Trust Aware Nero Fuzzy Based Agglomerative Hierarchical Clustering with Secure Whale Optimization Routing for Enhancing Energy Efficiency in WSN

[1]Sasikumar M S S and [2]Narayanan A E
[1,2] Department of Computer Science and Engineering, Periyar Maniammai Institute of Science &Technology,
Vallam, Thanjavur, India.
[1]sasi7273@gmail.com, [2]aenan_jack@pmu.edu

Correspondence should be addressed to Sasikumar M S S : sasi7273@gmail.com.

Article Info
Journal of Machine and Computing (http://anapub.co.ke/journals/jmc/jmc.html)
Doi: https://doi.org/10.53759/7669/jmc202404014
Received 02 June 2023; Revised from 25 August 2023; Accepted 02 November 2023.
Available online 05 January 2024.

Abstract – Wireless sensor networks (WSNs) comprise a network of dispersed, carefully positioned sensor nodes in their deployment environment to monitor and collect data on natural phenomena. These sensor nodes collaborate to transmit data via multi-hop communication, ultimately reaching a central base station for processing. However, WSNs face significant challenges due to the resource-constrained nature of these devices and the harsh, open environments in which they operate. Addressing energy optimization and ensuring secure communication are primary concerns in the successful operation of WSNs. This paper introduces anovelTrust aware Neuro Fuzzy Clustering head selection (TNFCH) and agglomerative hierarchical clustering approach (AHC) with Secure Whale Optimization (SWO) Algorithm Routing to enhance energy-efficient transmission in WSNs. Our proposed protocol (TNFCH-AHWO) efficiently organizes nodes by utilizing neural network and Fuzzy logic then securely transfers the data into the communication network. We employ a Trust calculation algorithm in our system to ensure Trust and data integrity, facilitating efficient lightweight operations such as key generation, encryption, decryption, and verification. This ensures hop-to-hop authentication among the nodes in WSNs. To assess the performance of our proposed protocol, we conducted simulations using the NS3 simulator. The findings of the simulation show that the suggested protocol greatly enhances various performance metrics, including energy consumption analysis, throughput, network delay, network lifetime, and packet delivery ratio when compared to existing protocols.

Keywords – Clustering, Cluster Head, Routing, Trust Awareness, Optimization, Network Energy Efficiency.

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a distinct network category within ad hoc networks. It comprises numerous nodes not fixed in a single location but randomly dispersed throughout a sensing field [1]. This random allocation of nodes in WSNs is crucial in monitoring and capturing data from locations that are typically inaccessible to humans [2]. Consequently, sensor nodes within WSNs are equipped with self-contained computing resources, including processing capabilities, storage capacity, and batteries [3]. A typical sensor node can execute three fundamental operations: sensing, transmitting, and processing data within the deployment area [4]. The deployment of sensor nodes is determined by their communication, energy, and storage capabilities [5]. Initially, energy consumption is noticeable when nodes initiate communication. If a region under surveillance is generally overlooked, there may be no feasible solution for repairing or restoring the sensor nodes [6]. The network's stability is compromised when an inactive node is detected, necessitating topology modifications and retransmissions. Consequently, the battery life of sensor nodes in WSNs is diminished, impacting the overall network lifetime [7]. Furthermore, addressing energy efficiency challenges is a crucial aspect of managing WSNs.

In WSNs, the conservation of energy in nodes with sensors is crucial [8]. It grouped different network nodes to enable effective communication between a Cluster Head (CH) and the base station. This is known as clustering [9]. Choosing an appropriate cluster and a suitable CH takes a lot of effort and time. Currently, many strategies are used to find appropriate CHs [10]. Clustering techniques are essential to WSNs because they provide flexible and scalable routing while proving energy efficiency. Each cluster must appoint a CH to manage crucial internal processes.

The clusters play a pivotal role by not only gathering data but also integrating and directing this integrated data towards the Base Station (BS) [11]. The CH assumes a central role within each cluster, facilitating communication with other sensor nodes, the BS, or CHs in different clusters. This communication addresses various factors critical for achieving efficient routing. Such interactions contribute significantly to enhancing network performance in terms of maximizing its lifetime and implementing energy-saving routing strategies in the context of WSNs [12].

Finding the shortest or ideal path for efficient data communication is one of the main goals of routing, which is an essential requirement in WSNs. The three basic categories into which WSN routing protocols fall are data-centric, hierarchical, and geographic-based routing protocols. By following routing algorithms, these protocols allow data to be transmitted from nodes that are sources to sink sites or the base station [15].

Energy conservation is paramount in the realm of WSNs. Designing energy-efficient algorithms for communication is imperative to ensure the network's longevity and effectiveness. One of the critical factors to consider is that as the routing distance within the network increases, so does the energy consumption [13][20]. Hence, it becomes vital to establish an efficient path for routing the data collected by sensor nodes to the base station.

In the context of this paper, a novel approach is proposed to address the energy-efficiency challenge by utilizing a fuzzy system for routing data along an optimal path. The existing Energy-Efficient Routing Framework (EERF) has been developed to support multi-hop routing. EERF achieves this by generating the least distant and most energy-efficient routing path, reducing the overall energy consumption in the network. However, this paper explores two additional routing strategies: TNFCH-AHWO algorithms which is routing by whale optimization algorithm, and clustering is adopted as the preferred method for data communication. Clustering leverages the principles of fuzzy logic to create unequal clusters within the network, optimizing energy consumption during data transmission. This innovative approach aims to strike a balance between energy efficiency and routing distance, ultimately enhancing the overall performance of the WSN.

The TNFCH-AHWO algorithms represent a comprehensive approach to optimizing wireless sensor networks. Through a three-step process involving neuro-fuzzy clustering, AHP-based CH selection, and secure data transfer using the Whale Optimization Algorithm (WOA), these algorithms aim to enhance network performance, energy efficiency, and data security. This multi-faceted approach ensures that the network operates efficiently and securely, meeting the demands of various applications and environments. The following contribution of this paper,

- The primary goal of the proposed scheme is to enhance the security of the data routing process in a WSN while minimizing energy consumption.
- This paper introduces a novel TNFCH-AHWO, a protocol that enhances energy efficiency in WSNs through innovative clustering techniques and routing optimization.
- agglomerative hierarchical clustering approach (AHC) with Secure Whale Optimization (WOA) Algorithm Routing contributes by introducing novel techniques that optimize clustering, routing, and energy efficiency in WSNs

In the structure of this paper, we have made the necessary adjustments to align the section titles with standard formatting. **Section 2** explores in detail a thorough analysis of related work, providing insights into prior research and developments in the field. **Section 3** outlines our proposed approach and its formulation, shedding light on our work's novel methods and techniques. In **Section 4,** we present our Clustering and Optimized Routing Algorithm, highlighting its innovative aspects and part in improving wireless sensor network performance. Moving on to **Section 5**, we conduct a detailed analysis of the results obtained from our experiments, offering valuable insights and observations. Finally, in **Section 6**, we draw our paper to a close by presenting our conclusions and discussing potential avenues for future research and development in this domain.

II. RELATED WORK

The basic structure of a hierarchical WSN is illustrated in **Fig 1** above. This network architecture comprises a two-level hierarchy, with clusters distributed throughout the network. Each cluster in the network designates a CH responsible for tasks such as data collection and aggregation. The nodes neighboring the cluster head belong to the upper-level nodes, while the other nodes in the network are categorized as subsequent-level nodes. The CHs within each cluster collect data from their neighboring Sensor Nodes (SNs) and transmit it directly to the Base Station (BS). After performing data aggregation, they may also route data through other intermediate cluster heads. However, it is essential to note that cluster heads consume more energy compared to cluster member (CM) nodes, primarily due to their involvement in long-distance communication with the BS [9].

The routing process in WSN-based networks presents common challenges, including energy consumption and the emergence of routing holes that can lead to sensor disconnections. Efficient routing techniques are essential to address these issues effectively. Proper routing techniques play a crucial role in extending the lifetime of sensors and ensuring the network's reliability. One widely adopted hierarchical-based routing technique is the Low Energy Adaptive Clustering Hierarchy (LEACH) [10]. LEACH operates with three main objectives:

- Network Lifetime Enhancement: LEACH aims to prolong the overall lifetime of the network by efficiently managing energy resources. This is achieved by dynamically selecting CHs in a round-robin fashion, allowing nodes to take turns assuming the CH role and evenly distributing the energy consumption across the network.
- Reducing Energy Dispersal: The protocol seeks to reduce energy wastage by aggregating data at the CH level before transmission. This aggregation minimizes the energy required for long-distance communication, thus conserving power.
- Minimizing Communication Overhead: LEACH reduces the network's data transmission, further conserving energy. It employs probabilistic methods to determine when nodes should communicate with the CHs, reducing unnecessary data exchanges.

The hierarchical WSNs are structured with clusters and CHs for efficient data collection and transmission. However, the energy consumption of CHs can be a concern, especially for long-distance communication. Routing challenges, such as routing holes, can disrupt the network. However, techniques like LEACH are designed to address these issues by enhancing network lifetime, reducing energy dispersal, and minimizing communication overhead.

Trust-aware routing uses a trust metric or model to evaluate the reliability of individual sensor nodes. These metrics assign numerical values based on node behaviour, historical performance, and network interactions. Trust considers data forwarding reliability, energy efficiency, security practices, and responsiveness to network requests. Trust values evolve, calculated from direct or indirect observations. Methods like weighted averaging or fuzzy logic aggregate these values to compute an overall trust score for each node. Routing decisions in trust-aware routing depend on node trustworthiness, favoring more trustworthy nodes as relay points to enhance data security and reliability.

Trust-aware routing approaches have been designed to detect deception using routing information. However, these methods may not effectively address various devastating attacks on routing protocols, such as Sybil attacks, sinkhole attacks, or wormhole attacks [17]. These routing-based security solutions may only cover some possible threat scenarios. WSNs are vulnerable to numerous security threats, including authentication attacks, stealthy attacks, and breaches of data secrecy [18]. Such attacks can compromise the network's ability to perform its intended functions and undermine the reliability of data transmission.

Many security techniques in WSNs leverage optimization algorithms to achieve secure data transmission. While these algorithms can enhance security, they often introduce additional time overhead, making data transmission more time-consuming and potentially affecting network performance negatively [19]. One of the primary challenges is establishing trust among sensor nodes. This process can be complex and resource-intensive, mainly due to the energy constraints of sensor nodes. Determining how to achieve trust efficiently remains to be determined. Moreover, disseminating trust information throughout the network poses a significant challenge as it can result in excessive energy usage and challenges in locating suspicious nodes [15][21]. While effective at managing intrinsic attacks in WSNs, trust-based schemes often rely heavily on specific route methodologies or platforms [16]. This over-reliance on a particular routing method can limit the adaptability and robustness of the security scheme, especially in dynamic network environments.

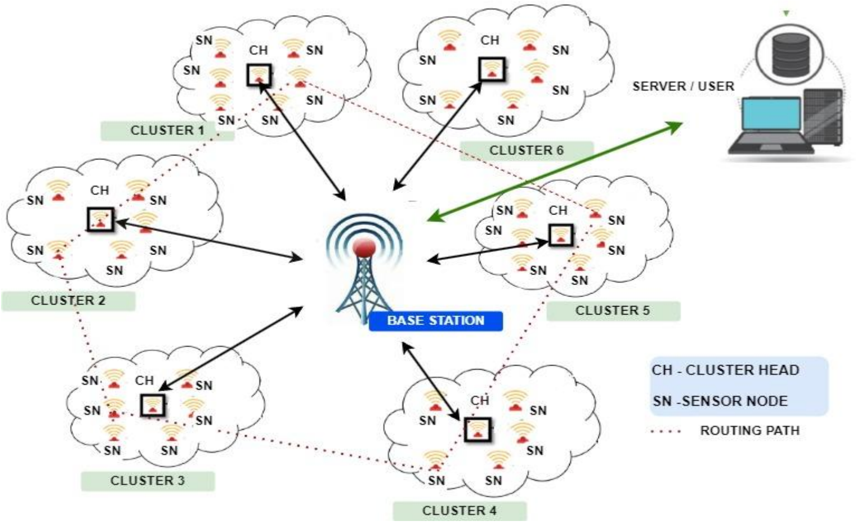


Fig 1. WSN System Representation Diagram

III. PROPOSED WORK AND FORMULATION

System Model

The network model of WSN is based on a set of fundamental assumptions that define its characteristics and operation shown in **Fig 1.** These assumptions include:

- *Homogeneous Sensor Nodes:* All sensor nodes in the network are considered homogeneous, meaning they possess identical initial energy levels and have equivalent communication and processing capabilities. However, it is essential to note that the energy levels of these sensor nodes cannot be extended or replenished after deployment.
- *Stationary Nodes:* After initial deployment, the sensor nodes and the Base Station remain stationary. They do not change their positions during the network's operation.
- *Location Awareness:* Sensor nodes are equipped with the capability to determine and transmit their geographical locations. This information can be crucial for various network operations and applications.
- *Base Station Resources:* The Base Station (BS) is assumed to have significantly higher computational power than the sensor nodes and is not subject to energy constraints. This allows the BS to perform complex data processing tasks efficiently.
- *Data Forwarding to Cluster Heads (CH):* Sensor nodes periodically estimate the network's infrastructure and systematically transmit data to their respective Cluster Heads (CH). Cluster Heads are key in aggregating and forwarding data to the BS.
- *BS Proximity:* The Base Station is strategically located within the transmission range of all sensor nodes to ensure reliable communication with the entire network.
- *Symmetric Links:* Communication links between sensor nodes and the Base Station are assumed to be symmetric, meaning the quality of communication in both directions is similar.
- *Cluster Head Election:* Cluster Heads (CH) are elected and strategically located within the network to effectively facilitate data transmission and routing processes.

Collectively, these assumptions provide the foundational framework for modelling and analyzing the behaviour and performance of the Wireless Sensor Network under consideration. Researchers and engineers can use these assumptions to design and evaluate various protocols, algorithms, and strategies for efficient data gathering and communication within the network.

Clustering Methods of WSN

The clustering strategy is a critically important approach for efficiently managing energy resources in wireless sensor networks (WSNs) and has garnered significant attention as a promising area of research. However, achieving balanced energy utilization remains a persistent issue due to the close relationship between Cluster Head (CH) activities and nodes' specific roles and locations within the sensing field. Clustering is highly favoured in the realm of routing strategies for WSNs [31, 32] for several compelling reasons, including:

- **Relay Packet Minimization**: Clustering reduces the number of relayed packets by aggregating data gathered by sensor nodes. This minimizes unnecessary data transmission, conserving energy.
- **Collision Prevention:** By restricting redundancy in coverage, clustering helps prevent medium access collisions, ensuring more efficient and reliable communication.
- **Scheduled Activities:** Clustering enables scheduling activities within the cluster, optimizing resource usage and enhancing overall network operations.
- **Topology Management**: It helps solve the overhead associated with topology management, ensuring the network structure remains stable and efficient.
- **Reduced Redundant Messages**: Clustering also mitigates redundant message exchanges, saving energy and reducing network congestion.
- **Bandwidth Conservation**: It conserves communication bandwidth by aggregating and optimizing data transmission.
- Route Localization: Clustering aids in the localization of route setup, improving the efficiency of data routing.

Sensor nodes in a clustered WSN are usually classified as cluster members if located inside a particular cluster's coverage area. Their primary function in a clustered WSN is to provide sensed data to the Cluster Head (CH), who is the appointed leader. Then, to reduce transmission energy usage, the CH is in charge of forwarding the gathered data to the sink node. This transmission can go via an ideal path made possible by other CHs in the network, or it can go straight to the sink node.

There are two types of traffic on the network in a clustered WSN: intra-cluster traffic and inter-cluster traffic. By clustering, the energy consumption of the CHs and the sensor nodes connected to them is balanced. Nevertheless, because of the closeness of the sink node to the volume of traffic it manages, the CH frequently runs out of energy more quickly. As a result, choosing the best CH is essential to improving network performance while using less energy.

As a result, various clustering techniques and cluster-aided routing protocols have been developed and implemented in WSNs [33, 34]. These techniques aim to address the challenge of unbalanced energy usage by strategically selecting and managing CHs, ultimately improving the overall efficiency and lifespan of the wireless sensor network.

Trust Aware

The primary goal of this approach is to create a trust model designed explicitly for trust-aware routing in WSN This trust model aims to reduce the chances of selecting suspicious or untrustworthy nodes as Cluster Heads (CHs) in the network.

We employ a mechanism called a set of trust parameters to identify trustworthy Cluster Heads. These trust parameters encompass:

- Integrity Factor: This assesses a node's data and actions for integrity and reliability.
- Consistency Factors: These evaluate a node's behaviour over time, searching for anomalies or deviations.
- Forwarding Rate Factor: This considers a node's performance regarding data forwarding and relaying.
- Availability Factors: These examine a node's responsiveness and availability within the network.
- Wireless Communication Mode: All WSN nodes communicate wirelessly and operate in specific modes. The trust model considers the unique communication characteristics of WSNs, emphasizing energy efficiency and resource conservation.
- Energy and Computational Efficiency: The trust model is well-suited for WSNs, as it prioritizes minimizing energy consumption and computational demands. This is crucial in resource-limited sensor networks where energy preservation is essential for extending the network's operational lifespan.

Two main key factors determine the trust relationship between nodes in a WAN: 1) the direct degree of trust and 2) the indirect degree of trust. This trust relationship is established based on the exchange of data packets over time. When evaluating a neighbour node's trustworthiness, nodes consider a trust degree value ranging from 0 to 1.

- A trust degree of 0 signifies a complete lack of trust between nodes.
- A trust degree of 1 indicates complete trust in the neighbouring node.

The trust degree (T) between nodes i and j in the WSN can be mathematically expressed using Equation (1):

$$T_{ij}(u)=\mu T_{ij}^{A}(u)+ŋT_{ij}^{B}(u) \tag{1}$$

In the provided context:

- The term $T_{ij}^{A}(u)$ represents the direct trust degree of node i in node j.
- $T_{ij}^{B}(u)$represents the indirect trust degree of the node i's neighbors in node j at time u.
- The symbols μ andŋ represent weighted constants.

The trust degree between nodes is determined by combining these direct and indirect trust factors using the specified weighted constants. Equations (2) and (3) outline the expressions for calculating the direct and indirect degrees of trust between two nodes in the WSN.

$$T_{ij}^{A}(u)=\frac{PK_{ij(u)}^{R}}{PK_{ij}^{S}(u)} \tag{2}$$

Where $PK_{ij(u)}^{R}$represents the total number of packets node i receives and $PK_{ij}^{S}(u)$expresses the total number of packets sent by node i.

$$T_{ij}^{B}(u)=\frac{1}{N}\sum_{u=1}^{N}T_{ij}^{A}(u) \tag{3}$$

"N" represents the number of neighbours of node i.The trust degree described in Equation (1) is subject to periodic updates over time, and a moving average model governs these updates. The expression for updating the trust model is provided in Equation (4):

$$T_{ij}(u+1)=\alpha T_{ij}(u)+(1-\alpha)T_{ij}(u+1) \tag{4}$$

Where $T_{ij}(u+1)$ represents the updated trust degree at time u+1, $T_{ij}(u+1)$ represents the trust degree of node j as perceived by node i at time u+1. The termα represents a weight factor that balances the trust at each iteration.

The update equation indicates how the trust degree between nodes i and j, denoted as $T_{ij}(u+1)$, is calculated at time t+1 based on the trust degree perceived by node i, and the weight factor αThis update process helps adjust the trust values between nodes as the network dynamics change. The formula for calculating would depend on the trust model and the trust update strategy used in the WSN.

Factor Availability

Node i transmits a source packet to determine whether node j can receive this packet. If i receives an acknowledgement from j, it confirms the availability of j. Equation (4) calculates the availability factor of neighbouring nodes**.**

$$A(u)=\frac{QPK_{ij}(u)}{QPK_{ij}(u)+NAPK_{ij}(u)} \tag{5}$$

Where $QPK_{ij}(u)$ represents the number of packets acknowledged, and $NAPK_{ij}(u)$ indicates the number of packets that have not yet received acknowledgement.

Energy Efficiency

The transmitter requires energy to power the radio electronics and the power amplifier. Similarly, the receiver expends energy to operate its radio electronics. Additionally, the energy consumption of a node is directly related to the amount of data to be transmitted and the distance over which it needs to be sent. To account for energy losses with distance, this model employs an energy loss formula of d^2 for relatively short distances and d^4 for longer distances, where "dij" represents the distance between sensor nodes i and j. The propagation distance (d) is compared to a threshold distance, d0, to determine which formula to use. If the propagation distance (d) is less than d0, the energy consumption of a node is proportional to d^2; otherwise, it is proportional to d^4. The energy a node consumes when transmitting an l-bit data packet is calculated using Equation 6**.**

$$E_{Total}(l,d) = l\,.E_{TR}+ l\,.\,E_{TR}.\,\varepsilon_{fs}.\,d^2 \quad \text{if } d<d0 = l\,.E_{TR}+ l\,.\,E_{TR}.\,\varepsilon_{mp}.\,d^4 \quad \text{if } d>d0 \tag{6}$$

In this context, E_{TR} represents the energy dissipation per bit for both the transmitter and receiver circuits. The value of E_{TR} is influenced by various factors, including digital coding, modulation techniques, and signal spreading. For free-space transmission, the amplifier energy is denoted as ε_{fs}. At the same time, the multi-path model is represented as ε_{mp}, and its specific value depends on the characteristics of the transmitter amplifier model.The energy expended by the receiver during the reception of an l-bit data packet can be calculated using Equation 7.

$$E_{RX}(\,l\,) = l\,.\,E_{TR} \tag{7}$$

Nero Fuzzy Based Clustering Head Selection

Neuro-fuzzy techniques are hybrid approaches that combine elements Combining fuzzy logic systems with artificial neural networks (ANNs) to tackle challenging issues. These techniques aim to leverage the strengths of both neural networks and fuzzy logic to create more flexible, adaptive, and interpretable systems. A mathematical approach called fuzzy logic addresses imprecision and uncertainty. It uses linguistic variables, fuzzy sets, and fuzzy rules to model and reason with vague or ambiguous information.

Computational models called artificial neural networks are based on the architecture and operations of the human brain. They consist of interconnected nodes (neurons) organized in layers for learning and decision-making, as shown in **Fig 2**.

Neuro-fuzzy techniques combine the principles of fuzzy logic and neural networks to create hybrid systems. One approach is to represent and reason with fuzzy logic linguistic variables and rules, while neural networks offer learning and adaptation capabilities. In neuro-fuzzy systems, neural networks are often used to adapt fuzzy membership functions, fuzzy rules, or other parameters based on input data. This adaptation allows the system to learn from examples and adjust its behaviour over time.

Neuro-fuzzy systems typically produce rule-based models that explain how inputs and outputs are related in a human-readable format. These rules are often expressed in natural language and provide insights into the system's decisions. The neuro-fuzzy techniques provide a robust framework for solving problems that involve uncertainty and require adaptive learning. They find applications in diverse fields where decision-making and modelling of complex systems are essential. These techniques offer the benefits of fuzzy logic and neural networks, making them valuable tools for addressing real-world challenges.

The proposed Routing WSN

The proposed BWSO algorithm plays a crucial role in the route optimization of the designed WSN routing strategy. This algorithm is specifically tailored for achieving effective communication in an energy-efficient manner. Here is an expanded explanation of the BWSO algorithm and its significance in WSN route optimization.

The BWSO algorithm is employed to enhance the routing strategy within the WSN. Its primary objective is to optimize the selection of CH and determine the optimal communication path between CHs to conserve energy during data transmission. The BWSO algorithm's enhanced convergence capabilities lead to a faster and more efficient route optimization process. This improved route selection ultimately translates into a more extended network lifetime and reduced energy consumption in the WSN. The algorithm's energy-efficient communication and route optimization contribute significantly to the overall performance and sustainability of the wireless sensor network.

The BWSO algorithm represents an innovative approach to WSN route optimization. Integrating elements and leveraging fitness-derived random number generation addresses the challenges of energy-efficient communication and route selection. This algorithm's ability to accelerate convergence and increase the network's longevity while conserving energy makes it a valuable tool in wireless sensor network design and management.

Energy efficiency of WSN

Conventional techniques for addressing security and trust-related challenges in WSNs often encounter several significant issues. The elaborates on these challenges and provides additional context, In light of these challenges, it is evident that security and trust management in WSNs require careful consideration and innovative solutions. Researchers and practitioners in WSNs must strive to develop security mechanisms that balance the need for trust and protection against various attack vectors while minimizing the impact on network performance and resource utilization. As WSNs continue to play critical roles in various applications, addressing these challenges is essential to ensure their reliability and security in real-world deployments.

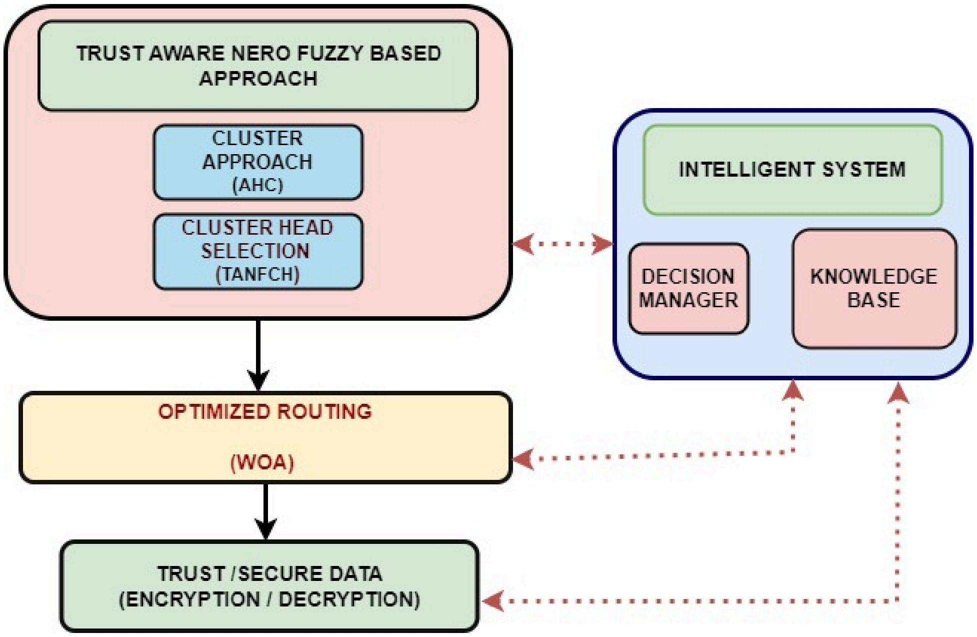

TRUST AWARE NERO FUZZY BASED APPROACH
CLUSTER APPROACH (AHC)
CLUSTER HEAD SELECTION (TANFCH)
INTELLIGENT SYSTEM
DECISION MANAGER
KNOWLEDGE BASE
OPTIMIZED ROUTING (WOA)
TRUST / SECURE DATA (ENCRYPTION / DECRYPTION)

Fig 2. Proposed Framework Diagram

III. CLUSTERING AND OPTIMIZED ROUTING ALGORITHM

The proposed TANFC-AHWO algorithms are designed to optimize the operation of WSNs through a comprehensive three-step process. These steps aim to improve the network's efficiency, reliability, and security while ensuring the successful transfer of data. The following are three steps of proposed an expanded explanation of each step:

- Clustering Using agglomerative hierarchical (AHC)
- Cluster Head Selection Using Neuro-Fuzzy Clustering (TANFCH)
- Secure Data Transfer Using Whale Optimization Algorithm (WOA)

Clustering Using Agglomerative Hierarchical

In the first step of the TANFC-SWO algorithms, the network undergoes clustering using the innovative neuro-fuzzy clustering technique, referred to as TANFC. Neuro-fuzzy clustering is a sophisticated approach that combines neural networks and fuzzy logic to organize sensor nodes into clusters efficiently.

Neuro-fuzzy clustering considers various factors such as node locations, sensing capabilities, and communication patterns to group nodes with similar characteristics together. This clustering enhances resource allocation and management within the network. By ensuring that nodes with shared responsibilities and tasks are grouped together, energy consumption is optimized, and the scalability of the network is improved.

The HAC (Hierarchical Agglomerative Clustering) algorithmis a straightforward and mathematically sound approach to data analysis. It can offer insightful descriptions and visualizations of potential data clustering structures, mainly when genuine hierarchical relationships are present in the data.

Applying the HAC algorithm to WSN we devised a six-step clustering process to create well-suited clusters.

Step 1: Acquire the Input Data Set

For HAC the input data consists of a component-attribute matrix. Components represent nodes to be grouped based on their attributes, such as node locations or connectivity data and distance by using the Euclidean distance formula.

Step 2: Calculate Resemblance Coefficients

Resemblance coefficients quantify the similarity between nodes using methods like Euclidean distance for quantitative data. These coefficients capture node relationships. Matches of attribute pairs between any two nodes, denoted as 'a' and 'b,' are counted to calculate the resemblance coefficient, represented as M(a, b) in the simple matching coefficient as shown in Equation (8).

$$M(a,b)=\frac{N_{11}-N_{10}}{N_{11}+N_{10}+N_{01}+N_{00}} \tag{8}$$

Where N_{00}. N_{11}, N_{10}, N_{01} are count of 1-1, 1-0, 0-1, 0-0 matches of attributes= pair of any two nodes.

Step 3: Execute the AHC Algorithm

AHC identifies minimum coefficients in the resemblance matrix, forming a hierarchical tree. It merges clusters iteratively, updating the matrix. Four primary HAC methods are used: SLINK(single linkage), CLINK(Complete Linkage), UPGMA(Un-weighted Pair-Group Method using arithmetic Averages), and WPGMA(Weighted Pair-Group Method using arithmetic Averages) is calculated from Equation 9 to Equation 12 respectively. The outcomes of the HAC algorithm are visualized using a binary tree or dendrogram.

$$M(SLINK)=Min\{M11, M12....Mij....Mmn\} \tag{9}$$

$$M(CLINK)=Max\{M11, M12....Mij....Mmn\} \tag{10}$$

$$M(UPGMA)=\frac{1}{mn}\sum_{i=1,j=1}^{m,n} M(i,j) \tag{11}$$

$$M(WPGMA)=\frac{1}{mn}\sum_{i=1,j=1}^{m,n} Wi\, M(i,j) \tag{12}$$

Step 4: Cluster Pruning

To prevent clusters from growing excessively, we prune the hierarchical tree using a predefined threshold, which can be based on factors like transmission radius, desired cluster count, or density. The transmission radius using the UPGMA method with quantitative data and Pruning ensures clusters maintain an appropriate size.

Step 5: Minimum Cluster Management

If a cluster falls below a predefined minimum size threshold, it merges with its nearest neighbouring Cluster shown in Figure 1, and execution of cluster form from **Algorithm 1.**

Algorithm1. Agglomerative Hierarchical Clustering (AHC)

```
function Agglomerative_Hierarchical_Clustering (data, linkage_metric, num_clusters):
# Initialize each data point as a separate cluster
    clusters = InitializeClusters(data)
    while len(clusters) > num_clusters:
# Find the pair of clusters with the smallest linkage_metric
     cluster1, cluster2 = Find_Closest_Clusters(clusters, linkage_metric)
# Merge the two closest clusters into a new cluster
    merged_cluster = Merge_Clusters(cluster1, cluster2)
        # Remove the merged clusters from the list of clusters
        clusters.remove(cluster1)
        clusters.remove(cluster2)
# Add the merged cluster to the list of clusters
        clusters.append(merged_cluster)
return clusters  # Hierarchical structure of clusters
```

Cluster Head Selection Using Neuro-Fuzzy Clustering (TANFCH)

Cluster Head Selection Using Neuro-Fuzzy Clustering (TANFCH) is used in WNS to determine suitable cluster heads among sensor nodes. This method combines neural networks and fuzzy logic to select cluster heads efficiently. Here's a general outline of how the TANFCH algorithm works:

Initialization:

- Initialize sensor nodes and set parameters like network size and communication range.
- Assign random initial energy levels to sensor nodes.

Data Collection:

- Sensor nodes gather data from their surroundings or perform initial data transmissions.

Neuro-Fuzzy Clustering:

- Apply a neural network-based clustering algorithm to group sensor nodes into clusters.
- Features like node distance, remaining energy, and data transmission history can be used as inputs to the neural network.
- The neural network assigns a membership value to each node for each cluster, indicating the node's likelihood of becoming a cluster head.

Fuzzy Logic Refinement:

- Use fuzzy logic to refine the cluster head selection further.
- Fuzzy rules can consider multiple criteria, such as energy levels, node centrality, and network load.
- Calculate a fuzzy score for each node based on these criteria.

Cluster Head Selection:

- Select nodes with the highest membership values or fuzzy scores as cluster heads.
- Cluster heads should have a balance between energy efficiency and network coverage.

Data Aggregation:

- Cluster heads collect data from their member nodes and perform data aggregation or compression to reduce traffic.

Data Transmission:

- Cluster heads transmit aggregated data to a sink node or base station.
- Non-cluster head nodes may enter a low-power state to conserve energy.

Network Maintenance:

- Handle node failures or changes in network topology by re-running the clustering and cluster head selection process as needed.

Performance Evaluationof the network's performance in terms of energy efficiency, data delivery, and other relevant metrics. Fine-tune algorithm parameters if necessary.TANFCH aims to prolong the network's lifetime by intelligently selecting cluster heads based on fuzzy logic and neural network techniques as shown in Figure 3. It optimizes the trade-off between energy conservation and data aggregation to improve the overall efficiency of WSNs. The specific implementation details and parameters may vary based on the requirements of a particular WSN application.

The neural network considers three crucial parameters: Trust(T), Energy(E), and Availability(A). These parameters control the minimum and maximum values passed to the next network layer. The neural network then calculates the weighting or importance of each factor based on their respective values. Afterwards, it analyses the cumulative values to determine the node within the cluster that best meets the criteria for being the cluster head.

Secure Data Transfer Using Whale Optimization Algorithm (WOA)

The third and final step of the TANFC-SWO algorithms is dedicated to the secure transfer of data within the network. This is achieved through advanced routing technology and, specifically, the use of the Whale Optimization Algorithm (WOA).

WOA is a metaheuristic optimization algorithm inspired by the social behavior of humpback whales. In this context, WOA is applied to routing technology to improve data transfer efficiency and security. WOA assists in optimizing the selection of routes for data packets by considering factors such as path reliability, energy consumption, and data integrity.

By incorporating WOA into the routing process, the network can ensure that data is securely transmitted from source to destination. This includes implementing encryption, authentication, and data encapsulation techniques to protect data from unauthorized access, tampering, or eavesdropping.

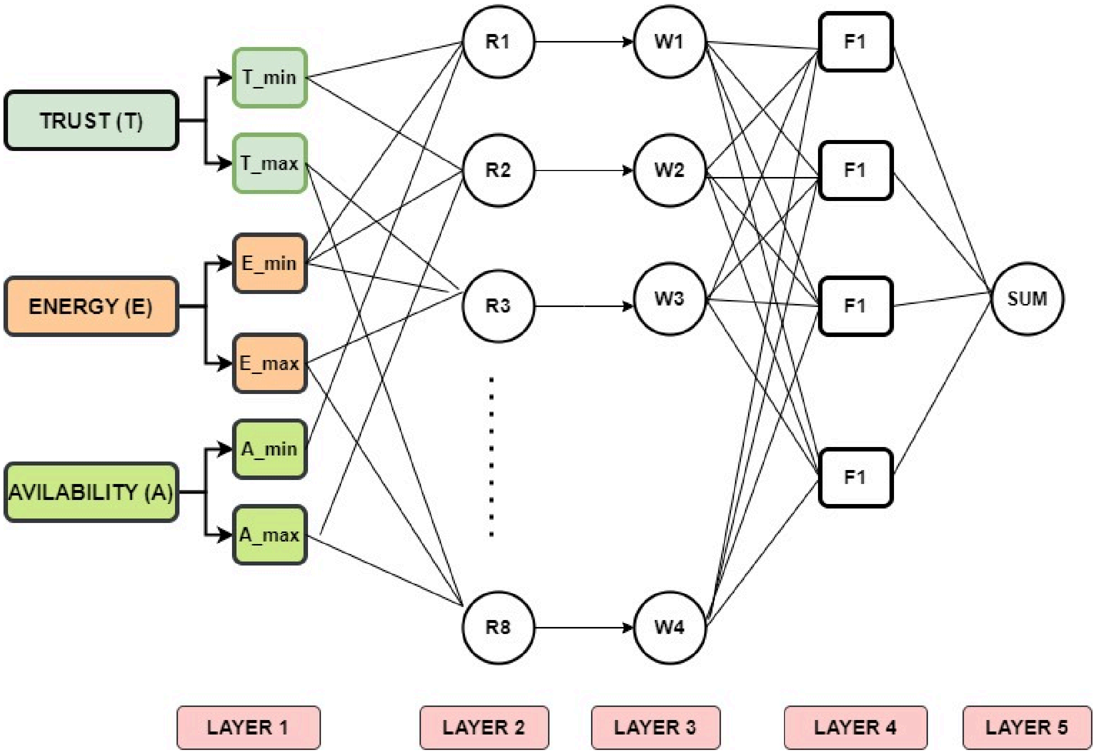


Fig 3. Five-layer Neuro Fuzzy System

One can categorize the WOA as a meta-heuristic algorithm. Its design and development are influenced by the innate behaviours of humpback whales (HW). Humpback whales produce Wheel-shaped bubbles in the water as they pursue their meal. According to initial research, humpback whales use bubble netting to catch their prey about 12 meters under the ocean's surface. They then convert these bubbles into spheres, which push them quickly to the surface. The mathematical representation is hunting, assaulting, circling, and searching for prey. When looking for prey, consider Algorithm 2, which uses random values greater than 1 to find prey.

Prey Encircling

The reaction to the present objective (prey) within the Prey Encircling WOA algorithm is considered sufficiently promising to arrive at a tenable solution. In the same way as humpback whales (HW) first locate and surround their prey, WORP uses a comparable principle. Once the hunting agent has been defined, other members align their positions to coincide with the most visible agent. Equations (13) and (14) are used in WOA to implement the encircling mechanism.

$$D=|P.X^*(u)-X(u)| \tag{13}$$

$$X(u+1)=X^*(u)-F.D \tag{14}$$

The coefficient vectors in these equations are represented by F and P, the iteration count is shown by u, the optimal solution location found in the completing iterations thus far is indicated by X*, and the current position is indicated by $Y(u)$. The absolute value of an integer is represented by the notation ‖·‖, where · stands for constituent multiplication.

In order to help encircle the prey successfully, Equation (14) is made to update the searching agent's location based on the best solution that is currently recognized. Note that X* needs to be updated after every cycle, but only if an improved approach has been discovered. The coefficients throughout are computed using equations (15) and (16) in the F and P vectors, where b is the random vector spanning inside the range [0, 1] and represents the surrounding component that decreases linearly from 3 to 0 throughout the iterations.

Bubble-Net Attack Strategy

Two different modelling techniques have been developed to mathematically simulate the bubble-net assault behaviour of humpback whales (HW): (i) encircling with the shrinking approach and (ii) position updating using a logarithmic spiral method.

Encircling Using Shrinking Method

This method uses a linear decrease of vector b through 3 to 0, as Equation (5) shows. It is vital to remember that vector F changes when vector b's significance is reduced. An alternative statement would be that vector F takes on random values between $-b$ and $+b$.

$$F=(2xbx\ r)-b) \tag{15}$$

$$P=2xr \tag{16}$$

Hence, during all iterations, b progressively drops from 3 to 0. The subsequent position of the investigating agent as it moves from its starting point to its current dominant location is characterized by appending an arbitrary number to vector F between the range of -1 to +1.

Location Update using Logarithmic Spiral Method

Humpback whales initially locate prey by measuring the distance between their current and prey's locations. Equations (17) and (18) provide a mathematical expression for the spiral flight route methodology, which each whale must use to modify its current location.

$$D'=|X^*(u)-X(u)| \tag{17}$$

$$X^*(u+1)=D'.\ ec^*m.\ \mathrm{Sin}(2m\pi)+X^*(u) \tag{18}$$

Where 'm' is generated at the random value within the range [-1, 1], 'D″ stands for the distance between the prey's location and the location of the currently best-found solution, 'c' stands for a constant number that the characterizes the shape of a spiral that is logarithmic, and '·' stands for constituent-based multiplication.

It is significant to remember that although HW (the predator) travels in a circle toward its prey, its general motion is modelled by a logarithmic spiral. To keep things simple, Equation (19) likely expresses the updated position of HW using either Equation (2) or Equation (6).

$$X^*(u+1)=\begin{cases} X*(u)-F\cdot D & \text{if } z>0.5 \\ D'\cdot e^{c*m}\cdot \mathrm{Sin}(2\times m\pi)+X*(u) & \text{if } z<0.5 \end{cases} \tag{19}$$

Seeking Prey

In actuality, whenever a HW agent plans to stray from adopting the solutions of others, they will all act randomly and seek out victims. In this stage, WOA concentrates on broadening the search field and encouraging search agents to travel far-off places for better answers. The vector F, whose values are greater than or equal to -1, is used to aid in a thorough search for prey. During the discovery phase, a search agent's location is updated by randomly selecting an agent instead of the best agent so far discovered. Unlike the exploitative phase, agents conducting searches closely follow the greatest-identified agent. WOA uses the vector F, having values larger than 1, to find global solutions without hitting local optima. Equations (20) and (21), where Xr is selected from the right now recognized random location vector, provide mathematical expressions for this idea.

$$D=|P.Xr-X| \tag{20}$$

$$X(u+1)=Xr-F.D \tag{21}$$

Levy Flight

WOA uses a Levy flying technique to spread out the search agents so they can avoid reaching local minima and investigate a more extensive search space. This tactic improves the harmony between the two processes. Equation (22) expresses how WOA uses the Levy flight approach to synchronise the HW location following its update.

$$X(u+1)=X(u)+(\delta\cdot sign[rv-0.5])\otimes Levy \tag{22}$$

The precise location of the j^{th} whale, or the vector F, at iteration u, is represented by $X(u)$ in Equation (22), where δ is randomly selected from a uniform distribution. $\otimes$ is a random number in the interval [0,1] and indicates the N-array circled times operator. Interestingly, $sign[r-0.5]$ only accepts the values -1, 0 and 1. Equation (23) uses a random walk approach to maximize the distance travelled in each step, allowing for practical search space exploration.

$$Levy\simeq v=1sh,\ 1\leq h\leq 3 \tag{23}$$

Algorithm 2. Whale Optimization Routing Algorithm

```
Initialize the population D$p$ ($p$ = 1, 2, 3, …, $q$).
Calculate the fitness of each search agent.
Determine D$*$ as the best-performing search agent.
Check if the termination condition.
$\boldsymbol{while}$ u<$maximum\_iteration$ is met.
For each searching agent:
Update parameters b, F, P, m, and z.
    i)   If (z < 0.5)
    ii)  If ($\|F\|$ < 1), update the location of the current searching agent using Eq. (2).
    iii) Else, if ($\|F\|$ > 1), choose a random searching agent (X$rv$) and update the location of the
         current searching agent using Eq. (19).
End if.
If (z > 0.5), update the location of the current searching agent using Eq. (18).
 End if.
End for every searching agent.
Update the location of each searching agent using the Levy flight.
Check if any searching agent has gone outside the target searching area and rectify it.
Recalculate the fitness of every searching agent.
Update X* if a better solution is found.
Increment the iteration counter, u.
Check the termination condition.
Return X*.
```

IV. RESULT AND ANALYSIS

The outcomes of implementing the suggested Nero Fuzzy WSN using the optimal tree routing protocol. The selection of the root channel is optimized through the proposed algorithm protocol method is implemented using Network Simulator 3 (NS-3). The experimental outcomes and the efficiency of the proposed method are described as follows:

NS-3 conduced simulations using the IEEE 802.11 MAC layer protocol, and Data was transmitted at a constant rate of 50 kbps in all simulations, with a simulation duration of 200 seconds. The total number of nodes used in our experiments varied, with configurations of 200, 400, 600, 800, and 1000 nodes, all within a 1000 m × 1000 m area. For propagation modelling, we employed the Two Ray Ground model and used omnidirectional antennas for data reception.

The CPU from Intel, the Core i7-4710 HQ processor, 8 GB RAM, the Windows 10 OS, and 4 GB Nvidia 860M GPU were the specifications of the system setup used for these simulations. The simulations were run several times with different setups, such as changing the number of nodes and cluster heads. It was envisaged that the sensing area of the network would be rectangular with dimensions of 100 by 100 square meters.

In **Fig 4**, we examine packet delay across various rounds of experimentation, showcasing the superior performance of our proposed algorithm when compared to existing algorithms such as PSO, BHO, TSO, FF, and GSO. Our algorithm consistently demonstrates lower packet delay, indicating its efficiency in minimizing delays in data transmission.

Moving on to **Fig 5**, we delve into packet drop rates and compare our proposed work and existing algorithms. The results clearly illustrate that our proposed algorithm outperforms its counterparts, exhibiting significantly lower packet drop rates. This superior performance underscores the robustness and reliability of our approach to maintaining data integrity and reducing packet loss.

In **Fig 6,** we investigate the packet delivery ratio, a crucial metric in assessing the effectiveness of communication systems. Here, our proposed algorithm once again shines, surpassing current techniques concerning the percentage of packet delivery. This outcome underscores the algorithm's ability to ensure a higher proportion of successfully transmitted packets, enhancing the overall communication quality within the network.

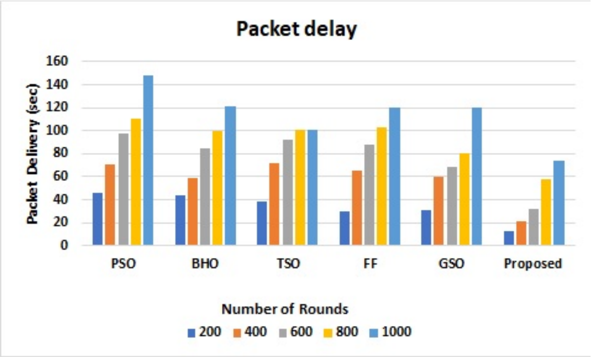


Fig 4. Packet Delay

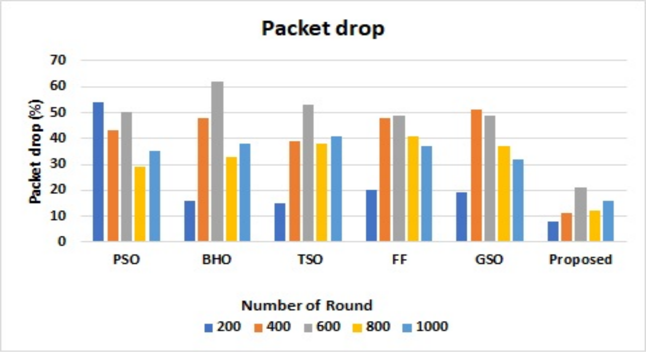
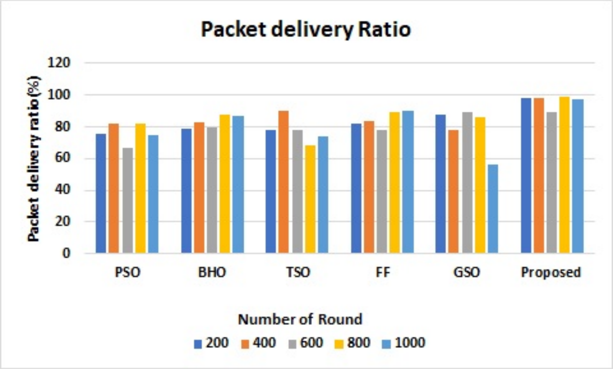


Fig 5. Packet Drop



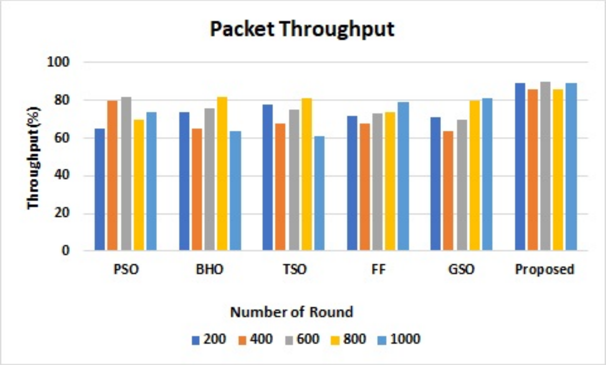
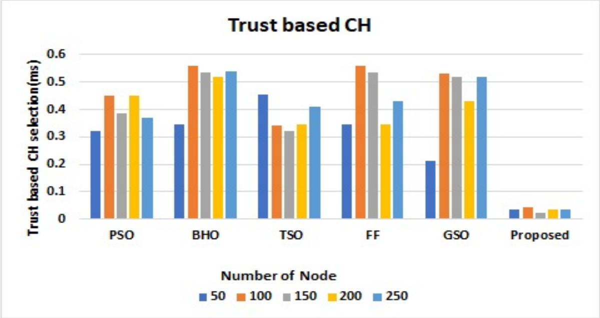


Fig 6. Packet delivery Ratio **Fig 7.** Packet Throughput

In **Fig 7,** we explore packet throughput and conduct a comparative analysis between our proposed algorithm and existing ones. The results reveal that our proposed algorithm exhibits superior packet throughput compared to existing algorithms. This signifies its capability to efficiently handle data traffic and achieve higher data transfer rates, ultimately improving network performance.

Fig 4 to **Fig 7 c**ollectively demonstrate the exceptional performance of our proposed algorithm in terms of packet delay, packet drop rates, packet delivery ratio, and packet throughput compared to existing algorithms. These findings highlight our approach's significant advancements and advantages to the field, contributing to more efficient and reliable WSN communication systems.



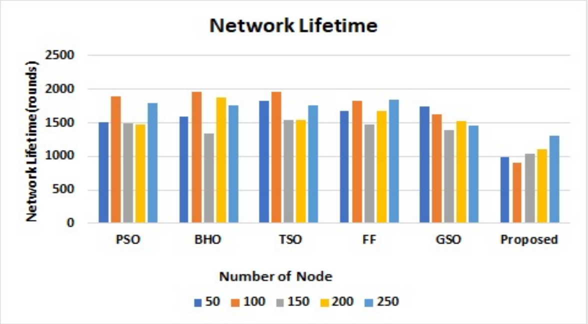


Fig 8. Trust Based Cluster Head **Fig 9.** Network Lifetime

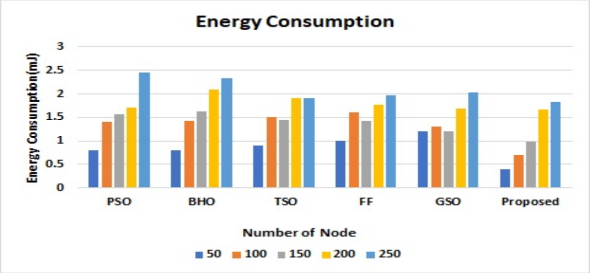


Fig 10. Energy Consumption

In **Fig 8,** we delve into the trust-based cluster head selection process, a crucial aspect of our research. Our proposed algorithm demonstrates remarkable efficiency by significantly reducing the time required for cluster head selection, measured in milliseconds, compared to existing methods. This improvement is consistent across different network sizes as we compare our results with configurations ranging from 50 to 250 nodes. The clear trend observed is that our proposed approach consistently outperforms the existing methods, highlighting its effectiveness in minimizing the time overhead associated with cluster head selection, which is critical for optimizing network performance.

Moving on to **Fig 9**, we examine network lifetime, a fundamental metric in evaluating the sustainability and longevity of wireless sensor networks. Our proposed algorithm stands out as it consistently offers an extended network lifetime compared to other approaches. This improvement in network longevity is evident across various network sizes, ranging from 50 to 250 nodes. By enhancing network lifetime, our proposed method contributes to the overall sustainability and reliability of the network infrastructure, ensuring that it remains operational for extended periods.

In **Fig 10,** we investigate the energy consumption patterns among the cluster nodes, a key consideration in wireless sensor network design. Our proposed algorithm excels, demonstrating lower energy consumption than existing methods. This advantage holds across different network sizes, from 50 to 250 nodes. By reducing energy consumption, our approach prolongs the operational life of individual nodes, thereby enhancing the overall efficiency and sustainability of the network. This is particularly important for applications where energy-efficient operation is crucial, such as remote monitoring and data collection in challenging environments.

The **Fig 8** to **Fig 10** collectively illustrate the superior performance of our proposed algorithm in various critical aspects of wireless sensor networks, including cluster head selection time, network lifetime, and energy consumption. These results are consistent across different network sizes, underscoring the versatility and effectiveness of our approach in improving the overall performance and sustainability of wireless sensor networks.

V. CONCLUSION AND FUCTURE WORK

In this paper, we addressed the critical challenges wireless sensor networks (WSNs) face concerning energy optimization and secure communication. These challenges arise from the resource-constrained nature of sensor nodes and the demanding operational environments in which they are deployed. To tackle these issues, we introduced a novel protocol, Trust aware Neuro Fuzzy Clustering head selection (TNFCH) combined with agglomerative hierarchical clustering (AHC) and Secure Whale Optimization (SWO) Algorithm Routing. This protocol, TNFCH-AHWO, enhanced energy-efficient data transmission in WSNs while ensuring data security and trustworthiness. Our approach efficiently organized sensor nodes using neural networks and Fuzzy logic, enabling the secure transfer of data within the communication network. A critical component of our system was the Trust calculation algorithm, which played a pivotal role in maintaining data integrity and facilitating lightweight operations such as key generation, encryption, decryption, and verification. This ensured hop-to-hop authentication among the nodes in WSNs, bolstering network security. To evaluate the effectiveness of our proposed protocol, we conducted extensive simulations using the NS3 simulator. The results of our simulations demonstrated significant improvements across various performance metrics compared to existing protocols. These enhancements encompassed reduced energy consumption, increased throughput, minimized network delay, prolonged network lifetime, and improved packet delivery ratios.

Future Work, while our proposed TNFCH-AHWO protocol has shown promising results in addressing energy efficiency and security concerns in WSNs, several avenues exist for future research and development. Extending our work to real-world deployments will offer insightful information about the proposed protocol's practicality. Field trials and experiments in diverse environmental conditions can further validate its effectiveness. Exploring advanced optimization techniques and algorithms can enhance the energy efficiency of the protocol even further. Investigating machine learning approaches for fine-tuning parameters or adapting to dynamic network conditions is intriguing.

Data Availability

No data was used to support this study.

Conflicts of Interests

The author(s) declare(s) that they have no conflicts of interest.

Funding

No funding agency is associated with this research.

Competing Interests

There are no competing interests.

References

[1]. F. Ren, J. Zhang, T. He, C. Lin, and S. K. D. Ren, “EBRP: Energy-Balanced Routing Protocol for Data Gathering in Wireless Sensor Networks,” IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 12, pp. 2108–2125, Dec. 2011, doi: 10.1109/tpds.2011.40.

[2]. K. Wang, C.-M. Yu, and L.-C. Wang, “DORA: A Destination-Oriented Routing Algorithm for Energy-Balanced Wireless Sensor Networks,” IEEE Internet of Things Journal, vol. 8, no. 3, pp. 2080–2081, Feb. 2021, doi: 10.1109/jiot.2020.3025039.

[3]. X. Liu, “Atypical Hierarchical Routing Protocols for Wireless Sensor Networks: A Review,” IEEE Sensors Journal, vol. 15, no. 10, pp. 5372–5383, Oct. 2015, doi: 10.1109/jsen.2015.2445796.

[4]. A. Ahmed, K. A. Bakar, M. I. Channa, K. Haseeb, and A. W. Khan, “TERP: A Trust and Energy Aware Routing Protocol for Wireless Sensor Network,” IEEE Sensors Journal, vol. 15, no. 12, pp. 6962–6972, Dec. 2015, doi: 10.1109/jsen.2015.2468576.

[5]. M. Adil, R. Khan, J. Ali, B.-H. Roh, Q. T. H. Ta, and M. A. Almaiah, “An Energy Proficient Load Balancing Routing Scheme for Wireless Sensor Networks to Maximize Their Lifespan in an Operational Environment,” IEEE Access, vol. 8, pp. 163209–163224, 2020, doi: 10.1109/access.2020.3020310.

[6]. H.-H. Liu, J.-J. Su, and C.-F. Chou, “On Energy-Efficient Straight-Line Routing Protocol for Wireless Sensor Networks,” IEEE Systems Journal, vol. 11, no. 4, pp. 2374–2382, Dec. 2017, doi: 10.1109/jsyst.2015.2448714.

[7]. Y. Yao, D. Xie, Y. Li, C. Wang, and Y. Li, “Routing Protocol for Wireless Sensor Networks Based on Archimedes Optimization Algorithm,” IEEE Sensors Journal, vol. 22, no. 15, pp. 15561–15573, Aug. 2022, doi: 10.1109/jsen.2022.3186063.

[8]. N. Ma, H. Zhang, H. Hu, and Y. Qin, “ESCVAD: An Energy-Saving Routing Protocol Based on Voronoi Adaptive Clustering for Wireless Sensor Networks,” IEEE Internet of Things Journal, vol. 9, no. 11, pp. 9071–9085, Jun. 2022, doi: 10.1109/jiot.2021.3120744.

[9]. M. Abo-Zahhad, S. M. Ahmed, N. Sabor, and S. Sasaki, “Mobile Sink-Based Adaptive Immune Energy-Efficient Clustering Protocol for Improving the Lifetime and Stability Period of Wireless Sensor Networks,” IEEE Sensors Journal, vol. 15, no. 8, pp. 4576–4586, Aug. 2015, doi: 10.1109/jsen.2015.2424296.

[10]. Y. Xu, W. Jiao, and M. Tian, “An Energy-Efficient Routing Protocol for 3D Wireless Sensor Networks,” IEEE Sensors Journal, vol. 21, no. 17, pp. 19550–19559, Sep. 2021, doi: 10.1109/jsen.2021.3086806.

[11]. N. A. Pantazis, S. A. Nikolidakis, and D. D. Vergados, “Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey,” IEEE Communications Surveys &amp; Tutorials, vol. 15, no. 2, pp. 551–591, 2013, doi: 10.1109/surv.2012.062612.00084.

[12]. Z. Han, J. Wu, J. Zhang, L. Liu, and K. Tian, “A General Self-Organized Tree-Based Energy-Balance Routing Protocol for Wireless Sensor Network,” IEEE Transactions on Nuclear Science, vol. 61, no. 2, pp. 732–740, Apr. 2014, doi: 10.1109/tns.2014.2309351.

[13]. S. Durairaj and R. Sridhar, “Task scheduling to a virtual machine using a multi-objective mayfly approach for a cloud environment,” Concurrency and Computation: Practice and Experience, vol. 34, no. 24, Jul. 2022, doi: 10.1002/cpe.7236.

[14]. T. Zhang, G. Chen, Q. Zeng, G. Song, C. Li, and H. Duan, “Routing Clustering Protocol for 3D Wireless Sensor Networks Based on Fragile Collection Ant Colony Algorithm,” IEEE Access, vol. 8, pp. 58874–58888, 2020, doi: 10.1109/access.2020.2982691.

[15]. S. Sahil Babu, A. Raha, and M. Kanti Naskar, “Trustworthy Route formation Algorithm for WSNs,” International Journal of Computer Applications, vol. 27, no. 5, pp. 35–39, Aug. 2011, doi: 10.5120/3294-4497.

[16]. G. Dhand and S. S. Tyagi, “SMEER: Secure Multi-tier Energy Efficient Routing Protocol for Hierarchical Wireless Sensor Networks,” Wireless Personal Communications, vol. 105, no. 1, pp. 17–35, Dec. 2018, doi: 10.1007/s11277-018-6101-y.

[17]. G. Zhan, W. Shi, and J. Deng, “Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs,” IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 2, pp. 184–197, Mar. 2012, doi: 10.1109/tdsc.2011.58.

[18]. S. S. Desai and M. J. Nene, “Node-Level Trust Evaluation in Wireless Sensor Networks,” IEEE Transactions on Information Forensics and Security, vol. 14, no. 8, pp. 2139–2152, Aug. 2019, doi: 10.1109/tifs.2019.2894027.

[19]. S. Karthick, “TDP: A Novel Secure and Energy Aware Routing Protocol for Wireless Sensor Networks,” International Journal of Intelligent Engineering and Systems, vol. 11, no. 2, pp. 76–84, Apr. 2018, doi: 10.22266/ijies2018.0430.09.

[20]. R. Sankaranarayanan, K. S. Umadevi, N. Bhavani, B. M. Jos, A. Haldorai, and D. V. Babu, “Cluster-based attacks prevention algorithm for autonomous vehicles using machine learning algorithms,” Computers and Electrical Engineering, vol. 101, p. 108088, Jul. 2022, doi: 10.1016/j.compeleceng.2022.108088.

[21]. K. S. Rekha, N. Venugopal, and D. Selvam, “Resource Management in Ambient Network using Network Processor,” International Journal of Computer Applications, vol. 1, no. 16, pp. 122–130, Feb. 2010, doi: 10.5120/332-503.