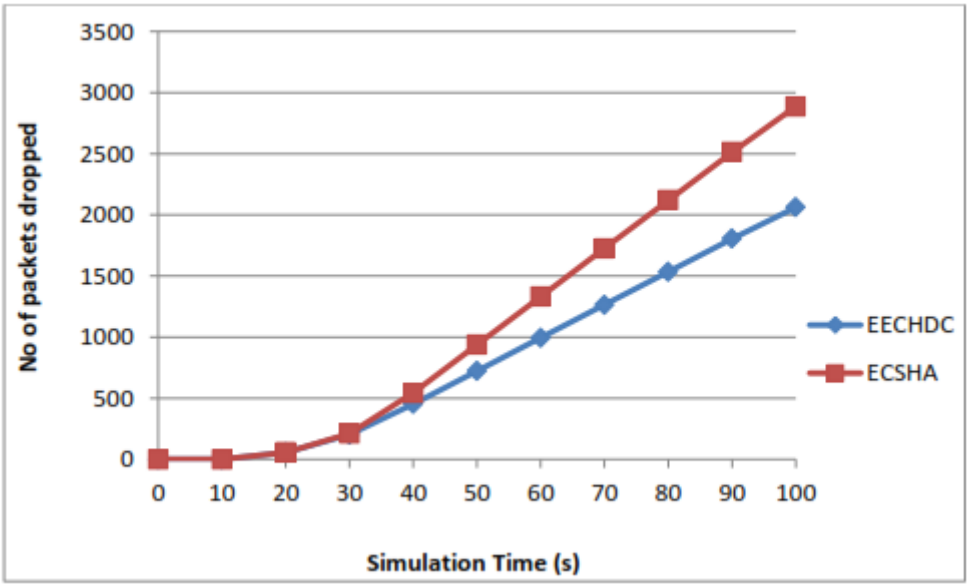


Figure 5.8 ECSHA and EECHDC Packet Loss Rates for 70 nodes

5.3.2.3 Throughput:

The ECSHA and EECHDC mechanisms' throughput is determined using equation 5.7. Table 5.9 contains the data for both of these techniques when working in a 70-node situation.

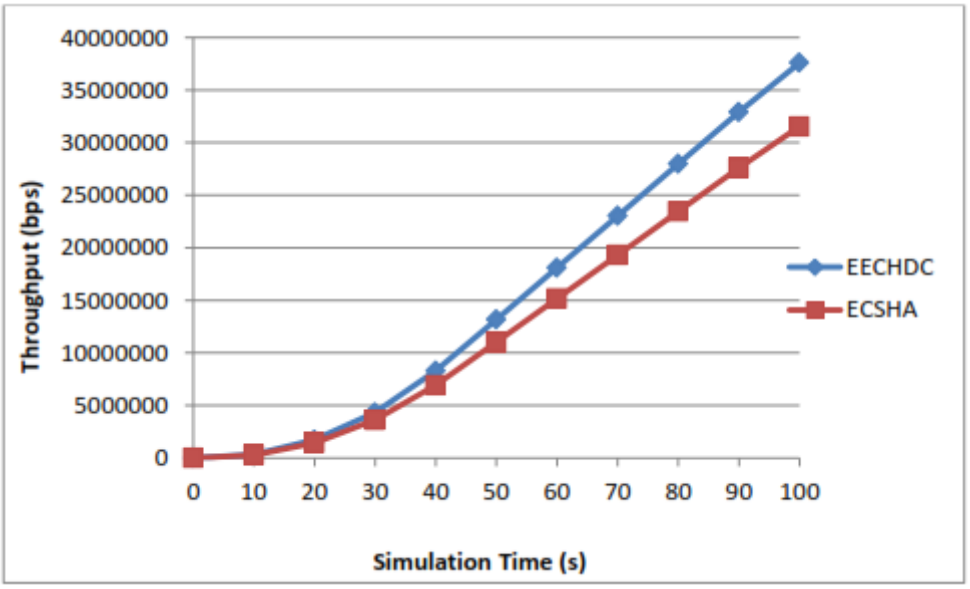


Figure 5.9 ECSHA and EECHDC throughput for 70 nodes

Table 5.9 ECSHA and EECHDC throughput values for 70 nodes

Simulation Time (s)	Throughput of ECSHA (bps)	Throughput of EECHDC (bps)
0	0	0
10	274890	329868
20	1441930	1727628
30	3624670	4333895
40	6915089	8292563
50	11018420	13162379
60	15162420	18098219
70	19306420	23034059
80	23450420	27969899
90	27594420	32905740
100	31531220	37594788

Figure 5.9 plots the throughput values for both the existing and proposed mechanisms to illustrate the differences visually. The comparison of EECHDC and ECSHA for a 70 node scenario reveals a 18.34 percent improvement in EECHDC.

5.3.2.4 Average Delay:

The delay between sending and receiving a packet is estimated using equation 5.8. Figure 5.10 illustrates the difference in average delay values for the ECSHA and EECHDC algorithms in a 70-node MANET. The delay at the ECSHA is therefore 29.07% larger than the delay at the EECHDC. Because the EECHDC protocol has a much lower hold than the current baseline, it is more usable.

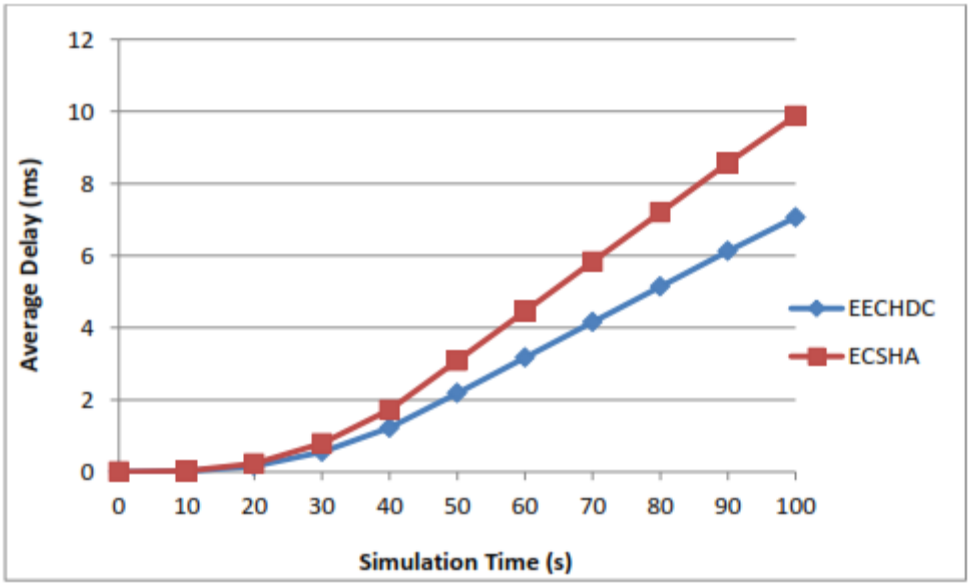


Figure 5.10 ECSHA and EECHDC Average Delay for 70 nodes

Table 5.10 ECSHA and EECHDC average delay values for 70 nodes

Simulation time (s)	Delay of ECSHA (ms)	Delay of EECHDC (ms)
0	0	0
10	0.02299	0.016093
20	0.230222	0.161154
30	0.78721	0.551041
40	1.719784	1.22166
50	3.088644	2.185591
60	4.460154	3.17144
70	5.831665	4.157289
80	7.203175	5.143138
90	8.574685	6.128987
100	9.877619	7.065544

5.3.2.5 Residual Energy:

Residual energy is the amount of energy that remains in a node at any given point in time.

Table 5.11 RE values of ECSHA and EECHDC for 70 nodes

Simulation Time (s)	RE of ECSHA (J)	RE of EECHDC (J)
0	10	10
10	9.715	9.77
20	9.62	9.695
30	9.525	9.62
40	9.43	9.54125
50	9.335	9.47
60	9.23525	9.395
70	9.145	9.32
80	9.04525	9.24125
90	8.95025	9.17
100	8.86	9.095

A residual energy measurement indicates the pace at which network processes consume energy. The residual energy values acquired throughout the simulation analysis are shown in Table 5.11.

According to Figure 5.11, the suggested scheme EECHDC has lower residual energy than the present scheme ECSHA. By employing the EECHDC protocol for routing, approximately 2.48 percent of energy is saved per node.

5.4 Summary:

The EECHDC method was simulated and examined using the network simulator, and the findings demonstrated that the EECHDC mechanism is more efficient than ECSHA. The suggested EECHDC mechanism increases total packet delivery by 12.48 percent, reduces packet loss by 24.28 percent, reduces average latency by 20.6 percent, increases throughput by 12.48 percent, and saves residual energy by 3.38 percent. As a result, the WSN's clustering topology employs the EECHDC method, increasing the communication network's efficiency.

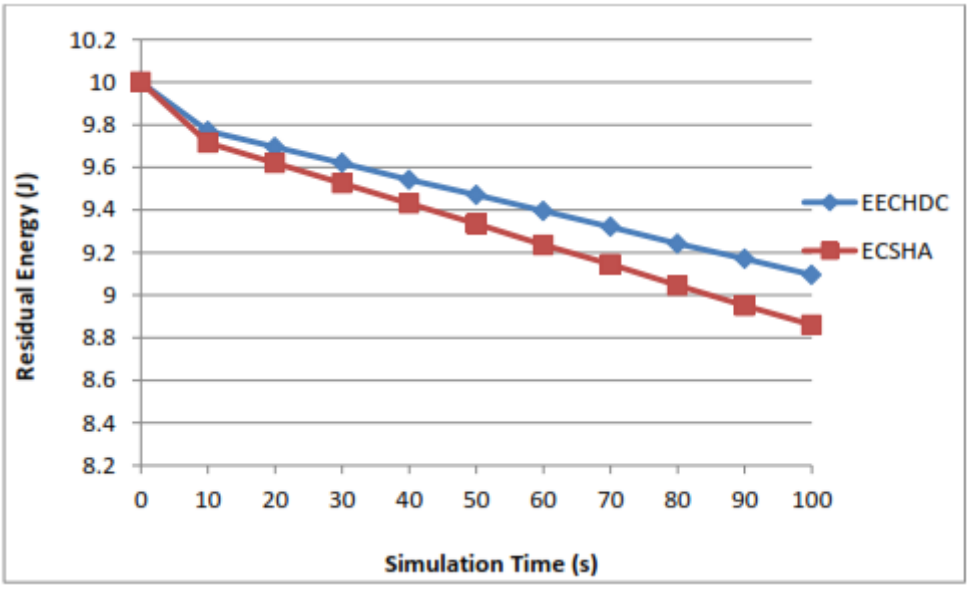


Figure 5.11 ECSHA and EECHDC Residual Energy for 70 nodes

CHAPTER 6

AN ENERGY-EFFICIENT SEGMENTATION STRUCTURE FOR OBSTACLES IN WIRELESS SENSOR NETWORKS

Extending the lifetime of WSN networks necessitates using clustering mechanisms. Clustering Sensor Nodes (SNs) and choosing CHS for each cluster make up the solution. This enables CHs to receive information from consonant clusters and then pass it on to the BS. Clustered WSNs are commonly assumed to have no obstruction. This research effort proposes the Energy Efficient Clustering Scheme for Obstacles (EECSO), which uses the CH value as the clustering criterion. Three different parameters are used to evaluate the quality of a connection: the quality of the connection, the amount of residual energy, and the node degree. In the presence of an obstruction, the POT determines the shortest path through the WSN. Decreasing the number of forwarders and reducing packet delay are accomplished by using POT.

6.1 RESEARCH FOR THE PROJECTED EECSO:

The spread sensing function of WSNs involves modest amounts of energy that use radio frequencies to carry out various operations. WSNs have diverse application fields in addition to agricultural, like detection of fire, gas, and chemical leakage, intellectual alarms, and health. WSN has focused research on cluster-based routing to maximise the network's lifetime while also enhancing scalability. Subnet Selection is the process of selecting a subset of sensor nodes (SNs) to serve as core nodes (CHs) for a particular set of wireless sensor networks (WSNs). This explains how WSNs are mostly impacted by the choice of CH. The residual energy in each subnetwork influences the selection of clusters in the Adaptive Decentralized Re Clustering (ADRC) protocol.

Geographic routing is an open technique because it is not dependent on the WSNs' overall architecture. A sensor's routing resolution is determined by its geological position and that of its nearby nodes. The sensors transmit data to the adjacent unit, which is located near the sink. This routing approach reduces the number of forwarders. Geographic routing, on the other hand, cannot maximise the number of forwarders when a node does not have a nearest neighbour to the BS. Numerous variables can contribute to the incident, including sparse sensor deployment, obstructions, and sensor node failures.

6.2 DEPICTION OF THE PROPOSED EECSO

As shown in figure 6.1, CHs collect and transmit data to the BS on a regular basis. For WSNs, an EECSO, a clustering technique, was devised. WSN entails a large number of sensors spread across a large area, as well as a BS located far from the SN. These sensors monitor the surroundings and provide data to the BS on a regular basis. The use of energy for information transmission should be minimized by splitting the network into clusters. The network's activities are divided into many phases. The EECSO scheme's architecture is depicted in Figure 6.2.

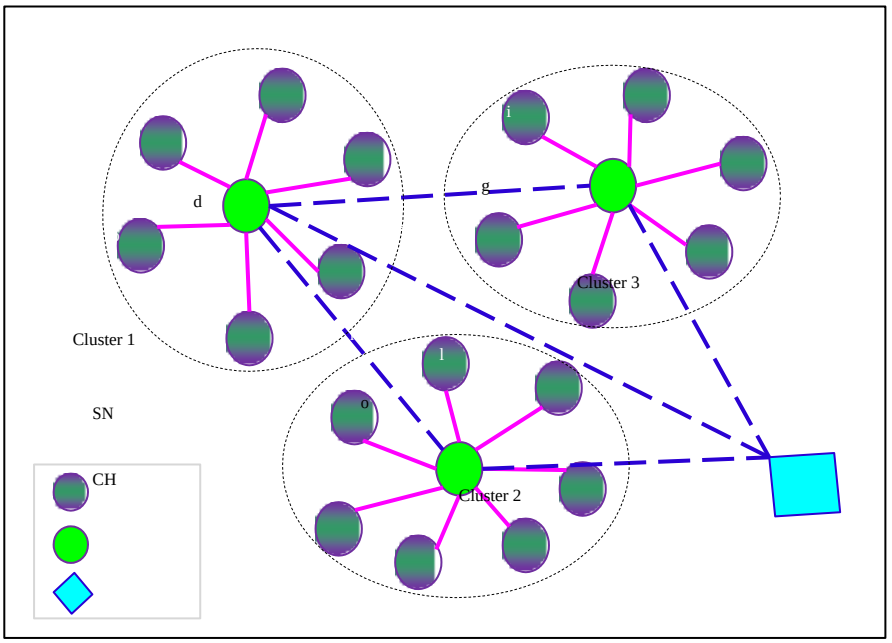


Figure 6.1 Cluster Topology Illustration

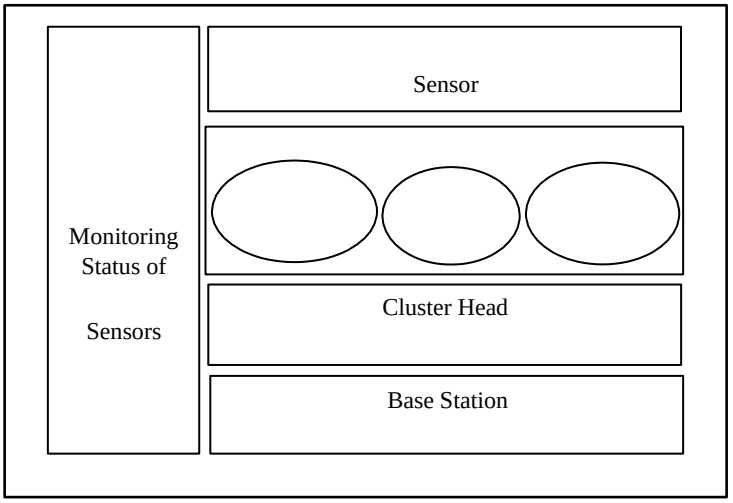


Figure 6.2 The EECSO scheme's architecture

6.2.1 PHASE OF DISTANCING

During this phase, each SN delivers data on its location, the reliability of the link, the node degree, and the amount of energy. The SNs use the Global Positioning System to establish their present location (GPS). Using BS methodology, the sensor node examines the quality factor of a sensor node and selects the CH if necessary.

6.2.2 PHASE OF ELECTION:

The CH is responsible for receiving and forwarding cluster-related data from SNs within clusters to the BS. In addition to assessing the connection robustness, node degree, and energy, the Quality Factor is used to evaluate the CH selection on the basis of node degree, and node degree and energy. A manufacturer has decided that a node with the highest quality factor will be chosen for a CH. Equation 6.1 is utilised to estimate the quality rating.

$$Quality\ Factor = Link\ robustness * Energy * NodeDegree \qquad (6.1)$$

6.2.3 OBSTACLE ESTIMATION PHASE:

The obstacle cost estimation phase decreases the number of forwarders encountered throughout the shortest path from source to backhaul. The first stage of this process is for the source to send the data to BS and locate any geographical barriers that exist between the source and BS. If there are no obstacles, information is transferred to BS regardless of where it is located. If Dijkstra's shortest path algorithm is used, the source first utilises it to discover the shortest path.

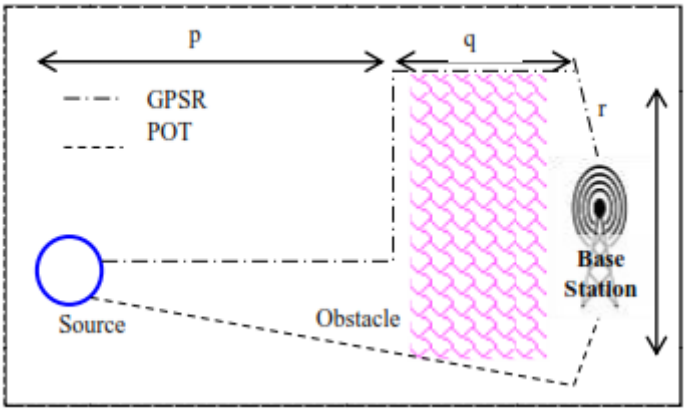


Figure 6.3 Illustrations of GPSR and POT

Figure 6.3 shows the route creation in GPSR and POT. The Euclidean distance is found to be equal to p plus q. The challenge lies in the length of the obstacle (r) and its width (q), and the base station is positioned behind the obstacles. POT and GPSR generate the path length using 6.2 and 6.3.

$$POT = \sqrt{(\frac{r}{2})^2 + p^2} + (\frac{r}{2} + q) \tag{6.2}$$

$$GPSR = p + r + q \tag{6.3}$$

In other words, if p is greater than or equal to q, the path in POT shrivels according to equation 6.4.

$$\frac{2p - (p^2 + \frac{p}{2})^2}{2p} * 100 = 19\% \tag{6.4}$$

Routing and sensing tasks can be optimised by employing path optimization. The network's lifetime is increased as a result.

6.2.4 PHASE OF TRANSMISSION

The three key activities involved in the phase of information communication are communication, sharing, and collaborating:

- Gathering evidence.
- Aggregation of facts.
- Transmission of information.

All SNs transmit information to their respective CHs during the sensing period, which in turn acquire information from cluster members. Rather than examining unnecessary material, the CHs discard it. Finally, the aggregated data is transmitted to the BS by the CHs.

6.3 ANALYSES OF SIMULATION:

NS2 is often used to analyse the EECSO system's performance. NS2 is an open source tool written in C++ and OTCL. NS2 is a time-based discrete event simulator that is mostly used to simulate network protocols. Nodes are used to distribute the simulation environment. Using the NS2 command node-config, the nodes must be established as mobile nodes. The settings used to simulate the EECSO scheme are listed in Table 6.1. The EECSO scheme is simulated in the simulation region 700 using 50 and 70 nodes. The nodes are randomly moved within the simulation area using the dynamic load balancing Random waypoint.

Table 6.1 EECSO Simulation Parameters

Parameter	Value
Type of Channel	Wireless Channel
Simulation Time	100 s
# Nodes	50, 70
MAC Type	802.11
Traffic Model	CBR
Simulation Area	700×700
Transmission Range	250m
Radio Propagation Model	TwoRayGround
Type of Network Interface	WirelessPhy
Mobility Model	Random Way Point
Antenna Model	Omni Antenna

The nodes communicate via the UDP protocol. To manage traffic, the CBR traffic model is utilized. The two-ray ground model is used to propagate radio waves. Each node's omnidirectional antenna receives signals in all directions.

The PDR, PLR, throughput, average latency, and residual energy are used to measure the EECSO scheme's performance.

6.3.1 CASE 1: N = 50 NODES:

The EECSO method is first simulated using a 50-node scenario.

6.3.1.1 PACKET DELIVERY RATE:

A PDR ratio is calculated by dividing the number of packets delivered to every destination by the total number of packets sent by the source node. To compute PDR, use the equation 6.5.

$$PDR = \frac{\sum_0^n Packets\ Received}{Time} \tag{6.5}$$

Table 6.2 summarises the ADRC and EECSO PDR values obtained during the simulated investigation of 50 nodes. Figure 6.4 illustrates the PDR of ADRC and EECSO. It demonstrates that the proposed scheme EECSO has a 29.63 percent higher PDR than the current ADRC.

Table 6.2 ADRC and EECSO PDR values for 50 nodes

Simulation Time (s)	PDR of ADRC	PDR of EECSO
0	0	0
10	8514	6960
20	41828	34184
30	88724	98727
40	135744	169487
50	182764	240247
60	229784	311007
70	276804	381767
80	323824	452527
90	370844	523287
100	415513	590509

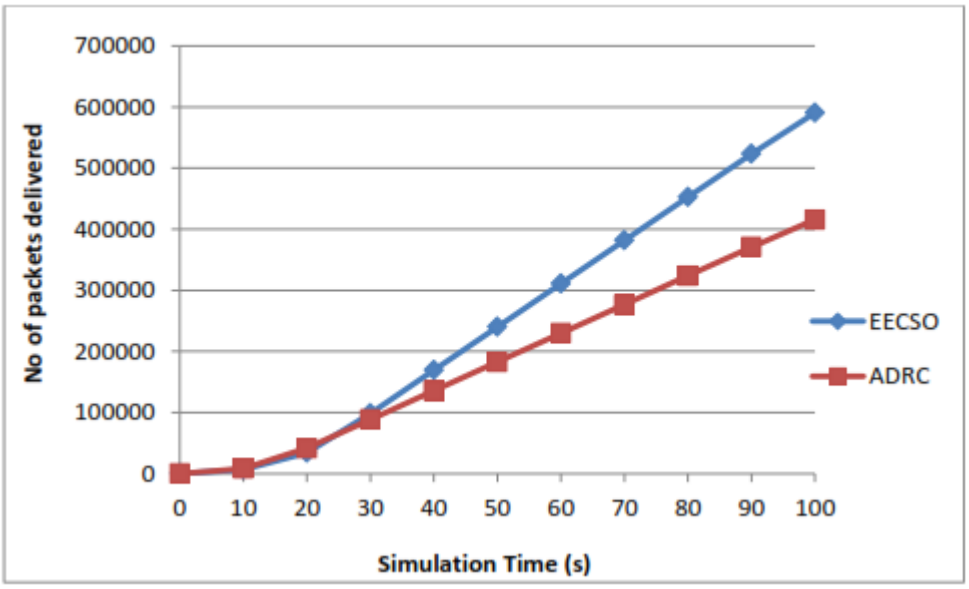


Figure 6.4 ADRC and EECSO Packet Delivery Rates for 50 nodes

6.3.1.2 PACKET LOSS RATE:

As specified in Equation 6.6, the PLR is defined as the difference between the number of packets transmitted and received in the network per unit time.

$$PLR = \frac{\sum_0^n Sent\ Pkts - Rcvd\ Pkts}{Time} \qquad (6.6)$$

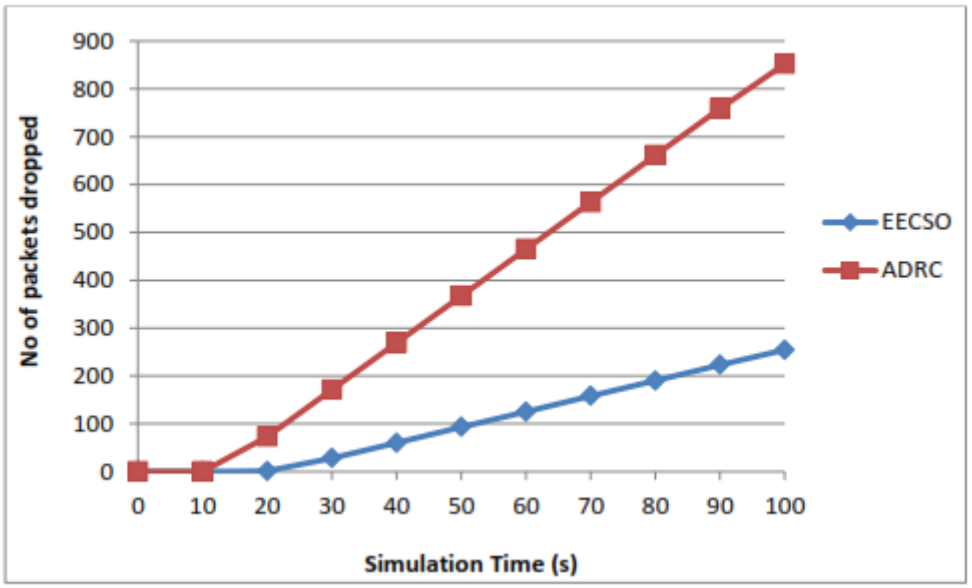


Figure 6.5 ADRC and EECSO Packet Loss Rates for 50 nodes

Table 6.3 PLR values of ADRC and EECSO for 50 nodes

Simulation Time (s)	PLR of ADRC	PLR of EECSO
0	0	0
10	0	0
20	73	1
30	171	28
40	269	60
50	367	93
60	465	125
70	563	158
80	661	190
90	759	223
100	852	254

The PLR values derived from the simulation analysis of ADRC and EECSO are shown in Table 6.3. According to Figure 6.5, the PLR of ADRC is 70.18 percent more than that of EECSO.

6.3.1.3 Throughput:

The term "throughput" refers to the total number of packets delivered successfully through a network for every 1000 packets sent. Equation 6.7 is used to calculate throughput.

$$Throughput = \frac{\sum_{0}^{n} Packets\ Received(n) * Packet\ size}{1000} \tag{6.7}$$

The values in Table 6.4 represent the throughput values obtained during simulation studies for the ADRC and EECSO mechanisms. As illustrated in Figure 6.6, the number of packets successfully received for every 1000 packets using EECSO is greater than 31.25 percent when compared to the ADRC mechanism.

Table 6.4 ADRC and EECSO throughput values for 50 nodes

Simulation Time (s)	Throughput of ADRC (bps)	Throughput of EECSO (bps)
0	0	0
10	851400	696000
20	4182800	3418400
30	8872400	9872700
40	13574400	16948700
50	18276400	24024700
60	22978400	31100700
70	27680400	38176700
80	32382400	45252700
90	37084400	52328700
100	41551300	59050900

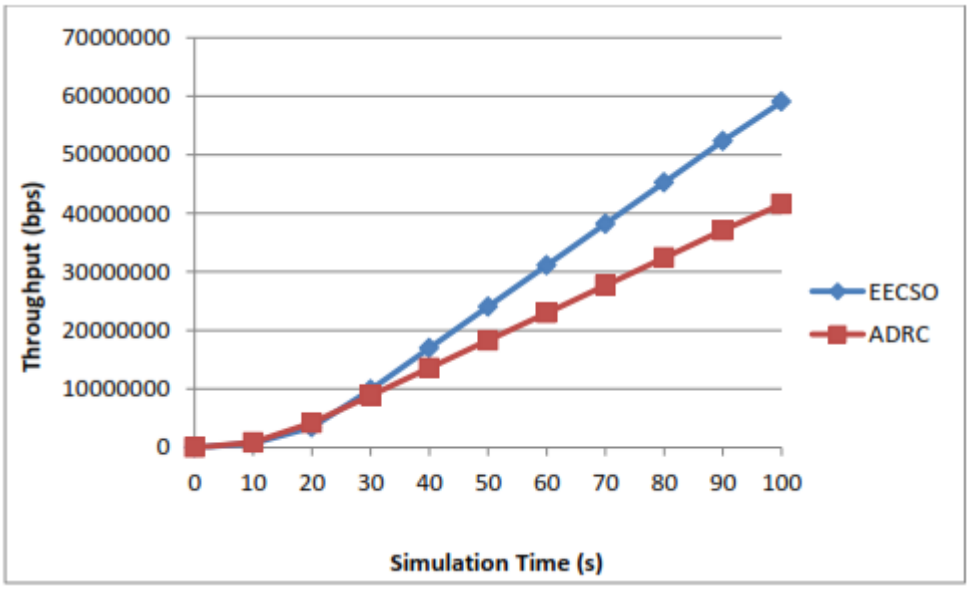


Figure 6.6 ADRC and EECSO throughput for 50 nodes

6.3.1.4 AVERAGE DELAY:

The average delay is the time that elapses between the current packets received and those that were previously received. Using the equation 6.8, which has the variable "n" representing the number of nodes, we find that.

$$Avg\ Delay = \frac{\sum_{0}^{n}(Packet\ Received\ Time - Packet\ Sent\ Time)}{n} \qquad (6.8)$$

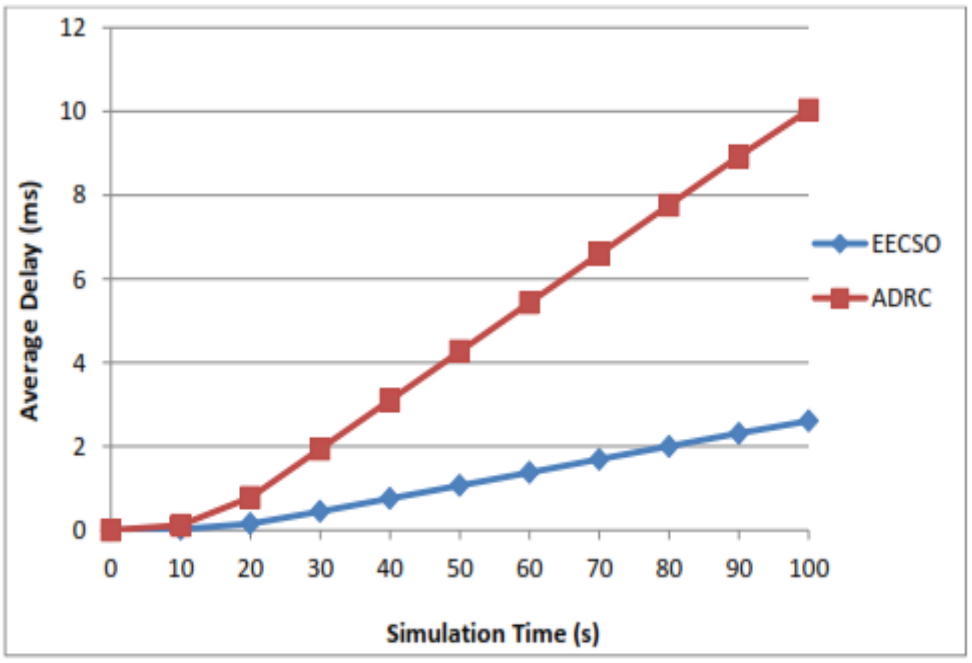


Figure 6.7 Average Delay of ADRC and EECSO for 50 nodes

The average delay derived from simulation studies of ADRC and EECSO methods for 50 nodes is shown in Table 6.5. According to Figure 6.7, the EECSO scheme has a 75.47 percent lower node delay than the ADRC method.

6.3.1.5 RESIDUAL ENERGY:

At the present instant, the remaining energy in a node is indicated by the term RE. It displays the network's operating rate in terms of units of energy consumption known as the RE.

The RE values obtained during the simulation analysis are shown in Table 6.6. According to Figure 6.8, the proposed scheme EECSO has a higher RE than the present scheme ADRC. By adopting the EECSO protocol for routing, approximately 7.6 percent of energy is saved per node.

Table 6.5 Average Delay values of ADRC and EECSO for 50 nodes

Simulation time (s)	Delay of ADRC (ms)	Delay of EECSO (ms)
0	0	0
10	0.114725	0.022955
20	0.777747	0.155563
30	1.941265	0.446616
40	3.10534	0.757343
50	4.269416	1.06807
60	5.433491	1.378798
70	6.597567	1.689525
80	7.761642	2.000252
90	8.925718	2.310979
100	10.03159	2.60617

Table 6.6 RE values of ADRC and EECSO for 50 nodes

Simulation Time (s)	RE of ADRC (J)	RE of EECSO (J)
0	10	10
10	9.90475	9.985075
20	9.81975	9.976575
30	9.73475	9.968075
40	9.64975	9.959575
50	9.56475	9.951075
60	9.47975	9.942575
70	9.39475	9.934075
80	9.30975	9.925575
90	9.22475	9.917075
100	9.144	9.909

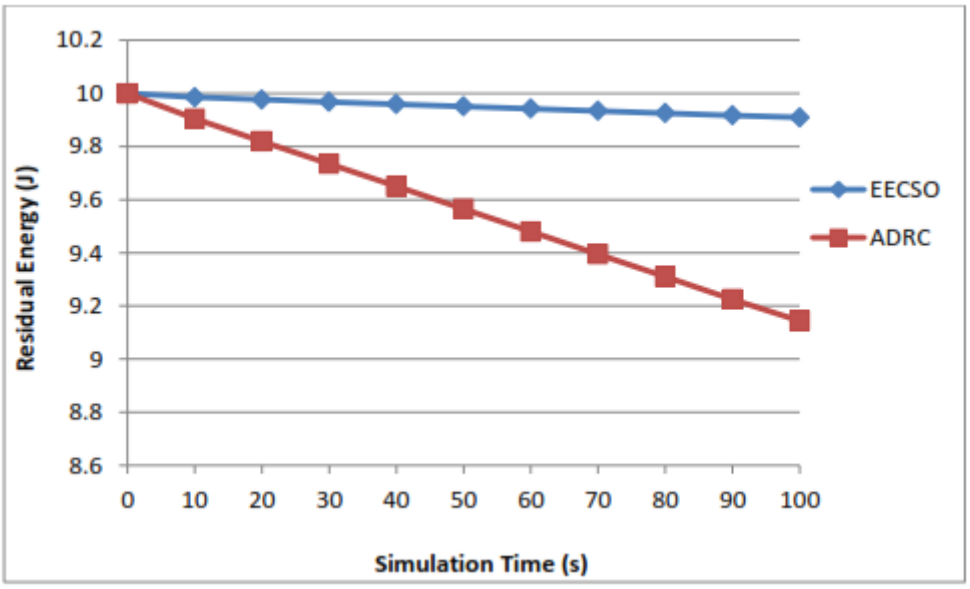


Figure 6.8 Residual Energy of ADRC and EECSO for 50 nodes

6.3.2 CASE 2: N = 70 NODES:

To investigate how performance changes as the number of nodes increases, N is increased to 70. The charts below show the same parameters as those for 50 nodes.

6.3.2.1 PACKET DELIVERY RATE:

As with the PDR of 50 nodes, the values are derived using equation 6.5 during ADRC and EECSO protocol simulations. Table 6.7 contains these results, which are also plotted in Figure 6.9.

Table 6.7 PDR values of ADRC and EECSO for 70 nodes

Simulation Time (s)	PDR of ADRC	PDR of EECSO
0	0	0
10	3101	2540
20	17797	14661
30	53876	44691
40	101943	100685
50	152943	164525
60	203945	228365
70	254965	292205
80	305985	356153
90	357005	420113
100	405474	480875

This demonstrates that the PDR of the EECSO mechanism is 15.67% bigger than that of the ADRC method. The number of nodes increases the PDR values, demonstrating EECSO's efficiency.

6.3.2.2 PACKET LOSS RATE:

For 70 nodes, the PLR is likewise determined similarly to the 50 nodes situation using equation 6.6.

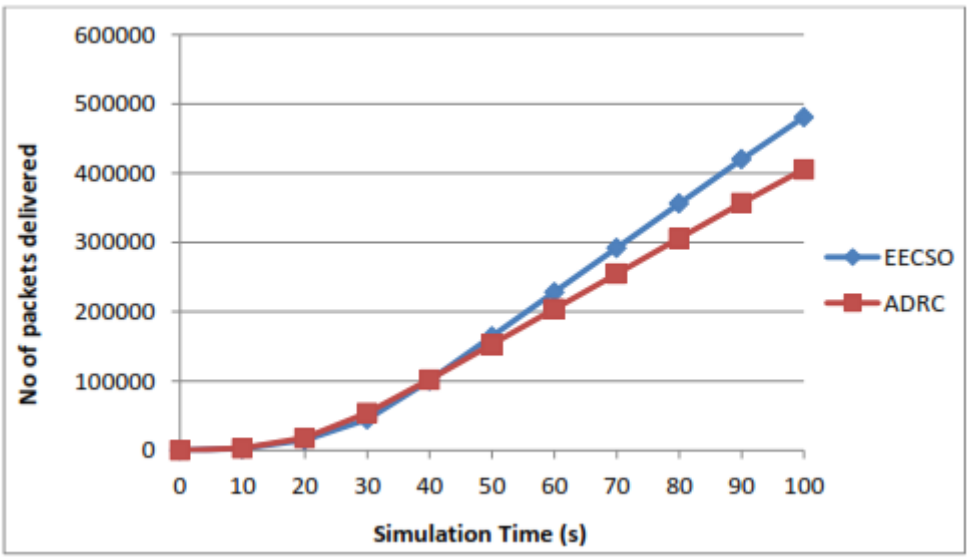


Figure 6.9 Packet Delivery Rate of ADRC and EECSO for 70 nodes

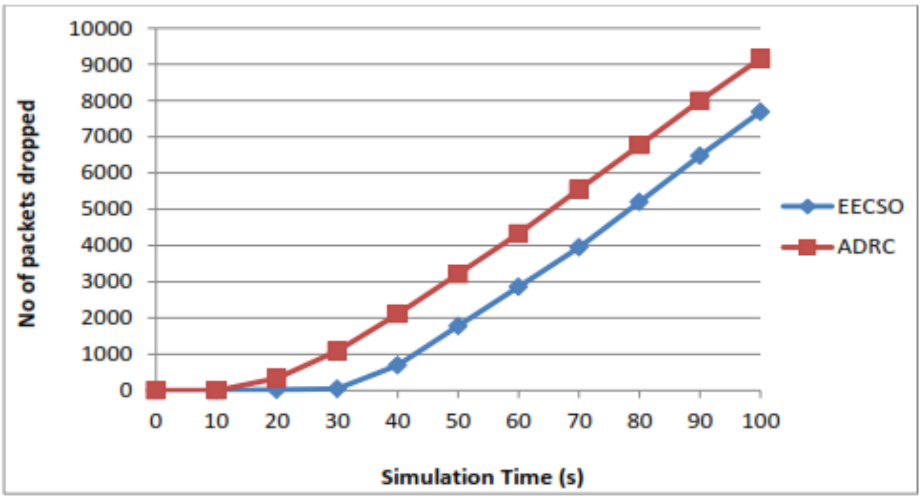


Figure 6.10 Packet Loss Rate of ADRC and EECSO for 70 nodes

Table 6.8 illustrates the PLR of ADRC and EECSO for 70 nodes. ADRC's PLR is 16.04 percent more than that of the EECSO method. Figure 6.10 illustrates the PLR of ADRC and EECSO for 70 nodes.

6.3.2.3 THROUGHPUT:

For both the ADRC and EECSO methods, throughput is calculated using equation 6.7. Table 6.9 contains the data for both of these techniques when working in a 70-node situation. Figure 6.11 plots the throughput values for both the existing and proposed mechanisms to illustrate the differences visually. The observation is that EECSO outperforms the ADRC by 16.92 percent in a 70 node situation.

Table 6.8 PLR values of ADRC and EECHDC for 70 nodes

Simulation Time (s)	PLR of ADRC	PLR of EECSO
0	0	0
10	0	0
20	334	18
30	1085	43
40	2109	693
50	3211	1776
60	4325	2859
70	5547	3943
80	6769	5198
90	7991	6473
100	9152	7684

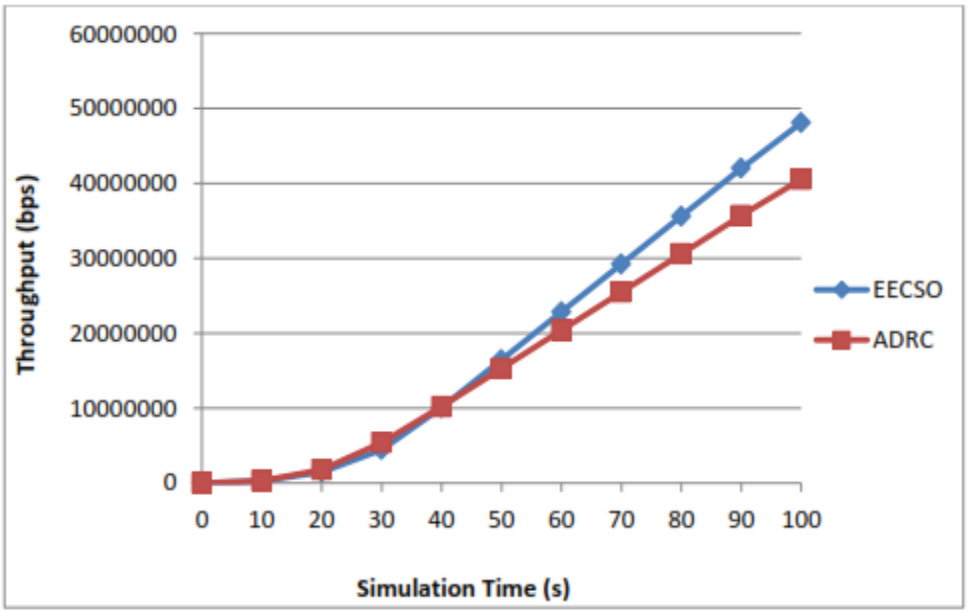


Figure 6.11 Throughput of ADRC and EECSO for 70 nodes

Table 6.9 Throughput values of ADRC and EECSO for 70 nodes

Simulation Time (s)	Throughput of ADRC (bps)	Throughput of EECSO (bps)
0	0	0
10	310100	254000
20	1779700	1466100
30	5387600	4469100
40	10194300	10068500
50	15294300	16452500
60	20394500	22836500
70	25496500	29220500
80	30598500	35615300
90	35700500	42011300
100	40547400	48087500

Table 6.10 Average Delay values of ADRC and EECSO for 70 nodes

Simulation time (s)	Delay of ADRC (ms)	Delay of EECSO (ms)
0	0	0
10	0.021458	0.00716
20	0.312409	0.1041
30	1.018772	0.361854
40	2.295759	0.816873
50	3.87547	1.346961
60	5.478625	1.877049
70	7.292782	2.407137
80	9.106939	3.093203
90	10.9211	3.7966
100	12.64455	4.464828

6.3.2.4 AVERAGE DELAY:

The average delay is calculated as the difference between the timings required to send and receive a packet across all nodes, as shown in equation 6.8. The difference in the average delay values for ADRC and EECSO methods in a 70-node MANET is shown in Table 6.10 and Figure 6.12. As a result, the ADRC's delay is 68.68 percent greater than the EECSO's. Due to the EECSO mechanism's short delay, it is more useable than the present baseline protocol.

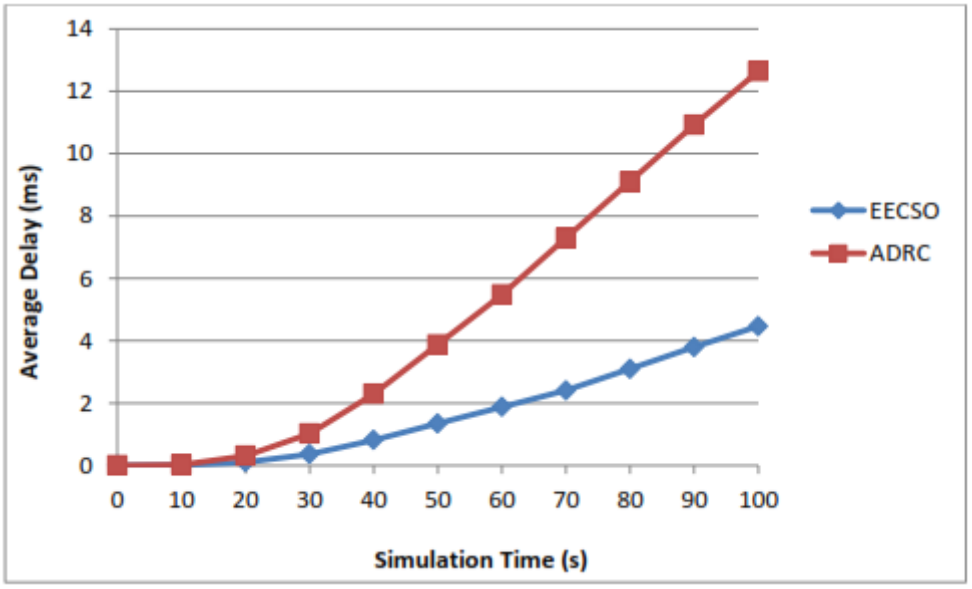


Figure 6.12 Average Delay of ADRC and EECSO for 70 nodes

6.3.5 RESIDUAL ENERGY:

The quantity of energy that remains in a node at any point in time is referred to as residual energy. A residual energy measurement indicates the pace at which energy is consumed by network processes.

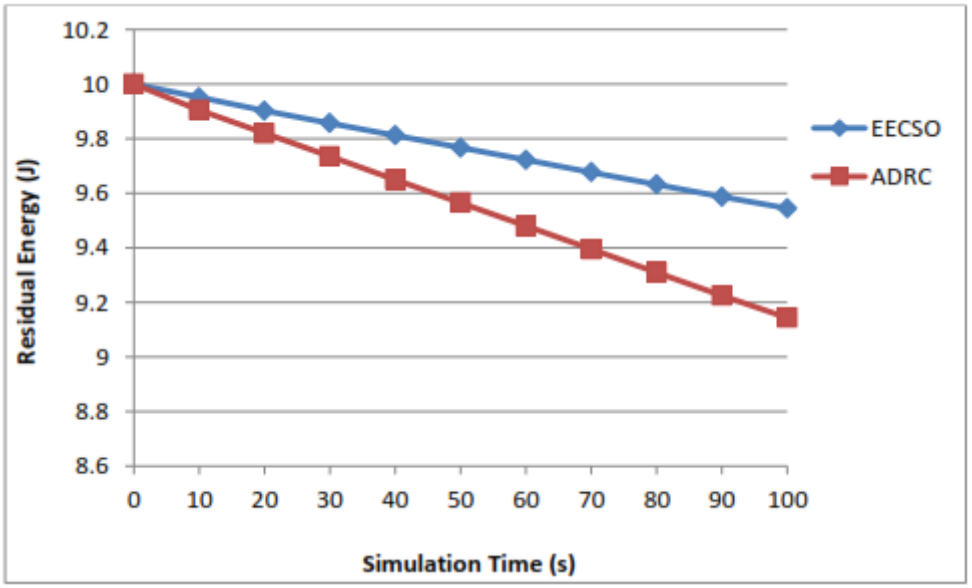


Figure 6.13 Residual Energy of ADRC and EECSO for 70 nodes

Table 6.11 RE values of ADRC and EECSO for 70 nodes

Simulation Time (s)	RE of ADRC (J)	RE of EECSO (J)
0	10	10
10	9.90475	9.95125
20	9.81975	9.90175
30	9.73475	9.85675
40	9.64975	9.81175
50	9.56475	9.76675
60	9.47975	9.72175
70	9.39475	9.67675
80	9.30975	9.63175
90	9.22475	9.58675
100	9.144	9.544

The residual energy values acquired from the simulation analysis are shown in Table 6.11. According to Figure 6.13, the proposed scheme EECSO has a lower residual energy than the present scheme ADRC. By employing the EECSO protocol for routing, approximately 4.19 percent of energy is saved per node.

6.4 SUMMARY:

The EECSO method was simulated and examined using the network simulator, and the findings demonstrated that the EECSO mechanism is more efficient than ADRC. In the suggested EECSO mechanism, total packet delivery is increased by 22.65 percent, packet loss is decreased by 43.11 percent, average latency is reduced by 69.35 percent, throughput is enhanced by 22.65 percent, and residual energy is conserved by 5.95 percent. As a result, the EECSO method is used by the clustering topology in the WSN, which boosts the communication network's efficiency.

CHAPTER 7
RESULTS AND DISCUSSION

Chapter 7 presents a comparison of all of the results acquired utilising the four postulated methods. This chapter analyses the network's performance, including the PDR, PLR, average latency, throughput, and RE. Analyzing all parameters with a variable number of nodes enables network simulations to determine the optimal protocol.

7.1 PERFORMANCE ANALYSIS:

The performance of all current and new mechanisms is analysed using the same network analysis technique. The network adheres to the random waypoint mobility paradigm, which allows nodes to travel in any direction within the topology area under consideration.

7.1.1 SIMULATION OF DCSC USING 50 NODES:

The network scenarios considered by the protocols for 50 nodes are depicted in Figure 7.1 (a-e). The source and destination are provided sequentially as inputs for the analysis of the various simulation scenarios. Routes are chosen based on the next hop selection made during the simulations.

In Figure 7.1a, 50 nodes are randomly distributed throughout the network. The dynamic range of the source and sink are depicted in Figure 7.1b. The clustering technique is depicted in Figure 7.1c.

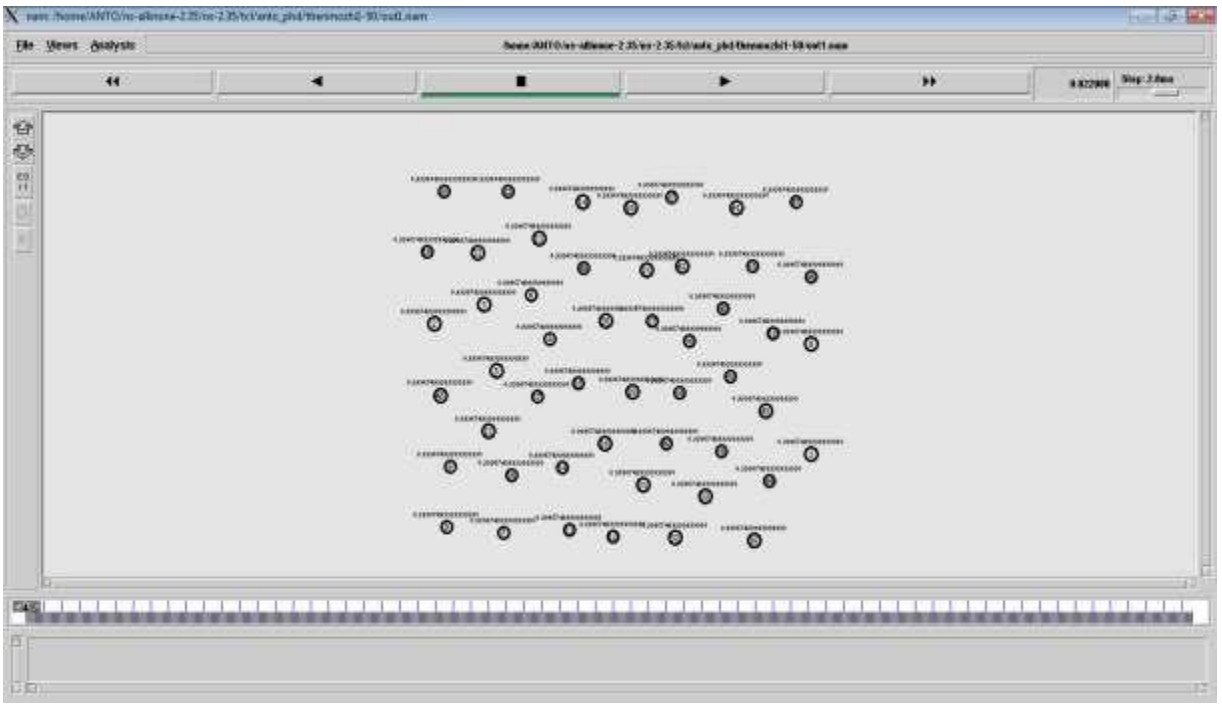


FIGURE 7.1A SNAPSHOT OF 50 NODES

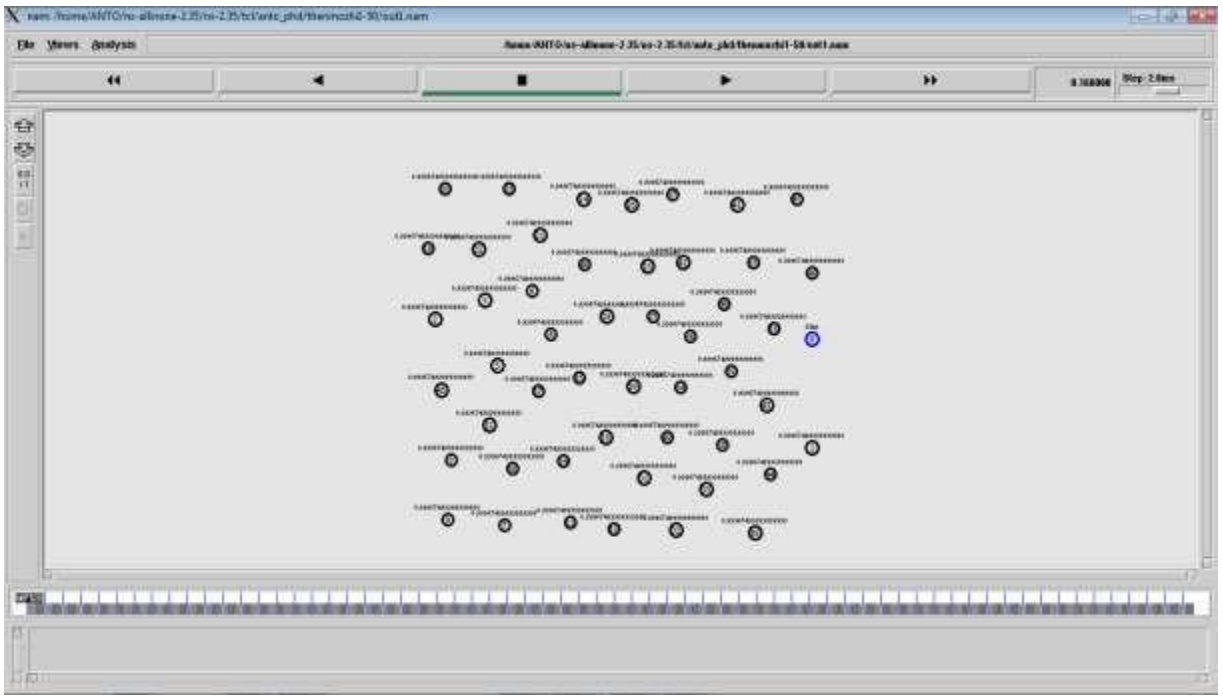


FIGURE 7.1B SNAPSHOT OF 50 NODES

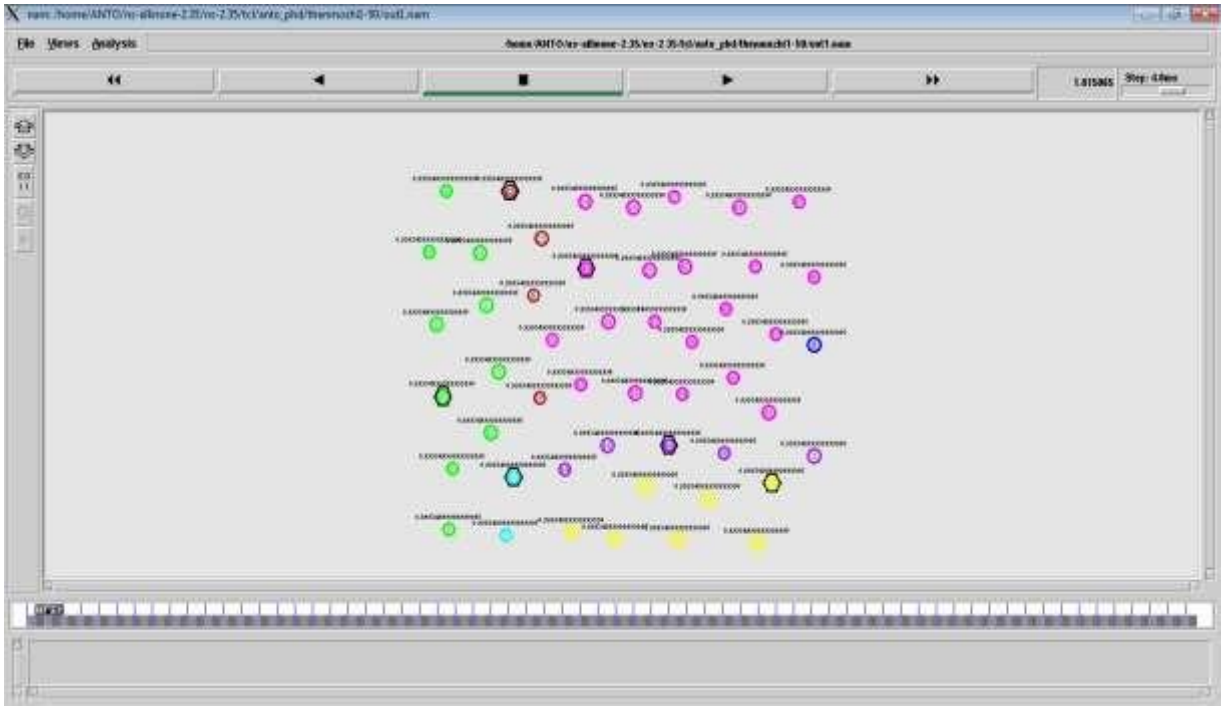


FIGURE 7.1C SNAPSHOT OF 50 NODES

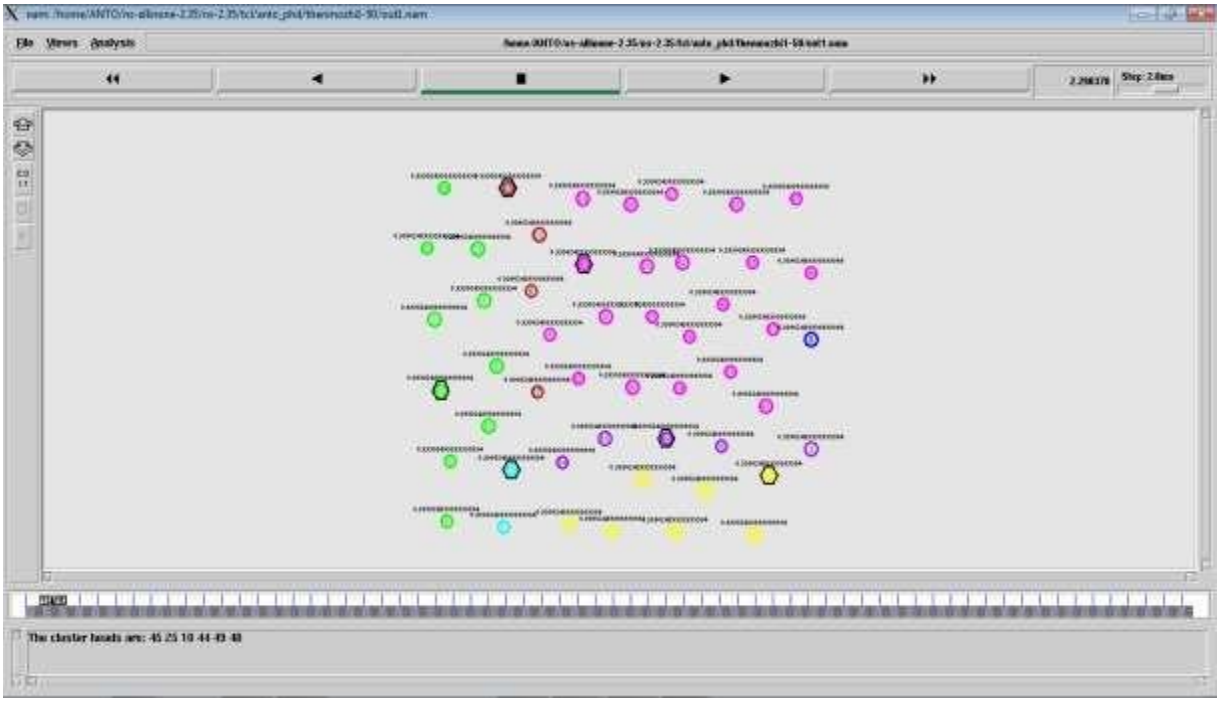


FIGURE 7.1D SNAPSHOT OF 50 NODES

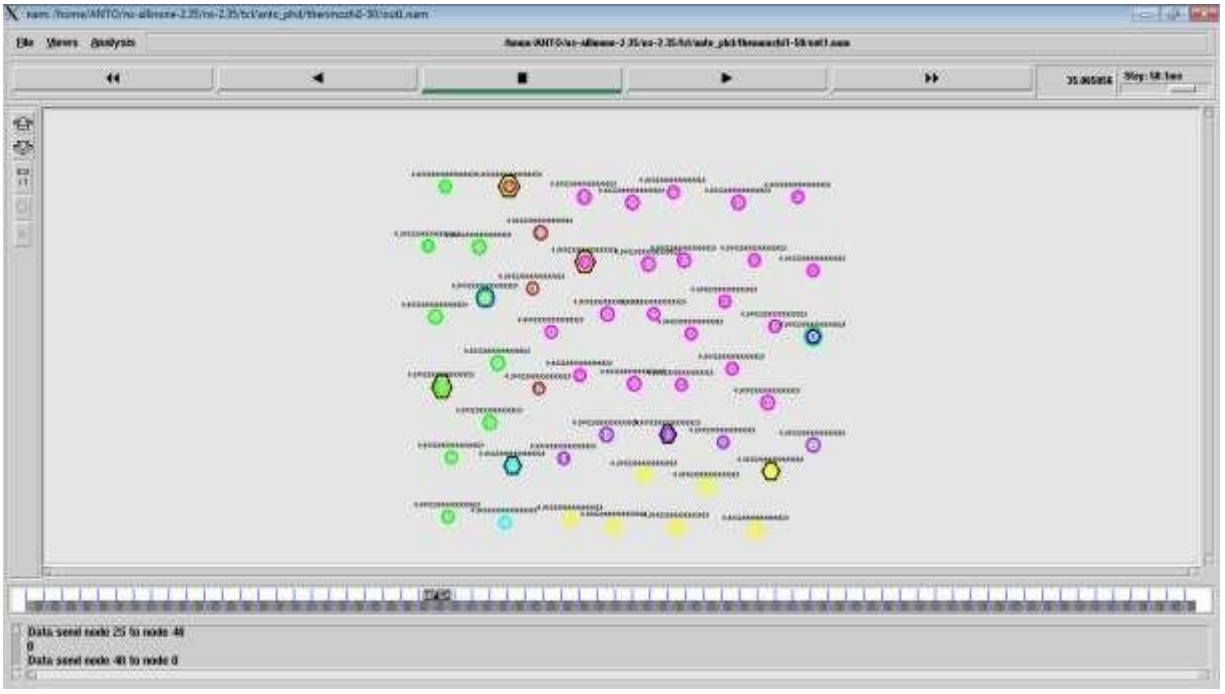


FIGURE 7.1E SNAPSHOT OF 50 NODES

The CH selection is depicted in Figure 7.1d. The transfer of data from source to destination is depicted in Figure 7.1e.

7.1.2 SIMULATION OF DCSC USING 70 NODES:

To assess the numerous simulation situations, the source and destination are dynamically provided as inputs one after the other. Routes are chosen based on the next hop selection made during the simulations.

The scenarios examined by the protocols for Random Way Point mobility simulations for the 70 nodes scenario are depicted in Figures 7.2 (a-e). In Figure 7.2a, 70 nodes are randomly distributed throughout the network. Figure 7.2b dynamic source and destination selection. The clustering process and CH selection are depicted in Figure 7.2c.

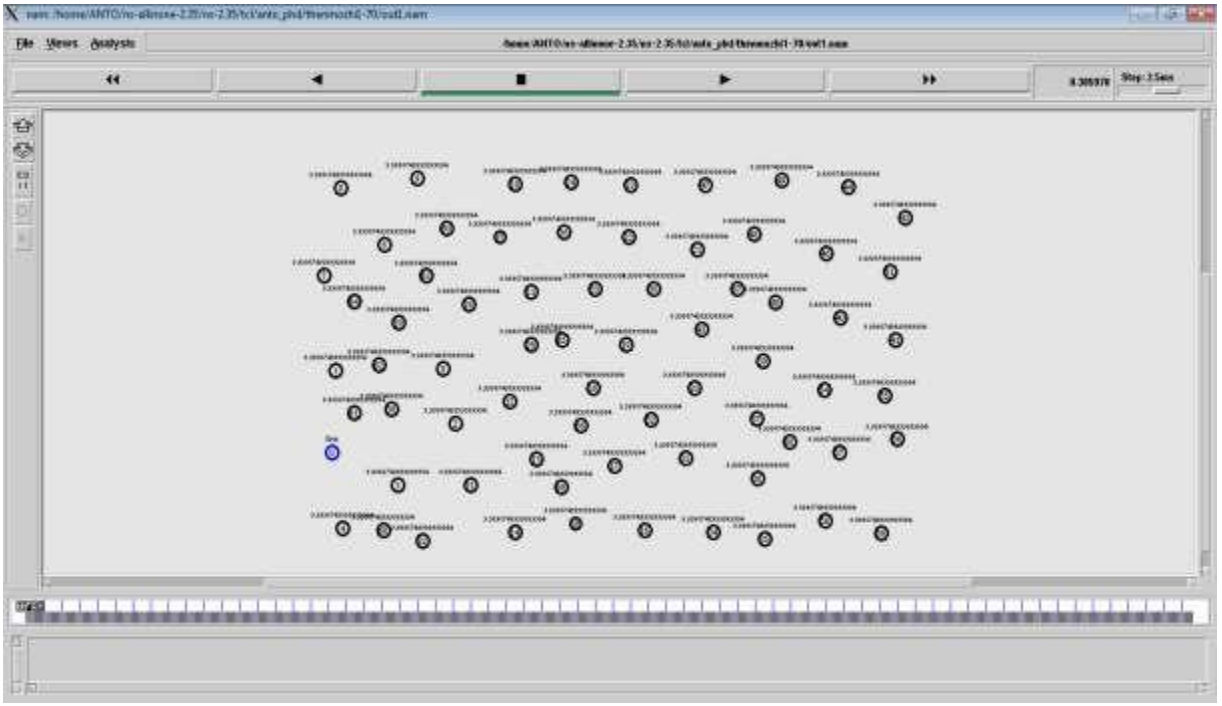


FIGURE 7.2A SNAPSHOT OF 70 NODES

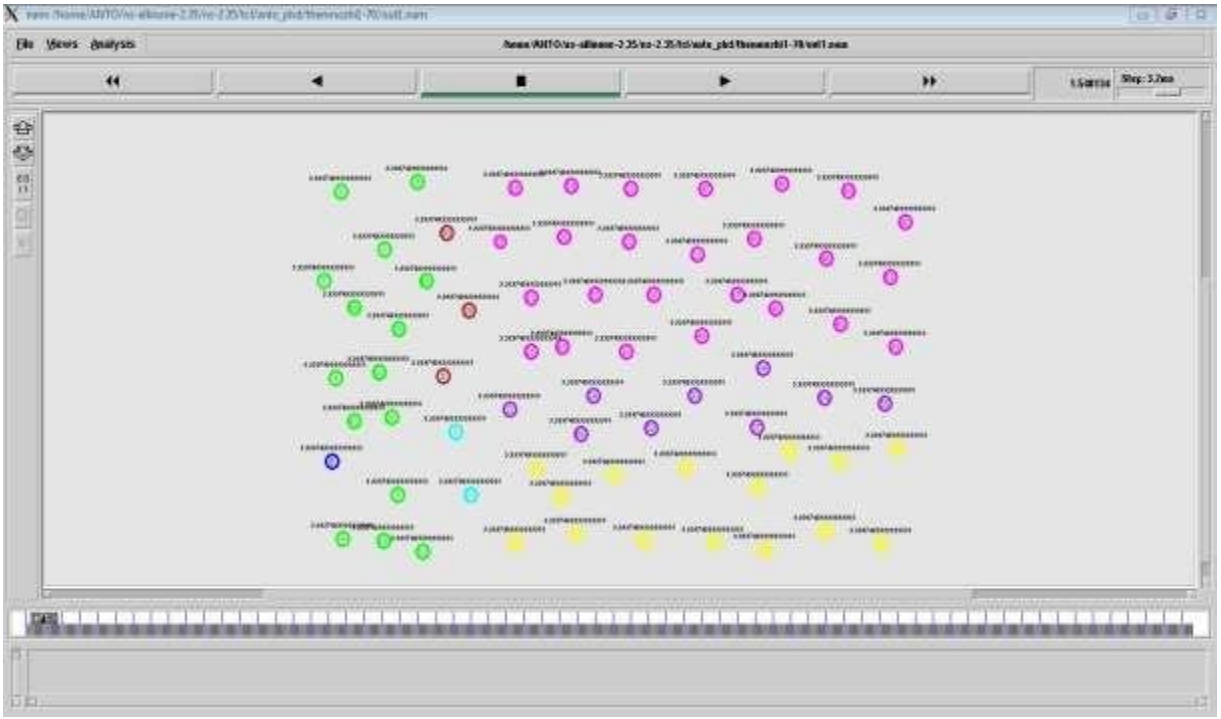


FIGURE 7.2B SNAPSHOT OF 70 NODES

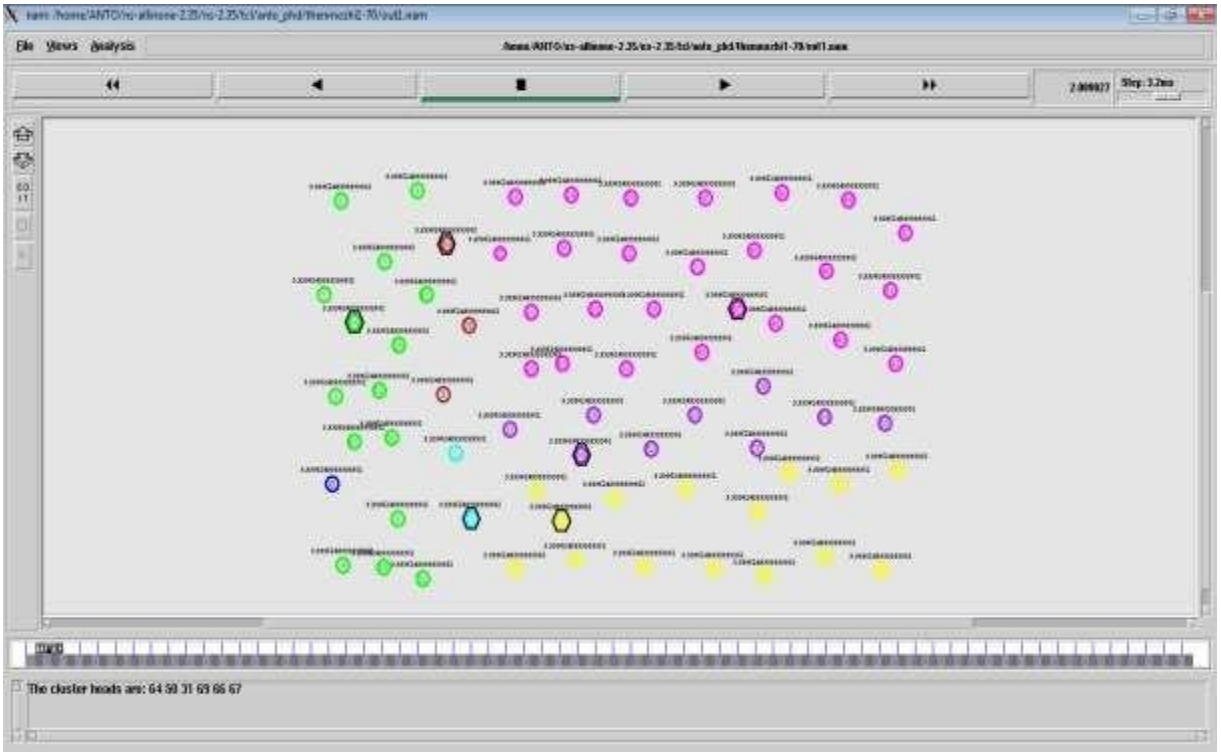


FIGURE 7.2C SNAPSHOT OF 70 NODES

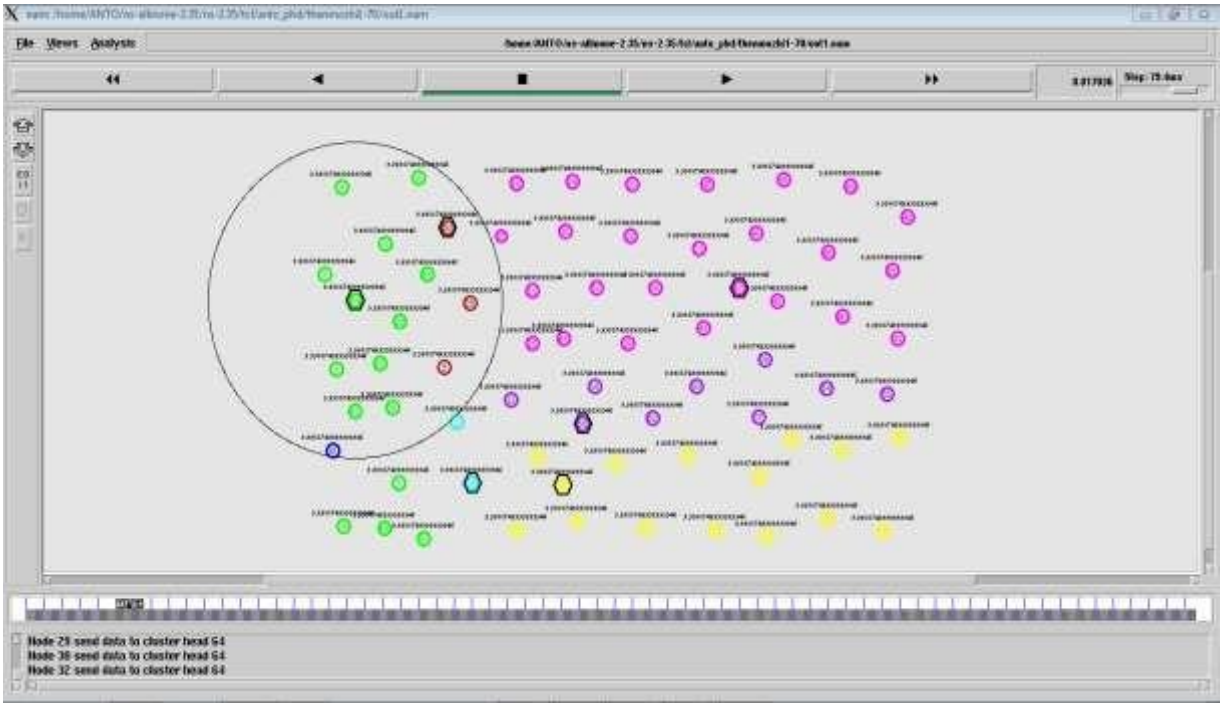


FIGURE 7.2D SNAPSHOT OF 70 NODES

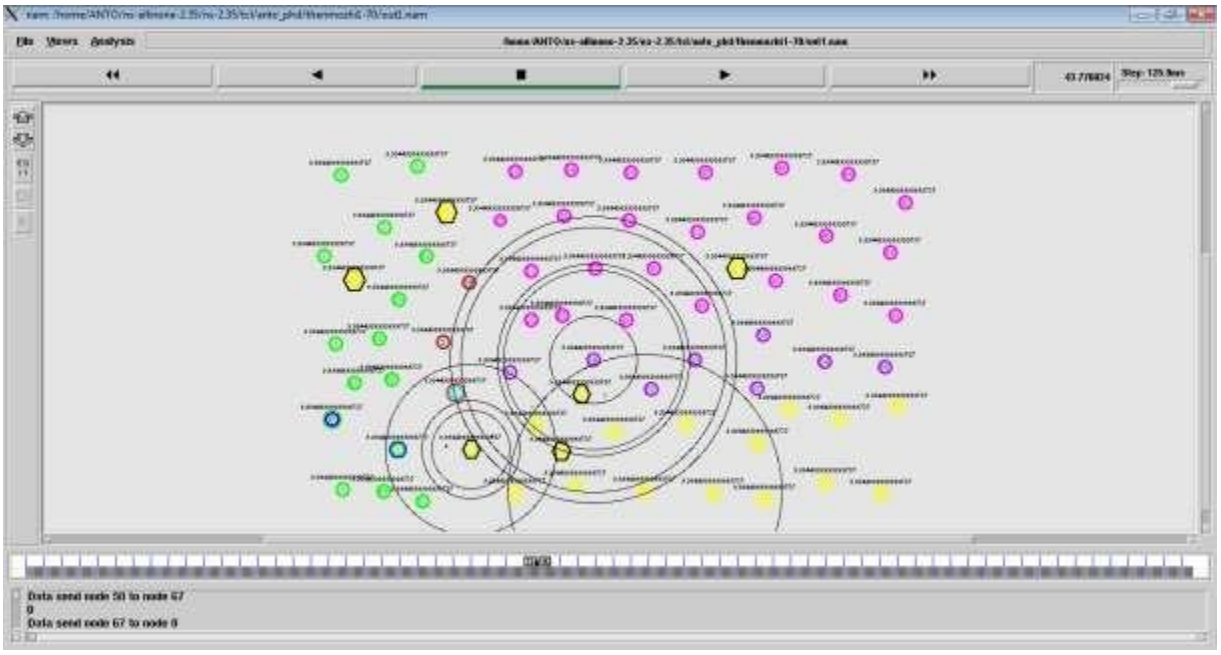


FIGURE 7.2E SNAPSHOT OF 70 NODES

Figure 7.2d depicts the data transmission from SNs to CH. Figure 7.2e displays the data transfer from source to destination in the communication network.

7.2 COMPARISONS OF METRICS:

The evaluation of a protocol is heavily reliant on the routing metrics of a network, given the protocol's ultimate goal is to transport data over it. As a result, the five primary parameters PDR, PLR, average delay, throughput, and residual energy are quantified in percentage terms.

7.2.1 PACKET DELIVERY RATE:

The PDR metric is used to calculate the success rate of data transmissions within a network. It is a critical measure for evaluating a network's performance. The figures 7.3 and 7.4 compare the PDRs of the four protocols TCSRS, DCSC, EECHDC, and EECSO for 50 and 70 nodes, respectively. When compared to all other protocols, EECSO clearly has a high PDR for 50 and 100 nodes.

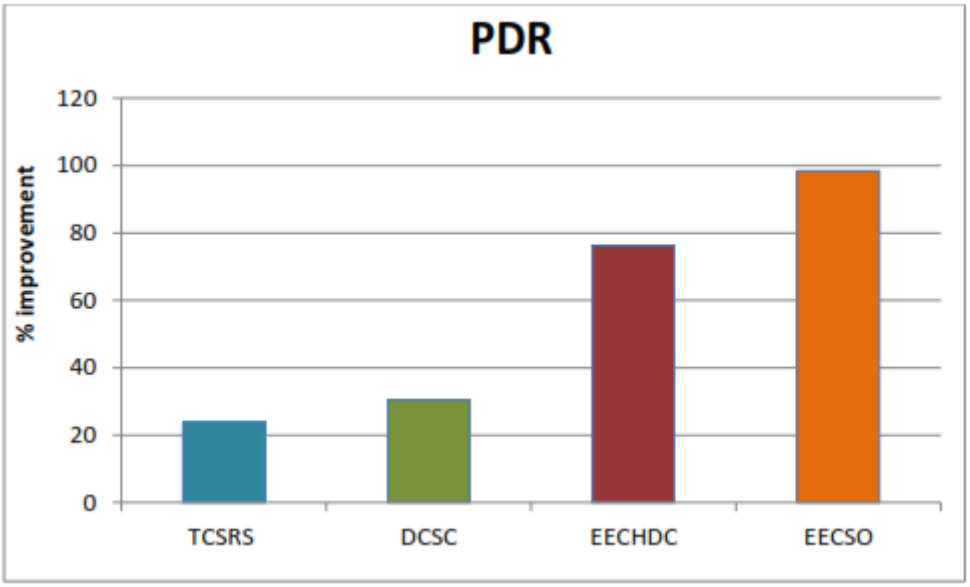


Figure 7.3 Packet Delivery Rate of TCSRS, DCSC, EECHDC and EECSO for 50 nodes

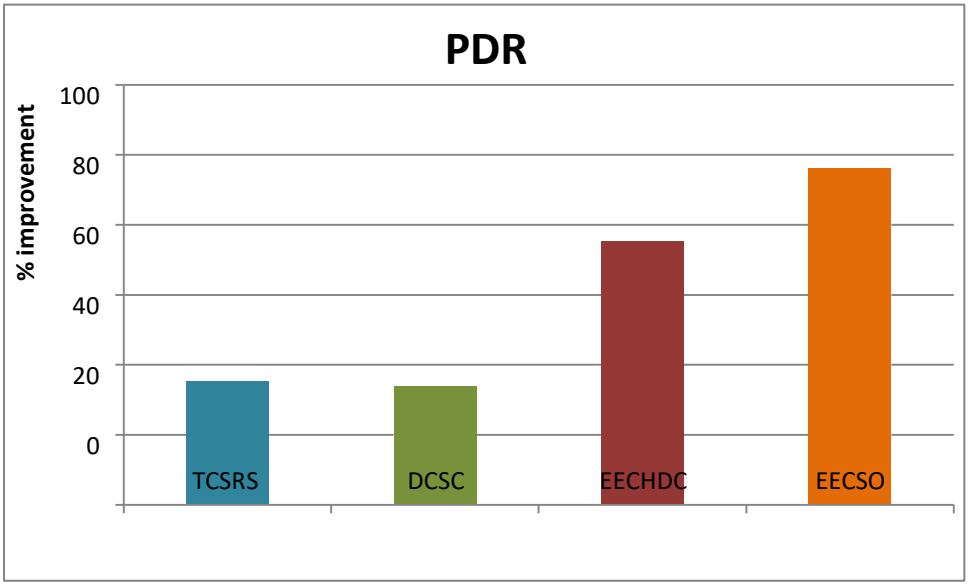


Figure 7.4 Packet Delivery Rate of TCSRS, DCSC, EECHDC and EECSO for 70 nodes

7.2.2 PACKET LOSS RATE:

The PLR identifies the number of packets lost during data transmission in a network. Additionally, the PLR aids in determining the routing protocols' network performance. The

figures 7.5 and 7.6 compare the PLR values for the TCSRS, DCSC, EECHDC, and EECSO protocols for 50 and 70 nodes, respectively.

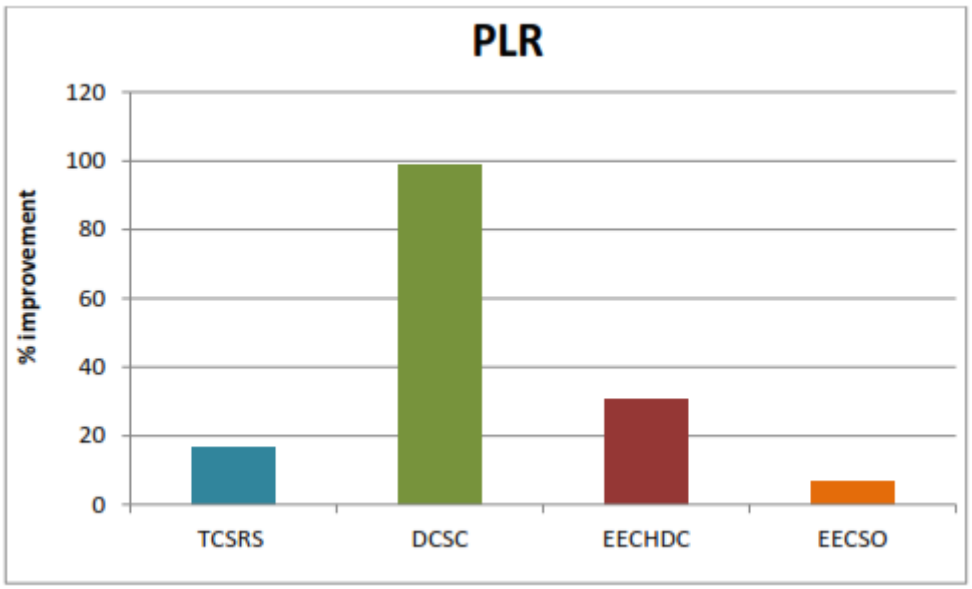


Figure 7.5 Packet Loss Rate of TCSRS, DCSC, EECHDC and EECSO for 50 nodes

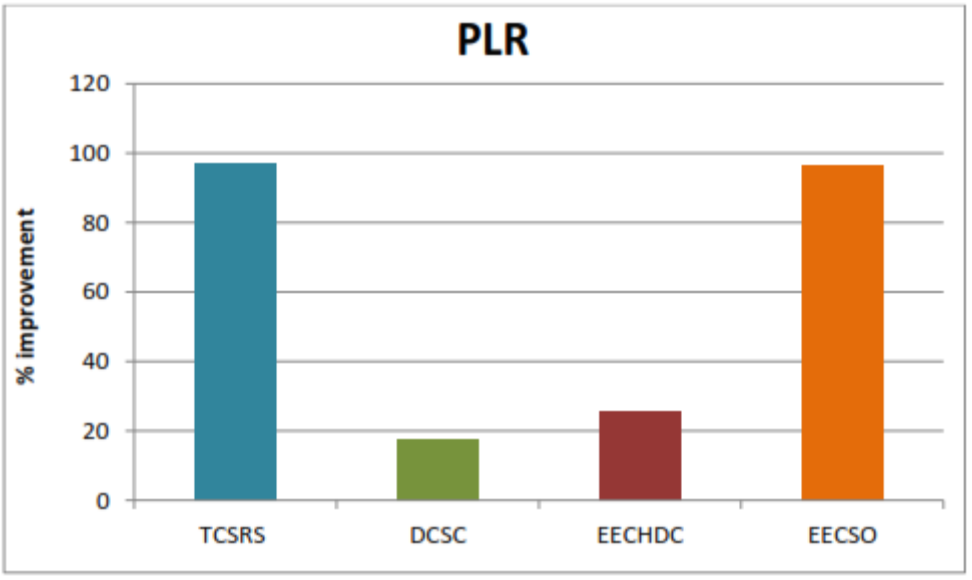


Figure 7.6 Packet Loss Rate of TCSRS, DCSC, EECHDC and EECSO for 70 nodes

Between 50 and 70 nodes, PLR is greater in the DCSC and TCSRS mechanisms. Due to the mechanism's obstacles and responses, there is a higher loss rate. For 50 and 70 nodes, EECSO and DCSC perform better in terms of packet loss rate.

7.2.3 AVERAGE DELAY:

The term "average delay" refers to the lag introduced by the data transmission process when the network's nodes communicate. The average time between various procedures in this research effort is depicted in Figures 7.7 and 7.8 for 50 and 70 node scenarios, respectively.

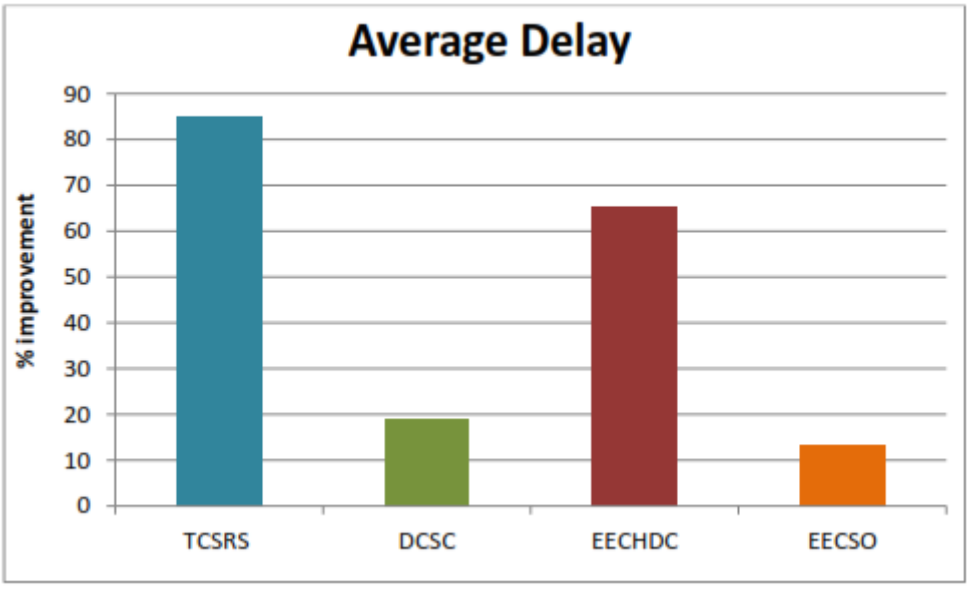


Figure 7.7 Average Delay of TCSRS, DCSC, EECHDC and EECSO for 50 Nodes

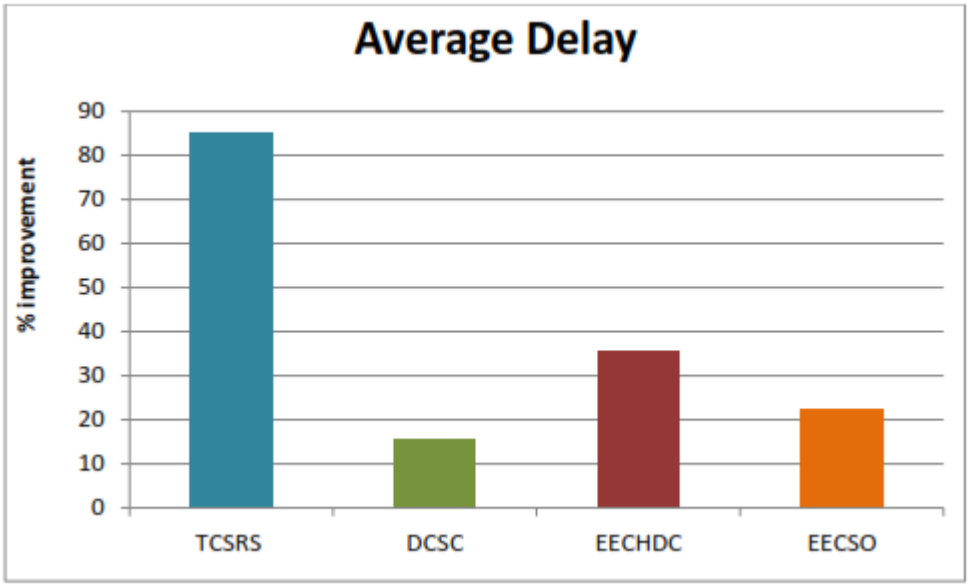


Figure 7.8 Average Delay of TCSRS, DCSC, EECHDC and EECSO for 70 Nodes

For 50 and 70 node cases, TCSRS has the longest delay. For 50 and 70 node cases, EECSO and DCSC offer the shortest delay.

7.2.4 THROUGHPUT:

The throughput of a network is defined as the total number of packets delivered to all destinations on the network. It is calculated for the TCSRS, DCSC, EECHDC, and EECSO protocols.

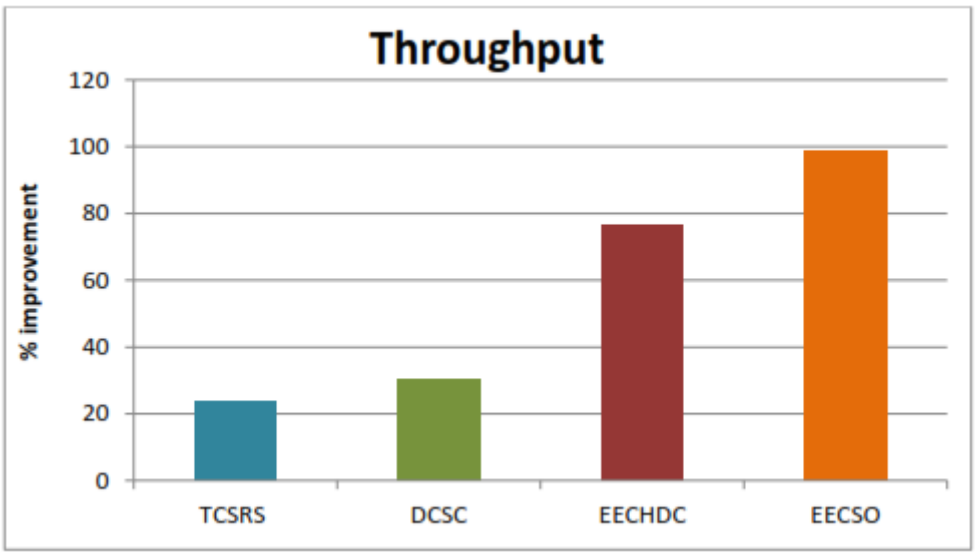


Figure 7.9 Throughput of TCSRS, DCSC, EECHDC and EECSO for 50 nodes

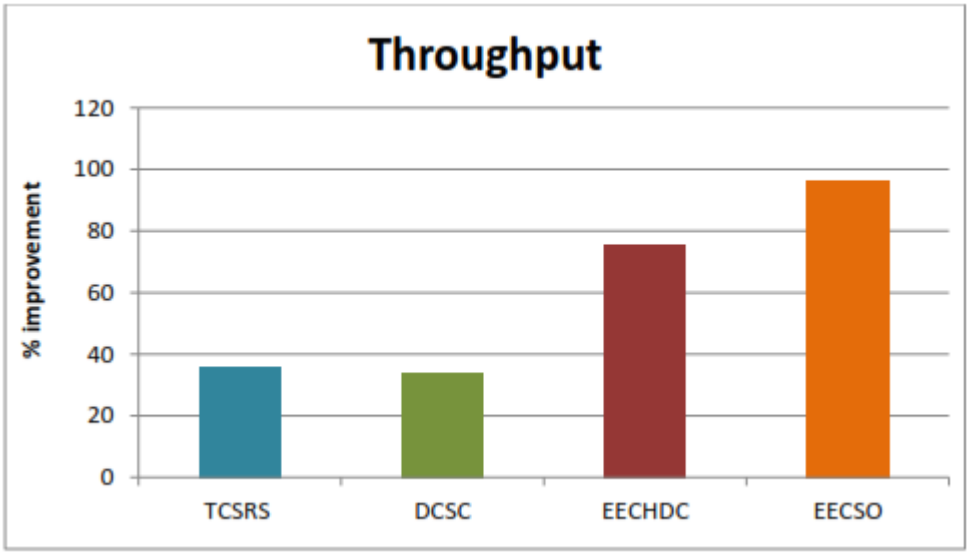


Figure 7.10 Throughput of TCSRS, DCSC, EECHDC and EECSO for 70 Nodes

The figures 7.9 and 7.10 compare the throughput values of the TCSRS, DCSC, EECHDC, and EECSO protocols at 50 and 70 nodes, respectively. EECSO protocol has a higher network throughput in both 50 and 70 node scenarios.

7.2.5 RESIDUAL ENERGY:

The quantity of energy remaining in a node at any point in time is referred to as residual energy. It is calculated for the TCSRS, DCSC, EECHDC, and EECSO protocols.

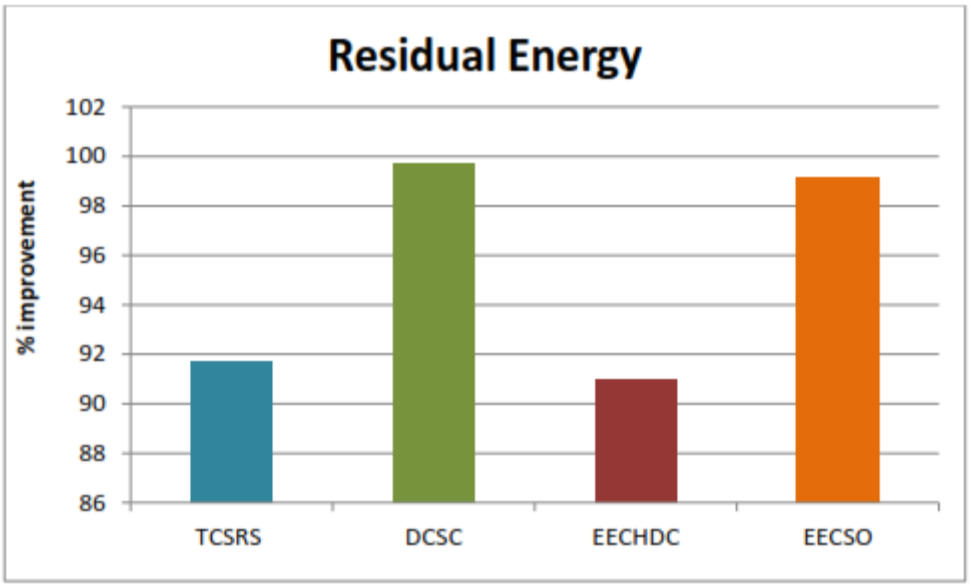


Figure 7.11 Residual Energy of TCSRS, DCSC, EECHDC and EECSO for 50 nodes

The figures 7.11 and 7.12 compare the residual energy values for the TCSRS, DCSC, EECHDC, and EECSO protocols at 50 and 70 nodes, respectively. For 50 and 70 node cases, the residual energy is larger for the DCSC protocol.

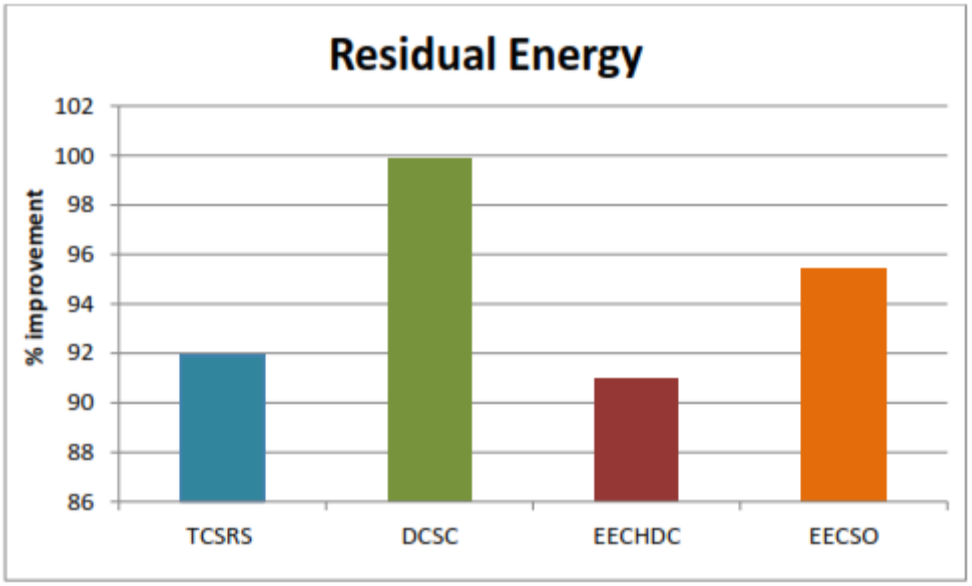


Figure 7.12 Residual Energy of TCSRS, DCSC, EECHDC and EECSO for 70 nodes

7.3 SUMMARY:

Each protocol proposed in this study effort is compared to its existing baseline protocol, along with the magnitude of improvement in each. Additionally, this section analyses the four protocols TCSRS, DCSC, EECHDC, and EECSO. EECSO has been shown to perform the best and so is more suitable for WSN critical monitoring applications.

CHAPTER 8

CONCLUSION AND SCOPE FOR FURTHER STUDY

8.1 CONCLUSION:

In Wireless Sensor Networks, Energy Efficient Cluster Head Selection is proposed and investigated in order to maximise throughput and packet delivery, which are critical components of effective communication. To accomplish the research objectives, four protocols have been devised and simulated in the NS2 tool for Wireless Sensor Networks. The protocols are as follows. I Trusted Clustering and Secure Routing (TCSRS) ii) Dominant Cluster Selection based on Credence (DCSC) iii) Energy Efficient Cluster Head Selection and Data Convening (EECHDC) iv) Energy Efficient Clustering Scheme Among Obstacles (EECSO) technique for wireless sensor networks (WSNs).

The simulation and analysis of the initial protocol TCSRS established the mechanism's superiority to the T-AODV. At each node, this scheme calculates the direct trust rating normalised to a fuzzy value between zero and one using a trust evaluation algorithm. The proposed method assessment resulted in a 33.72 percent increase in total packet delivery, 31.01 percent reduction in packet loss, 29.67 percent decrease in average delay, 31.72 percent increase in throughput, and 18.78 percent drop in residual energy, ensuring effective communication in wireless sensor networks.

The DCSC technique was simulated and examined, and the findings demonstrated that the suggested DCSC method is more efficient than the TCHE approach. The foundation for selecting trustworthy CHs is outlined in this section using a credence-based approach. The suggested DCSC mechanism increases total packet delivery by 47.72 percent, decreases packet loss by 59.89 percent, decreases average latency by 51.15 percent, increases throughput by 50.38 percent, and saves residual energy by 1.0 percent.

The EECHDC method was simulated, and the findings demonstrated that the EECHDC mechanism is more efficient than the ECSHA mechanism. The suggested EECHDC mechanism increases total packet delivery by 12.48 percent, reduces packet loss by 24.28 percent, reduces average latency by 20.6 percent, increases throughput by 12.48 percent, and saves residual energy by 3.38 percent.

The EECSO approach was simulated and examined using NS2, and the findings demonstrated the EECSO mechanism's superiority to the ADRC mechanism. The CH is chosen based on the quality factor determined by the link robustness, the node degree, and the energy. The suggested EECSO mechanism increases total packet delivery by 22.65 percent, reduces packet loss by 43.11 percent,

reduces average delay by 69.35 percent, increases throughput by 22.65 percent, and saves residual energy by 5.95 percent.

While the offered strategies are capable of adapting to dynamic changes, predicting the sensor network's life time boundaries is challenging. The energy level of the network is studied in isolation; predictability of the network must also be considered.

8.2 SCOPE FOR FURTHER STUDY

The system proposed in this study has a great deal of room for expansion. A multidisciplinary secure management scheme can be focused further to improve the system's precision and to avoid security softening the heterogeneous distant sensing systems sustainably. The messages that traverse the system's topology may overburden the CH, resulting in a bottleneck due to the additional message trades.

The integration of the Internet of Things (IoT) and sensor networks will be built on a set of open standards that will strive to provide scalability and dependability under a variety of operating situations and scenarios. However, the standards in their current state suffer from interoperability issues and should be improved further.

Thus, the future holds a more self-organized topological structure that is compliant with global suggestions in wireless sensor networks, resulting in the best execution in terms of meeting time, strength, and vitality of proficiency over the long haul. The analytical investigation to determine the primary weakness of the wireless sensor network environment in order to gain a better knowledge of the radio link and neighbourhood node dynamics is reserved for future research. Additionally, in the future, it is feasible to address the issue of interoperability between the two key standards - IEEE 802.15.4 for the access control layer and IEEE 802.11 for the transport layer.

References

[1] Abdullah, M.Y. and Hua, G.W. “Cluster-based security for wireless sensor networks”, In Communications and Mobile Computing, WRI IEEE International Conference on, Vol.3, pp.555-559, 2009.

[2] Adulyasas, A., Sun. Z. and Wang, N. “An event-driven clustering based technique for data monitoring in Wireless Sensor Networks”, in IEEE Conference on Consumer Communications and Networking, pp.653-656, 2013.

[3] Al-Karaki, J.N. and Kamal, A.E. “Routing techniques in wireless sensor networks: a survey”, IEEE wireless communications, Vol.11, No.6, pp.6-28, 2004.

[4] Al-Karaki, J.N., Ul-Mustafa, R. and Kamal, A.E. “Data aggregation in wirelesssensor networks-exact and approximate algorithms”, In High Performance Switching and Routing, IEEE HPSR, pp.241-245, 2004.

[5] Anderson, R., Chan, H. and Perrig, A. “Key infection: Smart trust for smart dust”, In Network Protocols, ICNP Proceedings of the 12th IEEE International Conference on, pp.206-215, 2004.

[6] Bandyopadhyay, S. and Coyle, E.J. “An energy efficient hierarchical clustering algorithm for wireless sensor networks”, 22nd Annual Joint Conference of the IEEE Computer and Communications, Societies, Vol.3, pp.1713-1723, 2003.

[7] Bohge, M. and Trappe, W. “An authentication framework for hierarchical ad hoc sensor networks”, In Proceedings of the 2nd ACM workshop on Wireless security, pp.79-87, 2003.

[8] Boubiche, D.E. and Bilami, A. “HEEP (Hybrid Energy Efficiency Protocol) based on chain clustering”, International Journal of Sensor Networks, Vol.10, pp.25-35, 2011.

[9] Braginsky, D. and Estrin, D. “Rumor routing algorithm for sensor networks”, In Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, pp.22-31, 2002.

[10] Bulusu, N., Heidemann, J. and Estrin, D. “GPS-less low-cost outdoor localization for very small devices”, IEEE personal communications, Vol.7, No.5, pp.28-34, 2000.

[11] Chen, B., Jamieson, K., Balakrishnan, H. and Morris, R. “Span: An energy- efficient coordination algorithm for topology maintenance in ad hoc wireless networks”, Wireless networks, Vol.8, No.5, pp.481-494, 2002.

[12] Chen, J., Zhang, H. and Hu, J. “An efficiency security model of routing protocol in wireless sensor networks”, In IEEE Second Asia International Conference on Modelling; Simulation (AMS), pp.59-64, 2008.

[13] Chen, W.P., Hou, J.C. and Sha, L. "Dynamic clustering for acoustic target trackingin wireless sensor networks", IEEE transactions on mobile computing, Vol.3, No.3, pp.258-271, 2004.

[14] Cheng, H.B., Geng, Y. and Hu, S.J. "NHRPA: a novel hierarchical routing protocol algorithm for wireless sensor networks", The Journal of China Universities of Posts and Telecommunications, Vol.15, No.3, pp.75-81, 2008.

[15] Clausen, T. and Jacquet, P., "Optimized link state routing protocol (OLSR)", No. RFC 3626, 2000.

[16] Ding, P., Holliday, J. and Celik, A. "Distributed energy-efficient hierarchical clustering for wireless sensor networks", In international conference on Distributed Computing in Sensor Systems, Springer Berlin Heidelberg, pp.322-339, 2005.

[17] Dixit, S.S. and Smol, J.P. "Diatoms as indicators in the environmental monitoring and assessment program-surface waters (EMAP- SW)", Environmental Monitoring and Assessment, Vol.31, No.3, pp.275-307, 1994.

[18] Doumit, S.S. and Agrawal, D.P.1 "Self-organizing and energy-efficient network of sensors", In Milcom, IEEE Proceedings, Vol.2, pp.1245-1250, 2002.

[19] Duarte-Melo, E.J. and Liu, M. "Analysis of energy consumption and lifetime of heterogeneous wireless sensor networks", In Global Telecommunications IEEE Conference, Vol.1, pp.21-25, 2002.

[20] Dutta, R., Paul, D., Gupta, S. and Das, M.K. "Comparison of Flooding and Gossiping Routing Protocols Using TOSSIM in Wireless Sensor Networks", IJCA, 2016.

[21] Fang, L., Du, W. and Ning, P. "A beacon-less location discovery scheme for wireless sensor networks", In 24th Annual Joint Conference of the IEEE Computer and Communications Societies, Proceedings, Vol.1, pp.161-171, 2005.

[22] Fang, Q., Zhao, F. and Guibas, L. "Lightweight sensing and communication protocols for target enumeration and aggregation", In Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing, ACM, pp.165-176, 2003.

[23] Faruque, J. and Helmy, A. "Gradient-based routing in sensor networks", ACM SIGMOBILE Mobile Computing and Communications Review, Vol.7, No.4, pp.50-52, 2003.

[24] Feng, R., Xu, X., Zhou, X. and Wan, J. "A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory", Sensors, Vol.11, No.2, pp.1345-1360, 2011.

[25] Feng, X., Ding, X. and Sun, S. “A security detection scheme based on evidence nodes in Wireless Sensor Networks”, In Biomedical Engineering and Informatics (BMEI), 6th IEEE International Conference on, pp. 689-693, 2013.

[26] Haas, Z.J. and Tabrizi, S. “On some challenges and design choices in ad-hoc communications”, In Proceedings of Military Communications Conference, IEEE MILCOM, Vol.1, pp.187-192, 1998.

[27] Heinzelman, W.B., Murphy, A.L., Carvalho, H.S. and Perillo, M.A. “Middleware to support sensor network applications”, IEEE network, Vol.18, No.1, pp.6-14, 2004.

[28] Heinzelman, W.R., Chandrakasan, A. and Balakrishnan, H. “Energy-efficient communication protocol for wireless microsensor networks”, In System sciences, IEEE Proceedings of the 33rd annual Hawaii international conference on, 2000.

[29] Heinzelman, W.R., Kulik, J. and Balakrishnan, H. “Adaptive protocols for information dissemination in wireless sensor networks”, In Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, pp.174-185, 1999.

[30] Hodge, V.J., O’Keefe, S., Weeks, M. and Moulds, A. “Wireless sensor networks for condition monitoring in the railway industry: A survey”, IEEE Transactions on Intelligent Transportation Systems, Vol.16, No.3, pp.1088- 1106, 2015.

[31] Ibriq, J. and Mahgoub, I. “A secure hierarchical routing protocol for wireless sensor networks”, In 10th IEEE Singapore International Conference on Communication Systems, pp.1-6, 2006.

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

[33] Ituen, I. and Sohn, G.H., “The environmental applications of wireless sensor networks”, International Journal of Contents, Vol.3, No.4, pp.1-7, 2007.

[34] Jimenez, F. and Torres, R. “Building an IoT-aware healthcare monitoring system”, In Chilean Computer Science Society (SCCC), 34th IEEE International Conference of the, pp.1-4, 2015.

[35] Johnson, D.B., Maltz, D.A. and Broch, J. “DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks,” Ad hoc networking, No.5, pp.139-172, 2001.

[36] Karlof, C. and Wagner, D. “Secure routing in wireless sensor networks: Attacks and countermeasures”, Ad hoc networks, Vol.1, No.2, pp.293-315, 2003.

[37] Kaur, N., Sharma, D. and Singh, P. "Classification of Hierarchical Routing Protocols in Wireless Sensor Network: A Survey", International Journal of P2P Network Trends and Technology, Vol.3, No.1, pp.56-61, 2013.

[38] Kim, Y.H., Han, Y.H., Mun, C.M., Park, C.Y. and Park, D.S. "Lifetime maximization considering connectivity and overlapped targets in wireless sensor networks", In Information Technology Convergence and Services, 2nd IEEE International Conference on, pp.1-6, 2010.

[39] Krishnamachari, B., Estrin, D. and Wicker, S. "Modeling data-centric routing in wireless sensor networks", In IEEE infocom, Vol.2, pp.39-44, 2002.

[40] Kulik, J., Heinzelman, W. and Balakrishnan, H. "Negotiation-based protocols for disseminating information in wireless sensor networks", Wireless networks, Vol.8, No.2/3, pp.169-185, 2002.

[41] Kumar, A. and Pahuja, S. "A Comparative Study of Flooding Protocol and Gossiping Protocol in WSN", International Journal of Computer Technology & Applications, Vol.5, No.2, pp.797-800, 2014.

[42] Lakhtaria, K.I. "Analyzing Zone Routing Protocol in MANET Applying Authentic Parameter", arXiv preprint arXiv:1012.2510, 2010.

[43] Langergraber, G., Fleischmann, N., Hofstaedter, F. and Weingartner, A., "Monitoring of a paper mill wastewater treatment plant using UV/VIS spectroscopy", Water science and technology, Vol.49, No.1, pp.9-14, 2004.

[44] Leu, J.S., Chiang, T.H., Yu, M.C. and Su, K.W. "Energy efficient clustering scheme for prolonging the lifetime of wireless sensor network with isolated nodes", IEEE communications letters, Vol.19, No.2, pp.259-262, 2015.

[45] Li, Q., Aslam, J. and Rus, D. "Hierarchical power-aware routing in sensor networks", In Proceedings of the DIMACS workshop on pervasive networking, 2001.

[46] Liao, Y., Qi, H. and Li, W. "Load balanced clustering algorithm with distributed self-organization for Wireless Sensor Networks", IEEE Sensors Journal, Vol.13, No.5, pp.1498–1506, 2013.

[47] Lindsey, S. and Raghavendra, C.S. "PEGASIS: Power-efficient gathering in sensor information systems", In IEEE Aerospace conference proceedings, Vol.3, 2002.

[48] Liu, X. "A survey on clustering routing protocols in wireless sensor networks", Sensors, Vol.12, No.8, pp.11113-11153, 2012.

[49] Lu, H., Li, J. and Guizani, M. “Secure and efficient data transmission for cluster-based wireless sensor networks”, IEEE transactions on parallel and distributed systems, Vol.25, No.3, pp.750-761, 2014.

[50] Manjeshwar, A. and Agrawal, D.P. “APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks”, In Proceedings of the International Parallel and Distributed Processing Symposium, Vol.2, 2002.

[51] Manjeshwar, A. and Agrawal, D.P. “TEEN: a protocol for enhanced efficiency in wireless sensor networks”, in Proceedings of the 1st International Workshop on Parallel and Distributed Computing. Issues in Wireless Networks and Mobile Computing, San Francisco, CA, 2001.

[52] Maraiya, K., Kant, K. and Gupta, N. “Efficient cluster head selection scheme for data aggregation in wireless sensor network”, International Journal of Computer Applications, Vol.23, No.9, pp.10-18, 2011.

[53] Messina, D., Ortolani, M. and Re, G.L. “A network protocol to enhance robustness in tree-based WSNs using data aggregation”, In IEEE International Conference on Mobile Adhoc and Sensor Systems, pp.1-4, 2007.

[54] Migabo, M.E., Djouani, K., Kurien, A.M. and Olwal, T.O. “Gradient-based Routing for Energy Consumption Balance in Multiple Sinks-based Wireless Sensor Networks”, Procedia Computer Science, Vol.63, pp.488-493, 2015.

[55] Mishra, S., Jena, L. and Pradhan, A. “Fault tolerance in wireless sensor networks”, International Journal, Vol.2, No.10, pp.146-153, 2012.

[56] Ni, M., Zhong, Z. and Zhao, D. “MPBC: A mobility prediction-based clustering scheme for ad hoc networks”, IEEE Transactions on Vehicular Technology, Vol.60, No.9, pp. 4549-4559, 2011.

[57] Ogier, R., Templin, F. and Lewis, M. “Topology dissemination based on reverse-path forwarding (TBRPF)”, No. RFC 3684, 2004.

[58] Oliveira, L.B., Ferreira, A., Vilaça, M.A., Wong, H.C., Bern, M., Dahab, R. and Loureiro, A.A. “SecLEACH - On the security of clustered sensor networks”, Signal Processing, Vol.87, No.12, pp.2882-2895, 2007.

[59] Oliveira, L.B., Wang, H.C. and Loureiro, A.A.F. “LHA-SP: secure protocols for hierarchical wireless sensor networks”, In Integrated Network Management, pp.31-44, 2005.

[60] Oliveira, L.B., Wong, H.C., Bern, M., Dahab, R. and Loureiro, A.A.F. "SecLEACH-A random key distribution solution for securing clustered sensor networks", In Fifth IEEE International Symposium on Network Computing and Applications, pp.145-154, 2006.

[61] Pal, V., Singh, G. and Yadav, R.P. "SCHS: Smart cluster head selection scheme for clustering algorithms in wireless sensor networks", Vol.4, pp.273- 280, 2012.

[62] Pei, G., Gerla, M. and Chen, T.W. "Fisheye state routing: A routing scheme for ad hoc wireless networks", In IEEE Communications, International Conference, Vol.1, pp.70-74, 2000.

[63] Pei, G., Gerla, M. and Hong, X. "LANMAR: landmark routing for large scale wireless ad hoc networks with group mobility", In IEEE Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing, pp.11-18, 2000.

[64] Perkins, C., Belding Royer, E. and Das, S. "Ad hoc on-demand distance vector (AODV) routing", No. RFC 3561, 2003.

[65] Perkins, C.E. and Bhagwat, P. "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers", In ACM SIGCOMM computer communication review, Vol.24, No.4, pp.234-244, 1994.

[66] Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V. and Culler, D.E. "SPINS: Security protocols for sensor networks", Wireless networks, Vol.8, No.5, pp.521-534, 2002.

[67] Rabin, M.O. "Efficient dispersal of information for security, load balancing, and fault tolerance", Journal of the ACM (JACM), Vol.36, No.2, pp.335-348, 1989.

[68] Razaque, A. and Elleithy, K.M. "Energy-efficient boarder node medium access control protocol for wireless sensor networks", Sensors, Vol.14, No.3, pp. 5074-5117, 2014.

[69] Romer, K. and Mattern, F. "The design space of wireless sensor networks", IEEE wireless communications, Vol.11, No.6, pp.54-61, 2004.

[70] Sadananda, P., Trojet, W. and Mouzna, J. "Multicast Authentication Framework for Hierarchical Networks using Chinese Remainder Theorem", International Journal of Computer Applications, Vol.82, No.11, 2013.

[71] Sebastian, A., Stephen R.K. and Patra, D.P. "A Secured Load Balanced Clustering Algorithm for Wireless Sensor Network", International Journal of Research in Computer and Communication Technology, Vol.3, No.4, pp.517- 520, 2014.

[72] Shen, C.C., Srisathapornphat, C. and Jaikaeo, C. "Sensor information networking architecture and applications", IEEE Personal communications, Vol.8, No.4, pp.52-59, 2001.

[73] SK, S. and KC, G. “Evaluation of Routing Protocols for Wireless Sensor Networks”, IJRCCT, Vol.2, No.6, pp.322-328, 2013.

[74] Slijepcevic, S., Potkonjak, M., Tsiatsis, V., Zimbeck, S. and Srivastava, M.B. “On communication security in wireless ad-hoc sensor networks”, In Enabling Technologies: Infrastructure for Collaborative Enterprises, IEEE Proceedings, Eleventh IEEE International Workshops on, pp. 139-144, 2002.

[75] Sohrabi, K., Gao, J., Ailawadhi, V. and Pottie, G.J. “Protocols for self- organization of a wireless sensor network”, IEEE personal communications, Vol.7, No.5, pp.16-27, 2000.

[76] Song, D. “Probabilistic modeling of leach protocol and computing sensor energy consumption rate in sensor networks”, Texas A & M University, 2005.

[77] Srinath, R., Reddy, A.V. and Srinivasan, R. “Ac: Cluster based secure routing protocolfor wsn”, In Networking and Services, ICNS IEEE Third International Conference on, pp.45-45, 2007.

[78] Subramanian, L. and Katz, R.H. “An architecture for building self- configurable systems. In Mobile and Ad Hoc Networking and Computing”, First IEEE Annual Workshop on, pp.63-73. 2000.

[79] Sung-Ho, L.E.E. and Yong-Jin, P.A.R.K. “A cluster head selection algorithm adopting sensing-awareness and sensor density for wireless sensor networks”, IEICE transactions on communications, Vol.90, No.9, pp.2472-2480, 2007.

[80] Syed, S.S.A. and Kumaran, T.S. “An energy efficiency distributed routing algorithm based on HAC clustering method for WSNs”, Indian Journal of Science and Technology, Vol.7, No.S7, pp.66-75, 2014.

[81] Tabassum, N., Urano, Y. and Haque, A.M.A. “GSEN: An efficient energy consumption routing scheme for wireless sensor network”, In IEEE International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006.

[82] Tarhani, M., Kavian, Y.S. and Siavoshi, S. “SEECH: Scalable energy efficient clustering hierarchy protocol in wireless sensor networks”, IEEE Sensors Journal, Vol.14, No.11, pp.3944-3954, 2014.

[83] Tilak, S., Abu-Ghazaleh, N.B. and Heinzelman, W. “A taxonomy of wireless micro-sensor network models”, ACM Sigmobile Mobile Computing and Communications Review, Vol.6, No.2, pp.28-36, 2002.

[84] Tubaishat, M., Yin, J., Panja, B. and Madria, S. “A secure hierarchical model for sensor network”, ACM Sigmod Record, Vol.33, No.1, pp.7-13, 2004.

[85] Varalakshmi, P., Nandakumar, R. and Umadevi, M. “An Efficient Cluster HeadSelection and Aggregation for Wireless Sensor Networks”, In Communications and Signal Processing, IEEE International Conference on, pp.1318-1321, 2014.

[86] Wang, Y. “Topology control for wireless sensor networks”, in Wireless Sensor Networks and Applications, Springer US, pp.113-147, 2008.

[87] Wu, D., Hu, G. and Ni, G. “Research and improve on secure routing protocols inwireless sensor networks”, In IEEE Circuits and Systems for Communications, 4th IEEE International Conference on, pp.853-856, 2008.

[88] Xiao, D., Wei, M. and Zhou, Y. “Secure-spin: Secure sensor protocol for information via negotiation for wireless sensor networks”, In Industrial Electronics and Applications, 1st IEEE Conference on, pp.1-4, 2006.

[89] Xu, Y., Heidemann, J. and Estrin, D. “Geography-informed energy conservation for ad hoc routing”, In Proceedings of the 7th annual international conference on Mobile computing and networking, ACM, pp.70- 84, 2001.

[90] Yadav, L. and Sunitha, C. “Low Energy Adaptive Clustering Hierarchy in Wireless Sensor Network (LEACH)”, International Journal of Computer Science and Information Technologies, Vol.5, No.3, pp.4661-4664, 2014.

[91] Yao, Y. and Gehrke, J. “The cougar approach to in-network query processing in sensor networks”, ACM Sigmod record, Vol.31, No.3, pp.9-18, 2002.

[92] Ye, F., Luo, H., Cheng, J., Lu, S. and Zhang, L. “A two-tier data dissemination model for large-scale wireless sensor networks”, In Proceedings of the 8th annual international conference on Mobile computing and networking, ACM, pp.148-159, 2002.

[93] Ye, M., Li, C., Chen, G. and Wu, J. “EECS: an energy efficient clustering scheme in wireless sensor networks”, 24th IEEE International Performance, Computing, and Communications Conference, pp.535-540, 2005.

[94] Ye, W., Heidemann, J. and Estrin, D. “An energy-efficient MAC protocol for wireless sensor networks”, Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE Proceedings, Vol.3, pp.1567- 1576, 2002.

[95] Yi, S., Heo, J., Cho, Y. and Hong, J. “PEACH: Power-efficient and adaptive clustering hierarchy protocol for wireless sensor networks”, Computer communications, Vol.30, No.14, pp.2842-2852, 2007.

[96] Younis, O. and Fahmy, S. “HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks”, IEEE Transactions on mobile computing, Vol.3, No.4, pp.366-379, 2004.

[97] Yu, Y., Govindan, R. and Estrin, D. “Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks”, 2001.

[98] Yuan, L., Zhu, Y. and Xu, T. “A multi-layered energy-efficient and delay- reduced chain-based data gathering protocol for wireless sensor network”, In Mechtronic and Embedded Systems and Applications, IEEE/ASME International Conference on, pp.13-18, 2008.

[99] Zhang, K., Wang, C. and Wang, C. “A secure routing protocol for cluster- based wireless sensor networks using group key management”, In 4th IEEE international conference on wireless communications, networking and mobile computing, pp.1-5, 2008.

[100] Zhou, Q. and Li, J. “Secure routing protocol cluster-gene-based for wireless sensor networks”, In First IEEE International Conference on Information Science and Engineering, pp.4098-4102, 2009.

Annexure – I

List of Publications

Journals

1. Rakesh Kumar Singh, Ajay Kumar Bharti ,"An Analytical Study on Variants of LEACH Protocol, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-10, August 2020

Conferences

2. Rakesh Kumar Singh, Ajay Kumar Bharti , "Computational Intelligence in WSN for Network Life Optimization ", 3rd International Conference on Advanced Computing and Software Engineering (ICACSE- 2021),February 19-20,2021

An Analytical Study on Variants of LEACH Protocol

Rakesh Kumar Singh[1] , Dr Ajay Kumar Bharti[2]

Abstract: ***There are many remote areas where traditional computer networks cannot render services due to unavailability of infrastructure. Among these infrastructure less networks, most popular choice for researchers are wireless sensor network in the modern era. Wireless Sensor networks perform the communication in remote areas where it is difficult to deploy the layout of network. Clustering hierarchy (LEACH) protocol is still a landmark as energy saving protocol for the researchers of wireless sensor network (WSN) even after 20 years of its existence. Since its inception, many modifications of LEACH protocol have been proposed. All the routing protocols have been divided into two categories namely single hop and multi hop scenarios. In this paper, we studied and surveyed various LEACH based routing protocols presented by researchers so far and discussed the advantages and functioning of them in comparison to LEACH protocol. The paper also discusses the merits and demerits of different successors of LEACH. In the end, paper concludes with future research directions in the Wireless sensor network area.***

INDEX TERMS: ***LEACH, single hop and multi hop, Wireless Sensor Network, Clustering, Cluster Head, Routing protocol.***

I. INTRODUCTION

"A Wireless Sensor Network (WSN) is a collection of large numbers of autonomous sensor nodes with limited sensing ability, battery power, computing and communication capabilities." There are one or more than one base stations and many tiny sensor nodes deployed in the close proximity around them. Sensor nodes transmit the data packets and base stations receive them for the sake of forwarding it to external world. WSN has wide application prospects, for example, temperature, pressure, dampness, territory observing, calamity, military observation, backwoods fire-following, security reconnaissance, Underwater, Underground, agriculture and a lot more [21]–[23].Sensors are deployed in large/small areas in remote places, where infrastructure laydown is cumbersome. There may be one or more than one Base Stations. The selection of accurate routing protocol has a great impact in the delivery of gathered data from source to the BS node. The routing technique used in WSN should ensure low energy dissipation as battery change in sensors are rarely possible. Research community has proposed a large number of power-efficient routing methods developed for stationary and mobile WSN, based on the usage and size of network. Design of a routing protocol in wireless sensor network

Rakesh Kumar Singh[1] , Research Scholar, Department of Computer Science, Maharishi University of Information Technology Lucknow(UP),India, Email:rksingh@knit.ac.in

Dr Ajay Kumar Bharti[2], ProfESSOR, Department of Computer Science,Maharishi University of Information Technology Lucknow(UP),India, Email:ajay_bharti@hotmail.com

network is a difficult task, due to low computational power, low bandwidth, self-organization and computational overheads.

As indicated by Pantazis et al. [23], routing methods might be ordered on four factors to be specific network system structure, topology, correspondence model and dependable routing plan. On the deployment premise, the network system structure plan can be additionally categorized into two sorts: flat and hierarchical schemes. With respect to as flat routing conventions are concerned, all sensor nodes have same functionalities in the system. Among flat routing plans, Flooding and Gossiping [24], Directed dissemination [25], Rumor [26], SPIN [27] are some popular routing plans. These kinds of networks are not scalable, as they are more suitable for small area networks. Hierarchical routing is capable to achieve more power efficiency and scalability on the basis of its architecture. The whole network is divided into clusters called as nodes. Among those nodes, some nodes are chosen as important entities called cluster heads (CHs), who performs the task of receiving, aggregation and compression of the information collected from member nodes. Ultimately CHs communicate the compressed data to Base Station. As cluster head offers extra types of assistance to different nodes in the cluster, it dissipates more power when contrasted with different nodes of the cluster. To balance the overall energy consumption, Cluster Heads should be rotated periodically deployed inside a cluster. Heinzelman et al. [28] proposed first hierarchical routing plan known as LEACH. A plenty of hierarchical clustering protocols have been presented around the LEACH as the primary routing protocol. Popular hierarchical clustering algorithms in WSNs are LEACH [28], HEED [29], PEGASIS [30], EECS [31], EEMC [32], TEEN [33], PANEL [34] and T-LEACH [35].

II. LEACH (LOW ENERGY ADAPTIVE CLUSTERING HIERARCHY) PROTOCOL

LEACH is a hierarchical cluster based routing protocol for WSN[14]. The primary goal of LEACH is to enhance the battery power efficiency by rotating CH selection through a random number generation technique. In LEACH, nodes are organized into local clusters. LEACH operates through several rounds and each round is comprised of two phases: set-up and steady-state [1,2]. In former phase, every sensor node generates a random number in the range 0 to 1, and makes the comparison with threshold value. If the generated number falls below the threshold value $T(n)$ then that node declares itself as

cluster head. At the point when a node is chosen as the cluster head, it communicates the message to all other sensor nodes. Sensor nodes decide to join a CH based on the RSSI (received signal strength indicator) of the message for present round and communicates a join message to concerned CH. When the group head gets demand message originating from a hub, CH declares node as its member node and records node's ID. Now each sensor nodes have information about their CH and cluster it belongs to. Once the cluster is formed, each cluster head generates a TDMA schedule table and broadcasts it to their cluster members. All member nodes get their time slot for communication. At the time when each sensor node realizes its TDMA plan, at that point set-up stage is finished and the consistent state stage begins. In steady-state phase, transmissions of gathered data are performed, from cluster nodes to the CHs and then CHs to the base station. Sensor nodes will send their data to CH as per plan of the TDMA schedule. CH will remove the redundancy of all accepted information sent by their member nodes and send them to base station. TDMA schedule table is also used in data transfer from the source CH to destination BS[18]. CH uses correlated data by applying data aggregation technique, which reduces energy consumption[19] due to eliminated data duplication. LEACH protocol uses clustering which poses less data transmission between member nodes and the base station, hence increasing the longevity of the network. Each member node sends their data in their time slot and other time they remain in sleep mode. The TDMA plan decreases the collision of information sent by member sensor nodes. Selection of cluster head is random. LEACH does not consider node energy for the election of CH, which forces some nodes to die early. Random distribution of nodes degrade the performance of this protocol, as in some clusters, CHs may be located at boundaries of the clusters. Those cluster heads which are far away from the base station, expend more battery power in contrast with those CHs which are close to the BS. Unnecessary energy consumption by high frequency of re-clustering may make LEACH a bad choice for routing in WSN. Following section discusses various routing protocols in Wireless Sensor Networks

III. SINGLE HOP COMMUNICATION PROTOCOL

A. C-leach (Centralized Leach) Protocol

LEACH-C is a centralized clustering protocol in which CH selection and Cluster formation are performed by the base station. LEACH-C also solves the problem of Leach, in which selection of cluster head is based on random cluster formation[3]. In LEACH-C, cluster formation at the base station is made by a centralized algorithm. This protocol has two phases. In set-up phase, the remaining energy and location information value of all the sensor nodes is being sent to the BS in every round. The base station calculates the mean power of sensor nodes. The nodes having more vitality have progressively opportunity to turn into the cluster head. If the sensor nodes have higher residual energy than average, the base station finds a group of cluster heads from the set of nodes. Now base station broadcasts the cluster head groups to sensor nodes in network. If the sensor node's ID is found in the cluster head group it received, the node will work as a cluster head otherwise behave like a simple node. In steady-state phase, the CHs will send the TDMA schedule to all member nodes of their corresponding cluster members. Data transmission begins in all clusters on the basis of the TDMA schedule [1,2]. As CH selection and Cluster formation are performed by the BS, energy consumption of CH nodes get reduced in comparison to LEACH. Costly device is used to know about location information of sensor nodes which consume more energy. It is centralized, so less scalable and cannot cover large area.

B. Q-Leach (Quadrant Leach) Protocol

Q-LEACH protocol is a quadrant-based routing protocol. It is combination of Q-DIR routing techniques and LEACH protocol. We partition the network into four quadrants. Sensor nodes are equally disturbed in each quadrant and the CHs and their cluster members are placed in the same quadrant[4]. In setup phase, the network is divided into four quadrants. Sensor node chooses a random number between 0 and 1. If this number is less than threshold T(n), then that node will become CH for current round. This process is repeated for all quadrant. Received Signal Strength Indicator (RSSI) are used for clusters selection. After clustering in each quadrant, TDMA schedule is sent by CHs to their cluster members in respective quadrant. Every node communicates to CH at its idle time interval. In steady-state phase, cluster heads receive all data from their member nodes in one round first. Afterwards data is aggregated and compressed before sending it to BS. Now one round completes and next round starts for cluster heads selection. Q-leach chooses shortest routes between source and destination, so network lifetime also enhances. Q-LEACH is used for energy conservation but CHs are not selected on the basis of residual energy and the CH changes in every round. To address the problem of Q-leach, enhanced Q-leach is proposed[5]. For cluster head selection, it uses threshold residual energy and CH does not change in every round. If the residual energy of the CH is larger than threshold residual energy then the cluster head same for the after that round.

C. T-Leach (Threshold-based Leach) Protocol

In the paper presented by Hong et al. in [6], a threshold of residual energy is used for cluster head selection. In traditional leach, CHs are selected in all the rounds but in T-leach, cluster heads are fixed for some rounds. In set-up phase, clusters are formed with the help of residual power based cluster creation method for selecting cluster head and balancing energy consumption for all sensor nodes. Steady-

state phase is like traditional LEACH routing with one difference. If the current residual energy of cluster head is larger than threshold of residual energy then CH will be same for next round, otherwise, cluster head will change after current round. T-Leach protocol decreases cluster head selection and rotation cost. Threshold of residual energy is used for changing the CH which increase network lifetime, but main drawback of T-Leach is uneven energy consumption by sensor nodes[16].

D. TB-leach (Time-based Leach) Protocol

According to Junping et al.[7], TB-LEACH is distributed and time-based protocol to increase network lifetime. In this protocol, cluster head selected by time-based threshold, results in constant number of CHs. It consists set-up phase and steady state phase in every round. In set-up phase, A counter is used to get constant value of CHs. Every sensor node generates a random number and it checks its advertisement message when timer expires. If sensor node's value is less than constant value of CH then node becomes CH itself. Cluster formation is done using advertisement message and RSSI. Each CH sends TDMA schedule to their member nodes. In steady-state phase, first data transmission is performed from cluster members to cluster head, then after cluster head communicates the aggregated data to base station. Cluster formation is done without using global information. Using constant number of clusters, it improve network lifetime.

E. B-Leach (Balanced-Leach) Protocol

As indicated by tong et al.[8], B-LEACH is proposed to address the issue of uneven clusters of LEACH. Randomly generated value of cluster nodes and leftover energy of nodes, are utilized for choosing CH in this convention. It is ordered into rounds and each round spans over set-up and steady state phases. In set-up stage, a threshold value is chosen to decide the cluster head. A period span is determined by utilizing equation of t=k/e (where k speaks to a consistent factor and e speaks to remaining power of every node). In first round, Cluster heads are chosen by utilizing LEACH algorithm while cluster heads notify message and remaining energy to every other sensor nodes. If the number of selected cluster heads is less than n*p (where n is number of sensor nodes and p is probability of CHs), then some nodes are selected as cluster heads which have less time interval. If the number of selected cluster heads are larger than n*p, then some CHs which have less residual energy are discarded and make number of CHs equal to n*p. Discarded CHs are converted into normal nodes. Steady-state phase is same as LEACH protocol[16]. In B-LEACH, equal load balancing and CHs are selected using residual energy, which improves energy efficiency.

F. V-LEACH (Vice-leach) Protocol

According to sasikala et al. [9], vice leach protocol improve the network lifetime using a vice cluster heads. We use vice cluster heads when without completing data transmission of current round, cluster head is out of energy. In this protocol, every cluster has CH, vice-CH and member nodes. Set-up phase and steady-state phase are two phases of V-LEACH. In set-up phase, CHs selection and clusters formation are done using same technique as in LEACH. Vice CH in each cluster is selected based on higher remaining battery power of member nodes. In steady-state phase, data communication is exactly same like LEACH protocol. V-LEACH guarantees the success of data delivery and enhances lifetime of network but it has the limitation of less scalability and high complexity[14] .

IV. Multi-hop communication protocol

A. MH-Leach (Multi-hop Leach) Protocol

According to V.Biradar et al. [10], Multi-hop leach is extended version of LEACH, which addresses the limitation of LEACH. Communication model suggests that power dissipation is proportional to distance between source and destination. It is directly proportional to d^4 in case of large distance (more than the threshold value) in contrast to d^2, where d denotes the distance between transmitter and receiver. Multi-hop LEACH increases energy efficiency of the wireless sensor network using intermediate node between CH and BS to shorten the distance below threshold value. Like traditional LEACH, Multi-hop LEACH is also divided into several rounds like LEACH algorithm. In setup phase, selections of CHs and clusters formation are performed. Cluster formation is done using advertisement message and TDMA schedule is send to member nodes. In steady-state phase, cluster nodes send data to CH using TDMA schedule. If distance between CH and base station is far away, then CH chooses an intermediate node to send data to base station, otherwise sends data directly to BS[20]. Multi-hop transmission between CHs and the BS, increases energy efficiency of WSN and provide high scalability. Due to inclusion of the intermediate nodes, computational complexity and network overhead increase in MS-LEACH.

B. TL-Leach (Two-Level Leach) Protocol

V.Loscriet al.[11] presented the concept of leach with two-level hierarchy of clusters to enhance the transmission of packets and network lifetime. In this protocol, cluster heads at top level are called primary CHs and cluster heads at bottom level are called secondary CHs. Data transmissions are performed from member nodes to secondary CHs, secondary CHs to primary CHs and finally, primary CHs to Base station. Partial local calculations is done by cluster head at secondary level and complete local calculations are done by cluster head at primary hierarchy. The operation of this protocol consists of four phases; in first phase, advertisement message is sent from primary CHs to secondary CHs and secondary CHs to normal nodes. In second phase, primary CHs know about their member nodes (secondary CHs) using join message from secondary CHs to primary CHs. Normal nodes choose

their secondary CHs using join message. Clustering is performed in this phase. In third phase, the primary CHs send TDMA schedule and CDMA code to all cluster members at secondary level to transmit their data using this code and allotted time. Secondary CHs communicate this information to their member nodes. CDMA code and TDMA schedule are used by member nodes to transmit data. In fourth phase, Secondary CHs send aggregated data to primary CHs, finally primary CHs send data to base station. Even consumption of energy by nodes within same cluster, extend the lifetime of a sensor network. This protocol is suitable for large area in contrast to LEACH and LEACH-C.

C. Orphan-Leach

According to Jerbi et al. [12], this protocol allows the orphan nodes for transmission of data. Orphan nodes[17] are those sensor nodes which does not belong to any cluster. A member node of cluster acts as a gateway for orphan nodes. Orphan nodes send their data to gateway member node. This protocol is categorized into two phases: set-up phase and steady state phase. In set-up phase, cluster head selection and cluster formation are done using certain algorithm. Cluster head sends TDMA schedule to their member nodes. Gateway or member of cluster tells about orphan nodes to CH. CH also allots a number of TDMA slot for orphan nodes. Gateway broadcasts TDMA schedule to orphan nodes. Member nodes and orphan nodes send data simultaneously. In steady-state phase, transmission of data takes place. Orphan nodes or neighboring members send their data to gateway. Gateway node aggregates the received data and sends it to their cluster head. CH collects data from their member and gateway nodes, removes the redundancy and ultimately sends to sink node. In O-LEACH, more availability of data transmissions is achieved due to orphan nodes. Maximum connectivity rate is provided due to high coverage of network. Gateways consume some time for searching the orphan nodes. It suffers from delay in delivering data when large number of orphan nodes are in the network.

D. MR Leach (Multi-hop Routing Leach) Protocol

Authors farooq et al. [13] proposed MR- Leach for enhancing overall life of network and reducing the power dissipation. In this protocol, whole network is divided into different layers of clusters. Clusters formation are of same size at each layers and sensor nodes send data to base station through equal number of relay nodes. Cluster heads receive data from their members and send them to CHs at upper layers. CHs also act as relay nodes for cluster heads at lower layers to transmitting data to base station. MR-Routing protocol works in rounds and every round is further divided into set-up and steady state phase. In former phase, sensors nodes join those CHs who have higher residual energy and higher RSSI value. A time (TDMA) schedule is being issued by BS to each and every CH in the layers and cluster head to their member nodes. In steady state phase, data transmission is from lower layers to upper layers. In this protocol, network is like rooted tree where BS is root node, CHs are intermediate nodes and sensor nodes at lower layer are called leaf nodes. MH-Routing provides equal distribution of load among the nodes. Complexity and Overhead are high [14] due to complex computations because excessive number of TDMA schedules are communicated. In steady state phase, data transmission happens from lower layers to upper layers. Multilayer architecture makes it more scalable as compared to its counterparts.

V. CONCLUSION

Comparison of various LEACH variants of single hop and multiple hop has been presented in table-I. All the routing algorithms presented in section III and section IV, are categorized on the basis of parameters viz. clustering type, overhead in cluster head selection, computational complexity, scalability and battery power efficiency. LEACH is a routing protocol which follows distributed clustering but it is suitable for small networks only. As for as power consumption is concerned, LEACH performs better till all the sensor nodes have sufficient battery power. To overcome these problems, some variants of LEACH routing protocol have been proposed in section-III and section-IV. All the mentioned routing protocols are better to leach in some criteria like energy dissipation efficiency, CH selection method, scalability and fixation of clusters. The survey summarizes the following conclusion based on presented Table-I.

1. As for as clustering approach is concerned, all the algorithms except LEACH-C use distributed clustering pattern. LEACH-C is capable to do massive calculations as it is equipped with fixed infrastructure having enough power. It can run complex algorithms to achieve optimized energy efficiency and increased network lifetime.

2. Use of non-conventional energy resources may very useful since all the sensor nodes are power constrained. Only one protocol Solar-LEACH uses solar energy as power source while all other protocols avoid it due to extra hardware cost and bulk size.

3. Network coverage issue has not been discussed in any of the tabulated protocols. More attention is needed to address this area.

4. Most of the applications require sensor nodes to be static. However mobile nodes are needed for some applications like tracking of wild life behaviour. The prime challenge in this area is frequent topology change. More extensive research is to be carried out for the mobility of both, sensor nodes and base stations.

5. Many successors of LEACH protocol use GPS device for efficient location monitoring. Though the GPS equipment cost makes the sensor nodes expensive, most

of the routing algorithms are more comfortable to decrease the time complexity with the help of this device.

6. Security issues are not discussed in any of the listed routing algorithm. As the applications of WSN will increase, there will be more demand for security measures inclusion in these routing algorithms.

VI. Future Challenges

The major challenges in the design of a good routing algorithm, includes increased power efficiency and elevated network lifetime. To achieve these objectives, many variants of LEACH are proposed by researchers. Most of these successor algorithms are distributed in nature, scalable due to distributed approach and vast network size. In some cases, network scalability may not be achieved due to centralised approach. Prime goals of successors of LEACH protocol are mentioned as below:

- Optimal cluster head selection.
- Network coverage.
- Energy efficiency.
- Security aspect.
- Reliability of routing protocols.
- Fault tolerant algorithms.
- Uniform load distribution.
- Quality of service.
- Sensor node deployment strategy.
- Placement of base station to increase scalability.
- Quality of service

The reviewed literature points that design of a LEACH successor protocol is concerned with user's application area. Since more than two decades, various researchers have investigated different aspects of LEACH protocol but many domains are yet to be discovered.

WSN Protocol	Energy Efficiency	Scalability	Complexity	Overhead	Clustering
LEACH	Moderate	Low	Low	High	Distributed
LEACH-C	High	Low	Moderate	Low	Centralized
LEACH-Q	High	High	High	High	Distributed
LEACH-T	High	High	High	Moderate	Distributed
LEACH-TB	Moderate	Moderate	High	High	Distributed
LEACH-B	High	Low	High	High	Distributed
LEACH-V	Very High	Low	High	Very high	Distributed
LEACH-MH	High	High	High	Moderate	Distributed
LEACH-TL	High	Low	Low	Low	Distributed
LEACH-O	High	High	High	High	Distributed
LEACH-MR	High	High	High	Moderate	Distributed

Table- I: Comparison of Routing Protocols

References

1. W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," Wireless Communications, IEEE Transactions on, vol. 1, no. 4, pp. 660-670, 2002.
2. Amandeep Kaur, Er. Swaranjee Singh and Navjot Kaur, " Review of LEACH Protocol and Its Types," International Journal of Emerging Engineering Research and Technology Volume 3, Issue 5, May 2015, PP 20-25.
3. Amit parmar and Ankit Thakkar," An Improved Modified Leach-C Algorithm For Energy Efficient Routing Protocol In Wsn," Nirma Univeristy Journal Of Engineering And Technology Vol. 4, N0. 2, Jul-Dec 2015.
4. B. Manzoor, N. Javaid, O. Rehman, M. Akbar, Q. Nadeem, A. Iqbal and M. Ishfaq, "Q-LEACH: A New Routing Protocol for WSNs," International Workshop on Body Area Sensor Networks (BASNet-2013).
5. Deepa S., C. N. Marimuthu and Dhanvanthri V, "Enhanced Q-Leach Routing Protocol For Wireless Sensor Networks," ARPN Journal of Engineering and Applied Sciences, Vol. 10, No. 9, May 2015.
6. Jiman Hong, Joongjin Kook, Sangjun Lee, Dongseop Kwon and Sangho Yi, "T-LEACH: The method of threshold-based cluster head replacement for wireless sensor networks," Inf. Syst. Frontiers, vol. 11, no. 5, pp. 513_521, 2009.
7. H. Junping, J. Yuhui, and D. Liang, "A time-based cluster-head selection algorithm for LEACH," *IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2008, pp. 1172_1176.
8. M. Tong and M. Tang, "LEACH-B: An improved LEACH protocol for wireless sensor network," 6th Int. Conf. Wireless Commun.Netw. Mobile Comput. (WiCOM), Sep. 2010, pp. 1_4.
9. A. S. D. Sasikala and N. Sangameswaran, "Improving the energy efficiency of LEACH protocol using VCH in wireless sensor network," Int. J. Eng. Develop. Res., vol. 3, no. 2, pp. 918_924, 2015.
10. Rajashree.V.Biradar , Dr. S. R. Sawant, Dr. R. R. Mudholkar and Dr. V.C. Patil, " Multihop Routing In Self-Organizing Wireless Sensor Networks," IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 1, January 2011.
11. V. Loscrì, G. Morabito, and S. Marano, "A Two-Levels Hierarchy for Low-energy Adaptive Clustering Hierarchy (TL-LEACH)," Vehicular Technology Conference, 1988, IEEE 38th · October 2005.
12. Wassim Jerbi, Abderrahmen Guermazi and Hafedh Trabelsi, "O-LEACH: The problem of orphan nodes in the LEACH of routing protocol for wireless sensor networks,".
13. Muhamnmad Omer Farooq, Abdul Basit Dogar and Ghalib Asadullah Shah, "MR-LEACH: Multi-hop Routing with Low Energy Adaptive Clustering Hierarchy," 2010 Fourth International Conference on Sensor Technologies and Applications.
14. Kiran Jadav and Dhara Vadher, "A Comparative Study on Cluster Routing Based on leach in wireless sensor network" International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 03,2016.

15. B. Kishore Kumar Reddy, "A Design on Clustering Routing Protocol for Improving an Distributed Network Using Leach Protocol", International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 3, March 2014.
16. Kiranjot and Er. Manoj Kumar, "Review Paper on LEACH and Its Descendant Protocols in Wireless Sensor Networks", IJLTEMAS, Volume VI, 2017.
17. B. Gong, L. Li, S. Wang, and X. Zhou, "Multi-hop routing protocol with unequal clustering for wireless sensor networks", In ISECS International Colloquium on Computing, Communication, Control, and Management, CCCM '08., Vol. 2, 2008, pp. 552 -556.
18. W.R. Heinzelman, A. Chandrakasan, "Energy efficient Communication Protocol for Wireless Microsensor Networks", In: IEEE Computer Society Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS '00),Vol. 8, 2000, pp. 8020.
19. K. Maraiya, K. Kant, and N. Gupta, "Efficient Cluster Head Selection Scheme for Data Aggregation in Wireless Sensor Network," International Journal of Computer Applications, vol. 23, 2011.
20. J. Wang, X. Yang, Y. Zheng et al., "An Energy-Efficient Multi-hop Hierarchical Routing Protocol for Wireless Sensor Networks," International Journal of Future Generation Communication & Networking, vol. 5, no. 4, 2012.
21. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, ''Wireless sensor networks: A survey,'' *Comput. Netw.*, vol. 38, no. 4, pp. 393– 422, 2002. A. Abed, A. Alkhatib, and G. S. Baicher, ''Wireless sensor network architecture,'' in *Proc. Int. Conf. Comput. Netw. Commun. Syst. (CNCS)*, vol. 35. Singapore, 2012, pp. 11–15.
22. S. Pino-Povedano, R. Arroyo-Valles, and J. Cid-Sueiro, ''Selective forwarding for energy-efficient target tracking in sensor networks,'' *Signal Process.*, vol. 94, pp. 557–569, Jan. 2014.
23. N. A. Pantazis, S. A. Nikolidakis, and D. D. Vergados, ''Energy- efficient routing protocols in wireless sensor networks: A survey,'' *IEEE Commun. Surveys Tuts.*, vol. 15, no. 2, pp. 551–591, 2nd Quart. 2013.
24. Z. J. Haas, J. Y. Halpern, and L. Li, ''Gossip-based ad hoc routing,'' *IEEE/ACM Trans. Netw.*, vol. 14, no. 3, pp. 479–491, Jun. 2006.
25. C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, ''Directed diffusion for wireless sensor networking,'' *IEEE/ACM Trans. Netw.*, vol. 11, no. 1, pp. 2–16, Feb. 2003.
26. Braginsky and D. Estrin, ''Rumor routing algorthim for sensor networks,'' in *Proc. 1st ACM Int. Workshop Wireless Sensor Netw. Appl.*, New York, NY, USA, 2002, pp. 22–31.
27. J. Kulik,and H. Balakrishnan, ''Negotiation-based protocols for disseminating information in wireless sensor networks,''*Wireless Netw.*, vol.8, no.2, pp.169–185, 2002.
28. W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, ''Energy- efficient communication protocol for wireless microsensor networks,'' in *Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci*., vol. 2, Jan. 2000, p. 10.
29. O. Younis and S. Fahmy, ''HEED: A hybrid, energy-efficient, distributed clustering approach for adhoc networks,'' *IEEE Trans. Mobile Comput.*, vol. 3, no. 4, pp. 366–379, Oct. 2004.
30. S. Lindsey and C. S. Raghavendra, ''PEGASIS: Power-efficient gathering in sensor information systems,'' in *Proc. IEEE Aerosp. Conf.*, vol. 3. Mar. 2002, pp. 3-1125–3-1130.
31. M. Ye, C. Li, G. Chen, and J. Wu, ''EECS: An energy efficient clustering scheme in wireless sensor networks,'' in *Proc. 24th IEEE Int. Perform., Comput., Commun. Conf.*, Apr. 2005, pp. 535–540.
32. 32.Y. Jin, L. Wang, Y. Kim, and X. Yang, ''EEMC: An energy-efficient multi- level clustering algorithm for large-scale wireless sensor networks,'' *Comput. Netw.*, vol. 52, no. 3, pp. 542–562, 2008.
33. 33, A. Manjeshwar and D. P. Agrawal, ''TEEN: A routing protocol for enhanced efficiency in wireless sensor networks,'' in *Proc. 15th Int. Parallel Distrib. Process. Symp.*, Apr. 2000, pp. 2009–2015.
34. 34. L.Buttyán and P. Schaffer, ''Panel: Position-based aggregator node election in wireless sensor networks,''in *Proc. IEEE Int. Conf. Mobile Adhoc Sensor Syst.*, Oct. 2007, pp. 1–9.

Rakesh Kumar Singh is working as associate Professor in Computer Sc. and Engg. Department,Kamla Nehru Institute of Technology Sultanpur(UP)-India. He received M.E. from Jadavpur University, Kolkata. Currently he is pursuing his Ph.D. from MUIT Lucknow (up)-India. His area of interest is adhoc network, sensor network and ubiquitous computing.

Dr. Ajay Kumar Bharti is working as Professor in Computer Science department ,MUIT Lucknow -India. He received his MCA degree from KNIT Sultanpur and Ph.D. degree in 2014 from BBA University , Lucknow(up)-India. His research interest includes service oriented architecture Knowledge Based System, e-Governance and Artificial Intelligence.

Computational Intelligence in WSN for Network Life Optimization

Rakesh Kumar Singh[1]
Research Scholar, Dept. of Computer Science
Maharishi University of Information Technology
Lucknow (UP),India
Email: rksingh@knit.ac.in

Dr Ajay Kumar Bharti[2]
Professor, Department of Computer Science
Maharishi University of Information Technology
Lucknow (UP),India
Email: ajay_bharti@hotmail.com

Abstract*—Computational Intelligence (CI) have been increasingly used by researchers in past years to Solve difficult problems. The sensor networks are controlled by battery and in this way they end up being dead after a specific period. Thus, improving the information exchange in power effective way still stays challenge for expanding the life expectancy of sensor gadgets. It has been demonstrated that the clustering technique could upgrade the life expectancy of WSNs. In the clustering approach, the choice of right cluster head in each cluster has been observed as the most appropriate technique for energy efficiency, which limits the transmission delay in WSN. Much exploration has been done in the recent past to decide an ideal path among source and goal sensor nodes, which will bring about improving the battery power dissipation of a system. The challenge is to design a scheduling algorithm that thinks about the significant issues of limiting power consumption and boosting system lifetime. Different ways of optimization are accessible to decide a proper routing method between a source and sink node. This paper investigates various optimization tools for effective routing in WSN. This article gives us a glimpse of the past investigations in WSN field during the period of 2010–2020. The outcomes listed in this article will guide to research community for bridging the gap in the WSN field and to discover new exploration in this area.

Keywords: Optimization techniques · Routing in WSN · Energy efficiency · Cluster head · Delay

I. INTRODUCTION

WSN is playing a key job in remote or unattended kind of infrastructure less networks for the numerous applications, like checking the environment conditions, traffic tracking, observation in war zone, disaster event counteraction, health monitoring, clinical observations, weather and climate observing, Industrial monitoring and so on.([1], Akyildiz et al. 2002). Collecting the information from the sensor field, processing the data and communicating with other SNs are major activities performed by sensor nodes. WSN has constrained force with restricted limit with regards to processing. In some application, the energy can be renewed by external source, for example, solar based cells ([2] Want et al.2005). However it is not able to make uninterrupted power supply due to weather and energy dissipation are prime issues to be addressed for the betterment of throughput in different application areas. Clustering plans, which partition the network with the aid of grouping the nodes, plays an important job in keeping up the network topology in successful way. It is inescapable to create clustering algorithm, which is proficient in preserving energy for hauling out the range of the system. Information is imparted from SN (for example it's starting point) to the base station (BS) or sink by single hop or multi hop communication. Trial results display that communication is relatively costly than computing which is less energy consuming.([3] Raghunathan et al., 2002). Transmitters and receivers consume much more power to communicate information than the processing counterpart. The energy dissipated by the sensors to sense information from surrounding is very small as compared to communication and computing activities. Power preservation techniques focuses on two parts: activity of sensor node and the communication protocol employed. Amalgam of various procedures can be applied for extensibility of the sensor system lifetime ([4] Anastasi et al., 2009). Routing is probably the most difficult issue for which we can't utilize deterministic algorithms. Along this line, optimization calculations are utilized to introduce low cost routes among various possible routes. By actualizing Swarm Intelligence (SI) based calculations, different routing calculations have been created. SI can be thought of as a similarity between machine behaviour and nature driven conduct of the swarm. These swarm based intelligent calculations can possibly accomplish ideal solutions for real world tasks. Ant Colony Optimization (ACO), Particle swarm Optimization (PSO), Firefly algorithm (FA), Artificial Bee Colony (ABC), Fuzzy logic and Bacterial Foraging Optimization (BFO) are few examples of most famous routing methods. Here we have presented a review with respect to these strategies and look at them to figure out which procedures are progressively suitable as far as power utilization and system lifetime are concerned. In this survey, we additionally talk about different difficulties in routing methods of WSN and recognize approaches to address these difficulties

utilizing optimization strategies. The primary goal is to examine the present status of-the-art enhancement methods utilized in routing information by means of WSN and identify proficient methodologies for routing in a WSN. The remainder of the article is sorted out as follows:

In Section II, a portion from the current related work with respect to taken subject is talked about. Section 3 explains various techniques to lead this review, while Sect. 4 describes a comparison of these optimization methods. Segment 5 is comprised of discussions and future directions and at last, Section 6 concludes this work.

II. LITERATURE REVIEW

Zengin et al. [5] directed an overview where various routing strategies were examined to manage the issues of energy, expendability, intricacy, survivability and computational overhead. As indicated by this review, ant based methodology is viewed as a decent methodology and has pulled in numerous scientists than some other algorithm.

Parwekar et al. [6] gives investigation of enhancement strategies to WSN. They recognized few difficult issues as routing, node localization and clustering. These issues can't be solved using deterministic methodology. Hence optimization algorithms are increasingly reasonable for them. They give basic investigation of all optimization strategies and utilize this for future research.

Ali et al. [7] led a study on MANETs and WSNs dependent on swarm knowledge. They recognized that in loop free, power efficient and multi hop routing the “Ant Colony Optimization (ACO)” and “Particle Swarm Optimization (PSO)” give all the more encouraging outcomes. This article incorporates detailed examination of all methods for wired and wireless network and states that PSO and ACO beat the other routing protocols.

An overview on routing with a point of upgrading energy utilization was introduced by Saleh et al. [8]. This gives a complete overview of residual power centric convention in WSN. It gives an outline of significant sensor nodes’ attributes that are utilized in various routing methods. Diverse routing conventions that fall under ACO algorithm are discussed with their pros and cons.

A review on Swarm intelligence based scheduling convention in WSNs was led by Saleem et al. [9] , in which design and implementation plans are talked about. The point is to recognize viable optimization methods to discuss the issues of scalability, fault tolerant property and adaptability. They additionally give a few insights about swarm intelligence and its conceivable execution for communication in a WSN. A rundown of basic highlights is recognized to bring up the difficultiesin evaluation procedure and consider this for actualizing real-world implementation.

SGui et al. [10] led an overview on swarm based routing convention. They first introduced the properties of swarm intelligent methods, then after they investigated routing protocols to have new optimization method. They talk about the properties of “ant colony and spider monkey optimization”. They additionally discuss about the issues present in this approach and show future bearings.

Zungeru et al. [11] presented a survey by looking at “Swarm based routing” conventions with traditional routing protocols. Routing protocols are ordered as information driven, level based, geographic location based and Quality of service (QOS). Distinctive routing protocols are re-evaluated utilizing MATLAB based test system to see the outcomes and give a benchmark to future work.

Guo et al. [12] directed an overview of intelligent routing conventions in a WSN with a point of upgrading system lifetime. They talked about intelligent algorithms, for example, “Fuzzy Logic (FL), Reinforcement learning (RL), Neural Networks (NNs), and Genetic Algorithm (GA)”, to examine their behaviour regarding the system lifetime.

III. ROUTING IN WSN USING DIFFERENT OPTIMIZATION TECHNIQUES

A. Fuzzy logic based routing protocols

“Fuzzy Logic is a decision making control framework approach that fits usage in frameworks extending from straightforward, little, inserted smaller scale controllers to huge, organized, multi-channel PC or workstation-based information securing and control frameworks”. It may be actuated in hardware, software, or hybrid model. FL gives a straightforward method to arrive to a distinct end result dependent on dubious, questionable, uncertain, noisy, or missing information. FL's way to deal with control issues emulates how an individual would settle on choices a lot quicker. FL joins a straightforward, rule-based IF A AND B THEN C way to deal with a taking care of control issue instead of setting a framework mathematically. The FL model is observation based, depending on user's experience as opposed to their specialized technical knowledge of the framework. For instance, as opposed to managing temperature control in terms, for example, "BT =100F", "T <500F", or "20C <TEMP <200C", terms like "IF (process is too hot) AND (process is getting hotter) THEN (add coolant to the process)" or "IF (process is too cold) AND (process is cooling rapidly) THEN (add heat to the process quickly)" are used. These terms are loose but extremely descriptive of what should really occur. Consider what you do in the shower if the temperature is excessively cool, you will make the water agreeable rapidly with little difficulty. FL is fit for mirroring this kind of behaviour at exceptionally high rate. FL is comprised of two steps. A fuzzy membership-function is designed to generate the membership for

an input of a linguistic variable. The membership-function can be formulated in a precise manner to represent the needed output pattern of an objective-function. FL also offers a "fuzzy aggregation operator, Ordered Weighted Averaging (OWA)", to design a multi-objective cost function as an alternative. Normally, the "And-like" and "Or-like" OWA operators are used in FL. Control systems such as automobile systems, energy systems, image processing, pattern matching, home appliances, and elevators etc. are some applications where FL is very effective. FL is also suitable for optimized clustering and routing to find different objectives. Sometimes non-optimal solutions are generated. This issue can be resolved by re-learning of fuzzy rule base.

Gupta et al. [13] proposed a FL based FCH protocol to addresses cluster-head election for WSNs. In this approach, cluster-heads are selected by the sink node in each round. For each node, residual power, node density and nodes' intra cluster distance are considered as inputs to evaluate the criteria to be the cluster head. Node density is calculated as number of nodes by which the concerned node is surrounded, and intra cluster distance is treated as nodes' centrality with respect to the cluster. The node energy and node density linguistic variables have three levels: low, medium and high. Intra cluster distance has the levels: close, moderate and far. The output for presentation of the node's chance to become cluster head was levelled into seven stages: "very small, small, rather small, medium, rather large, large, and very large". The fuzzy rule base look like: if the residual energy and node density is high and intra cluster distance is close then there is very large chance for the node to become cluster head. In this manner there are 3^3=27 rule base permutations. To demonstrate medium and adequate fuzzy sets, triangle membership functions are used. Trapezoid membership functions are used to demonstrate low, high, close and far fuzzy sets. As far as performance is concerned, FCH has a substantial edge over network lifetime in comparison to LEACH routing protocol. Gupta et al.[13] claims that round in which first node is dead, is about 1.8 times better than LEACH. However, this protocol is not scalable due to a non-distributed approach.

"Cluster head election using fuzzy logic (CHEF) [40]", presents a clustering method in distributed manner via fuzzy logic approach. Initially CHEF selects CHs on the basis of probability approach. Operational CHs are chosen from initially selected CH list using remaining power, and intra cluster separation of nodes. Fuzzy inference computes the input parameters. The result parameter chance is indicator to choose a node as CH. Nodes having higher chance value are the candidate for CH. It has a major disadvantage that input variable intra cluster distance does not suit for network sizes apart from 200m × 200m.

"Energy aware distributed dynamic clustering protocol using fuzzy logic (ECPF) [41]" performs all the operations in setup and steady state phases. Cluster Head election and formation of cluster are done in set-up phase. TDMA schedule formation and data communication happens in steady state phase. Degree and centrality of node are the input parameters and fuzzy output cost is treated as the decision making value. Every node will wait for a delay time (1/ residual energy). If no tentative CH is received by node within its delay time, it declares itself as tentative CH and broadcasts a message which includes its id, fuzzy cost, and its status. Now it checks in the cluster whether there is any other node with lower fuzzy cost value. If it does not find any, concerned node declares itself as the CH, and informs every member node with final CH message within its cluster range.

B. Particle Swarm Optimization (PSO)

Nature inspired the invention of "Particle Swarm optimization technique by Eberhart and Kennedy [14]". This strategy adopts the social behaviour of flying birds in a flock where all the birds have equal status and decision making capacity. They haphazardly discover their food by that bird, which is closest to the food position. All the animals have property to move in the group, especially birds and fishes. They never crash into one another because of the fact that each individual from the flock follows their head bird and alters its position and speed accordingly. This phenomenon also reduces the effort time for searching the food. position and area of food are broadcasted by all the birds in the flock. In PSO, 'bird' represents a solitary solution. In some cases it is also called as particle. All the particles have its wellness value to access the nature of the solution. "Two-tier Particle Swarm Optimization (PSO)" routing convention has been created by numerous specialists to solve the clustering and routing issues. With the aid of PSO, it is now possible to choose optimal cluster head to improve network lifetime, throughput, scalability, and delay etc. in wireless sensor network. Routing protocol adopts "particle encoding scheme" and wellness output to access the optimal route from source to destination. Authors in Paper [15], discusses about two issues: routing and clustering. PSO with multi-objective wellness function has been executed to mimic the routing method. LP and NLP formulations are used to improve the behaviour. "Optimized energy efficient routing protocol (OEERP)" is mentioned in [16]. This methodology increases network lifetime by consistently depleting nodes' power. Proposed methodology has no reference point based transmission to arrive at the passage. One disadvantage of "OEERP" methodology is that remaining sensor nodes are considered in set-up stage, which reduces framework lifetime as contrast with different methodologies. During formation of clusters, few nodes do not get included in any cluster. This phenomenon gives birth to residual

node formation. Such remaining nodes transmit the detected information either legitimately to the BS or by getting suitable gateway node through control messages. Excessive increase in control messages results in reduced network lifetime. Authors in [17], proposed Enhanced optimized energy efficient routing protocol (E-OEERP). This protocol minimizes the chance of residual nodes creation to improve the energy efficiency. Clustering and routing are performed with the assistance of "Particle swarm optimization (PSO) and Gravitational search algorithm (GSA)" in route construction phase. Saranraj et al.[18] combined ACO with PSO to create Particles with "Ant Swarm optimization" for finding CH in a wireless sensor network. Authors applied pheromone path to the PSO for the particles' position synchronization. This method attains the best objective value to find the optimal path from source to sink node. In [19] and [20], authors combined PSO and neural networks characteristics to make a scalable and secure system. They figured out that fixed base station frequently experiences hotspot issue as they have more traffic density close to the sink hub. To improve the hot spot problem, the authors of [20] presented algorithm for mobile sink nodes with control parameters to improve delay and network life. Particle Swarm Optimization Routing (PSOR) protocol has been proposed in [21] to create best path for less energy consumption in data communication. Though there are many routes between source and destination, this protocol uses leftover node power as a fitness function to discover the optimized route. We come to conclusion that PSO is good for single-hop communication, however it is not efficient for multi-hop communication.

C. *Firefly Algorithm (FA)*

Firefly calculation (FA) is another enhancement method initially proposed by Dr. Xin She [22]. This strategy copies the manner in which genuine flies get pulled in to one another dependent on flash light. Fireflies produce unique pattern by their flash dependent on the species. Fireflies attract each other with two fundamental patterns: mating and preys. Female fireflies answer with some remarkable flash light pattern to the male in mating case. The separation between fireflies is contrarily relative to the light emitted by fireflies. This implies fascination between fireflies is dependent on the intensity of Light emitted by them. As the separation increases, received light brightness will diminish. This behavior is inherited in firefly algorithm where fireflies are represented as generated solutions and fitness function is linked with the light intensity. WSN can be implemented with the help of firefly algorithm. It uses various parameters like remaining power, intra and inter cluster node distance, node density etc.to optimize path between Cluster Head and base station.

In [23], firefly algorithm was implemented by decreasing fitness value as hop count of any route increases. This is worth in WSN to conserve the energy of nodes, and add residual energy in its fitness value. Authors [24], proposed a power saving algorithm using ACO and firefly algorithms. They claim that FA outperforms the ACO for less distant routes while ACO is good in the case of longer routes. Mobile sink node has been introduced in a paper proposed by authors [25], named as mobile data transporter (MDT). It gathers data from every sensor node to send the collected stuff to the BS. In this FA approach, average path length decreases in comparison to Ant Colony Optimization. Firefly algorithm (EDFA) is presented in [26] to solve vehicular routing problem with time windows (VRPTW). This algorithm aims to optimize (min) the number of possible paths in a network. Algorithm is suitable for multi-objective optimization problems. This technique faces the problem of delay in path search.

D. Genetic algorithm (GA)

Genetic algorithm (GA) is one of the techniques proposed by Holland et al. [27], which solve search and optimization problems. This technique is based on the Darwin theory of biological evolution, reproduction and "survival of the fittest". It copies the behaviour of genes transfer from parents to children through crossover, mutation and selection operators. In selection phase, few genes are chosen for crossover and mutation; genes get swapped in crossover for children production, whereas new attributes are added in mutation phase. The same characteristic is mimicked in Genetic Algorithm. In this algorithm, population is constituted as chromosomes and each string of chromosome is written as binary or real numbers. First of all, the random generation of population is performed, then process of selection, crossover and mutation [28] generate next generation of population. Strength of produced chromosome in a population is examined by the objective function. In [29], GA has been taken to optimize the inter node distance for energy conservation. The objective function incorporates the transmission distance between nodes and CH within a cluster and from the cluster head to the BS. Node with maximum residual battery power and minimum intra cluster distance is selected as CH, to minimize the communication cost and increase the life of network. Authors in [30] presented an algorithm which reduces the chance of weak node consideration in any route selection. Authors [31], considered clustering and routing issues using Genetic Algorithm (GA),which gives better result. According to paper presented in [32], authors have used the advantages of genetic algorithm and simulated annealing together for efficient energy utilization via efficient route selection. Authors [33] applied GA on hierarchical based clustering protocol to make network properties better. To maximize the network lifetime and to minimize the average intra cluster distance, paper [34] applied

GA based algorithm. This algorithm is not suitable in the paradigm of mobile sensor nodes.

E. Ant Colony Optimization (ACO)

Darigo and Gambardella [35] in 1997 proposed Ant Colony Optimization technique. It mimics ants' behaviour. It tackles the issue of ideal path discovery between source and goal, based on genuine ants' characteristic. In beginning, ants move in any direction to search food. Upon the successful discovery of food source, ants turn towards colony. Ants release pheromones while going back to home which in turn guides way for food source. Different ants follow a similar way to reach on food source. When these ants copy the same path, fair amount of Pheromones are deposited to indicate a stronger path. The quantity of deposited pheromones is directly proportion to quality and magnitude of food source. At a point of time when food sources diminish, quantity of deposited pheromones also decreases to inform the ants about less or no availability of food. Authors in [36] applied ACO to find optimal path for data communication in WSN. ACO is applicable in the case of predefined source and destination. It works well only for symmetric paths. According to authors [37], Pheromone quantity is computed in terms of hop count between source and destination. Nodes receive data values as Destination Address (DA), Next hop (NH), Pheromone value (PH) and stores in routing table. An algorithm named "optimal-distance based transmission strategy (ODTS)" based on ACO optimization is mentioned in [38]. This strategy searches for the optimal distance among the sensor nodes for cluster head selection, which ultimately improve energy efficiency and life of the network. To minimize the earlier death of sensor nodes, ACO based load balancing in WSN is presented in article [39].

IV. Comparison and Research Gap

Summary of various surveys for different class of problems and applications are summarized in Table I. We derive the conclusion as mentioned below:

- Residual energy is the basic criteria for most routing protocols to improve the network life time.
- Most routing protocols have complete knowledge of the network.
- Node coverage issue were not discussed in depth.
- Fault tolerant and scalability are less explored.
- Cross-layer methods, mobility, non-uniform deployment, etc. are not discussed much.
- Most routing protocols assumed BS as stationary. Use of multiple BS is also not taken into consideration.
- Novel approaches should be addressed for mobility.
- The relation between heterogeneity and routing is not addressed.
- Most researchers have considered performance metrics such as intra cluster distance, power consumption,
- Network life, packet delivery ratio and delay. The metrics such as reliability, load balancing, computational
- Conversion of simulated experiments into real-world applications is a big challenge for future.

V. Conclusion

Various Optimization techniques like Fuzzy Logic, ACO, FA, PSO, GA were used for optimization in WSN. The parameters mentioned in Table-I have been considered for the comparison of these optimization techniques. In this study, we have surveyed some challenges of routing in WSN. Few optimization methods are discussed here to suggest the best technique for a particular application. Though many optimization techniques are available, still there are plenty of open issues and challenges for pursuance of optimal solution in a Wireless Sensor Network. Most of these algorithms are still being improved by the researchers. The tabulated results given in this article may help researchers working in this field. This paper gives insight about some challenges also, which are not explored yet. This article will probably guide new researchers to fill the gap in the area of Wireless Sensor Network.

TABLE- I

Parameters	**ACO**	**PSO**	**FA**	**GA**	**Fuzzy Logic**
Representation	Undirected Graph	Dimensions for vector position and speed	Distance based attraction	Random binary number	Multidimensional vector values between 0 and 1
Operators	Pheromone updates and trial evaporation	Evaluation and update Current state	Attraction, intensity of light	Selection, crossover, mutation	Fuzzy aggregation operator, Ordered Weighted Averaging
Control Parameters	Magnitude of ants, iteration, pheromone decay rate	Position, magnitude of pheromone, Range, weight, iterations	Force of attraction, light intensity	Population size, selection procedure, crossover and mutation probability, magnitude	Fuzzy Membership Function

				of chromosomes	
Node Deployment	Placed in distributed manner, used in dynamic applications	Random, Centralized nodes deployment	Random manner	Both	Distributed and random both
Clustering and routing	Explore closest route between source and destination for better transmission	Find optimal path by choosing high energy nodes as CH in every round	Choose cluster head on distance basis	Number of predefined clusters are chosen to reduce communication distance	Selects CH on basis of energy, concentration and centrality etc.
Advantages	1.Can be used in dynamic applications like travelling salesman problem	1. It finds best positioned nodes for CH. 2. Inherently continuous, 3. no overlapping and mutation calculation	Used in optimization with multi objective functions	1. Solve complex problems where parallel operations are required 2. Discrete in nature	1. Ideal for problems with imprecise and vague data 2. Can Model nonlinear problems of arbitrary complexity
Disadvantages	1. Only local search 2. More energy Consumption for more number of paths	1. Not suitable for distributed paradigm 2. Suitable for coordinate system only	Suitable for nodes which are deployed randomly.	Suited for arbitrarily placed sensor nodes.	1.The results are perceived based on assumption, 2. not accurate always

References

[1]. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E., 2002. Wireless sensor networks: a survey. Comput. Networks 38, 393–422. https://doi.org/10.1016/S1389-1286(01)00302-4.

[2]. Want, R., Farkas, K.I., Narayanaswami, C., 2005. Guest Editors' Introduction: Energy Harvesting and Conservation. IEEE Pervasive Comput. 4, 14–17. https://doi.org/10.1109/MPRV.2005.12

[3]. Raghunathan, V., Schurgers, C., Sung Park, Srivastava, M.B., 2002. Energy-aware wireless microsensor networks.IEEE Signal Process.Mag.19,40–50 https://doi.org/10.1109/79.985679

[4]. Anastasi, G., Conti, M., Di Francesco, M., Passarella, A., 2009. Energy conservation in wireless sensor networks: A survey. Ad Hoc Networks 7, 537–568. https://doi.org/10.1016/J.ADHOC.2008.06.003

[5]. Zengin, A., & Tuncel, S. (2010). A survey on swarm intelligence-based routing protocols in wireless sensor networks. International Journal of Physical Sciences, 5, 2118–2126.

[6]. Parwekar, P., Rodda, S., & Kalla, N. (2018). A study of the optimization techniques for wireless sensor networks (WSNs). In Information systems design and intelligent applications (pp. 909–915). Berlin:Springer.

[7]. Ali, Z., & Shahzad, W. (2013). Analysis of routing protocols in ad hoc and sensor wireless networks based on swarm intelligence. International Journal of Networks and communications, 3, 1–11.

[8]. Shamsan Saleh, M., Ali, B. M., Rasid, M. F. A., & Ismail, A. (2014). A survey on energy awareness mechanisms in routing protocols for wireless sensor networks using optimization methods. Transactions on Emerging Telecommunications Technologies, 25, 1184– 1207

[9]. Saleem, M., Di Caro, G. A., & Farooq, M. (2011). Swarm intelligence-based routing protocol for wireless sensor networks: Survey and future directions. Information Sciences, 181, 4597–4624.

[10]. Gui, T., Ma, C., Wang, F., & Wilkins, D. E. (2016). Survey on swarm intelligence-based routing protocols for wireless sensor networks: An extensive study. IEEE International Conference on Industrial Technology (ICIT), 2016, 1944–1949.

[11]. Zungeru, A. M., Ang, L.-M., & Seng, K. P. (2012). Classical and swarm intelligence-based routing protocols for wireless sensor networks: A survey and comparison. Journal of Network and Computer Applications, 35, 1508–1536.

[12]. Guo, W., & Zhang, W. (2014). A survey on intelligent routing protocols in wireless sensor networks, Journal of Network and Computer Applications, 38, 185–201.

[13]. Gupta I, Riordan D, Sampalli S., Cluster-head election using fuzzy logic for wireless sensor networks, Proceedings of the 3rd Annual Communications Networks and Services Research Conference 2005, p.255–260.

[14]. Eberhart, R., & Kennedy, J. (1995). A new optimizer using particle swarm theory. In MHS'95. Proceedings of the sixth international symposium on micro machine and human science (pp. 39–43).

[15]. Kuila, P., & Jana, P. K. (2014). Energy efficient clustering and routing algorithms for wireless sensor networks: Particle swarm optimization approach. Engineering Applications of Artificial Intelligence, 33, 127–140.

[16]. Chand, K. K., Bharati, P. V., & Ramanjaneyulu, B. S. (2012) Optimized energy efficient routing protocol for life-time improvement in wireless sensor networks. In IEEE-international conference on advances in engineering, science and management (ICAESM-2012) (pp. 345–349).

[17]. RejinaParvin, J., & Vasanthanayaki, C. (2015). Particle swarm optimization-based clustering by preventing residual nodes in wireless sensor networks. IEEE Sensors Journal, 15, 4264–4274.

[18]. Saranraj, G., & Selvamani, K. (2017). Particle with ant swarm optimization for cluster head selection for wireless sensor networks. Journal of Computational and Theoretical Nano science, 14,2910–2914.

[19]. Stephen, K. V. K., & Mathivanan, V. (2018). An energy aware secure wireless network using particle swarm optimization. In 2018 Majan international conference (MIC) (pp. 1–6).

[20]. Wang, J., Cao, Y., Li, B., Kim, H.-J., & Lee, S. (2017). Particle swarm optimization-based clustering algorithm with mobile sink for WSNs. Future Generation Computer Systems, 76, 452–457.

[21]. Sarangi, S., & Thankchan, B. (2012). A novel routing algorithm for wireless sensor network using particle swarm optimization. IOSR Journal of Computer Engineering (IOSRJCE), 4, 26–30.

[22]. Yang, X.-S. (2010). Nature-inspired metaheuristic algorithms. Bristol: Luniver Press.

[23]. Manshahia, M. (2015). A firefly-based energy efficient routing in wireless sensor networks. African Journal of Computing & ICT, 8, 27–32.

[24]. Okwori, M., Bima, M., Inalegwu, O., Saidu, M., Audu, W., & Abdullahi, U. (2016). Energy efficient routing in wireless sensor network using ant colony optimization and firefly algorithm. In International conference on

information and communication technology and its applications (pp.28–30).

[25]. Yogarajan, G., & Revathi, T. (2018). Nature inspired discrete firefly algorithm for optimal mobile data gathering in wireless sensor networks. Wireless Networks, 24, 2993–3007.

[26]. Osaba, E., Carballedo, R., Yang, X.-S., & Diaz, F. (2016). An evolutionary discrete firefly algorithm with novel operators for solving the vehicle routing problem with time windows. In Natureinspired computation in engineering, pp. 21–41. Berlin: Springer.

[27]. Holland, J. (1975). Adaptation in natural and artificial systems: an introductory analysis with application to biology. In Control and artificial intelligence, Cambridge: MIT Press

[28]. Deif, D. S., & Gadallah, Y. (2013). Classification of wireless sensor networks deployment techniques. IEEE Communications Surveys & Tutorials, 16, 834–855.

[29]. Aziz, L., Raghay, S., Aznaoui, H., & Jamali, A. (2016). A new approach based on a genetic algorithm and an agent cluster head to optimize energy in wireless sensor networks. In 2016 international conference on information technology for organizations development (IT4OD) (pp. 1–5).

[30]. Yao, G.-S., Dong, Z.-X., Wen, W.-M., & Ren, Q. (2016). A routing optimization strategy for wireless sensor networks based on improved genetic algorithm. Journal of Applied Science, Engineering and Technology, 19, 221–228.

[31]. Gupta, S. K., & Jana, P. K. (2015). Energy efficient clustering and routing algorithms for wireless sensor networks: GA based approach. Wireless Personal Communications, 83, 2403–2423.

[32]. Chakraborty, S. K. M., & Naskar, M. K. (2011). A Genetic algorithm inspired routing protocol for wireless sensor networks. International Journal of Computational Intelligence Theory and Practice, 6, 1–8.

[33]. Shurman, M. M., Al-Mistarihi, M. F., Mohammad, A. N. Darabkh, K. A., & Ababnah, A. A. (2013). Hierarchical clustering using genetic algorithm in wireless sensor networks. In 2013 36th international convention on information and communication technology, electronics and microelectronics (MIPRO) (pp. 479–483).

[34]. Heidari, E., & Movaghar, A. (2011). An efficient method based on genetic algorithms to solve sensor network optimization problem. arXiv preprint arXiv :1104.0355.

[35]. Darigo, M., Gambardella, L., & Maria, L. (1997). Ant colonies for the travelling salesman problem. Bio-Systems, 43, 73–81.

[36]. Sudarshan D Shirkande, Rambabu A Vatti, “ACO based routing algorithm for ad-hoc (WSN, MANET) networks: survey” International Conference on Communication Systems and Network Technologies 2013.

[37]. Varnika Bains, Kanchan Sharma “Ant colony based routing in wireless sensor networks” International Journal of Electronics and Computer Science Engineering ISSN 2277-1956

[38]. Xuxun Liu, “An optimal-distance based transmission strategy for lifetime maximization of wireless sensor networks”, IEEE Sensors journals, Vol.15, No.6, June 2015.

[39]. Mamta Tewari, Kunwar Singh Vaisla “Optimized Hybrid Ant Colony and Greedy Algorithm Technique based Load Balancing for Energy Conservation in WSN” International Journal of Computer Applications, October 2014

[40] J.-M. Kim, S.-H. Park, Y.-J. Han, and T.-M. Chung, “CHEF: Cluster Head Election mechanism using Fuzzy logic in wireless sensor networks,” in Proceedings of the 10th International Conference on Advanced Communication Technology, pp. 654–659, Gangwon-Do, South Korea, February 2008. Wireless Communications and Mobile computing 13

[41]. H. Taheri, P. Neamatollahi,O. M. Younis, S. Naghibzadeh, and M. H. Yaghmaee, “An energy-aware distributed clustering protocol in wireless sensor networks using fuzzy logic,” Ad Hoc Networks, vol. 10, no. 7, pp. 1469–1481,2012.

Rakesh Kumar Singh is working as associate Professor in Computer Sc. and Engg. Department,Kamla Nehru Institute of Technology ultanpur(UP)-India. He received M.E. from Jadavpur University, Kolkata. Currently he is pursuing his Ph.D.
from MUIT Lucknow (up)-India. His area of interest is ad hoc network, sensor network and ubiquitous computing.

Dr. Ajay Kumar Bharti is working as Professor in Computer Science department .MUIT Lucknow –India. He received his MCA degree from KNIT Sultanpur and Ph.D. degree in 2014 from BBA University , Lucknow(up)-India. His research interest includes service oriented architecture Knowledge Based System, e-Governance and Artificial Intelligence.

Curriculum Vitae

Name : RAKESH KUMAR SINGH
Designation: ASSOCIATE PROFESSOR
Date of Birth: 23/09/1967
Date of Joining: 02/02/1993
Address: Conputer Science @ Engg. Department
KNIT SULTANPUR
Email Address: rksingh@knit.ac.in
Mobile No: 9415962461
Qualification :

Degree	Name of University	Year of Passing	Area
Post doc.	--	--	--
Phd.	Pursuing	--	Sensor Network
Post graduation	Jadavpur University	2002	Comp. Engineering
Under graduation	Gorakhpur University	1990	Comp. Science

Area of Specialization: Wireless Adhoc Network, Databases, Algorithm Design
Experience:
Teaching: 28 years
Industrial: --
Research: --
M.Tech Supervised (Nos):
Completed: 16
Ongoing : 02
Publications (Nos): 15
Workshop/Seminars:
Organized: 01
Attended : 11

Expert Lecture/Invited Talk: 02

Roles and Responsibilities: various responsibilities held in previous years
(Currently Controller of Examination)
Residential Address: 52, Laxmanpur, Sultanpur (UP)

Date-22/09/2021
Place-KNIT Sultanpur