Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 3s (2025)

Optimized Energy-Aware Routing for Internet of Things Enabled WSNS using Neuro-Fuzzy Clustering and Quantum Firefly Algorithm

Mrs. J. Karthikeyini[1], Dr. K. S. Mohanasathiya[2]

[1]Ph.D Research Scholar (Full Time), Department of Computer Science, VET Institute of Arts and Science (Co-education) College, Thindal, Erode. jkarthy535@gmail.com

[2]Assistant Professor & Research Supervisor, Department of Computer Science, VET Institute of Arts and Science (Co-education) College, Thindal, Erode. sathyaanandh08@gmail.com

Article History:

Received: *24-09-2024*

Revised: *10-11-2024*

Accepted: *27-11-2024*

Abstract:

Researchers and industry professionals are highly interested in Wireless Sensor Networks (WSNs) due to their importance in utilizing low-cost, low-power microelements, such as radios, computers, and sensors, which are often integrated onto a single chip. Recently, the integration of the Internet of Things (IoT) with WSNs has been extensively explored. Effective routing techniques are crucial for optimizing power usage, ensuring Quality of Service (QoS), and maintaining network reliability in IoT-enabled WSNs. This paper presents an enhanced energy-aware navigation system that employs the Quantum Firefly Optimization (QFO) method and Neuro-Fuzzy Clustering for IoT-enabled WSNs. The Neuro-Fuzzy Clustering method extends the system's lifetime by automatically grouping sensor nodes into energy-efficient clusters. The QFO method is used to determine the optimal routing paths by considering factors such as energy consumption, QoS, and trust metrics. By incorporating these advanced methodologies, the proposed solution outperforms existing approaches in terms of energy efficiency, routing accuracy, and overall network stability. Simulation results demonstrate that this novel approach has the potential to significantly improve current routing protocols and expand the capabilities of IoT-enabled WSNs. Additionally, to enhance efficiency in mobile computing environments, the security of the intrusion detection system was strengthened through the use of deep learning techniques.

Keywords: Energy Efficiency; Neuro-Fuzzy Clustering; Quantum Firefly Optimization; Routing Algorithms; Wireless Sensor Networks; Quality of Service; Intenet of Things

1 Introduction

WSNs consist of tiny sensing units called nodes that have limited computational capabilities, low battery power, and restricted storage. Due to the power constraints of these sensor networks, a suitable and energy-efficient method is essential for securely communicating the collected information. Security is critical in routing, as flooding attacks can overwhelm the network's bandwidth with excessive packets, while packet dropping can reduce network efficiency [1]. Cluster-based routing is a key method for transmitting information with minimal energy consumption in WSNs. The effectiveness of clustering can be enhanced by utilizing soft computing techniques such as artificial intelligence, fuzzy logic, and rule-based systems.

IoT-based sensor networks incorporate sensing devices, networking applications, and connected sensors to gather data from nodes and transmit it to a Base Station (BS) for more efficient decision-making [2]. The IoT ecosystem, by leveraging internet connectivity enables the synchronized operation of multiple devices, delivering essential functionalities. IoT architectures based on sensor

networks must address challenges related to network technology, such as security and data transmission [3]. The literature includes numerous studies on the various design challenges of IoT-enabled sensor networks including issues related to data transmission. As new types of IoT devices are introduced, existing standards across conventional, wireless, and connected sensor networks may no longer be adequate. New routing algorithms for network connectivity are required to effectively gather and transmit information across WSNs within the IoT context shown in Figure 1 [4].

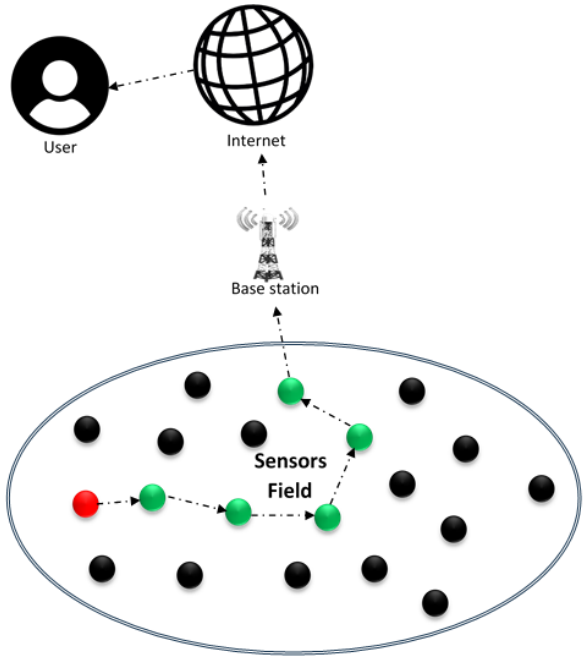


Figure 1: A simple WSN-Assisted IoT environment

Every sensor node in a WSN has the same level of sensing capability, which is effectively utilized to monitor their environment and collect data. Many IoT applications rely on the deployment of sensor networks, including home monitoring, healthcare, industrial process surveillance, wildfire detection, and agricultural management involving high-risk human interactions [5]. WSN can be employed to detect and gather information from various environments, whether for the aforementioned purposes or other applications involving critical conditions. IoT-enabled sensor networks hold significant potential in disaster prevention, military applications, and medical monitoring. It can also be integrated into automated transportation systems, communication networks, commercial activities, agriculture, and knowledge management platforms [6]. By acting as a bridge between the physical and virtual worlds through the interconnection of smart devices, IoT with its inherent capabilities for information exchange, interaction, and operations has expanded the reach of the internet. The advancement of IoT has facilitated the proliferation of technology worldwide, permeating various aspects of lives across diverse industries, including smart cities, defense, healthcare, agriculture, and commerce [7]. As IoT encompasses a wide array of technologies and continues to unlock new opportunities, its rapid growth has attracted researchers globally, encouraging them to explore new perspectives and identify emerging application areas [8].

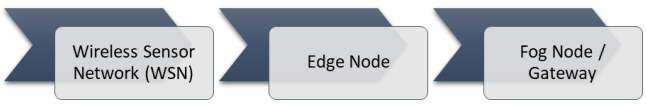


Figure 2: Fog WSN framework

Due to its low connectivity requirements, cost-effectiveness, and energy efficiency, this new connected sensor technology offers excellent solutions for tracking and surveillance-related applications. Fog computing an emerging technology in cloud storage has seen significant advancements to its improved latency, security, privacy, mobility, and geographically distributed characteristics [9]. Fog computing revitalizes WSNs by providing enhanced data processing and storage capabilities, making them suitable for a variety of context-sensitive, delay-sensitive applications that operate in real-time [10]. As illustrated in Figure 2, gateways equipped with fog computing and integrated with connected wireless sensors facilitate the transfer of IoT data. For the IoT to achieve the desired efficiency in deployed environments, a reliable, efficient, and secure communication infrastructure is essential, given the presence of heterogeneous devices with limited power, memory, and computational capabilities [11]. Before implementing proposed solutions, routing techniques must consider challenges related to sensor node capacity limitations, communication uncertainties, packet loss, and unexpected delays. Figure 3 presents an organization of several common methods for routing information, highlighting the importance of addressing these issues to ensure the effective deployment of IoT-enabled WSNs [12].

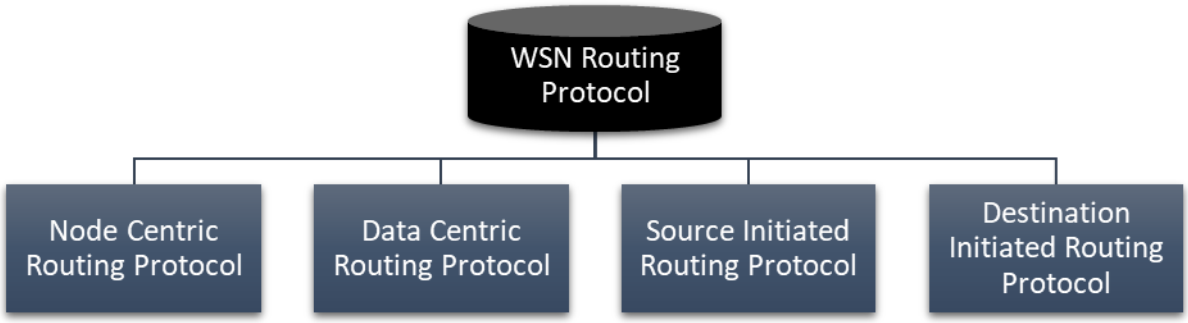


Figure 3: Routing protocols classification in WSNs

Data mining techniques, such as clustering, are employed to efficiently organize data; they are unsupervised learning methods that do not require predefined classification labels for the dataset. Explored clustering to develop cluster-based routing methods. In many practical scenarios, the central station needs to receive data collected by sensor nodes to make more effective routing and resource allocation decisions [13]. Clustering enables the selection of Cluster Heads (CH) and the routing of packets through these Heads, thereby extending the network's lifetime through improved load distribution. The routing algorithm proposed in this work introduces a trust-based secure protocol that enhances both security and energy efficiency by incorporating novel energy efficiency and trust metrics alongside traditional QoS measures. Utilizes a trust architecture with a calculation method for determining trust ratings, providing an effective cluster-based secure forwarding mechanism. The system selects the optimal network route based on parameters such as route reliability, power consumption, and hop count, ensuring secure and efficient network management [14].

1.1 Problem Statement

The IoT environment relies heavily on WSNs to facilitate information exchange and seamless interaction among multiple devices. WSNs face numerous challenges that hinder their efficient operation, primarily related to energy consumption, network reliability, and QoS. Existing routing methods often struggle to address these complex issues, leading to reduced network lifespan and diminished efficiency. For IoT applications to perform optimally, QoS and network reliability are crucial, as they require consistent data transmission and low latency. Therefore, in IoT-enabled WSNs, there is an urgent need for an improved routing method that can ensure QoS, enhance system

stability, and dynamically optimize energy usage. This study aims to tackle these challenges by developing a novel routing method that integrates QFO with Neuro-Fuzzy clustering. This comprehensive approach is designed to extend the lifespan and improve the efficiency of IoT-enabled WSNs, addressing the critical needs for better path selection, QoS assurance, and energy optimization.

1.2 Motivation

Several major challenges hinder the effective implementation of WSNs in IoT environments particularly in terms of energy consumption, network reliability, and QoS. The dynamic and heterogeneous nature of IoT settings requires resilient and adaptable routing systems to ensure reliable and efficient data transmission. Traditional routing strategies often struggle to balance the conflicting demands of energy efficiency, reliability, and QoS, highlighting the need for novel approaches that can continuously adapt to changing network conditions and optimize resource utilization. Proposed solution lies in the combination of advanced techniques such as QFO and Neuro-Fuzzy Clustering. It can automatically group sensor nodes into energy-efficient clusters, while QFO optimizes routing paths by considering various factors such as trust metrics, QoS, and energy consumption. The goal of this study is to develop an energy-aware, optimized routing method that leverages these cutting-edge techniques to enhance the lifespan and efficiency of IoT-enabled WSNs.

2. Related Works

The primary purpose of WSNs is to gather scalar information for environmental monitoring. The data collected by the sensors is then transmitted to a central station or mobile sink nodes for further processing. WSNs are employed in a variety of fields including military operations, medical monitoring systems, weather forecasting, biological ecosystem surveillance, security systems, manufacturing automation, smart cities, parking structures, and aviation [15]. Despite their wide range of applications, WSN sensors are resource-constrained and distributed, with limited power and storage capacity. It is crucial to design WSNs in a way that maximizes their lifespan by ensuring efficient operation. One of the significant challenges with WSNs is maintaining network security and ensuring the safe transmission of information. The lack of central management makes WSN sensors more susceptible to security threats, as malicious nodes can pose as legitimate ones and compromise the data [16].

Focused on reducing energy consumption in WSNs, suggesting that turning off the radio network instead of keeping it idle could save power. Energy consumption increases during the data transmission and collection phases, with the physical layer having three possible states: active, idle, and sleep. Employing a duty cycle strategy which synchronizes the nodes' states, is an effective technique for conserving energy [17]. The duty cycle's efficiency forms the basis of the Sparse-Topology and Energy-Management (STEM) methodology, where information transfer is triggered by specific requirements, and sleeping nodes are periodically awakened to check for any data exchange needs [18].

Energy usage solutions that aim for high productivity, low latency, and fairness in WSNs, particularly focusing on the MAC protocols optimized for energy conservation. Identified that the duty cycle used to prevent idle listening is a significant power consumer in typical WSN setups [19]. It concluded that MAC layer interactions between communication and idle periods greatly influence node lifespan and energy consumption since the same channels are used. This led to the development of a method that balances security, power consumption, and transmission efficiency using a confidence-based approach and grey theory problem-solving [20]. Their proposed secure transport method, which selects a trustworthy and safe transmission node based on this trade-off, also helps

prevent defamation attacks. Experimental results demonstrated that the Grey-based Trust Management Scheme (GDTMS) outperforms similar methods [21].

Numerous energy-efficient routing methods have been explored in the literature on WSN design. Proposed an energy-efficient routing protocol combining clustering with energy efficiency improvements, which extended network lifetime. Introduced the Fuzzy-Based Cluster Formation Protocol (FBCFP) as a useful routing technique for wireless sensor networks. Their approach involved an unequal clustering method using fuzzy logic for cluster formation differed from previous works by addressing issues such as CH overload that could lead to increased communication delays and energy consumption [22]. This approach did not consider security issues, which are critical in WSNs. Conducted a comprehensive survey on decentralized and centralized clustering-based routing techniques, providing insights into the advantages and limitations of existing methods. Proposed a virtual force-based clustering approach for efficient node grouping in mobile WSNs, focusing on reducing energy consumption and optimizing network lifetime by routing traffic through CHs. Research did not address network security threats could also significantly impact energy consumption and network performance [23].

Research Gap

An energy-efficient clustered method is necessary from the standpoint of power-aware techniques, minimizing intercluster traffic in the entire network, and extending the lifespan of WSN. To improve safety, more attention must be paid to cloud computing and WSN integration for information aggregating and encrypted communication with the implementation of detection and prevention algorithms. The literature study makes clear that a variety of study efforts have been completed in the fields of safe transmission of data, energy-aware clustering remedies, and identifying attacks in sensor networks that are wireless. Numerous studies remain unanswered, particularly regarding the topics of group development, cluster head choosing, obtaining the best possible path, and identification of attacks and forecasting using bioinspired methods and deep learning-based security breach detection mechanisms to improve WSN efficiency.

3. Proposed System

Many methods in the scientific community for secure routing, including key management systems, data mining techniques, and trust analysis-based approaches, have proven inadequate in countering new types of attacks that are prevalent in computer networks. The persistent presence of malicious nodes within the routing path also significantly impacts the efficiency of WSN routing. To enhance secure communication, this paper proposes three different methods. Two of these methods focus on improving routing security to ensure reliable communication in WSNs by employing fuzzy temporal rules, QoS analysis, trust assessment, and outlier detection techniques.

Figure 4 illustrates the design of the proposed QoS and cluster-based routing elements, as well as the secure routing system introduced in this study. In this framework, the spectral graph theory is applied to group nodes by creating appropriate matrices that determine the optimal number of clusters. The proposed framework consists of seven main components: the selection supervisor, security component, QoS supervisor, power supervisor, rules and clustering-based navigation supervisor, sensor nodes, and the database. A distinctive feature of the security component is the trust modeling capability. Additionally, the security component is responsible for implementing an authentication method to enhance security. The selection supervisor manages the Secure QoS Energy-Efficient Routing (SQEER) system proposed in this research.

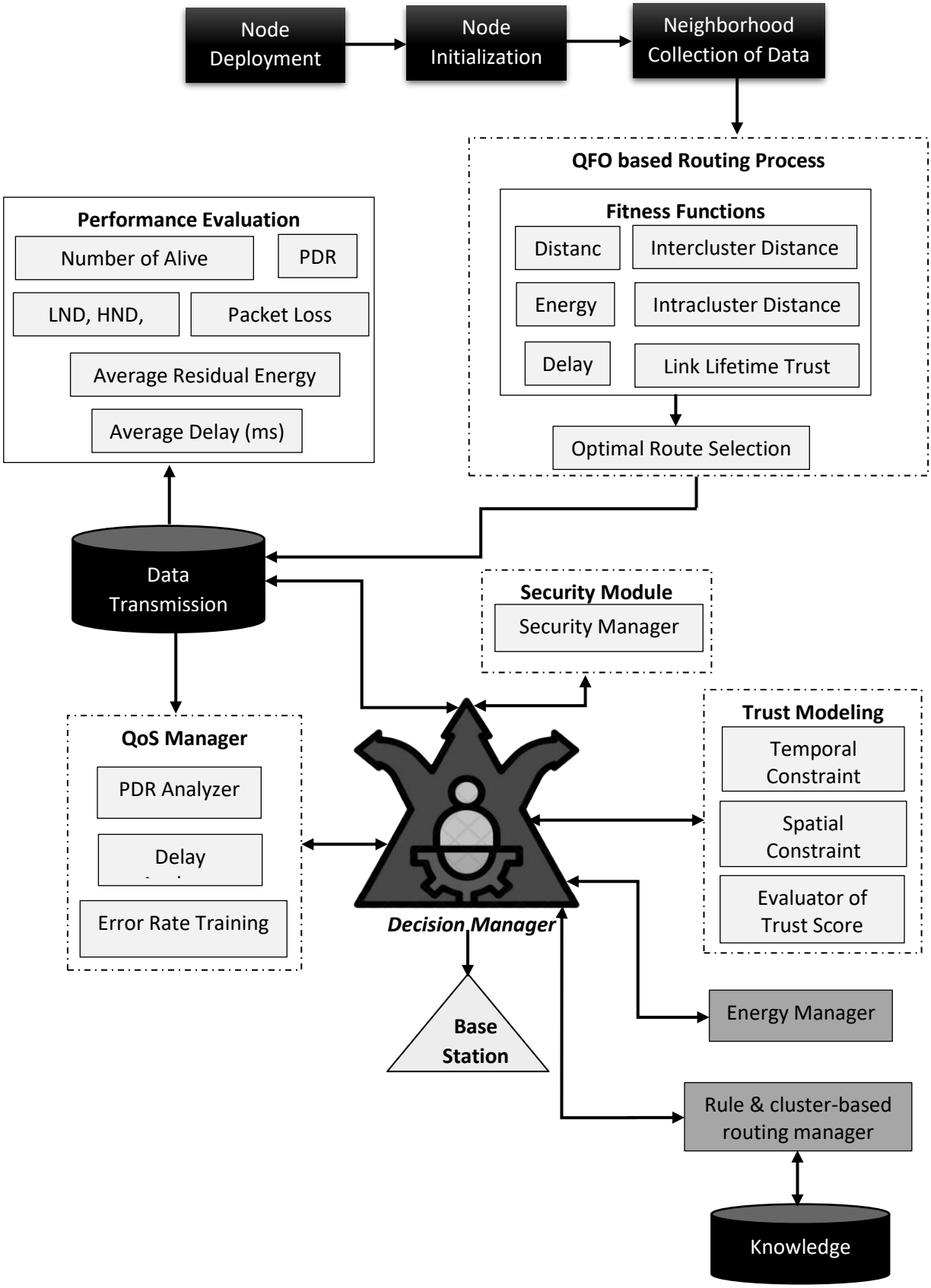


Figure 4: Proposed Architecture

This system utilizes technologies like the Manager, Safety Manager, and Power Manager to ensure secure data transmission. The Rule Administrator and Cluster-Based Navigation are employed to make more effective routing decisions. The QoS Manager, integrated into this architecture, analyzes information packets through the Packet Delivery Ratio (PDR) detector and uses explanation-based argumentation. For efficient verification of QoS variables, it leverages the features of errors generated by the Rate Analyzer and Delay Analyzer sub-modules. The Safety Module collaborates with the Safety Administrator to provide robust authentication support and maintains network trust through temporal and geographic constraint management. Energy consumption management is a critical aspect of this system. It calculates the power consumption of nodes and forwards this information to the Decision Manager enabling better decision-making to ensure energy savings during the routing process. The proposed model is designed to select the most efficient paths to the final destination. Potential routes are identified after the system generates a fitness function based on the provided mathematical equation, optimizing the routing process for energy efficiency and security.

3.1 Datasets

Each dataset provides a variety of features that facilitate the evaluation of the proposed algorithm's performance across different WSN and IoT scenarios. The combination of synthetic, real-world, and urban datasets ensures a comprehensive assessment, enabling the algorithm to be tested under diverse conditions and environments shown in Table 1.

Table 1: Dataset Description

Dataset Name	Description	Source	Size	Features
WSN-DS	A synthetic dataset designed for WSN applications, includes various network configurations.	UCI Machine Learning Repository	512 MB	Node ID, Energy level, Packet rate, Node location, Connectivity status
CityPulse	A dataset capturing urban IoT deployments, including traffic, pollution, and weather data.	CityPulse EU Project	16 GB	Sensor ID, Location, Data type (traffic, pollution, weather), Measurement values, Timestamp
IoT-23	A comprehensive dataset capturing lot network traffic and behaviors in different scenarios.	Stratosphere Laboratory, AIC Group, Czech Technical University	22 GB	Timestamp, Source IP, Destination IP, Packet size, Protocol, Source/Destination ports

Intel Lab Data	Sensor readings collected from Intel Berkeley Research lab, focusing on indoor environment.	UCI Machine Learning Repository	2.4 GB	Timestamp, Mote ID, Temperature, Humidity, Light, Voltage
Sensor Scope	Environmental monitoring dataset collected from WSN nodes deployed in various locations.	EPFL Open Data	2.2 GB	Sensor ID, Temperature, Humidity, Light intensity, Battery level, Timestamp
GreenOrbs	A real-world dataset collected from a large-scale WSN deployed in a forest environment.	IEEE DataPort	12 GB	Node ID, Energy consumption, Data transmission rate, Node mobility, Environmental conditions

3.2 Cluster Formation Protocol using Neuro-Fuzzy Rules

The system utilizes a neural network architecture comprising one input layer, sixteen hidden layers, and one output layer. The hidden layers include convolutional layers that process and analyze the input data. Training of the neural network is performed using network trace information from both past and current interactions. The initial training phase involves using historical data to adjust weights based on fuzzy rules triggered by an uncertain inference structure. The network continually updates the other cluster participants based on power supply and distance from the CH. Convolutional Neural Networks (CNNs) are employed to analyze transport methods and power usage across various nodes. The CNNs generate rules to identify the optimal paths with minimal energy consumption. Learning occurs at the base station, with instructions distributed only to data-collecting nodes. Evaluation is performed by sharing the gathered data among sensor nodes to validate the effectiveness of the routing method proposed.

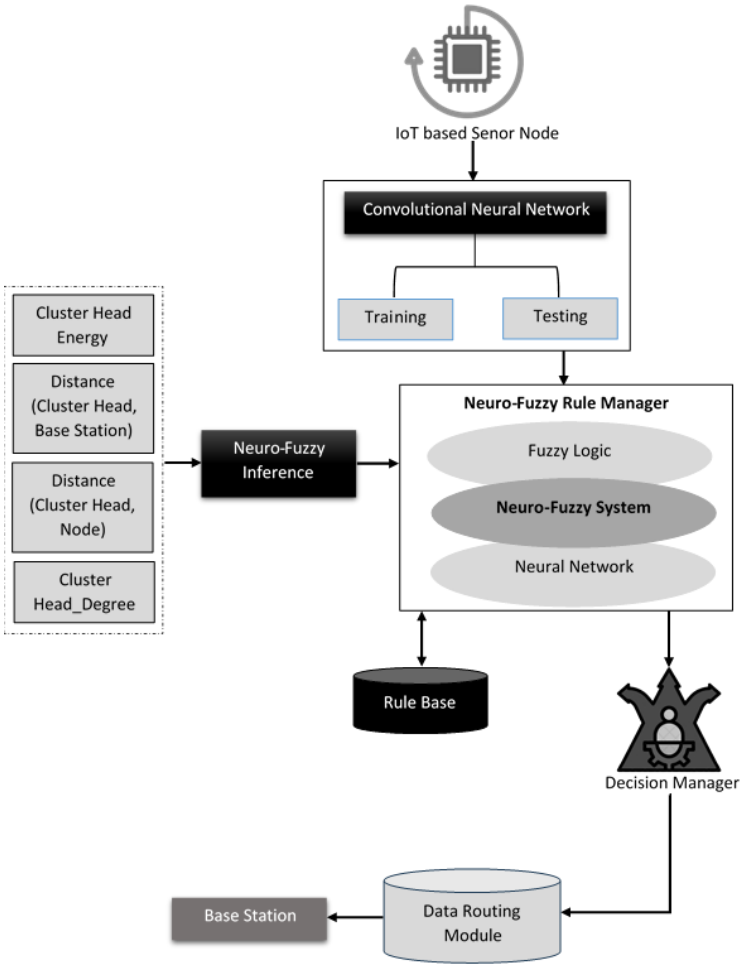


Figure 5: Fuzzy rule based routing system architecture

To ensure an energy-efficient routing method, the system employs a convolutional neural network for deep computation of node communication behaviors. For effective cluster formation, four parameters are considered: the current power level of the CH, the distance between the CH and the sink, the distance between nodes and the CH, and the degree of the CH. After electing the CH, additional nodes can join the system by associating with an appropriate CH, which approves their inclusion based on fuzzy rules. Figure 5 illustrates the design of the fuzzy rule-based navigation scheme used in the Fuzzy Cluster Formation Protocol (FBCFP). The framework consists of one output from the output layer, four inputs from the input layer, and 256 rules from the hidden layers. Four linguistic parameters, each with three distinct categories, are used in this method, along with the proposed parameter for the CH degree.

IoT-based nodes for sensors, an artificial neural network module for development and evaluation, a neuro-fuzzy deduction structure, a neuro-fuzzy rule supervisor, a rule foundation, a base station, an information the routing component, a choice as an administrator, and group separation administration components make up the main modules of the proposed sending structure diagrammed in Figure 5. To achieve environmental sustainability, all of these components work together to execute gathering information, navigation, and making choices more effectively.

CNNs are employed in this work to train the nodes that collect data and the data connection architecture of the IoT-based WSN. By using neuro-fuzzy rules, this method allows the network's components to determine the shortest route from the nodes to the heads of clusters and ultimately to

the sinking node. NFIS combines a network of convolutional neural networks with the triangle and trapezoidal functions of membership described in to provide rules for making decisions. Fuzzy classification functions provided in Equations (1) and (2) are utilized by the neuro-fuzzy rule framework.

$$\mu_{A1}(z) = \begin{cases} 0, & z \le a1 \\ \frac{z-p1}{q1-p1}, & p1 \le z \le q1 \\ \frac{r1-z}{r1-q1}, & q1 \le z \le r1 \\ 0, & r1 \le z \end{cases} \quad (1)$$

$$\mu_{A1}(z) = \begin{cases} 0, & z \le d2 \\ \frac{d2-z}{d2-r2}, & r2 \le z \le d2 \\ 1, & d2 \le z \le r2 \\ \frac{d2-z}{d2-r2}, & r2 \le z \le d2 \\ 0, & d2 \le z \end{cases} \quad (2)$$

Cluster is a crucial strategy to improve energy savings and network effectiveness in WSNs. Using a Neuro-Fuzzy structure, clusters can be created dynamically based on the position, degree of energy, and information communication rates among sensor nodes.

3.2.1 Fuzzy Membership Functions

To apply Neuro-Fuzzy rules for cluster formation

Energy Level (E)

Low Energy (LE): $\mu_{LE}(E) = max\,(0, min\,(1, \frac{E_{max}-E}{E_{max}-E_{low}}))$ (3)

High Energy (HE): $\mu_{HE}(E) = max\,(0, min\,(1, \frac{E-E_{low}}{E_{high}-E_{low}}))$ (4)

Distance to Nearest Cluster Head (D)

Near (N): $\mu_N(D) = max\,(0, min\,(1, \frac{D_{max}-D}{D_{max}-D_{near}}))$ (5)

Far (F): $\mu_F(D) = max\,(0, min\,(1, \frac{D-D_{near}}{D_{far}-D_{near}}))$ (6)

Node Density (N)

Sparse (S): $\mu_S(N) = max\,(0, min\,(1, \frac{N_{max}-N}{N_{max}-N_{sparse}}))$ (7)

Dense (D): $\mu_D(N) = max\,(0, min\,(1, \frac{N-N_{sparse}}{N_{dense}-N_{sparse}}))$ (8)

3.2.2 Fuzzy Rule Base

The Neuro-Fuzzy system uses a set of fuzzy rules to make clustering decisions. These rules combine the fuzzy sets to evaluate the suitability of nodes for becoming cluster heads or joining clusters.

Rule 1: If the Energy Level is High and Distance to Nearest Cluster Head is Near, then Node is a Suitable Cluster Head.

Rule 2: If the Energy Level is Low and Node Density is Sparse, then Node is not a Suitable Cluster Head.

Rule 3: If the Energy Level is High and Node Density is Dense, then Node is a Good Candidate for Cluster Formation.

3.2.3 Defuzzification

Finally, the aggregated fuzzy output is converted into a crisp decision using defuzzification methods. The Centroid Method is commonly used:

$$C = \frac{\sum_x (i_x . \mu_x)}{\sum_x \mu_x} \quad (9)$$

Where are the possible values of the output, and μ_x are the degrees of membership.

Fuzzy member functions and fuzzy rules are used in the Neuro-Fuzzy-based cluster creation procedure to evaluate node qualities and cluster head appropriateness, respectively. Through the integration of various methods, the protocol creates clusters that improve energy consumption and performance of networks dynamically.

3.3 Optimized Energy-Aware Routing for IoT-Enabled WSNs

The elements of the proposed work's basic network concept are nodes with sensors, which are haphazardly placed for tracking an area. The sensor nodes also share the same beginning power and are homogenous. The central stations and the sensor nodes are stationary. While the sink has an endless supply of power, the monitoring network's components are power-limited and left alone after setup. The routed information is gathered from the nodes by the central location, also known as the sink. The performance assessment is carried out by the QoS administrator. Enhancing safety and energy conservation is the responsibility of the safety management and the power management. Inference is carried out by the rule manager to assist in the decision-making process for cluster creation, CH choice, and cluster-based forwarding. The energy framework and fuzzy behavioral rules are applied by the system for routing in the proposed model to ensure optimal usage of energy.

3.3.1 Energy Model

Optimized energy-aware routing in IoT-enabled WSNs involves several key factors: energy efficiency, route optimization, and trustworthiness.

$$E_T(I,d) = \begin{cases} lE_{elec} + l\varepsilon_{fs} d^2 for\ d < d_0 \\ lE_{elec} + l\varepsilon_{mp} d^4 for\ d < d_0 \end{cases} \quad (10)$$

Where $d_0 = \sqrt{\varepsilon_{fs}/\varepsilon_{fs}}$

$$E_R(I) = lE_{elec} \quad (11)$$

where E_{elec} - electronic energy; ε_{fs} - amplifier energy in free space; ε_{mp} - amplifier energy in multipath.

Energy-Aware Routing: The goal is to select routes that minimize energy consumption while ensuring reliable communication. The energy-aware routing algorithm uses the following Residual Energy (RE) Equations:

$$RE_x = E_{initial} - E_{consumed} \quad (12)$$

where: $E_{initial}$ is the initial energy of the node. $E_{consumed}$ is the energy consumed by the node for communication and processing. Energy Consumption (EC) for transmitting a packet over a distance d is:

$$EC = E_{ti}\, d^{\gamma} \quad (13)$$

where: E_{ti} is the energy required to transmit a packet per unit distance. γ is the path loss exponent, typically between 2 and 4. Energy Efficiency (EE) for a route R consisting of nodes {1, 2,..., n} is:

$$EE_R = \frac{1}{\sum_{x=1}^{n} EC_x} \quad (14)$$

where EC_x is the energy consumption of node x in the route.

Trust Score Integration: Incorporating trust scores ensures that routes are not only energy-efficient but also reliable. The trust score of a node x is computed based on its historical performance:

Trust Score (TS) is calculated using: $TS_x = \alpha . TS_{previous} + \beta . Performance_x$ (15)

where: TS_{previous} is the trust score from previous observations. $Performance_x$ is a measure of the node's reliability in previous interactions. α and β are weighting factors that balance the importance of historical performance and recent behavior. Node Reliability (NR) in terms of trust is:

$$NR_x = \frac{TS_x}{\max(TS)} \quad (16)$$

where max(TS) is the maximum trust score observed among all nodes.

Optimized Routing Decision: Combining energy efficiency and trust score, the routing decision for a path P is based on:

Path Energy Efficiency (PEE): $PEE_p = \frac{\sum_{x=1}^{n} EE_x}{n}$ (17)

where EE_x is the energy efficiency of node x in the path.

Path Trust Score (PTS): $PTS_P = \frac{\sum_{x=1}^{n} TS_x}{n}$ (18)

where TS_x is the trust score of node x in the path.

Combined Routing Metric (CRM): $CRM_P = \frac{PEE_P . PTS_P}{max(PEE).max(PTS)}$ (19)

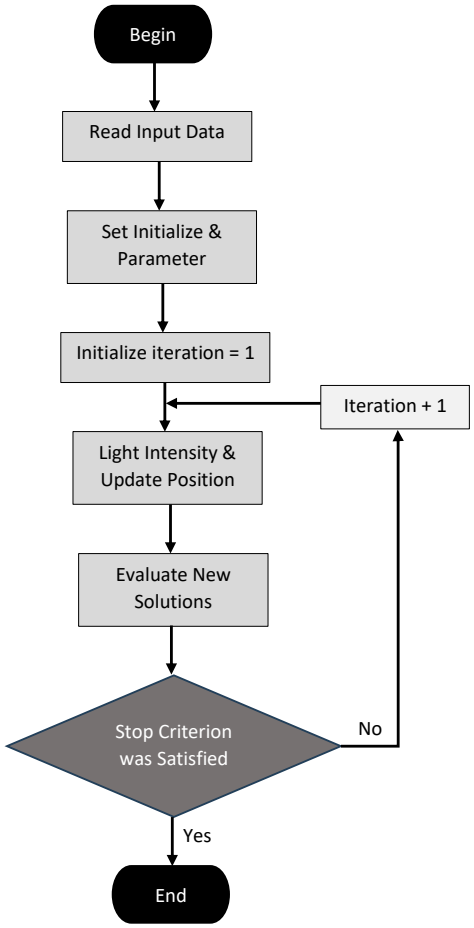


Figure 6: QFO technique

The path with the highest CRM value is selected for routing, ensuring that the route is both energy-efficient and reliable. The optimized energy-aware routing protocol integrates energy consumption, node trust scores, and route efficiency. By calculating energy efficiency, trust scores, and combined routing metrics, the protocol selects the most suitable paths, balancing energy conservation and reliability in IoT-enabled WSNs

3.4 Optimized Energy-Aware Routing for IoT-Enabled WSNs using Neuro-Fuzzy Clustering and Quantum Firefly Algorithm

The most effective route selection to the target is the goal of the proposed QFO system. The potential routes to the goal are discovered once the model that is being given generates a fitness function shown in Figuer 6. Subsequently, the QFO algorithm selects the best path to the target among the options. It is presumed that the method of finding the best route from source S to target D is a binary search issue. In this case, the destination including k pathways made utilizing an intermediate node between source and destination nodes is indicated by $D = \{p_1, p_2, \ldots, p_k\}$. One firefly's amount of light is determined by the encoded cost function's structure; the intensity corresponds to the goal success function's value.

Algorithm: Optimized Energy-Aware Routing for IoT-Enabled WSNs

Step 1: Initialization

Network Setup: Deploy sensor nodes randomly in the network field. Initialize node parameters: initial energy $E_{initial}$, transmission power E_{ti}, and node density.

Clustering: Use Neuro-Fuzzy Clustering to form clusters based on node attributes such as energy levels, distances, and node density.

Step 2: Neuro-Fuzzy Clustering:

Fuzzy Membership Functions: Define fuzzy sets for attributes:

Energy Level (E):

$$\mu_{LE}(E) = max\,(0, min\,(1, \frac{E_{max}-E}{E_{max}-E_{low}})) \quad (20)$$

$$\mu_{HE}(E) = max\,(0, min\,(1, \frac{E-E_{low}}{E_{high}-E_{low}})) \quad (21)$$

Distance to Nearest Cluster Head (D)

$$\mu_N(D) = max\,(0, min\,(1, \frac{D_{max}-D}{D_{max}-D_{near}})) \quad (22)$$

$$\mu_F(D) = max\,(0, min\,(1, \frac{D-D_{near}}{D_{far}-D_{near}})) \quad (23)$$

Node Density (N)

$$\mu_S(N) = max\,(0, min\,(1, \frac{N_{max}-N}{N_{max}-N_{sparse}})) \quad (24)$$

$$\mu_D(N) = max\,(0, min\,(1, \frac{N-N_{sparse}}{N_{dense}-N_{sparse}})) \quad (25)$$

Rule Base and Inference: Apply fuzzy rules to determine cluster heads:

Rule 1: If E is High and D is Near, then Node is a Suitable Cluster Head.
Rule 2: If E is Low and N is Sparse, then Node is not a Suitable Cluster Head.

Fuzzy Inference System: Calculate the degree of membership and aggregate results to determine cluster heads.

Step 3: Quantum Firefly Algorithm for Routing Optimization

Initialize fireflies with random positions and velocities in the search space.

Define objective functions for energy and trust metrics.

Objective Functions

Energy Efficiency (EE): $EE_R = \frac{1}{\sum_{x=1}^{n} EC_x}$ (26)

Trust Score (TS): $TS_x = \alpha.TS_{previous} + \beta.Performance_x$ (27)

Firefly Update Rules: Update positions and velocities of fireflies based on attractiveness and distance:

$$v_x(t+1) = wv_x(t) + c_1r_1(p_x - i_x) + c_2r_2(g - i_x) \quad (28)$$
$$i_x(t+1) = i_x(t) + v_x(t+1) \quad (29)$$

Fitness Function: Compute the combined routing metric:

$$CRM_P = \frac{PEE_P.PTS_P}{max(PEE).max(PTS)} \quad (30)$$

where PEE_P and PTS_P are the energy efficiency and trust score for the path P, respectively.

Step 4: Routing Decision: Select the route with the highest CRM.

Step 5: Simulation and Evaluation

Implement the algorithm in a network simulator.
Evaluate performance metrics

Step 6: Update Clusters: Periodically update clusters and routing paths based on current network conditions and node statuses.

The algorithm integrates Neuro-Fuzzy Clustering for cluster formation and QFO algorithm for routing optimization, balancing energy efficiency and trustworthiness. It uses fuzzy logic to dynamically form clusters and quantum-inspired techniques to optimize routing paths, ensuring effective and efficient communication in IoT-enabled WSNs

4. Results and Discussions

The 200x200 m^2 area has the sensor nodes dispersed at random. The initial power source of 2J is used to deploy a range of 20 to 100 sensor nodes. The proposed method is assessed and assessed using appropriate criteria of proposed and existing systems shown in Figure 7.

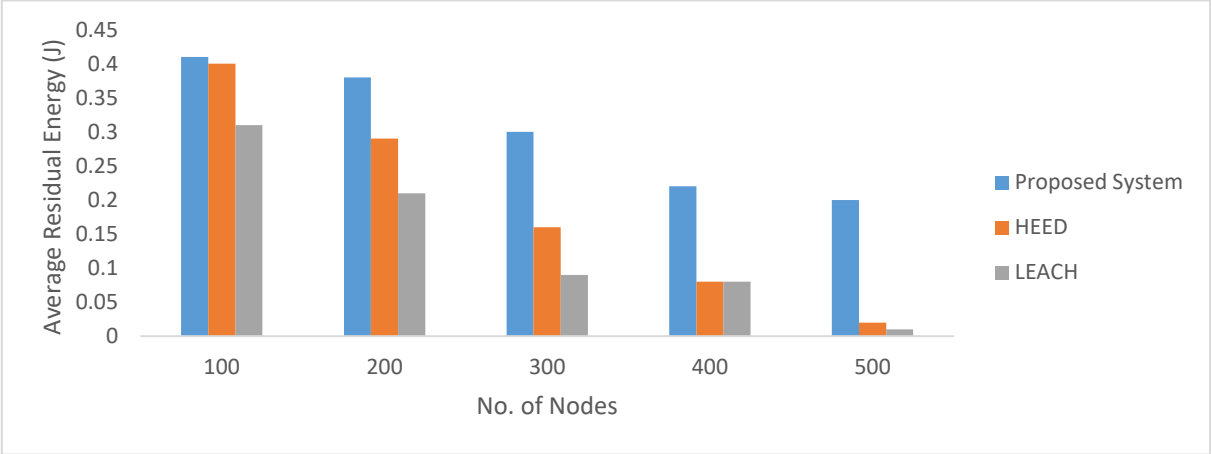


Figure 7: Analysis of Residual Energy on cluster-based routing

Comparing this study with LEACH and HEED, Figures 8 depict the network's efficiency assessment based on the remaining energy and lifetime of the network. The median residual energy remaining after a certain number of rounds is shown in Figure 8. The investigation reveals that compared to current methods, the proposed technique has greater residual energy.

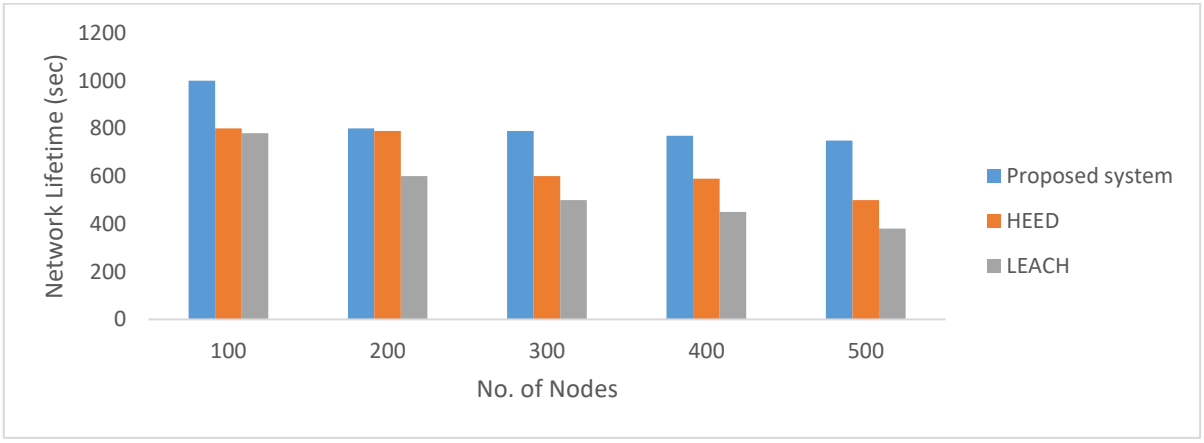


Figure 8: Network Lifetime analysis of cluster-based routing algorithm

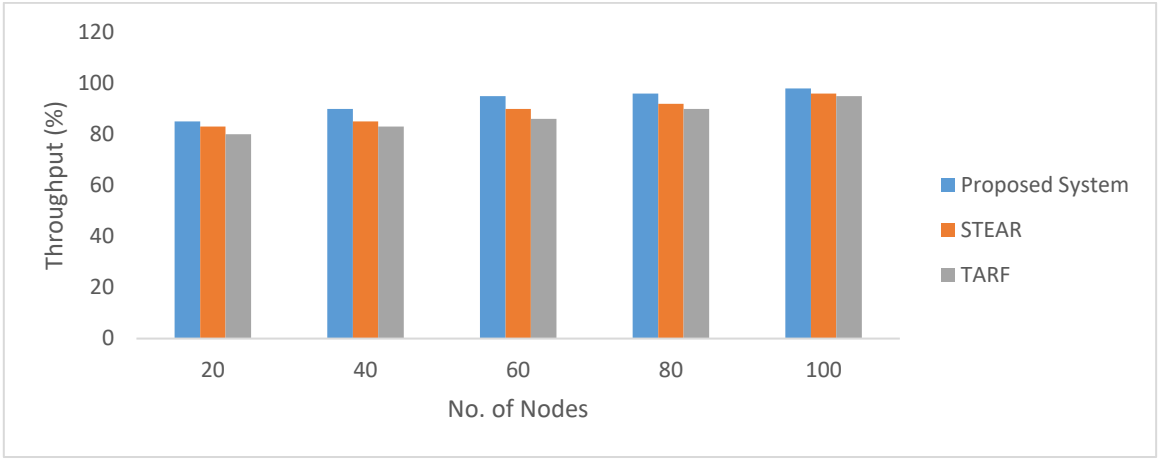
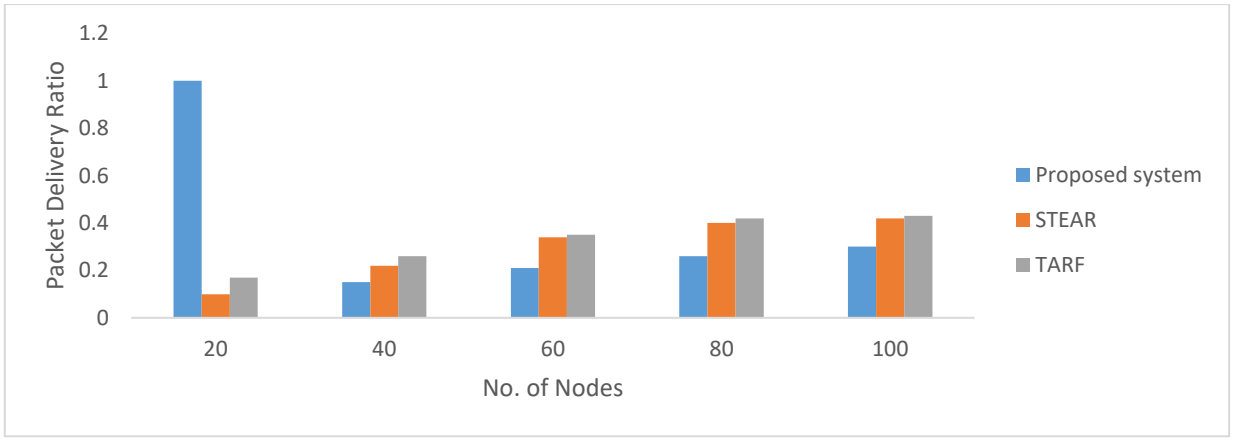
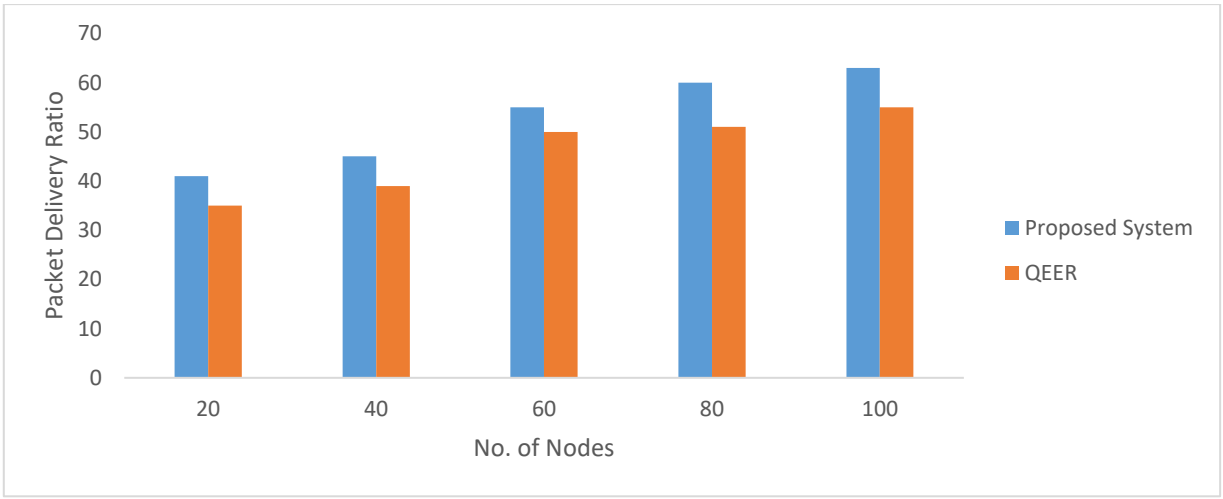


Figure 9: Analysis of Throughput (secured routing algorithm)

The throughput study is carried out in Figure 9 by contrasting the proposed method with two related methods, TARF and STEAR. The STEAR method outperforms the TARF method in terms of throughput. It has been demonstrated that the throughput of this proposed algorithm is superior to that of the other existing methods, specifically STEAR and TARF.



(a) Analysis of PDR (Security)



(b) Analysis of PDR (Energy)

Figure 10: Analysis of PDR

When contrasted with the two current algorithms—STARF and STEAR—Figure 10 (a) shows that the proposed method offers a higher PDR. By separating the malicious node using trust modeling and preventing packet drops by the malicious nodes, the proposed method improves efficiency. Using confidence modeling, these methods were contrasted for secured transportation. Fuzzy temporal restrictions were employed in the proposed technique to enhance safety performance. The proposed algorithm outperforms the existing QEER method in Figure 10 (b) in terms of optimized power use and a higher ratio of packets delivered.

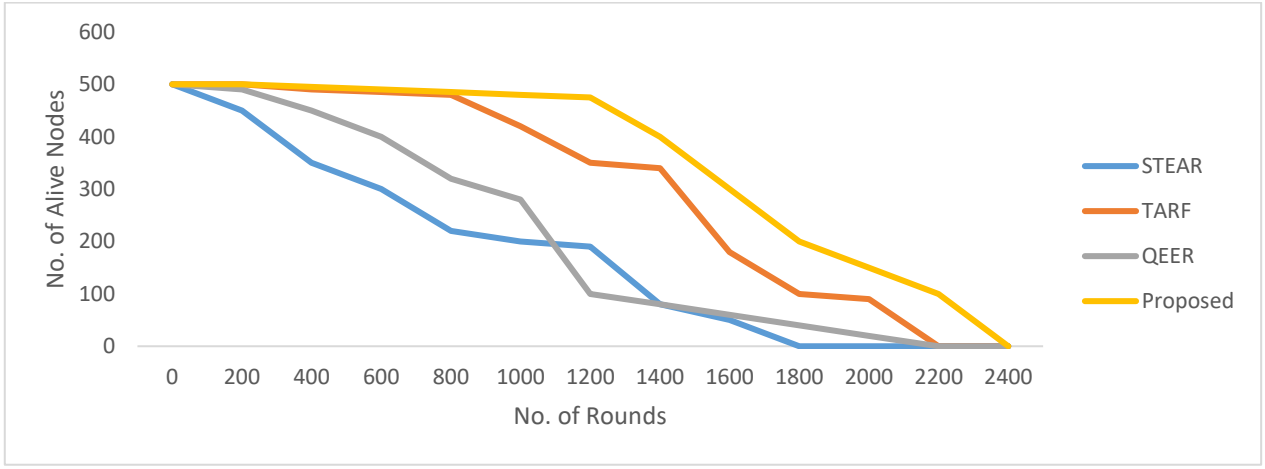


Figure 11: Analysis of No. of alive nodes

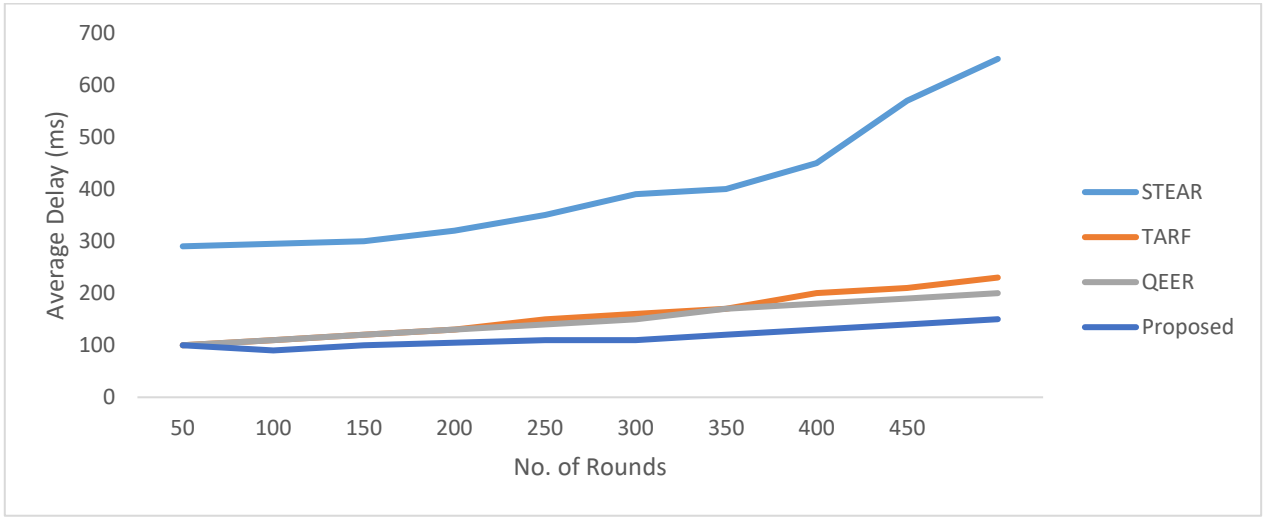


Figure 12: Average delay analysis

Figures 11 and 12 present the mean delay assessment of the QFO technique using current methodologies. The graphic illustrates how the QFO approach has demonstrated superior performance with the lowest median latency under different node counts. Packet loss analysis shown in Figure 13

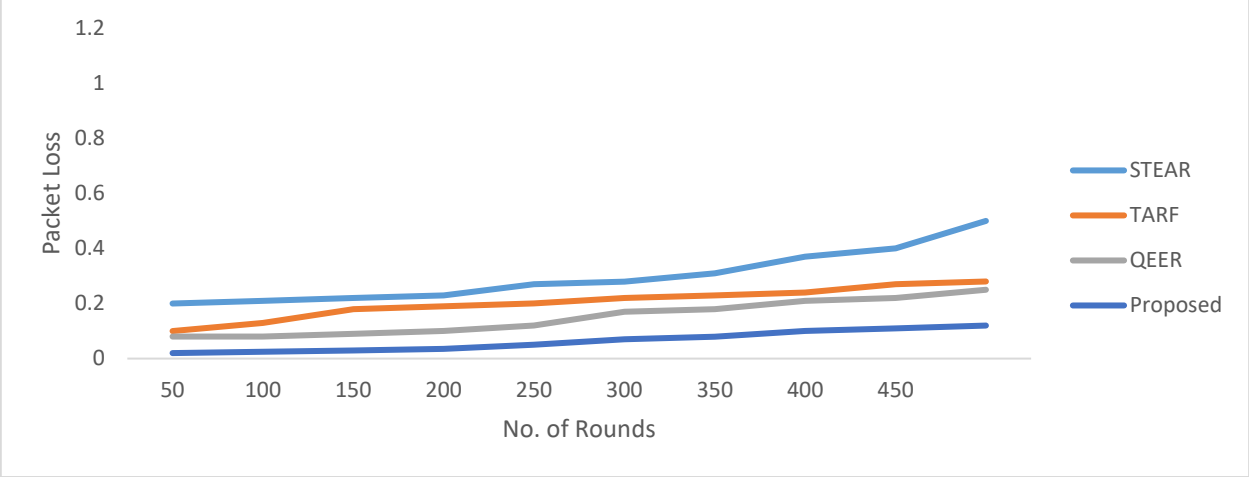


Figure 13: Proposed model packet loss analysis

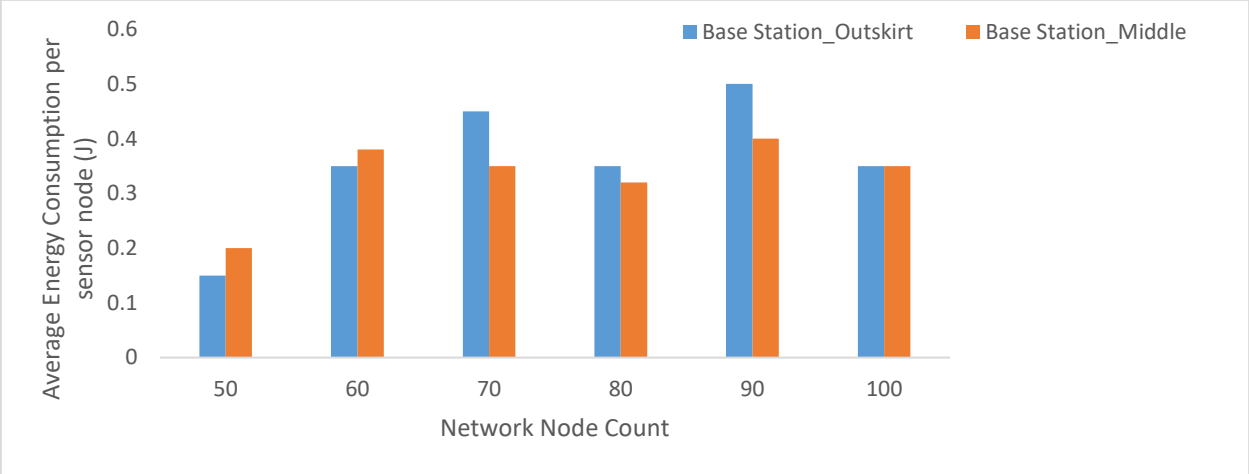


Figure 14: Average energy consumed per sensor node based on node count in the sensing field

According to Figure 14, the median amount of energy used by a sensor node within the network's detecting field during Scenario 1 is 0.14 J, while whenever the distributed node count reaches 50 is 0.18 J. The amount of power that each sensor node uses will keep rising as more nodes join the network together.

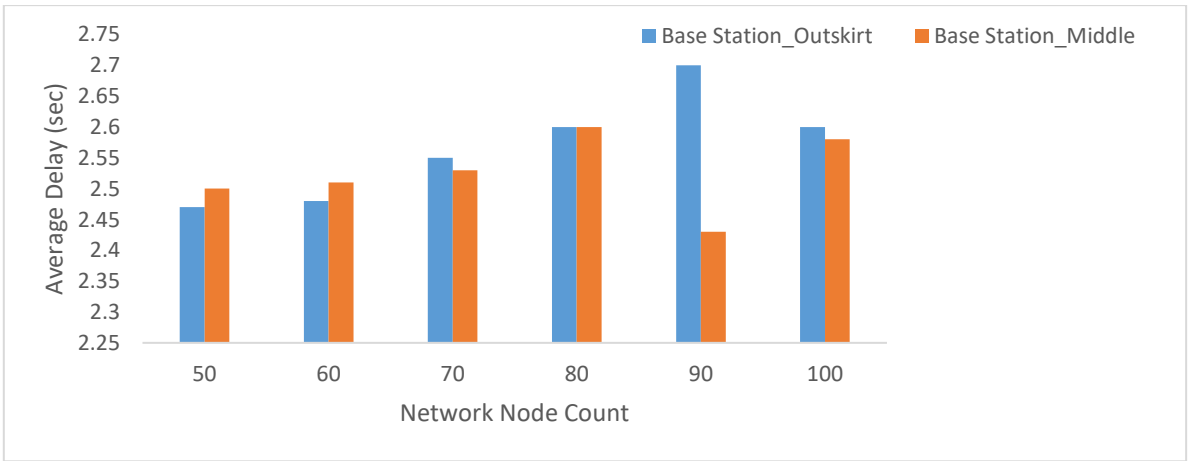


Figure 15: Network delay at different networking node count

Growth in the number of network nodes should reduce the time needed to process packets arriving at the sink node in an effective tree-based network. Figure 15 indicates a modest increase in the packet reception latency.

5. Conclusions

By employing the QFO for routing improvement and Neuro-Fuzzy Clustering for smart cluster development, the proposed method significantly improves energy utilization through route selection improvement. Longer network lifetimes and lower operating costs are the outcomes. QFO significantly refines choices regarding routing according to conservation of energy and trust measures, while the incorporation of Neuro-Fuzzy Clustering guarantees precise and dependable cluster formation. By including trust scores in the routing process issues with unreliable nodes are addressed, and data transmission reliability is increased. The algorithm exhibits scalability and adaptability, as it can proficiently manage fluctuations in network conditions and growing network sizes by periodically updating clusters and routing patterns. Empirical findings reveal significant enhancements in energy usage, packet delivery percentage, and network longevity rendering the proposed approach a workable and efficient resolution for actual IoT-connected wireless sensor networks.

References

[1] Verma, V., & Jha, V. K. (2024). Secure and energy-aware data transmission for IoT-WSNs with the help of cluster-based secure optimal routing. *Wireless Personal Communications*, *134*(3), 1665-1686.
[2] Lei, C. (2024). An energy-aware cluster-based routing in the Internet of things using particle swarm optimization algorithm and fuzzy clustering. *Journal of Engineering and Applied Science*, *71*(1), 135.
[3] Siddiq, A., & Ghazwani, Y. J. (2024). Hybrid Optimized Deep Neural Network Based Intrusion Node Detection and Modified Energy Efficient Centralized Clustering Routing Protocol for Wireless Sensor Network. *IEEE Transactions on Consumer Electronics*.
[4] Suresh, S. S., Prabhu, V., Parthasarathy, V., Senthilkumar, G., & Gundu, V. (2024). Intelligent data routing strategy based on federated deep reinforcement learning for IOT-enabled wireless sensor networks. *Measurement: Sensors*, *31*, 101012.
[5] Heidari, E. (2024). A novel energy-aware method for clustering and routing in IoT based on whale optimization algorithm & Harris Hawks optimization. *Computing*, *106*(3), 1013-1045.
[6] Srivastava, A., & Paulus, R. CTSR-DL: Cluster based trusted secure aware routing for WSN Assisted IoT using deep learning technique.
[7] Karunkuzhali, D., Meenakshi, B., & Lingam, K. (2024). A QoS-aware routing approach for Internet of Things-enabled wireless sensor networks in smart cities. *Multimedia Tools and Applications*, 1-27.
[8] Janarthanan, A., & Srinivasan, V. (2024). Multi-objective cluster head-based energy aware routing using optimized auto-metric graph neural network for secured data aggregation in Wireless Sensor Network. *International Journal of Communication Systems*, *37*(3), e5664.
[9] Syed, L., Sathyaprakash, P., Shobanadevi, A., Nguyen, H. H. C., Alauthman, M., Vedaraj, M., & Premalatha, R. (2024). Deep learning-based route reconfigurability for intelligent vehicle networks to improve power-constrained using energy-efficient geographic routing protocol. *Wireless Networks*, *30*(2), 939-960.
[10] Sakthimohan, M., Deny, J., & Rani, G. E. (2024). Secure deep learning-based energy efficient routing with intrusion detection system for wireless sensor networks. *Journal of Intelligent & Fuzzy Systems*, (Preprint), 1-17.
[11] Gupta, D., Bajpai, A., Tiwari, N. K., & Yadav, S. (2024). Energy-Efficient Routing Optimization for Underwater Internet of Things using Hybrid Q-Learning and Predictive Learning Approach. *Procedia Computer Science*, *235*, 45-55.
[12] Aravind, K., & Maddikunta, P. K. R. (2024). Optimized fuzzy logic based energy-efficient geographical data routing in internet of things. *IEEE Access*.
[13] Xiao, Y., & Voronkova, D. K. (2024). A new energy-aware technique to improve the network lifetime of wireless Internet of Things using a most valuable player algorithm. *Cluster Computing*, 1-21.
[14] Udayaprasad, P. K., Shreyas, J., Srinidhi, N. N., Kumar, S. D., Dayananda, P., Askar, S. S., & Abouhawwash, M. (2024). Energy Efficient Optimized Routing Technique With Distributed SDN-AI to Large Scale I-IoT Networks. *IEEE Access*.
[15] Wang, Y., & Yang, Y. (2024). A Novel Secure and Energy-efficient Routing Method for the Agricultural Internet of Things Using Whale Optimization Algorithm. *Journal of Cyber Security and Mobility*, 725-750.

[16] Salim, A., Khedr, A. M., & Osamy, W. (2024). Enhancing IoT-enabled Sustainable Smart Cities with Secure and Energy-Aware Data Collection using Meta-heuristic Technique. *IEEE Sensors Journal*.
[17] Balraj, L., & Prasanth, A. (2024). An energy-aware software fault detection system based on hierarchical rule approach for enhancing quality of service in internet of things-enabled wireless sensor network. *Transactions on Emerging Telecommunications Technologies*, *35*(4), e4971.
[18] Sagar, V., Chander, G. B., & Guravaiah, K. (2024). Learning-based intelligent energy efficient routing protocols in WSN. In *Intelligent Wireless Sensor Networks and the Internet of Things* (pp. 19-44). CRC Press.
[19] Saritha, K., & Sarasvathi, V. (2024). An Energy-Efficient and QoS-Preserving Hybrid Cross-Layer Protocol Design for Deep Learning-Based Air Quality Monitoring and Prediction. *SN Computer Science*, *5*(3), 307.
[20] Hu, L., Han, C., Wang, X., Zhu, H., & Ouyang, J. (2024). Security Enhancement for Deep Reinforcement Learning-Based Strategy in Energy-Efficient Wireless Sensor Networks. *Sensors*, *24*(6), 1993.
[21] Yadawad, S., & Joshi, S. M. (2024). Efficient energy consumption and fault tolerant method for clustering and reliable routing in wireless sensor network. *Peer-to-Peer Networking and Applications*, 1-17.
[22] Le, V. T., Vo, N. S., Bui, M. P., & Le, L. P. (2024, February). Energy and Distance Aware Clustering-Based Routing for Low-Power IoT-Enabled Wireless Sensor Networks. In *International Conference on Industrial Networks and Intelligent Systems* (pp. 139-154). Cham: Springer Nature Switzerland.
[23] Kumar, S., Mahadev, R. G., Kamal, P., & Aggarwal, A. (2024). Original Research Article An optimized deep learning-based fault-tolerant mechanism for energy efficient data transmission in IoT. *Journal of Autonomous Intelligence*, *7*(4).