Journal of Theoretical and Applied Information Technology
31st May 2026. Vol.104. No.10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INTEGRATING GRAPH CONVOLUTIONAL NETWORKS FOR ENHANCED TRUST-AWARE CLUSTER HEAD SELECTION IN WIRELESS SENSOR NETWORKS

GAJJALA SAVITHRI [1, 2], N. RAGHAVENDRA SAI [3*]

[1] Research Scholar, Department Of Computer Science And Engineering, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, AP, India
[2] Department Of Animation, Dr. YSR Architecture And Fine Arts University, Kadapa, AP, India
[3] Professor, Department Of Computer Science And Engineering, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, AP, India.

E-mail: [1,2]savithrigreddy@gmail.com , [3*]nallagatlaraghavendra@kluniversity.in

ABSTRACT

Wireless Sensor Networks (WSNs) play an important role in many applications, necessitating strong trust mechanisms to ensure reliable communication and data integrity. This paper presents GLENET, a novel model that incorporates Graph Convolutional Networks (GCN) into the Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol to improve cluster head selection in WSNs. GLENET's trust model employs adaptive penalty coefficients, which allow for dynamic adjustments in response to abnormal behavior, thereby fostering network trust. This work aims to improve the effectiveness of WSNs by addressing the limitations of traditional clustering protocols. GLENET's uniqueness lies in its comprehensive trust assessment, which combines direct, indirect, and energy trust metrics. The model responds dynamically to changing network conditions, aligning penalties with contextual abnormalities to discourage malicious behavior. The results show that GLENET achieves a throughput of 18520 kbps while outperforming comparable methods in computation time (48.34 seconds) and residual energy conservation (13.18 Joules). The model's adaptability and prioritization of nodes with sustainable energy levels help to ensure long-term stability, making it a promising approach for future WSN applications.

Keywords: *Wireless Sensor Networks, Trust Model, Glenet, Graph Convolutional Networks, Leach Protocol.*

1. INTRODUCTION

This study was undertaken to address a critical and growing challenge in the deployment of Wireless Sensor Networks: the absence of trust-aware mechanisms in traditional cluster head selection protocols, which exposes networks to malicious node activity and accelerates energy depletion in security-sensitive applications. As WSNs are increasingly deployed in healthcare monitoring, industrial control, and environmental surveillance, the consequences of unreliable cluster head selection extend beyond performance degradation to include data integrity failures and potential safety risks. Existing protocols such as LEACH, while energy-efficient, do not incorporate trust evaluation, leaving a fundamental security gap. This work was therefore motivated by the need to develop a cluster head selection framework that simultaneously ensures network trustworthiness, energy efficiency, and adaptability to dynamic network conditions requirements that no single existing protocol fully satisfies.

Wireless Sensor Networks (WSNs) are the foundation of modern communication systems, connecting a variety of sensors to monitor and collect data across a wide range of environments [1-3]. WSNs are important in a variety of applications, including environmental monitoring, industrial automation, and healthcare systems, due to their widespread use and versatility [4]. However, the inherent distributed and dynamic nature of WSNs creates unique challenges, particularly in terms of security and dependability [5]. Trust, a fundamental aspect of secure communication, is critical in ensuring the integrity and authenticity of transmitted data within WSNs [6-7]. This paper proposes an innovative methodology for improving the trustworthiness and security of WSNs by integrating trust models and deep neural networks. Security in WSNs is a multifaceted

issue, and trust is an essential component for protecting against
malicious activity and unauthorized access [8]. In this context, trust is defined as assessing the reliability of network nodes based on their behavior and interactions [9-11]. Given the dynamic nature of
WSNs, understanding network behavior is critical for effective security measures [12-15]. This necessitates the computation of various trusts, which consider factors such as direct communication, historical interactions, and energy sustainability [16].

Cluster head selection is another critical aspect of WSN security, as cluster heads serve as pivotal nodes responsible for data aggregation and transmission [17]. Traditional clustering protocols, while effective in some cases, frequently fall short of capturing the intricate network dynamics and contextual information required for robust security measures [18]. This limitation emphasizes the importance of advanced methodologies that go beyond traditional approaches [19]. Deep Neural Networks (DNNs), particularly Graph Convolutional Networks (GCNs), have emerged as effective tools for extracting complex relationships and patterns from graph-structured data. This paper contributes to the integration of GCNs into the Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol, which is a traditional clustering approach in WSNs. This integration, known as GLENET, aims to revolutionize cluster head selection by taking into account both local and global network characteristics. GLENET aims to address the shortcomings of conventional methods by enhancing traditional protocols with deep learning capabilities, thereby improving the overall security and performance of WSN. To summarize, this paper presents a comprehensive methodology for fortifying the security of WSNs using trust models and deep neural networks. The importance of trust computation in understanding network behavior, combined with the need for advanced cluster head selection mechanisms, drives the development of novel methodologies. The incorporation of deep neural networks, specifically GCNs, into traditional protocols represents a paradigm shift toward more adaptive, resilient, and secure WSNs.

The paper begins with an in-depth introduction that emphasizes the importance of security and trust in Wireless Sensor Networks (WSNs). It describes the difficulties encountered by WSNs, introduces the proposed methodology, and emphasizes the importance of incorporating trust models and deep neural networks for improved security. The literature review investigates recent advances in WSNs, with a focus on security, trust models, and clustering protocols, laying the groundwork for the proposed methodology. Section 3 describes the proposed system's step-by-step approach, which includes trust parameter definition, trust computation, and the integration of Graph Convolutional Networks (GCNs) into the LEACH protocol to create the GLENET model. This section explains the model architecture and mathematical equations that underpin the methodology. The Results and Analysis section summarizes the results of implementing the proposed methodology, including a thorough evaluation of trust values, cluster head selections, and overall network performance. Graphs and statistical analyses show that GLENET outperforms traditional methods. The paper concludes by summarizing key findings, discussing implications, and proposing future research directions, thereby adding valuable insights to the field of secure and resilient wireless sensor networks.
The central problem addressed in this work is the unreliable and energy-inefficient selection of cluster heads in Wireless Sensor Networks (WSNs) deployed in trust-sensitive environments. In WSNs serving healthcare monitoring, industrial automation, and environmental sensing applications, cluster heads are responsible for data aggregation and transmission to the base station — making their selection critical to network performance and data integrity. The problem arises because conventional clustering protocols such as LEACH select cluster heads based solely on energy levels and probabilistic thresholds, without considering the trustworthiness of candidate nodes. This creates two specific risks: first, malicious or compromised nodes may be elected as cluster heads, leading to data manipulation, eavesdropping, or denial of service; second, nodes with low trust scores but adequate energy may be selected over reliable nodes, degrading overall network reliability. The problem is most critical for network administrators and application developers deploying WSNs in sensitive domains where both security and energy efficiency are non-negotiable requirements.

The rationale for integrating Graph Convolutional Networks (GCN) with the LEACH protocol in the proposed GLENET model is grounded in the structural properties of WSNs and the limitations of existing approaches. WSNs are inherently graph-structured — nodes communicate across a topology that changes dynamically in response to energy depletion and mobility. GCNs are specifically designed to operate on graph-structured data, making them a natural and principled choice for capturing both local neighbourhood interactions and global network topology in cluster head selection decisions (Eq. 13-15). Alternative deep learning approaches such as LSTMs and standard CNNs treat node features independently and do not model the relational structure of the network, resulting in suboptimal cluster head decisions that ignore inter-node trust propagation. The LEACH protocol provides an established and computationally efficient foundation for cluster formation (Eq. 12), and augmenting it with GCN-based trust assessment rather than replacing it entirely preserves its low-energy overhead advantages while adding the trust-aware intelligence that it lacks. The comprehensive trust model combining direct trust (Eqs. 5-8), indirect trust (Eq. 9), and energy trust (Eq. 10) provides a multi-dimensional node reliability assessment that single-metric trust schemes cannot match. Together, these design choices make the GLENET approach both technically justified and practically plausible for deployment in real WSN environments.

2. RELATED WORKS

The Literature Review section examines recent and significant works in the field of Wireless Sensor Networks (WSNs), with a focus on security, trust models, and clustering protocols. By reviewing existing literature, the paper lays the groundwork for the proposed methodology, highlighting the advances, challenges, and insights gained from recent WSN research.

Su et al. (2020) proposed a trust model for opportunistic routing based on node behaviour for trust assessment [20]. While the model produced promising results, its localized focus raises questions about its ability to detect malicious patterns on a network-wide scale. Baskar et al. (2021) introduced the data fusion trust model, which assesses trust using temporal attributes and behaviour analysis [21]. However, the model's efficacy is heavily dependent on the reliability of the data it processes, and the potential impact of incomplete or falsified information on its accuracy must be carefully considered. Jadhav et al. (2021) proposed an atomic search sunflower optimization algorithm for trust-based routing [22]. Despite their innovative approach, the computational complexities associated with such algorithms may pose difficulties, especially as network size and complexity grow.

Saleh et al. introduced the reliable routing protocol (RRP) in 2017 [23], with the goal of improving communication reliability in vehicular networks. Their approach used a variety of routing techniques to ensure efficient data packet delivery in dynamic and highly mobile vehicular environments. However, the study had limitations because it did not specifically address network scalability issues or the dynamic nature of vehicular networks. Vinodhini et al. introduced the MOMHR (Dynamic Multi-hop Routing Protocol for Wireless Sensor Networks Using Heuristic Based Multi-objective Function) in 2020 [24], which uses a heuristic-based multi-objective function to improve routing efficiency in Wireless Sensor Networks (WSNs). While their approach improved performance in WSNs, its applicability to other network types was unclear.

Maglaras and Katsaros investigated distributed clustering in vehicular networks in 2012 [25], highlighting the advantages of clustering in vehicular communication management. However, their research did not go into the complexities of routing protocols or the potential difficulties in maintaining cluster stability in highly dynamic vehicular environments. Muhammad Rizwan Ghori et al. conducted a thorough review of routing protocols in 2018 [26], focusing on evaluating existing protocols rather than proposing novel routing solutions. Malik and Sahu conducted a comprehensive study on routing protocols in 2019 [27], examining various protocols, presenting their benefits and drawbacks, and introducing the Dynamic Source Routing (DSR) protocol.

Mu et al. introduced a routing algorithm in 2019 that takes into account energy balance and alternative awareness [28], demonstrating favorable characteristics for Wireless Body Area Networks (WBANs). However, its direct

application to other network types, such as Vehicular Ad hoc Networks (VANETs), may be restricted. Subbaiah et al. (2023) investigated the use of an energy-aware routing protocol for mobile Ad Hoc networks in WBAN-based healthcare systems [29]. While effective in healthcare-specific situations, its broader applicability to mobile Ad Hoc networks may be limited.

The review of existing literature reveals four research gaps that motivate the proposed GLENET framework. First, existing trust models for WSNs [20-22] typically evaluate node trust using limited dimensions — either direct communication history or energy levels alone — without combining direct trust, indirect trust, and energy trust into a unified comprehensive trust metric. Second, while GCNs have demonstrated effectiveness in graph-structured learning problems, their integration into WSN clustering protocols for trust-aware cluster head selection has not been investigated in the reviewed literature [20-29]; most clustering approaches rely on heuristic or rule-based trust thresholds. Third, the adaptive penalty coefficient mechanism for dynamically adjusting trust penalties in response to detected abnormal behaviour — as employed in GLENET (Eqs. 1-4) — has not been explored in existing WSN trust frameworks, which use static penalty values that do not adapt to evolving network conditions. Fourth, none of the reviewed routing and clustering protocols [23-29] simultaneously address energy efficiency, trust awareness, and convergence speed within a single hybrid framework, leaving a gap in methods that can optimize all three objectives concurrently. These gaps collectively define the scope of the present investigation and establish GLENET as a targeted solution to unaddressed challenges in WSN security and performance.

3. PROPOSED SYSTEM

The research design follows a simulation-based experimental methodology implemented in MATLAB. The study is structured in five sequential phases. Phase 1 — Network Initialization: a WSN of n sensor nodes is deployed in a three-dimensional space of dimensions xm x ym x zm (Fig. 5), with node positions randomly distributed and energy levels initialized uniformly. Channel conditions are modelled using standard WSN energy parameters (E_elec, E_fs, E_mp) and a distance-based energy consumption model (Eq. 10). Phase 2 — Trust Model Computation: for each simulation round, direct trust (DT, Eqs. 5-8), indirect trust (IT, Eq. 9), and energy trust (ET, Eq. 10) are computed for each node, and combined into a comprehensive trust score (CT, Eq. 11) using weighting factors m1, m2, and m3. Adaptive penalty coefficients (ACj, Eqs. 1-4) dynamically adjust trust values in response to detected abnormal behaviour proportions. Phase 3 — GLENET Cluster Head Selection: the LEACH protocol probability function (Eq. 12) and the GCN forward propagation (Eq. 13) produce independent cluster head candidacy scores, which are combined using a weighted fusion (Eqs. 14-15) with weights w_LEACH and w_GCN to determine final cluster head assignments. Phase 4 — Performance Monitoring: for each round, four metrics are recorded — number of dead nodes (Eq. 16), packets transmitted to BS (Eq. 17), packets transmitted to CHs (Eq. 18), throughput (Eq. 19), and energy consumption (Eq. 20). Phase 5 — Comparative Evaluation: the proposed GLENET method is compared against prior works.

The proposed system methodology, illustrated in Figure 1, is a comprehensive and systematic approach to improving the performance and trustworthiness of wireless sensor networks (WSNs) using the innovative GLENET model. The methodology consists of several steps, beginning with the definition of trust model parameters (a1 through a12) and the initialization of the adaptive penalty coefficient (ACj) over a specified range. The trust values (theta1, theta2, theta3, and theta4) are then calculated using ACj's logistic functions and the specified parameters. The variation in trust values is represented by plotting them against ACj using various parameter sets. Following that, parameters for direct trust calculation, such as gamma (g) and lambda (l), are defined, and trust-related variables (DT, HT, IT) are initialized. The calculation of direct trust (DT) and history trust (HT) is simulated over a range of abnormal behavior proportions (ACj), with network behavior influencing the updates. The methodology also includes the generation of random values for nodes (Bh) and the calculation of indirect trust (IT) using pairwise trust values. Energy trust is calculated using node positions and energy consumption. The comprehensive trust (CT) for each node is then calculated by adding the direct, indirect, and energy trust

values. CT is plotted against round time (r) to examine the evolution of trustworthiness over time.

The methodology incorporates the LEACH protocol for cluster formation and cluster head election, creating a hybrid model (GLENET) by incorporating Graph Convolutional Networks (GCN) into the LEACH protocol. The GCN model is trained on trust-related features and network topology, and cluster head selection is improved by combining LEACH and GCN results. The hybrid approach's performance is monitored using metrics such as dead nodes, packets transmitted, throughput, and energy consumption. The adaptive training mechanism for the GCN model is discussed, which allows for periodic updates based on changing network conditions. The methodology concludes with a visualization of the training process and adaptations of the GCN model, which provides insights into how it adjusts to changes in trust dynamics. Overall, the proposed system methodology is a comprehensive and innovative framework that addresses various aspects of WSNs, such as trust modelling, energy efficiency, and cluster head selection, with the goal of improving network performance and reliability.

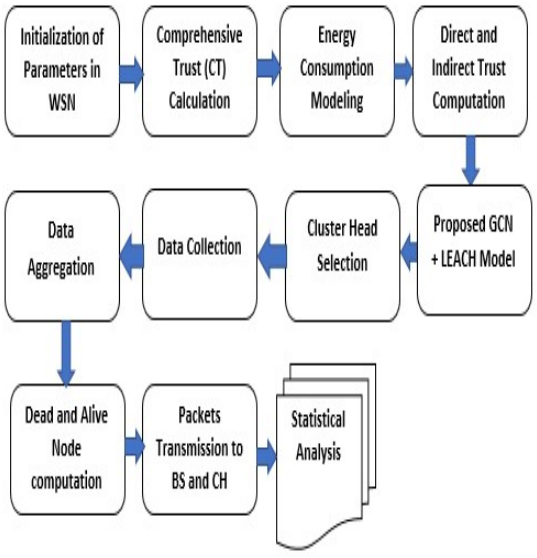

Figure: 1 Proposed System Block Diagram

Let us now elaborate on the above-mentioned proposed system methodology using probable mathematical equations.

Define the parameters of the trust model, such as a1 through a12. Initialize the adaptive penalty coefficient (ACj) across a range of values. Use the defined trust model and parameters to calculate trust values (theta1, theta2, theta3, and theta4).

Let $a1,a2,a3,a4,a5,a6,a7,a8,a9,a10,a11,a12$ are parameters of the trust model and *ACj* is initialized across a range of values (0 to 1 in steps of 0.2).

The trust values ($\theta1,\theta2,\theta3,\theta4$) are calculated using the following equations:

$$\theta_1 = 1 - \frac{a_1}{1+\exp(-a_2 AC_j + a_3)} \quad \text{..... (1)}$$

$$\theta_2 = 1 - \frac{a_4}{1+\exp(-a_5 AC_j + a_6)} \quad \text{..... (2)}$$

$$\theta_3 = 1 - \frac{a_7}{1+\exp(-a_8 AC_j + a_9)} \quad \text{..... .(3)}$$

$$\theta_4 = 1 - \frac{a_{10}}{1+\exp(-a_{11} AC_j + a_{12})} \quad \text{..... .(4)}$$

In summary, the trust values are calculated based on the logistic functions of the adaptive penalty coefficient (*ACj*) using the specified parameters ($a1,a2,\ldots,a12$).

Plot the trust values (theta1, theta2, theta3, theta4) against the adaptive penalty coefficient (ACj). Observe the variation in trust values with changing ACj and different parameter sets.

Set parameters such as gamma (g) and lambda (l) for direct trust calculation.

γ (gamma) and λ (lambda) are parameters for direct trust calculation. In this work let us set the values as γ=0.5 and λ=0.5.

Trust-related variables are initialized as follows:

DT (Direct Trust) is initialized as zeros array of length n.

HT (History Trust) is initialized as ones array of length n.

IT (Indirect Trust) is initialized as zeros array of length n.

Simulate direct trust calculation over a range of abnormal behaviour proportions (ACj).

For each node i in the network (n):

Calculate Rj (Receive Trust) using the equation:

$$Rj = \frac{\theta \cdot receive\_messagej - rejectionj}{messagej} \quad ....(5)$$

Calculate Sj (Send Trust) using the equation:

$$Sj = \frac{\theta \cdot send\_messagej - un\_sendj}{messagej} \quad .... (6)$$

Update DT[i] using the equation:

$$DT[i] = \gamma \cdot HT[i] + (1-\gamma) \cdot (Rj + Sj) \quad .... (7)$$

Update HT[i+1] using the equation:

$$HT[i+1] = \lambda \cdot (HT[i] + DT[i]) \quad ...... (8)$$

Display and analyze the direct trust (DT) and history trust (HT) values.

These values represent each node's direct and history trust. In summary, the direct trust calculation updates DT and HT based on network behavior and past trust values. The equations include calculations for receiving trust (Rj) and send trust (S j). The trust values are updated across a range of abnormal behavior proportions (ACj). Generate random values for Bh (nodes) and calculate indirect trust (IT) based on pairwise trust values.

For each node u in the random sample Bh:

For each node q in the network (n):

Calculate IT[u] (Indirect Trust for node u) using the equation:

$$IT[u] = IT[u] + \frac{1}{q} \cdot (DT[i] \cdot DT[j]) \quad ...... (9)$$

DT[i] and DT[j] are the direct trust values for nodes i and j respectively.

Display and analyse the indirect trust values. These values represent the indirect trust for each node in the random sample Bh using pairwise trust values (DT). In summary, indirect trust is calculated by iterating over a random sample of nodes (Bh) and computing the indirect trust value for each node using pairwise direct trust values (DT). The equation for IT[u] takes into account the product of direct trust values for node pairs i and j in the network. The final step is to display and analyse the calculated IT values. Initialize parameters related to energy trust calculation.

xm, ym,zm: Dimensions of the sensor network.
sink.x,sink.y,sink.z: Coordinates of the base station (sink). n: Number of nodes in the network. l: Energy supplied to each nod E_elec: Energy consumed for radio transmission/reception (per bit). E_fs: Amplification energy when distance (d) is less than d_0. E_mp: Amplification energy when distance (d) is greater than or equal to d_0. d_0: Threshold distance for switching between E_fs and E_mp. E_0: Initial energy level.

For each node i in the network:

Calculate the distance (d[i]) between node i and the base station.
Calculate energy consumption (Es[i]) based on the distance and energy parameters.
Es[i] can be calculated using the following conditions:

$$E_s[i] = \begin{cases} l \cdot E_{elec} + l \cdot E_{fs} \cdot d[i]^2 & if\ d[i] < d0 \\ l \cdot E_{elec} + l \cdot E_{mp} \cdot d[i]^4 & if\ d[i] \geq d0 \end{cases} \quad .... (10)$$

The Es[i] values represent each node's energy trust, which is determined by its position and consumption. In summary, the energy trust calculation takes into account the node positions, calculates energy consumption based on distance, and displays/analyses the energy trust values for each node in the network. Combine direct, indirect, and energy trust values to compute comprehensive trust (CT) for each node.

For each node i in the network:

Calculate CT[i] (Comprehensive Trust) by combining Direct Trust (DT[i]), Indirect Trust (IT[i]), and Energy Trust (ET[i]):

$$CT[i] = m1 \cdot DT[i] + m2 \cdot IT[i] + m3 \cdot ET[i] \quad .... (11)$$

Here, m1, m2, and m3 are weighting factors representing the importance of each trust component.

Plot CT against round time (r). Analyse the trend of comprehensive trust over time. Analyse the trend of comprehensive trust over time to see how nodes' trustworthiness changes throughout the simulation. Look for patterns, anomalies, or consistency in the overall trust values. To summarize, the comprehensive trust calculation combines the direct, indirect, and energy trust values for each node. The resulting

comprehensive trust values are then plotted against round time to examine the trend of trustworthiness throughout the simulation.

Implement the LEACH protocol for cluster formation and election of cluster heads.
Probability of a node becoming a cluster head:

$$p_{CH}(i,r) = \frac{p}{1-p \cdot mod(r, round(\frac{1}{p}))} \ldots\ldots\ldots\ldots\ldots (12)$$

Simulate communication between nodes and cluster heads. Integrate GCN-based cluster head selection alongside LEACH protocol creating a hybrid model known as GLENET (described elaborately in Section 3.1).
Define parameters for the GCN model and train it using trust-related features and network topology. Use the trained GCN model to predict cluster heads based on trust values and node relationships.
Let X be the input feature matrix, A the adjacency matrix, W the weight matrix, and σ the activation function.
Forward propagation in a GCN layer:

$$Z = \sigma(A \cdot X \cdot W)\ldots\ldots\ldots\ldots\ldots\ldots\ldots (13)$$

Combine the cluster head selections from both LEACH and GCN methods.

$$pcombined(i) = w_{LEACH} \cdot p_{LEACH}(i) + w_{GCN} \cdot p_{GCN}(i)\ldots\ldots\ldots\ldots\ldots\ldots\ldots (14)$$

where w_{LEACH} and w_{GCN} are weights

The cluster head selection in GLENET involves combining the results from both LEACH and GCN. A weighted sum or a similar mechanism can be used:

$$ClusterHeadi = \alpha \cdot LEACH\_Resulti + (1-\alpha) \cdot GCN\_Resulti\ldots\ldots\ldots\ldots\ldots\ldots (15)$$

where α is a weighting factor.

Monitor performance metrics for the hybrid approach, including the number of dead nodes, packets transmitted, throughput, and energy consumption. Calculate and store metrics for each round (r) for the hybrid approach.

Number of Dead Nodes (Dead):

$$Deadr = \sum_{i=1}^{n} \begin{cases} 1 & if\ node\ i\ is\ dead \\ 0 & otherwise \end{cases} \ldots\ldots\ldots (16)$$

Packets Transmitted to Base Station (Packets_TO_BS):

$$Packets\_TO\_BS\_r + 1 = Packets\_TO\_BS_r + Packets\_TO\_BS\_Per\_Round\_r + 1\ldots\ldots (17)$$

Packets Transmitted to Cluster Heads (Packets_TO_CH):

$$Packets\_TO\_CH\_r + 1 = Packets\_TO\_CH_r + Packets\_TO\_CH\_Per\_Round\_r + 1\ldots\ldots (18)$$

Throughput:

$$Throughput_{r+1} = Packets\_TO\_BS\_r + Packets\_TO\_CH\_r\ldots\ldots\ldots\ldots (19)$$

Energy Consumption:

$$Energy_{r+1} = \sum_{i=1}^{n} Energy\_i, r + 1 \ldots\ldots\ldots (20)$$

Consider incorporating an adaptive training mechanism for the GCN model. Periodically update the GCN model based on evolving network conditions, trust values, or other relevant factors. Visualize the training process and adaptations of the GCN model over rounds or epochs. Analyse how the GCN model adjusts to changes in trust dynamics. Summarize the key findings and insights from the simulations. Interpret the results in the context of the trust model, LEACH protocol, and the integration of GCN. Highlight the advantages and limitations of the hybrid approach.

3.1 Proposed GLENET Model

In our innovative model, GLENET, we use Graph Convolutional Networks (GCN) to improve the effectiveness of the LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol in wireless sensor networks. The incorporation of GCN introduces a novel method for cluster head selection that takes into account the complexities of network topology and inter-node interactions. Traditional clustering protocols, such as LEACH, frequently fall short of capturing critical contextual information, resulting in poor performance. GLENET addresses this limitation by incorporating GCN layers that enable the

exchange and aggregation of information based on the network graph. This harmonious integration enables nodes to make informed decisions about cluster head selection, taking into account both local and global network characteristics.

GLENET's GCN layers play an important role in the adaptive and dynamic cluster head selection procedure. GLENET is made up of two essential components: Graph Convolutional Layer 1 (GC-L1) and Graph Convolutional Layer 2 (GC-L2). It captures local relationships within immediate clusters and extends its influence to broader network features. GC-L1 allows for the exchange of information between neighboring nodes, promoting localized decision-making, whereas GC-L2 operates on a larger scale, allowing nodes to consider global network attributes. The incorporation of these GCN layers into the LEACH protocol is seamless and transformative. Throughout the clustering process, nodes use the information propagated through the GCN layers to determine their suitability for becoming cluster heads. The GCN-enhanced decision mechanism prioritizes nodes with well-connected neighbourhood's and higher centrality in the network graph, resulting in greater adaptability and resilience during lustering. This integration improves energy efficiency and extends the overall life of the wireless sensor network.

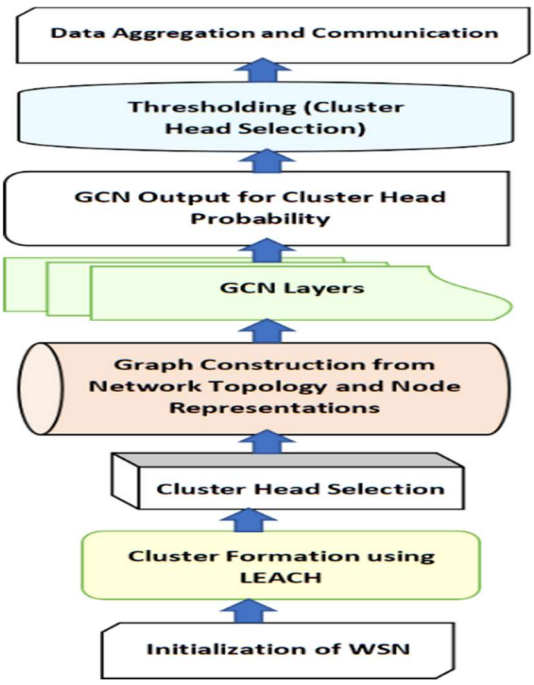

Figure: 2 Architecture of Proposed GLENET

The GLENET model uses sophisticated mechanisms to create a trust-rich environment in the wireless sensor network. By incorporating adaptive penalty coefficients, the model dynamically adjusts penalties in response to abnormal behavior, discouraging malicious behavior and fostering trust. Comprehensive trust calculations combine direct, indirect, and energy trust to provide a more nuanced measurement of node reliability. Direct trust computation takes into account both received and sent messages, which helps to evaluate trustworthiness in direct communication. Indirect trust measures node influence based on network interactions, whereas energy trust assesses node sustainability.

The integration of Graph Convolutional Networks into the LEACH protocol improves cluster head selection by taking into account local and global network characteristics, resulting in a more reliable election process. GLENET's dynamic adaptability ensures effective responses to changing network conditions, reinforcing confidence in the model's ability to adapt to evolving scenarios, threats, and node behaviors.

GLENET pioneered the integration of Graph Convolutional Networks (GCN) into the LEACH protocol, revolutionizing cluster head selection. This novel approach takes into account both local and global network characteristics, which improves adaptability and efficiency. The model introduces a comprehensive trust assessment by combining direct, indirect, and energy trust, resulting in a more nuanced understanding of node reliability. Adaptive penalty coefficients adjust dynamically in response to abnormal behaviour, discouraging malicious activity and aligning penalties with the network context. GLENET's dynamic adaptability allows for effective responses to changing network conditions, and the inclusion of energy trust prioritizes nodes with sustainable energy levels, which contributes to long-term stability. The enhanced cluster head selection process considers node connectivity, influence, and centrality, resulting in a highly effective and trustworthy wireless sensor network model.

The originality of GLENET rests on three specific innovations that distinguish it from all reviewed prior works. First, the integration of Graph Convolutional Networks into the LEACH clustering protocol represents a novel architectural contribution: GCN layers (GC-L1

and GC-L2, Eq. 13) enable cluster head selection to consider both local neighbourhood connectivity and global network topology simultaneously, which neither standard LEACH nor any reviewed trust-based protocol achieves. Second, the adaptive penalty coefficient mechanism (ACj, Eqs. 1-4) introduces a dynamic trust adjustment that responds to the proportion of abnormal behaviour in real time, rather than using fixed penalty thresholds — a design innovation not present in any reviewed trust model [20-22]. Third, the comprehensive trust formulation (Eq. 11) combining direct trust (Eqs. 5-8), indirect trust (Eq. 9), and energy trust (Eq. 10) into a weighted composite score provides a richer and more reliable measure of node trustworthiness than single-dimension trust schemes.

3.2 Algorithm

The stepwise algorithm for the proposed GLENET model is outlined below to provide a clear and systematic understanding of how the model operates at each step.

Algorithm: GLENET Model

Step 1: Initialization
// InitializeWirelessSensorNetwork ()
Step 2: Architecture Setup
// ImplementGLENETArchitecture ()
Step 3: Graph Convolutional Layers
// DefineGraphConvolutionalLayer1()
// DefineGraphConvolutionalLayer2()
Step 4: Cluster Head Selection
// For each node in the network:
PropagateInformationThroughGCNLayers ()
DetermineNodeSuitabilityForClusterHead ()
Step 5: Trust Model Integration
// IncorporateAdaptivePenaltyCoefficients ()
// PerformComprehensiveTrustCalculatios ()
Step 6: Direct Trust Computation
For each node in the network:
// ComputeDirectTrust ()
Step 7: Indirect Trust Computation
For each node in the network:
// CalculateIndirectTrust ()
Step 8: Energy Trust Assessment
For each node in the network:
// AssessEnergyTrust ()
Step 9: Dynamic Adaptability
// LeverageDynamicAdaptability ()
Step 10: Model Evaluation
// EvaluateGLENETPerformance ()
Step 11: Conclusion
ConcludeImplementation()

4. RESULT AND ANALYSIS

Figure 3 shows the adaptive penalty coefficient AC j(abnormal behaviour) is depicted over multiple rounds or iterations. This coefficient is a critical parameter in trust models, representing the penalty imposed on nodes that exhibit untrustworthy behaviour. The graph shows the dynamic nature of the penalty coefficient, highlighting any fluctuations or trends. A spike in values could indicate an increased sensitivity to abnormal behaviour, whereas a drop could indicate a relaxed response. Analysing this figure reveals how the network adjusts its penalty mechanisms in response to changing trust dynamics.

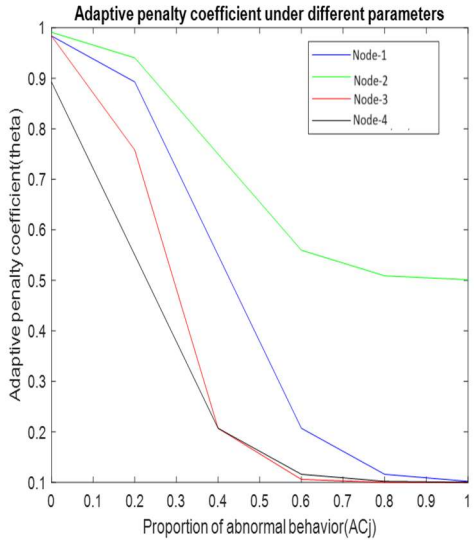

Figure: 3 Adaptive Penalty Coefficient For Abnormal Behaviours

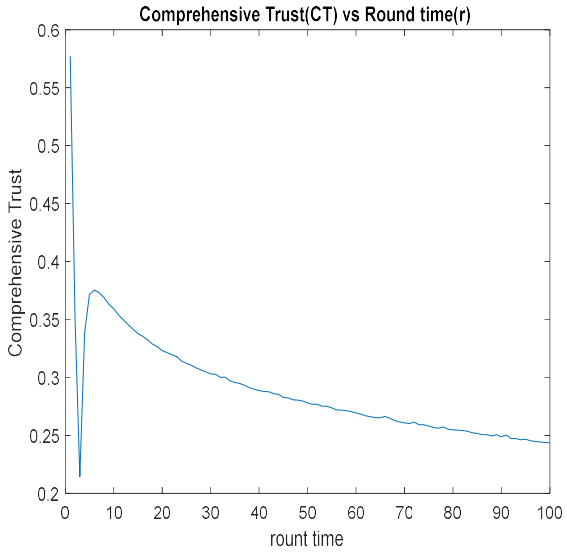

Figure: 4 Comprehensive Trust

Figure 4 shows the trend of comprehensive trust computed over rounds. Notably, there is a significant drop in the first few rounds, followed by a gradual increase until stability around 100 rounds. This graph depicts the evolving trustworthiness of nodes in the network. The initial drop indicates a period of uncertainty or adjustment, whereas the subsequent rise indicates a general recovery in trust. Stabilization implies that the trust values have achieved a consistent state. Analysing this diagram is critical for understanding how the proposed trust model adapts and establishes trustworthiness over time.

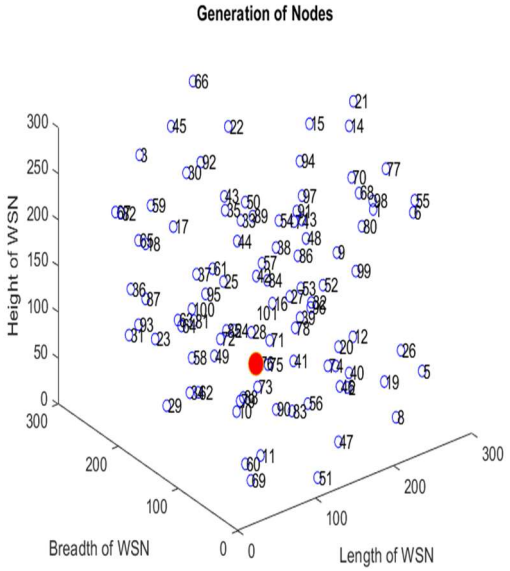

Figure: 5 Generation of Nodes

This 3D visualization in Fig. 5 depicts the generation of nodes in a Wireless Sensor Network. A 3D topology depicts the spatial distribution of nodes along the length (x-axis), height (y-axis), and breadth (z-axis). The visualization helps to understand how nodes are distributed throughout the network, which influences coverage, interference, and connectivity. Analysing this figure provides valuable insights into the network's foundational aspects, guiding future optimizations and analyses based on node spatial placement patterns.

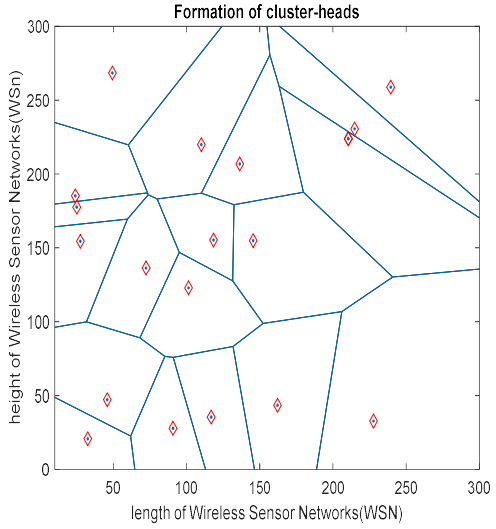

Figure: 6 Cluster Head Formation

Figure 6 depicts the formation of cluster heads using a Voronoi diagram in 2D. The x-axis represents the WSN's length, while the y-axis represents its height. The Voronoi diagram depicts the spatial distribution of cluster heads, highlighting areas of influence for each. Analysing this figure is critical for determining the cluster formation algorithm's effectiveness. Understanding the distribution of cluster heads allows you to assess the network's ability to organize itself efficiently, which is critical for overall performance.

Figure 7 depicts the prediction status of live nodes in the network. The x-axis can represent various nodes, while the y-axis represents the prediction status, which indicates whether a node is alive or dead. Assessing the accuracy of live node predictions is critical for determining the proposed system's reliability. Understanding the patterns or trends in live node predictions reveals

information about the network's ability to adapt to changing conditions and ensures reliable performance.

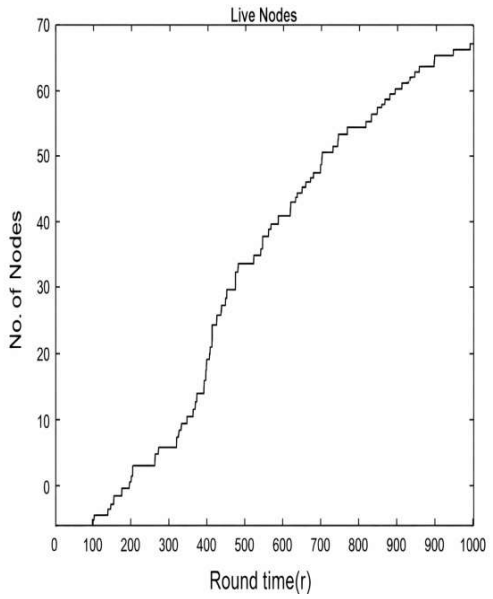

Figure: 7 Prediction Of The Live Nodes

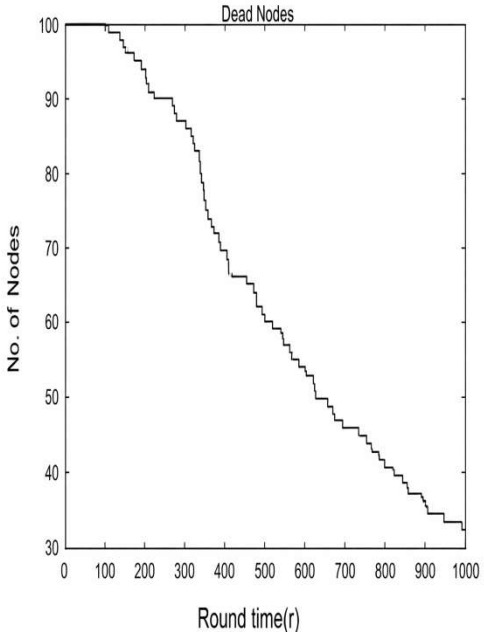

Figure: 8 Prediction Of The Dead Nodes

Figure 8, like Figure 7, shows the prediction of dead nodes in the network. The x-axis represents different nodes, while the y-axis indicates whether a node is predicted to be dead. Analysing this figure allows you to assess the accuracy of dead node predictions, which is useful for effective network management and maintenance.

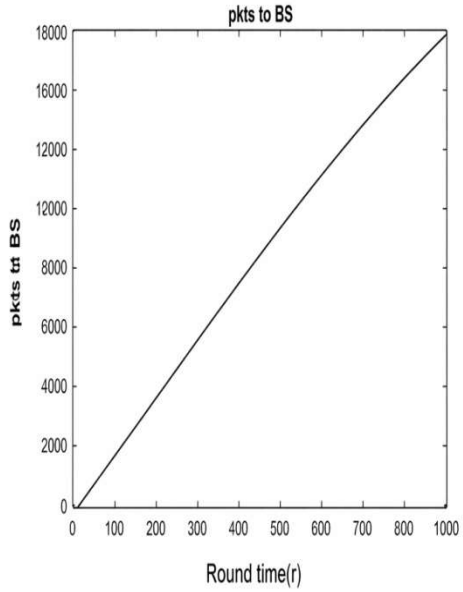

Figure: 9 Number Of Packets Transmitted From The Nodes To The Base Station (BS)

Figure 9 depicts the number of packets transmitted from nodes to the Base Station (BS) across various rounds. The x-axis represents rounds, while the y-axis denotes packets. Analysing packet transmission trends to the BS provides insight into data routing efficiency. Changes in packet transmission may be correlated with changes in trust dynamics, cluster formation, or other network parameters.

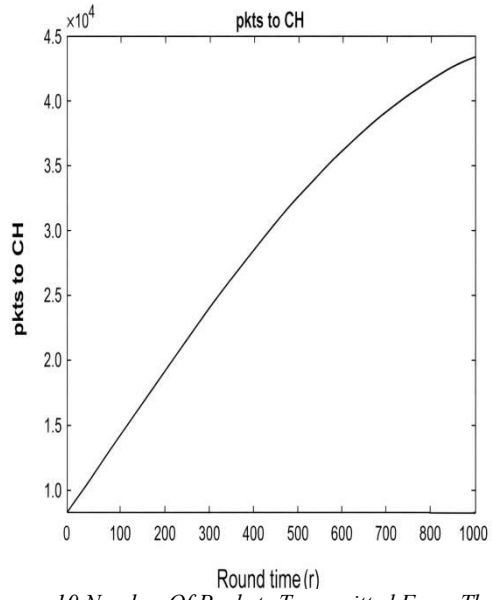

Figure: 10 Number Of Packets Transmitted From The Sensor Nodes To The Cluster Heads (Chs)

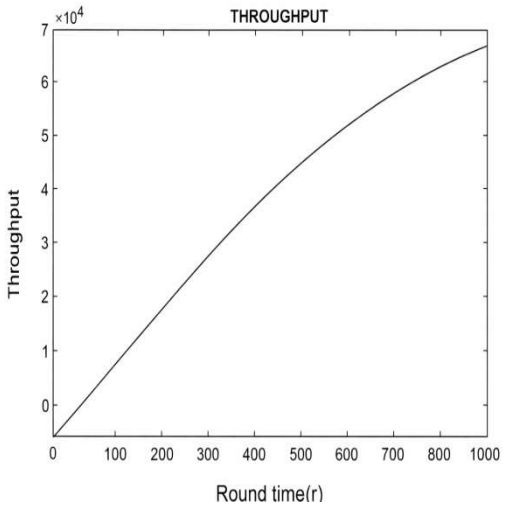

Figure: 11 Throughput Parameter Vs Round Time

Similar to Fig. 9, Fig. 10 depicts the number of packets sent from sensor nodes to Cluster Heads. This figure aids in determining the efficacy of the cluster head selection method. Analyzing variations in packet transmission to cluster heads reveals how well the proposed system optimizes data routing within the network.

Figure 11 depicts the throughput parameter across different rounds. Throughput is an important performance metric, and this figure shows how it changes over time. Correlating throughput trends with comprehensive trust and cluster formation provides an overall view of the network's efficiency and performance.

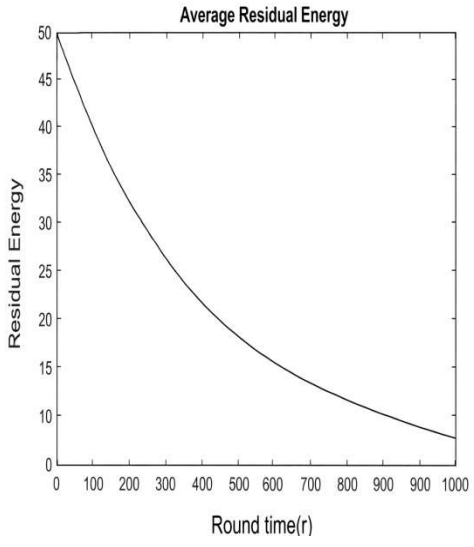

Figure: 12 Average Residual Energy

Figure 12 depicts the average residual energy of nodes in the network. This diagram is critical for understanding the energy consumption patterns of nodes. Analyzing trends in average residual energy reveals information about how trust-aware mechanisms influence energy efficiency. The figure assesses the energy reserves of individual nodes to help evaluate the network's sustainability and longevity.

Table 1 compares key parameters in a WSN across rounds of 100, 500, and 1000. It shows key metrics like throughput (kbps), packets to base station (kbps), packets to cluster heads (kbps), and elapsed time (secs). The data transfer rate is represented by throughput, which is measured in kilobits per second (kbps), and the table shows how it varies across rounds, indicating the network's data transmission capacity. The "Pkts to BS" metric shows the rate in kbps at which data packets are transmitted from sensor nodes to the Base Station. Meanwhile, "Pkts to CH" represents the rate at which data packets are routed to Cluster Heads. Elapsed Time is a useful metric for evaluating the network's time efficiency because it measures simulation duration in seconds.

Table 1: Comparison Of Various WSN Parameters For Different Rounds

Network Parameters	Rounds		
	100	500	1000
Throughput (kbps)	18520	6880	8850
Pkts to BS (kbps)	4910	1520	2810
Pkts to CH (kbps)	16210	5320	6460
Elapsed Time (secs)	48.31	61.13	67.89

Figure 13 supplements Table 1 by depicting the changes in WSN parameters as the number of rounds increases. These fluctuations could represent a variety of aspects of the WSN's performance. The Throughput graphical plot depicts changes in the network's data transfer capability over time, as influenced by factors such as network congestion and changing data loads. The plots for "Pkts to BS" and "Pkts to CH" show the efficiency of data transmission to the base station and cluster heads, respectively. These metrics may fluctuate as the simulation

progresses due to changes in network topology, cluster head selection, or data aggregation processes.

Examining Fig. 13 and Table 1 provides a comprehensive understanding of the WSN's evolving performance metrics. This analysis can assist network administrators in increasing data transmission efficiency and overall performance across rounds.

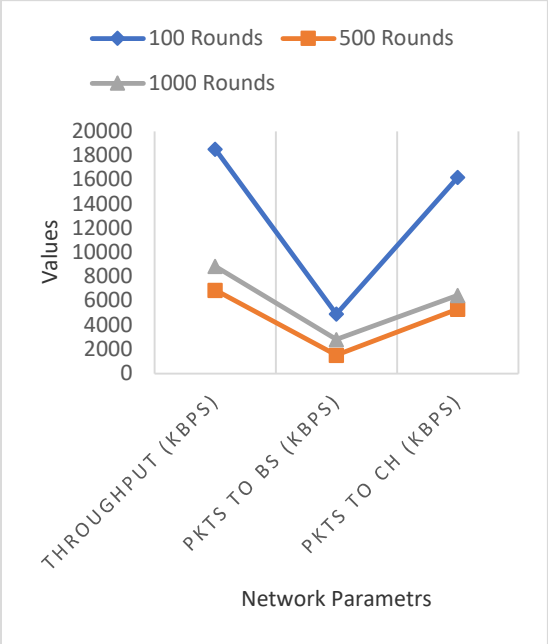

Figure: 13 Comparative Graphical Plot For WSN Parameters (Kbps)

Performance Assessment

Table 2 examines the proposed method's throughput performance to that of existing methods, including RRP [23], MOMHR [24], AODV with Graphs [25], and Traditional AODV [26]. The proposed method outperforms existing approaches in terms of data transmission efficiency within the network. This is backed up by the graphical representation in Fig. 14, which compares throughput values. The plot clearly shows that the proposed method consistently achieves higher throughput, indicating that it is effective in improving data communication in a Wireless Body Area Network (WSN) environment.

Table 2: Performance Evaluation Of The Proposed Method Based On Throughput

Techniques used	Throughput (kbps)
RRP [23]	5000
MOMHR [24]	2400
AODV using Graphs [25]	14400
Traditional AODV [26]	1500
Proposed Method	18520

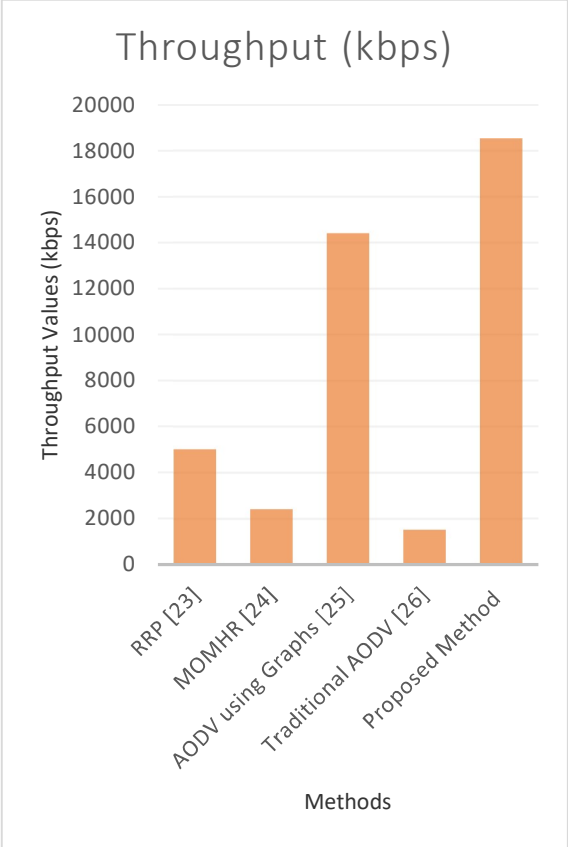

Figure: 14 Throughput Values Comparison

Table 3 evaluates the performance of the proposed method, with computation time as a key metric. The results show that the proposed method is exceptionally efficient in delivering solutions quickly, with a computation time of 48.34 seconds. This fast processing is especially important for real-time healthcare applications, where quick decisions are critical. The associated plot in Fig. 15 visually reinforces these findings by depicting the relative computation times. The graph clearly shows that the proposed method is more efficient in terms of computation time than alternative methods. This demonstrates the proposed method's promising potential for

wireless sensor network (WSN) applications, particularly those that require rapid and responsive data processing capabilities.

Table: 3 Performance Evaluation Of The Proposed Method Based On Time

Techniques used	Elapsed Time /Computation/Simulation Time (secs)
RRP [23]	100
Traditional AODV [26]	3500
DSR [27]	400
Proposed Method	48.34

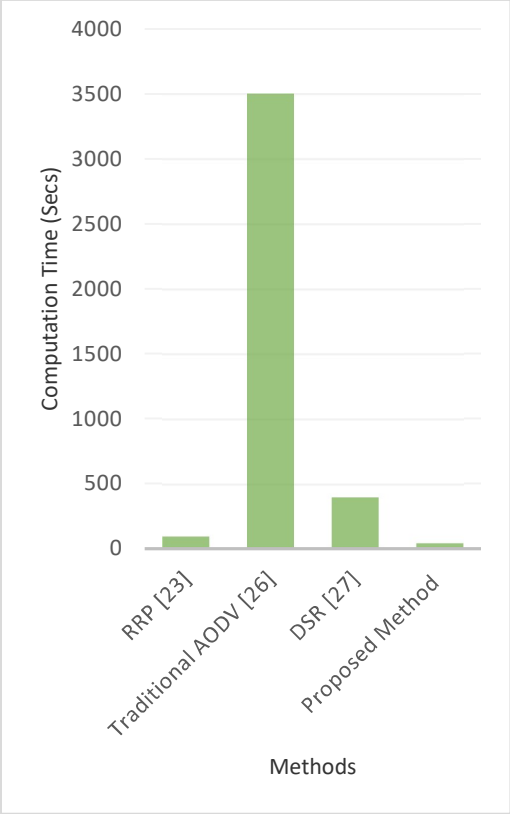

Figure: 15 Computation Time Comparison

Table 4: Residual Energy Based Performance Evaluation

Techniques used	Residual Energy
SEAR [28]	10.23
IBOLSR [29]	10.69
Proposed Method	13.18

Table 4 compares the proposed method to the Simplified Energy-Balanced Alternative-Aware Routing Algorithm (SEAR) [28] and IBOLSR [29], focusing on network performance in terms of residual energy. The proposed method shows superior utilization of residual energy, with a notable value of 13.18 (Joules), which is critical for effective energy conservation in preparation for future use. This improved performance is visually reinforced by the corresponding plot in Figure 16. The graph demonstrates the proposed method's ability to manage energy resources, ensuring long-term network operation and sustainability. These findings highlight the proposed method's distinct advantages over existing solutions, demonstrating its superiority in terms of throughput, computation time, and energy efficiency. These advantages make the proposed method a promising candidate for improving wireless sensor networks (WSNs) in healthcare systems.

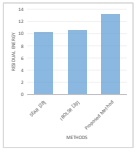

Figure: 16 Residual Energy Comparison

4. CONCLUSION

Finally, this study introduces GLENET, a novel model that seamlessly integrates Graph Convolutional Networks (GCN) into the Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol, improving cluster head selection in Wireless Sensor Networks (WSNs). The innovative trust model within GLENET, which includes adaptive penalty coefficients and

dynamic adjustments, provides a more nuanced understanding of node reliability. Through extensive simulations, GLENET has demonstrated exceptional performance metrics. It achieves an impressive throughput of 18520 kbps, outperforming comparable methods, and has a computation time of 48.34 seconds, demonstrating its efficiency. Furthermore, the model efficiently conserves energy, with a residual energy value of 13.18 Joules, which is critical for long-term network stability. These metrics demonstrate GLENET's superiority in terms of dependability, energy efficiency, and adaptability to changing network conditions.

The success of GLENET lays the groundwork for future research and development in WSNs and trust-based protocols. Future efforts could focus on improving scalability, strengthening security measures, moving to real-world implementations, fine-tuning adaptive learning mechanisms for the GCN model, and investigating integrations with emerging technologies such as edge computing and blockchain. Furthermore, extending GLENET's applicability to new domains and working toward standardization and interoperability will help to shape the evolution of reliable and resilient wireless sensor networks.

The simulation results and comparative analysis reveal three overarching themes that warrant further investigation. The first theme is the trade-off between trust granularity and computational overhead: GLENET's comprehensive trust model (Eq. 11) achieves superior performance but requires computation of three trust dimensions per node per round. As network scale increases beyond the tested range, this overhead may become a bottleneck, and investigating lightweight trust approximation methods for large-scale WSNs is a priority research direction. The second theme is the dependence of GCN performance on network topology stability: the GCN model (Eq. 13) is trained on trust-related features and the current network graph, and its performance may degrade under highly dynamic topologies where node mobility causes frequent graph restructuring. Extending GLENET to incorporate online or incremental GCN retraining mechanisms deserves further study. The third theme is the generalizability of the adaptive penalty coefficient (ACj) to heterogeneous attack models: the current evaluation addresses abnormal behaviour in a generalized sense, but specific attack types in WSNs — such as selective forwarding, Sybil attacks, and wormhole attacks — may require attack-specific penalty functions. Investigating GLENET's resilience under targeted attack scenarios and refining the penalty model accordingly represents a significant open research question for future work.

The identified future directions, combined with the exceptional metrics achieved, provide a promising roadmap for ongoing research, practical implementation, and advancements in the field.

REFERENCES:

[1.] K. Yong and Y. Y. Xin, "Study on Trust Management-Based Cluster-Head Selection in Wireless Sensor Networks," 2015 4th International Conference on Advanced Information Technology and Sensor Application (AITS), Harbin, China, 2015, pp. 43-46, doi: 10.1109/AITS.2015.18.

[2.] J. Li, R. Li and J. Kato, "Future Trust Managemen tFramework for Mobile Ad Hoc Networks: Security in Mobile Ad Hoc Networks", *IEEE Communications Magazine*, vol. 46, no. 4, Apr. 2008, pp. 108-114.

[3.] Djedjig N, Tandjaoui D, Medjek F, et al. Trust-aware and cooperative routing protocol for IoT security. J Inf Secur Appl. 2020;52:102467. doi:10.1016/j.jisa.2020.102467.

[4.] Jing Qi and Tang Liyong, "Trust Management in Wireless Sensor Networks [J]", *Journal of Software*, 2008, pp. 1716-1730.

[5.] G. Savithri and N. R. Sai, "Dynamic deep learning for enhanced reliability in wireless sensor networks: The DTLR-Net approach," Computers, Materials & Continua, 2024, doi: 10.32604/cmc.2024.055827.

[6.] Chen Zhanwei and Li Qian, "Research and mplementation of Video the Host Network for Wireless Sensor Networks", *Journal of Harbin University of Science and Technology*, pp. 33-37, 2009.

[7.] A. V. Krishna and A. Anny Leema, "Efficient routing algorithm for improving the network performance in Internet of Things," *International Journal of Internet Protocol Technology*, vol. 15, no. 2, Jun. 2022, pp. 107–115, doi: 10.1504/IJIPT.2022.123586.

[8.] Tyagi, L. K. ., & Kumar, A. . (2023). A Hybrid Trust Based WSN protocol to Enhance Network Performance using Fuzzy Enabled Machine Learning Technique. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(9s), 131–144.

[9.] T. Gui, C. Ma, F. Wang, and D. E. Wilkins, "Survey on swarm intelligence based routing protocols for wireless sensor networks: an extensive study," in Proceedings of the IEEE International Conference on Industrial Technology, Taipei, Taiwan, May 2016, pp. 1944–1949.

[10.] John A Stankovic. Wireless sensor networks. IEEE Computer, 41(10):, 2008, 92–95

[11.] Wei Wang, Vikram Srinivasan, and Kee-Chaing Chua. Using mobile relays to prolong the lifetime of wireless sensor networks. In Proceedings of the 11th annual international conference on Mobile computing and networking, ACM, 2005 pages 270–283.

[12.] Guoxing Zhan, Weisong Shi, and Julia Deng. Design and implementation of tarf: A trust-aware routing framework for wsns. Dependable and Secure Computing, IEEE Transactions on, 2012, 9(2):184–197.

[13.] C. K. Ho and H. T. Ewe, "A hybrid ant colony optimization approach (hACO) for constructing load-balanced clusters," in 2005 IEEE Congress on Evolutionary Computation, Edinburgh, UK, 2005 pp. 2010–2017.

[14.] Narayan, V., & A. K., D. (2023). FBCHS: Fuzzy Based Cluster Head Selection Protocol to Enhance Network Lifetime of WSN. ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal, 11(3), 285–307. https://doi.org/10.14201/adcaij.27885

[15.] V. K. Akula, T. K. Tak, P. R. Kshirsagar, S. V. Sonekar, and G. Ginnela, "A tolerant and energy optimization approach for Internet of Things to enhance the QoS using adaptive blended marine predators algorithm," Computers, Materials & Continua, vol. 83, no. 2, 2025, pp.2449–2479, doi: 10.32604/cmc.2025.061486.

[16.] A. Rasheed and R.N. Mahapatra. The three-tier security scheme in wireless sensor networks with mobile sinks. Parallel and Distributed Systems, IEEE Transactions on, May 2012, 23(5):958–965,.

[17.] Yi Ren, Vladimir I Zadorozhny, Vladimir A Oleshchuk, and Frank Y Li. A novel approach to trust management in unattended wireless sensor networks. IEEE Transactions on Mobile Computing, 2014, 13(7):1409–1423.

[18.] G. Sudha & C. Tharini (2023) Trust-based clustering and best route selection strategy for energy efficient wireless sensor networks, Automatika, 64:3, 634-641, DOI: 10.1080/00051144.2023.2208462

[19.] Yang L, Lu Y, Liu S, et al. A dynamic behavior monitoring game-based trust evaluation scheme for clustering in wireless sensor networks. IEEE Access. 2018;6:71404–71412. doi:10.1109/ACCESS.2018.2879360.

[20.] Su, B., Du, C., & Huan, J. "Trusted opportunistic routing based on node trust model." IEEE Access, vol. 8, 2020, pp. 163077-163090.

[21.] Baskar, S., Selvaraj, R., Kuthadi, V. M., & Shakeel, P. M. "Attribute-based data fusion for designing a rational trust model for improving the service reliability of internet of things assisted applications in smart cities." Soft Computing, 2021, 25(18), 12275-12289.

[22.] Jadhav, P. P., & Joshi, S. D. "Atom search sunflower optimization for trust-based routing in internet of things." Int J Numer Model, 202134(3), e2845.

[23.] A. I. Saleh, S. A. Gamel, and K. M. Abo-Al-Ez, "A reliable routing protocol for vehicular ad hoc networks," Comput. Electr. Eng., vol. 64, 2017, pp. 473–495.

[24.] Vinodhini, R., Gomathy, C. MOMHR: A Dynamic Multi-hop Routing Protocol for WSN Using Heuristic Based Multi-objective Function. *Wireless Pers Commun* **111**, (2020), 883–907. https://doi.org/10.1007/s11277-019-06891-0

[25.] Maglaras L A and Katsaros D, "Distributed Clustering In Vehicular Networks", IEEE, 2012, pp. 593-599.

[26.] Muhammad Rizwan Ghori, Ali Safa Sadiq and Abdul Ghani, VANET Routing Protocols: Review, Implementation and Analysis, 2018 J. Phys.: Conf. Ser. 1049 012064

[27.] Malik, Suman & Sahu, Prasant. (2019). A comparative study on routing protocols for VANETs. Heliyon. 5. e02340. 10.1016/j.heliyon.2019.e02340.

[28.] Mu, Jiasong & Liu, Xiang & Yi, Xiangdong. (2019). Simplified Energy-Balanced Alternative-Aware Routing Algorithm for Wireless Body Area Networks. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2925909.

[29.] Subbaiah, C.V., Govinda, K. Implementing routing protocol for energy-aware mobile Ad Hoc networks for WBAN-based healthcare systems. *Soft Comput* (2023). https://doi.org/10.1007/s00500-023-07975-7