IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

An Energy Efficient Secure Multipath Data Transmission Approach For Grid Based Wireless Sensor Network Using Light Weight Cryptography

Dr.P.DURGHADEVI

Associate Professor

Global Institute of Management Sciences

Abstract

Wireless sensor networks (WSNs) represent a sophisticated technology that faces challenges in managing numerous sensor nodes, data collection, transmission, and enabling actions across diverse applications, including tracking, surveillance, and forest fire detection, in both civilian and military sectors. This architecture is considerably more vulnerable to threats, hacking, and exploitation due to the distribution context, features of the sensor-equipped nodes, and their transmission procedures, in contrast to traditional networks. Consequently, an ideal strategy is necessary to provide protection in these networks while considering essential limits related to energy conservation and data protection. This research presents an energy-efficient secure multipath transmission method for grid-based wireless sensor networks (EESMPT). The proposed approach contains three phases. The initial phase involves the creation of the grid-based network. At this stage, a grid header was chosen via the multi-criteria optimization technique. The second stage involves the development of a lightweight cryptographic method for secure data transport. In the third stage, multiple paths are chosen to identify the quickest route for secure data transmission. The subsequent measures are employed to evaluate the efficacy of the suggested approach: energy usage, packet delivery ratio, and the count of active and dead nodes.

Keywords: Wireless Sensor Network, Energy Efficient, Secure data transmission, Light weight cryptography, Multi-path transmission, Grid based network.

1. Introduction

Wireless Sensor Networks (WSNs) consist of small sensor nodes designed for data sensing, computing, transmission, and reception duties [1]. In contrast to traditional network configurations, WSN convey sequences of environmental information from one point to other using unsecured channels. Every sensor node in this scenario is designed to transmit beacon notification to surrounding nodes that have been discovered in order to create multi-hop pathways [2]. At the same time, each sensor node must hear the requests originating from other sensor nodes. Consequently, the sensor nodes expeditiously use substantial energy during listening states. Due to the susceptibility of sensor nodes to resource constraints in real-time scenarios, wireless network protocols and communication frameworks must incorporate energy-efficient features [3]. The primary challenge encountered with WSN is protection, as wireless signals are vulnerable to several threats [4]. The proliferation of WSNs across diverse applications has led to significant susceptibility to malevolent threats [5]. Consequently, to safeguard message from malevolent intruders, effective security mechanisms must be developed for WSN applications.

The hierarchical clustering routing technique [6][7] has demonstrated efficacy in conserving energy resources and extending network longevity, wherein sensor nodes are organized into many clusters. Figure 1 shows the structure of cluster based network. Each cluster comprises a single cluster head (CH) and any number of member nodes. The CHs are tasked with managing operations inside their cluster, including data reception, data fusion, and the communication of aggregated information to the sink device. The member node exclusively converse via their CH. Following a designated period, the responsibility of the CH must be reassigned to different node to equilibrate the power utilization throughout the network nodes [8]. This arises from the necessity for CHs to manage numerous activities and relay message across extensive distances. Consequently, they deplete rapidly. The primary benefit of the grouping strategy is that nodes minimize transmission path cost, lower the volume of message communicated to the base server, and enter sleep state while completing message transmission.

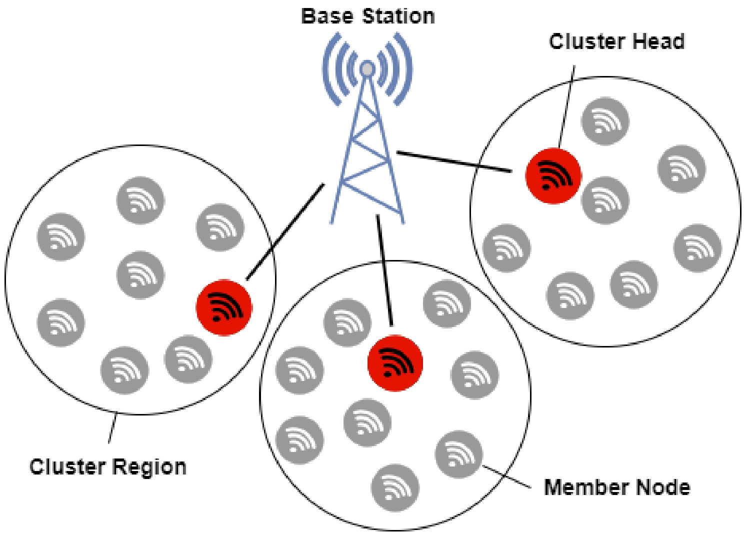

Figure 1 Structure of Cluster based network

Many researchers suggested cluster based secure routing [9][10] for WSN. Nonetheless, the previous routing methodologies are deficient in effective energy conservation and data privacy protection. Consequently, a routing system that is both energy-efficient and secure for wireless sensor networks must be established to ensure secure transmission. This study introduces an energy-efficient secure multipath transmission technique for grid-based wireless sensor networks (EESMPT). The suggested methodology comprises three stages. The preliminary stage entails the establishment of the grid-based network. A grid header was elected using the multi-criteria optimal method at this stage. The second stage entails the formulation of a lightweight cryptographic technique for safe data transmission. In the third stage, many routes are selected to find out the expedient approach for secure message communication. The significant contribution of this work as follow:

- An energy-efficient secure multipath transmission (EESMPT) method is proposed for grid-based wireless sensor networks to enhance the power, security and performance of the WSN.
- To develop grid-based network architecture aimed at achieving energy conservation and ensuring secure data transfer in WSN. Select the grid header with a multi-criteria optimization (MCO) technique that accounts for power, proximity to the sink, and the count of adjacent nodes.
- To develop a lightweight symmetric key cryptographic algorithm for secure data transmission this includes simple lightweight operations.
- To present a multi-path secure routing strategy aimed at minimizing total network energy use and hence extends the network's longevity.

The subsequent sections of the paper are organized as follows: Section 2 presents the pertinent literature associated with the research. Section 3 delineates the suggested energy-efficient secure multipath data transmission. Section 4 evaluates the efficacy of the suggested approach via simulation outcomes, while Section 5 delineates the conclusions and prospective research endeavors.

2. Related Works

In recent years, numerous researchers have formulated diverse routing protocols aimed at reducing energy consumption and enhancing network longevity. Below, several articles pertaining to various routing methodologies in WSNs are examined. Typically, in grid-based networks, grid heads serve as a controlling entity, playing a pivotal role in data collection and transmission. As the central hub for all activities within a grid, they are susceptible to rapid energy depletion due to high network traffic. Consequently, the selection of optimal grid heads significantly influences network performance, particularly regarding stability and homogeneity.

Bouakkaz et al. [11] introduced the Power Efficient Grid-Chain Routing Protocol (PEGCP) to reduce power consumption in message communication by partitioning the entire network area into a grid comprising cells and employing chain creation techniques for both intra and inter-cluster transmission, wherein message is broadcasted solely through minimum link multi-hop connections. The method offers superior power effectiveness and network lifespan in comparison to LEACH. PEGCP failed to account for the proximity among the selected CH nodes and the base server, resulting in cluster head nodes that may be situated distant from the sink device.

Sivasankarareddy et al. [12] propose an energy-efficient and safe routing method for WSN in smart buildings. The initial phase entails the development of an optimal routing protocol utilizing a grid grouping strategy. The grid head is determined through the sailfish optimization approach. Following this, a fuzzy expert system is employed to identify the communicate node that facilitates the minimum path for message communication. The subsequent phase focuses on the creation of a trust model for safe message communication, employing the two-fish algorithm.

Lin et al. [13] introduced an energy-efficient adaptive clustering formation method for wireless sensor networks (ECFE), wherein cluster heads are selected based on energy efficiency welfare, incorporating the remaining power of sensors and the proximity within the similar group. It enhances power effectiveness by organizing nodes into a grid structure. Nonetheless, message communication among intra and inter-grid nodes, as well as to the sink, results in significant energy expenditure.

Hussein et al. [14] propose a rapid, dependable, and secure methodology for key distribution and management to protect the reliability of communications within WSN. An enhancement of the LEACH algorithm has been suggested to improve the power effectiveness, ease, and load-balancing capabilities of networks. A hybrid approach utilizing dispersed key swap and management techniques grounded in elliptic curve cryptography is suggested to secure node communication.

Duy Tan et al. [15] proposed an energy-efficient routing protocol based on grid cells (EEGT). In EEGT, the whole network region is separated into effective grid cells (clusters). Subsequently, a cluster head node is determined based on energy levels and distance. Furthermore, an ant colony model is utilized to identify pathways for spreading messages from cluster head to the base server (external to the cell) to minimize power consumption.

Srinivasiah et al. [16] offer a trust-aware clustering and routing protocol, termed TCRP, utilizing atom search optimization to pick secure CH for WSN. Moreover, the established routing pathway is safeguarded using node verification, wherein the fitness factor for a node is delineated by proximity, reliability, and power levels. The secure protocol offers protection against hostile nodes along the chosen direction-finding while minimizing power utilization. It identifies an ideal route and maintains the reliability and secrecy of the network data.

Regilan et al. [17] propose a methodology employing evolutionary algorithms to select the CH and enhance routing in WSN utilizing grid-based structures. It iteratively formulates strategies according to factors of node weight, proximity, and power consumption by leveraging the evolutionary potential of the genetic algorithm. Delay, coverage, and power effectiveness is employed to assess the strategy. The procedure dynamically chooses Cluster Heads and use Genetic Algorithm-guided optimization to establish pathways.

Kiran Kumar et al. [18] offer an optimized meta-heuristic clustering-based routing strategy for privacy key agreement. A gateway-based network is established to formulate a key management procedure which enhances confidentiality in transmission. This technique entails the formation of sensor node clusters, enabling the effective selection of cluster heads that prioritize nodes exhibiting minimal alteration.

Khashan et al. [19] presents a novel Proxy Re-encryption (PRE) strategy to improve safe communication among nodes in the network and an external information server. The strategy enhances effectiveness by incorporating simple symmetric and asymmetric cryptographic methods, thus reducing processing expenses during PRE procedures and preserving power for resource-limited nodes. This technique ensures the encryption of messages and assigns secure re-encryption responsibilities solely to cluster leaders, thereby enhancing confidentiality and reliability.

Verma et al. [20] propose cluster-based secure optimal routing for protected and power-efficient data communication in IoT-WSNs. Optimal CH is selected for data aggregation via the Boltzmann Selection Probability-centric Gravitational Search method. The actions are performed subsequent to the initialization of the network's nodes. Subsequently, the members are integrated with an neighboring Cluster Head to form a group. The Enhanced Elliptic Curve Cryptography method is used to encode the data that guarantees the security of the data. Subsequently, the encrypted data is transmitted to the sink along the optimum path determined using Deep Learning algorithm.

3. Proposed Methodology

A wireless sensor network comprises a limited number of sensors capable of detecting or controlling physical attributes (noise, weather, and humidity) within a certain geographical region. Wireless sensor nodes transmit data to the base server or sink, as well as to other nodes, using wireless channels. The primary challenges encountered in sensor networks are power effectiveness and safety. Numerous scholars have developed a comprehensive routing procedure to attain optimal power efficiency and safety. The clustering approach is the predominant method for structuring routing procedure in wireless sensor networks. Nonetheless, traditional clustering has limits, including difficulty, high delay, and challenges in attaining an enhanced packet delivery proportion. The suggested method utilizes grid grouping to achieve power-efficient and secure multipath routing for improved message transfer in wireless sensor networks. The general architecture of the suggested approach is shown in Figure 2.

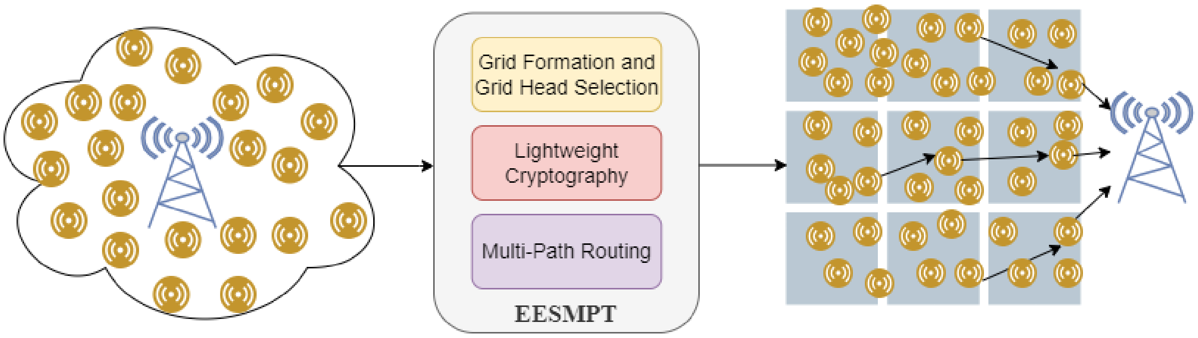

Figure 2 General Architecture of proposed work

The suggested methodology comprises three phases. The initial phase entails the establishment of the grid-based network. A grid header was selected using the multi-criteria optimization method at this phase. The second phase includes the formulation of a lightweight cryptographic technique for safe data transmission. In the third phase, multiple paths are selected to determine the most expedient approach for secure data transmission.

Initially nodes arbitrarily spread in a specified zone and a base server is located in center of the grid. The base server has no restriction on power, storage, or computation capacity. Figure 3 shows the network model.

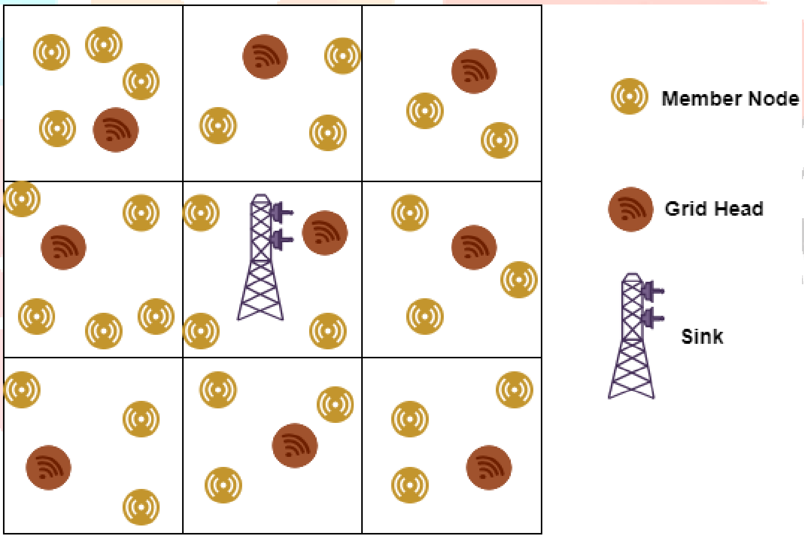

Figure 3 Network Model

This network topology led to the formulation of certain assumptions, which are detailed below.

- Each sensor node is deployed arbitrarily, lacking any discernible structure in the deployment process.
- The nodes were presumed to be immobile and fixed.
- The sink is positioned at the center of the grid.
- Each node start with two Joules of energy. Upon energy depletion, the designated node is removed.
- Nodes within a grid can interact with nodes in an adjacent grid with single hop.

3.1 Grid Head Selection

This section explains the proposed grid head selection approach. In a grid configuration, nodes are typically arranged arbitrarily, with each node assigned a distinctive ID. The elements within the designated grid are termed grid members. A grid head is chosen to balance the load across each grid. The chosen node serves as the grid head for a specified duration. Upon the conclusion of the designated timeframe for which specific node, the new grid head is selected based on selection criteria. The three primary factors for selecting the grid head are proximity, neighbor count, and residual energy. The proximity from a specific node to the base server is determined using the Euclidean distance. The positions of the nodes are monitored with a GPS monitoring device. The Euclidean distance utilized for determining the proximity among a specific node and the base server is formulated as,

$$dis(n1, n2) = \sqrt{(n1_x - n2_x)^2 + \left(n1_y - n2_y\right)^2} \qquad (1)$$

Where $n1_x$, $n1_y$ and $n2_x$, $n2_y$ indicates the x and y location of current node and sink or neighbor node of n1.

Another essential parameter evaluated regarding selection of the grid head is the surplus power at the node. The formula for determining the surplus power in the sensor's charge is presented as,

$$R_{eng} = T_{eng} - U_{eng} \qquad (2)$$

Where R_{eng} denotes the remaining energy of node, T_{eng} represents the total energy, whereas U_{eng} denotes the energy consumed of the node.

The number of neighbor is considered as another factor for selection of the grid head. The remaining power of the neighbor node is computed using,

$$Avg_{Neigh_{eng}}(i) = \frac{1}{NeighC_i} \sum_{j=1}^{NeighC_i} R_{eng}(j) \qquad (3)$$

Where $NeighC_i$ represents the number of neighbor count of i^th node and $R_{eng}(j)$ indicates the remaining energy of j^th node.

Theses multi-criteria are used to find the grid header and finally compute the fitness value based on these criteria using,

$$Ft = Dist_{avg} + (1 - R_{eng}) + \left(1 - Avg_{Neigh_{eng}}\right) \qquad (4)$$

Where $Dist_{avg}$ is the average distance between sink and neighbor nodes. The minimum value of the Ft is selected as grid head.

. Algorithm -1 explains the proposed grid head selection.

Algorithm-1 Grid Head Selection

```
Input: No of Sensor Nodes (SN), No of grid (G), Location of nodes (x,y)
Output: Grid Head in each grid
Step1:  For i =1 to G
Step2:     minFit = Maximum value
Step3:     ghId = 0
Step4:     For j = 1 to No. of Nodes in G
Step5:         Compute  distance between neighbor nodes and sink using Eq. (1)
Step6:         Compute remaining energy of the node using Eq. (2)
Step7:         Compute remaining  energy of neighbor nodes using Eq. (3)
Step8:         Compute fitness (Ft) using Eq. (4)
Step9:         if (Ft < minFit) then
Step10:            minFt = Ft
Step11:            ghId = $j^{th}$ node id
Step12:        end if
Step13:    end for
Step14:    Set ghId as $i^{th}$ grid head
Step15: end for
```

3.2 Lightweight Cryptography

To safeguard the data from diverse security dangers, the transferred information is encrypted with an encryption method and subsequently decrypted at the receiving end utilizing lightweight cryptography. The suggested method employs a lightweight symmetric encryption algorithm for data protection. Algorithm-2 explains the proposed encryption algorithm.

Algorithm-2 Lightweight symmetric encryption

```
Input: 128 bits message (M), Key k1
Output: Encrypted message (em)
Step1:  Divide M into 2 parts (m1,m2)
Step2:  Convert m1 into 8 * 8 matrix (mat1)
Step3:  Convert m2 into 8 * 8 matrix (mat2)
Step4:  Apply matrix scrambling for mat1 and mat2
Step5:  Reconvert mat1 and mat2 into message m1' and m2'
Step6:  Left shift m1' by 8 bit
Step7:  Right shift m2' by 8 bit
Step8   $enc1 = m1' \oplus k1$
Step9:  $enc2 = m2' \oplus k1$
Step10: Combine enc1 and enc2 to generate encrypted message (em)
Step11: Return em
```

The input data, comprising 128 bits, is separated into two parts of 64 bits each. Transform the 64-bit message into an 8 by 8 matrix. The matrix scrambling technique is utilized to transform the original matrix into a permuted matrix. Reconstruct the permuted matrix into a message. A left shift and a right shift (by 8 bits) operation are applied to the permuted message. Apply the XoR technique to encrypt the shifted message.

3.3 Multipath Routing

In this multipath routing, several pathways are found among the source and the base server. This study identifies three paths according to distance, power, and path count. The optimal route is determined by historical successful communication data.

4. Simulation Results

This section analyzes the effectiveness of the suggested EESMPT using energy consumption, packet delivery ratio, count of active and dead nodes. The proposed approach was tested using python programming language and compared with PEGCP [11] and EEGT [15]. The experimental investigation was conducted using 100 nodes randomly deployed within a 100m × 100m area, with the total energy of each distributed node fixed at 2 J.

The nodes are initially installed in the designated region to detect various forms of information. The deployed nodes are subsequently organized into grids according to their intercommunication range. Figure 4 illustrates the grid creation utilizing the intercommunication range. Grid members are the entities that are situated inside the grid.

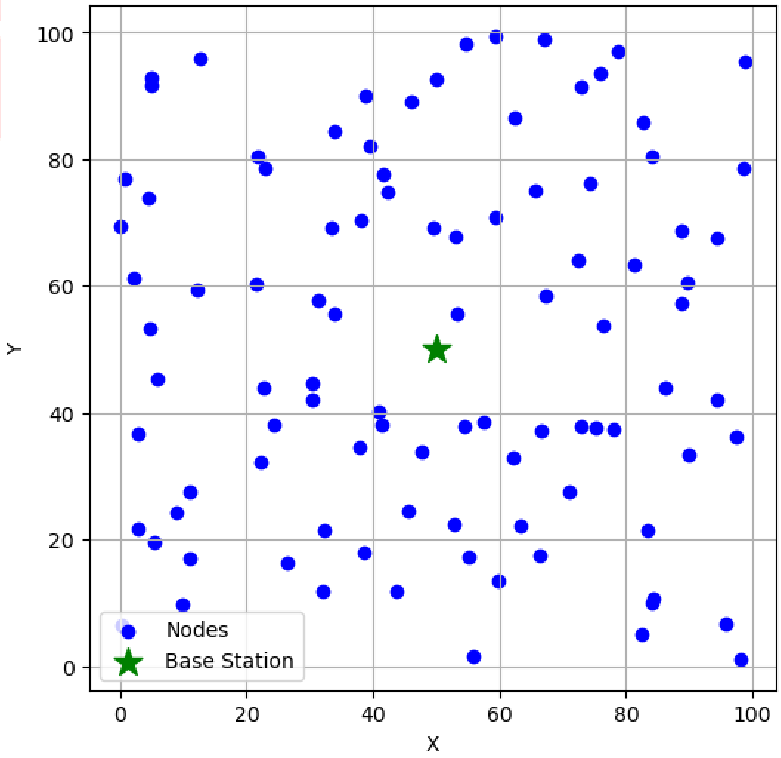

Figure 4 Node deployment in grid

For a predetermined duration, particular node from each grid was designated as the grid head. The multi-criteria optimization algorithm selects the grid head based on three critical factors: distance, remaining energy, and neighboring nodes. The selection of the grid head is depicted visually in Figure 5. Data from each grid element is relayed to the grid head. Subsequently, the data must be conveyed from the grid head to the base server.

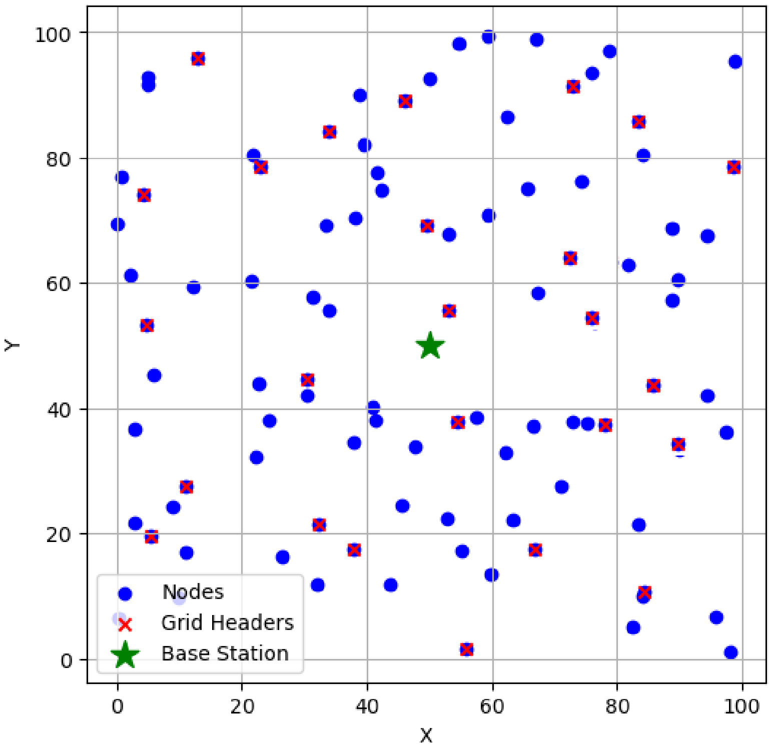

Figure 5 Grid header selection

The comparison of active sensor nodes of network is shown in Figure 6. The suggested protocol achieves superior energy consumption balance compared to existing protocols by choosing the CH based on appropriate criteria, hence prolonging network lifetime.

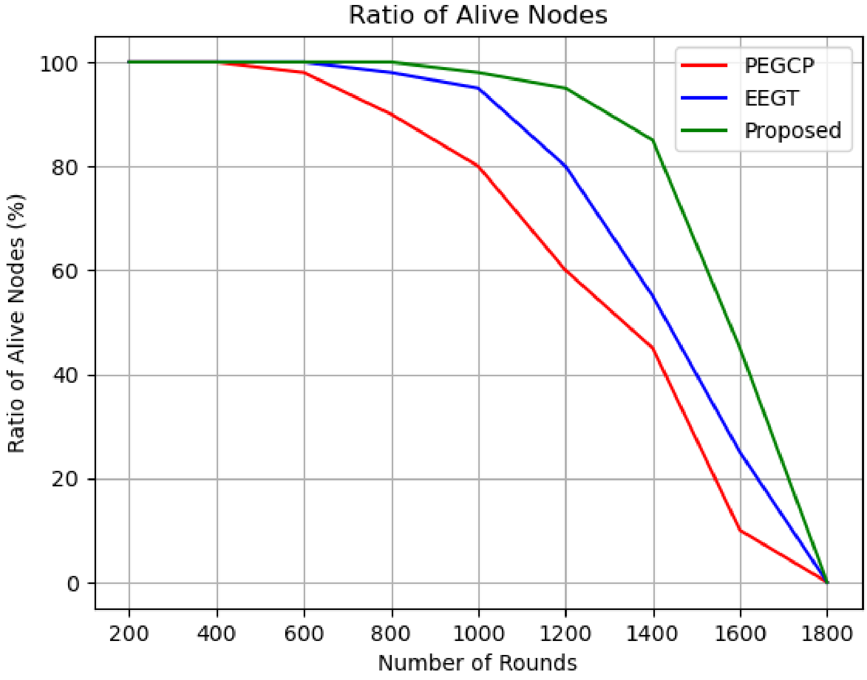

Figure 6 Comparison of Alive nodes (%)

The evaluation of energy utilization of all nodes in network is shown in Figure 7. The findings indicate that the suggested method utilizes less power than alternative methods by circumventing long-distance communication. In prior research, most cluster heads send messages straight to the sink. In contrast, the proposed approach permits cluster heads to relay data messages to the sink through an optimally selected path. Consequently, it enhances power effectiveness and extends the network's duration evaluated to other methods.

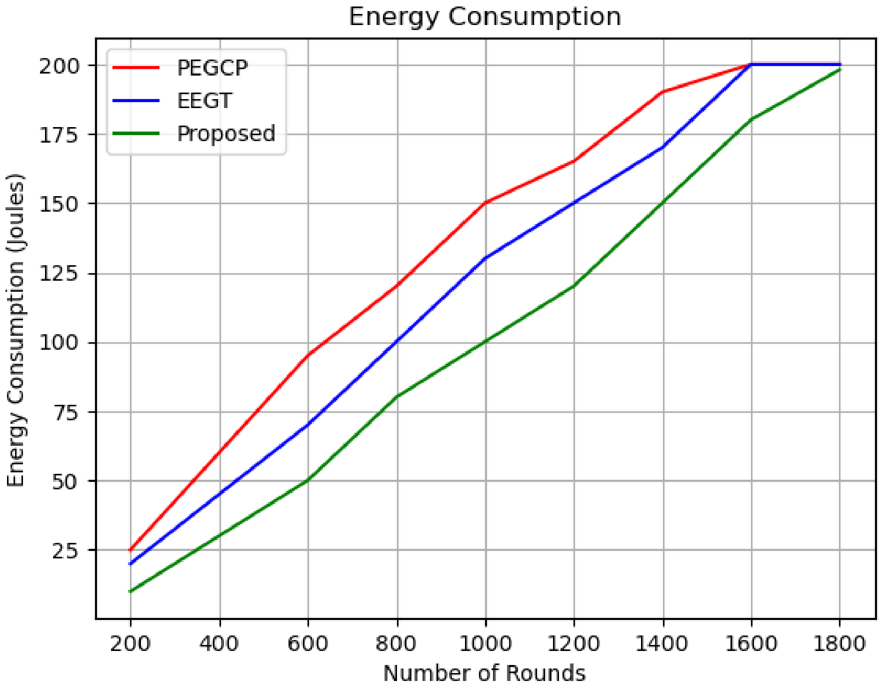

Figure 7 Comparison of Energy Consumption

Figure 8 shows the dead node comparison. The PEGCP, EEGT, and suggested methods exhibit a 5% dead node ratio at about the 550th, 800th, and 900th rounds, ceasing operation at the 1570th, 1690th, and 1800th rounds, respectively.

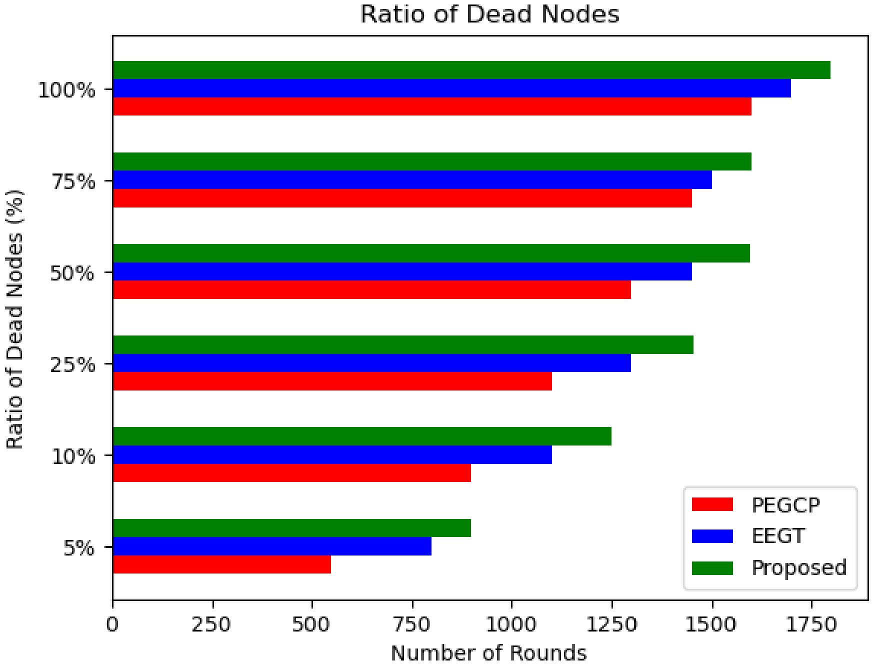

Figure 8 Comparison of dead nodes (%)

Figure 9 shows the percentage of data packets correctly transmitted to the base server.

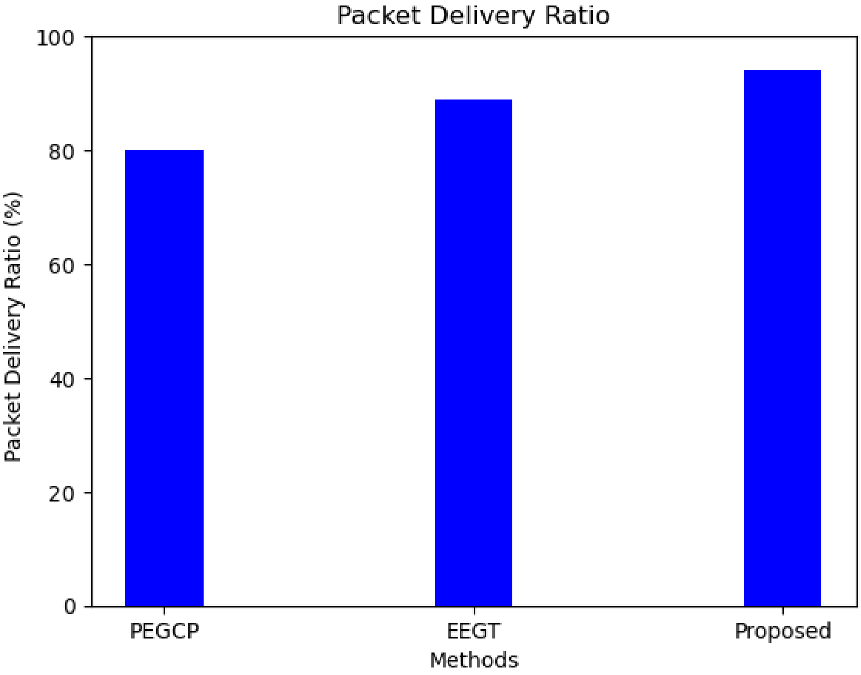

Figure 9 Comparison of Packet Delivery Ratio

The ratio of data packets delivered to the base server in our suggested method is enhanced by roughly 17.5% and 5.6% in comparison to PEGCP and EEGT, respectively. The proposal attained an equilibrium of power usage between the sensor nodes in the network; a more equitable power usage results in enhanced energy effectiveness.

5. Conclusion

The primary concern in Wireless Sensor Networks in recent years has been power reduction and protection vulnerabilities which affect network effectiveness. This study established an optimal network model for enhancing the performance of WSN through a grid-based clustering strategy. The grid head is chosen by a multi-criteria optimization method. The information obtained from the member node is encrypted using lightweight cryptography and sent to the grid head. Multipath routing is employed to send message from the grid head to the base server aiming to reduce power utilization. The simulation study was undertaken to assess the efficacy of the suggested strategy. The effectiveness indicators was computed and juxtaposed against conventional methods to illustrate the superior efficacy of the suggested architecture.

References

[1] Mohan Ram, G., & Ilavarasan, E. (2024). Secure and Energy-Based STEERA Routing Protocol for Wireless Sensor Networks. Journal of Interconnection Networks, 24(03), 2350018.

[2] Rajaram, V., & Kumaratharan, N. (2021). Retracted article: multi-hop optimized routing algorithm and load balanced fuzzy clustering in wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 12(3), 4281-4289.

[3] Dhabliya, D., Soundararajan, R., Selvarasu, P., Balasubramaniam, M. S., Rajawat, A. S., Goyal, S. B., ... & Suciu, G. (2022). Energy-efficient network protocols and resilient data transmission schemes for wireless sensor Networks—An experimental survey. Energies, 15(23), 8883.

[4] Pathak, A., Al-Anbagi, I., & Hamilton, H. J. (2022). An adaptive QoS and trust-based lightweight secure routing algorithm for WSNs. IEEE Internet of Things Journal, 9(23), 23826-23840.

[5] Hu, H., Han, Y., Yao, M., & Song, X. (2021). Trust based secure and energy efficient routing protocol for wireless sensor networks. IEEE access, 10, 10585-10596.

[6] Yadav, R. K., & Mahapatra, R. P. (2021). Energy aware optimized clustering for hierarchical routing in wireless sensor network. Computer Science Review, 41, 100417.

[7] Daanoune, I., Abdennaceur, B., & Ballouk, A. (2021). A comprehensive survey on LEACH-based clustering routing protocols in Wireless Sensor Networks. Ad Hoc Networks, 114, 102409.

[8] Elsmany, E. F. A., Omar, M. A., Wan, T. C., & Altahir, A. A. (2019). EESRA: Energy efficient scalable routing algorithm for wireless sensor networks. IEEE Access, 7, 96974-96983.

[9] Deepa, C., & Latha, B. (2019). HHSRP: a cluster based hybrid hierarchical secure routing protocol for wireless sensor networks. Cluster Computing, 22, 10449-10465.

[10] Kim, D., Yun, J., & Kim, D. (2020). An energy-efficient secure forwarding scheme for qos guarantee in wireless sensor networks. Electronics, 9(9), 1418.

[11] Bouakkaz, F., & Derdour, M. (2021). Maximizing WSN life using power efficient grid-chain routing protocol (PEGCP). Wireless Personal Communications, 117(2), 1007-1023.

[12] Sivasankarareddy, V., Sundari, G., Rami Reddy, C., Aymen, F., & Bortoni, E. C. (2021). Grid-based routing model for energy efficient and secure data transmission in wsn for smart building applications. Applied Sciences, 11(22), 10517.

[13] Lin, D., Kong, L., Zhao, C., Gao, J., Ouyang, H., Yang, Z., & Zhang, Z. (2022). An energy-efficiency-adaptive clustering formation mechanism for the wireless sensor networks. IET Communications, 16(3), 255-265.

[14] Hussein, S. M., López Ramos, J. A., & Ashir, A. M. (2022). A secure and efficient method to protect communications and energy consumption in IoT wireless sensor networks. Electronics, 11(17), 2721.

[15] Duy Tan, N., Nguyen, D. N., Hoang, H. N., & Le, T. T. H. (2023). EEGT: Energy efficient Grid-based routing protocol in wireless sensor networks for IoT applications. Computers, 12(5), 103.

[16] Srinivasiah, V. P. B., Ranganathasharma, R. H., & Ramanna, V. (2023). TCRP: Trust-aware Clustering and Routing Protocol Based on Atom Search Optimization for WSNs. International Journal of Intelligent Engineering & Systems, 16(4).

[17] Regilan, S., & Hema, L. K. (2024). Optimizing energy efficiency and routing in wireless sensor networks through genetic algorithm-based cluster head selection in a grid-based topology. Journal of High Speed Networks, 30(4), 569-582.

[18] Kiran Kumar, G., K Prashanth, S., Padmalatha, E., Venkata Krishna Reddy, M., Rama Devi, N., Abualigah, L., Chithaluru, P. and Kumar, M., (2024). An optimized meta-heuristic clustering-based routing scheme for secured wireless sensor networks. International Journal of Communication Systems, 37(11), p.e5791.

[19] Khashan, O. A., Khafajah, N. M., Alomoush, W., & Alshinwan, M. (2024). Innovative energy-efficient proxy Re-encryption for secure data exchange in Wireless sensor networks. IEEe Access, 12, 23290-23304.

[20] Verma, V., & Jha, V. K. (2024). Secure and energy-aware data transmission for IoT-WSNs with the help of cluster-based secure optimal routing. Wireless Personal Communications, 134(3), 1665-1686.