National Conference on Recent Trends in Artificial Intelligence and Data Science (NCRTAIDS-26)
Sri Vasavi College, Erode, Tamil Nadu, India

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Energy-Efficient and Secure Data Transmission in Wireless Sensor Networks Using Trust-Aware Hybrid Optimization and Learning

[1]Dr.P.Suresh Babu, [2]Ms.K.Hemapriya
[1]Associate Professor, Bharathidasan College of Arts and Science, Erode
[2]Assistant Professor, Bharathidasan College of Arts and Science, Erode

Abstract - Wireless Sensor Networks (WSNs) are widely deployed in monitoring and control applications where reliable data delivery and prolonged network lifetime are critical. However, the limited energy capacity of sensor nodes and the presence of insecure or unreliable routing paths significantly degrade network performance. Existing solutions often address energy efficiency and security independently, resulting in sub-optimal operation under dynamic network conditions. In this paper, a trust-aware and energy-efficient data transmission framework is proposed for WSNs by integrating hybrid meta heuristic optimization with a lightweight learning-based trust evaluation mechanism. The proposed approach jointly optimizes cluster head selection and routing path formation by considering residual energy, node trustworthiness, inter-node distance, and link quality. A multi-objective fitness function guides the optimization process to balance energy consumption and secure communication. Experimental evaluation using a benchmark WSN data set demonstrates that the proposed framework significantly reduces energy consumption, extends network lifetime, and improves data confidentiality and data integrity compared with state-of-the-art routing techniques. The results confirm the suitability of the proposed method for secure and sustainable WSN deployments.

Keywords - Wireless Sensor Networks, Energy-Efficient Routing, Secure Data Transmission, Trust-Aware Routing, Hybrid Optimization.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) consist of a large number of small, low-cost sensor nodes that collaboratively sense, process, and transmit data to a central base station. These networks play a crucial role in applications such as environmental monitoring, industrial automation, healthcare systems, smart cities, and defense surveillance. Despite their advantages, WSNs face inherent challenges due to limited battery power, dynamic network topology, unreliable wireless links, and vulnerability to security attacks. Energy consumption remains the most critical constraint in WSNs, as sensor nodes are often deployed in inaccessible or harsh environments where battery replacement is impractical. Inefficient routing and frequent re transmissions can rapidly deplete node energy, leading to network partitioning and reduced operational lifetime. In parallel, the open wireless medium exposes WSNs to various security threats, including packet dropping, data tampering, and unauthorized access. These attacks not only compromise data integrity and confidentiality but also increase energy wastage through malicious behavior.

Recent research has explored bio-inspired optimization algorithms and artificial intelligence techniques to improve routing efficiency in WSNs. Although such methods have demonstrated promising results in optimizing energy utilization, many of them overlook security considerations or rely on computationally expensive cryptographic mechanisms. Trust-based and blockchain-enabled secure routing schemes improve security but often increase latency and energy consumption, making them unsuitable for resource-constrained WSNs.

Motivated by these limitations, this work proposes a unified framework that simultaneously addresses energy efficiency and secure data transmission. By integrating hybrid optimization techniques with

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

adaptive trust evaluation, the proposed approach ensures reliable routing decisions while minimizing energy expenditure. The framework is lightweight, scalable, and suitable for real-world WSN deployments.

The main contributions of this paper are summarized as follows:
A novel trust-aware hybrid optimization framework for energy-efficient and secure data transmission in WSNs.
A multi-objective fitness function that balances energy consumption, trust level, distance, and link quality.
A lightweight learning-based mechanism for dynamic trust evaluation of sensor nodes.
Comprehensive performance evaluation demonstrating the effectiveness of the proposed approach.

II. RELATED WORK

Energy-efficient routing and secure data transmission have been extensively studied in the context of WSNs. Traditional clustering protocols such as LEACH and its variants focus on reducing communication overhead through periodic cluster head selection. Although these protocols improve energy efficiency, they do not consider node trustworthiness, making them vulnerable to malicious attacks.

Bio-inspired optimization techniques, including Particle Swarm Optimization, Ant Colony Optimization, Whale Optimization Algorithm, and Coot Optimization Algorithm, have been applied to cluster head selection and routing path optimization. These methods enhance energy efficiency by balancing load distribution among nodes. However, most of these approaches prioritize residual energy and distance metrics, with limited consideration of security factors.

Trust-based secure routing schemes evaluate node behavior based on packet forwarding history, energy usage, and communication reliability. While these methods improve data security, they often introduce additional communication overhead for trust computation and dissemination. Blockchain-based solutions further enhance security but are generally unsuitable for resource-constrained WSNs due to high computational and storage requirements.

In contrast to existing studies, the proposed work integrates trust evaluation directly into the optimization process, enabling secure routing decisions without excessive overhead. By combining hybrid meta heuristic optimization with learning-based trust updates, the framework achieves a balanced trade-off between energy efficiency and security.

System Model and Problem Formulation

Network Model

The considered WSN consists of N sensor nodes randomly deployed in a two-dimensional sensing area. Each node is initialized with a finite amount of energy and is capable of sensing, processing, and wireless communication. A single base station with sufficient computational resources is located either within or outside the sensing area. Sensor nodes transmit sensed data to the base station through multi-hop communication using selected cluster heads.

Energy Consumption Model

The first-order radio energy model is adopted to estimate energy consumption during communication. The energy required to transmit a k-bit packet over a distance (d) is given by:

$$E_{tx}(k,d) = E_{elec} \cdot k + E_{amp} \cdot k \cdot d^2$$

The energy consumed to receive a k-bit packet is:

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

$$E_{rx}(k) = E_{elec} \ . \ k$$

where k is the packet size in bits, d is the transmission distance, E_{elec} represents the electronic energy, and E_{amp} denotes the amplifier energy. This model reflects the direct relationship between transmission distance and energy expenditure.

Trust Evaluation Model

Trust evaluation is used to identify reliable sensor nodes for secure routing. Each node maintains a trust score based on its communication behavior, which includes successful packet forwarding rate, residual energy level, and packet drop ratio. The trust value of node i is computed as:

$$T_i = \alpha \cdot SR_i + \beta \cdot \frac{E_i^{res}}{E_i^{init}} + \gamma \cdot (1 - DR_i)$$

where SR_i represents the successful packet forwarding rate of node i, DR_i denotes the packet drop rate, E_i^{res} and E_i^{init} are the residual and initial energy levels, respectively. The weighting factors α, β, and γ satisfy $\alpha + \beta + \gamma = 1$

Proposed Trust-Aware Hybrid Optimization Framework

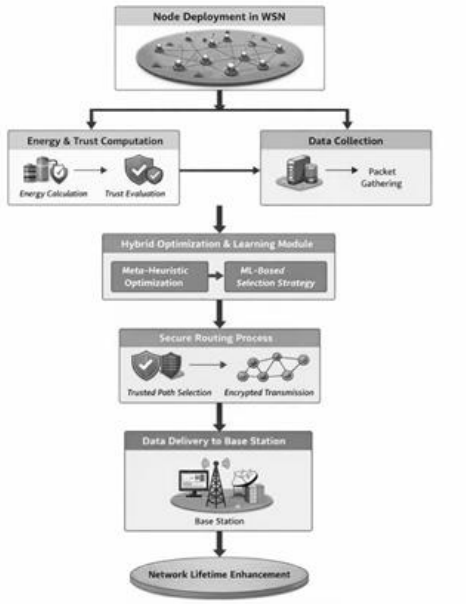

Figure 1 Architecture of the proposed trust-aware hybrid optimization framework

Framework Overview

The proposed framework operates in four main stages: network initialization, trust and energy computation, hybrid optimization-based decision making, and secure data transmission. Initially, sensor nodes are deployed and their energy levels are recorded. Trust values are then computed based on observed communication behavior. Hybrid optimization is applied to select energy-efficient and trustworthy nodes for cluster head selection and routing. Finally, data packets are transmitted through the selected secure paths.

Hybrid Optimization Strategy

To effectively balance global exploration and local exploitation, a hybrid optimization strategy combining Coot Optimization Algorithm (COA) and Particle Swarm Optimization (PSO) is employed. COA provides strong global search capability by mimicking the collective movement of coots, while PSO accelerates convergence by refining candidate solutions based on velocity and position updates.

Fitness Function Design

The fitness of each candidate solution is evaluated using a multi-objective function defined as:

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

$$F = w_1 \cdot (1/E_{cons}) + w_2 \cdot T_i + w_3 \cdot (1/d_{ij}) + w_4 \cdot LQ_{ij}$$

where E_{cons} represents the energy consumption, Ti denotes the trust value of node i, d_{ij} indicates the inter-node distance between nodes i and j, and LQ_{ij} represents the link quality. The weighting factors w_1, w_2, w_3, w_4 control the influence of each objective and satisfy $w_1 + w_2 + w_3 + w_4$ =1.

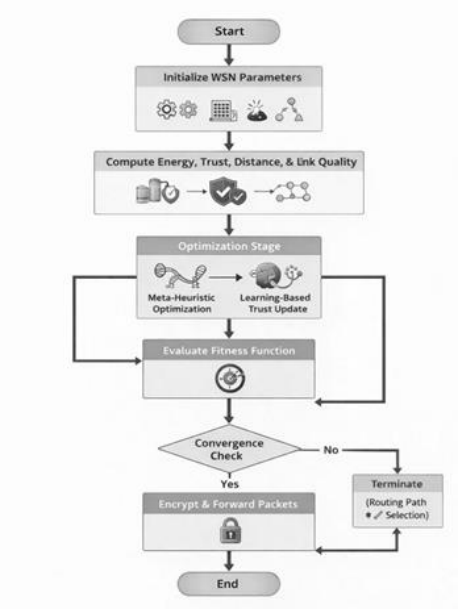

Figure 2. Flowchart of the proposed trust-aware hybrid optimization and secure routing process

Learning-Based Trust Update

A lightweight supervised learning mechanism is employed to update trust values dynamically based on historical transmission data. This adaptive process enables timely identification of malicious or unreliable nodes, ensuring robust and secure routing decisions.

Algorithm 1: Trust-Aware Hybrid Optimization-Based Secure Routing
Input: Number of sensor nodes N, initial energy E, transmission range R
Output: Optimal cluster heads and secure routing paths

- Deploy N sensor nodes randomly in the sensing area.
- Initialize residual energy and trust value for each node.
- For each round do:

Compute residual energy and packet forwarding statistics.
Update node trust using learning-based trust model.
Apply COA for global exploration of cluster head candidates.
Refine candidate solutions using PSO-based local exploitation.
Evaluate solutions using the multi-objective fitness function.
Select optimal cluster heads and routing paths.

- Transmit sensed data through selected secure routes.
- Update energy levels of participating nodes.
- Repeat until network termination.

Experimental Setup and Performance Metrics

Dataset Description

The proposed framework is evaluated using a benchmark Wireless Sensor Network dataset obtained from Kaggle. The dataset includes attributes related to node energy, transmission power, signal strength, noise level, packet loss rate, and network lifetime.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Simulation Parameters
Simulations are conducted with varying numbers of sensor nodes ranging from 100 to 500. Initial node energy is set between 0.5 J and 2 J, and packet size is fixed at 4000 bits. Performance is evaluated over multiple simulation rounds to ensure result consistency.

Performance Metrics
The effectiveness of the proposed framework is measured using the following metrics: energy consumption, network lifetime, data confidentiality rate, and data integrity rate.

Results and Discussion
Energy Consumption Analysis
Figure 3 compares the energy consumption of the proposed method with existing routing protocols. The proposed trust-aware hybrid optimization framework achieves the lowest energy consumption due to balanced cluster head selection and optimized routing paths.

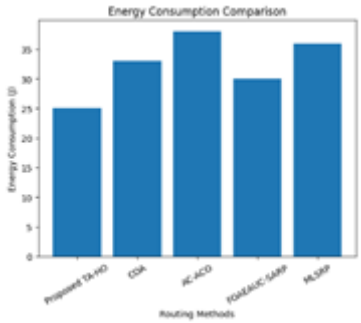

Figure 3. Comparison of energy consumption for different routing methods in WSN

Network Lifetime Analysis
Figure 4 illustrates the network lifetime achieved by different routing schemes. The proposed method significantly prolongs network lifetime by avoiding low-energy and untrustworthy nodes during routing decisions.

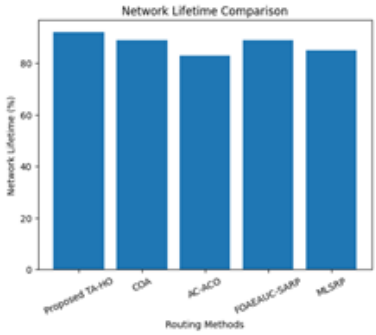

Figure 4. Network lifetime comparison of the proposed method with existing routing protocols.

Security Performance Analysis
Data Confidentiality
As shown in Figure 5, the proposed framework achieves a higher data confidentiality rate by selecting trusted routing paths and mitigating malicious node behavior.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Figure 5. Data confidentiality rate comparison under different routing schemes.

Data Integrity

Figure 6 demonstrates the improvement in data integrity achieved by the proposed approach. The integration of trust evaluation and learning-based updates ensures reliable and tamper-resistant data transmission.

Figure 6. Data integrity rate comparison of secure routing methods in WSN

Complexity Analysis

The computational complexity of the proposed framework is O(N.I), where N denotes the number of sensor nodes and I represents the number of optimization iterations. The learning-based trust update introduces minimal overhead, making the framework scalable for large-scale WSN deployments.

III. CONCLUSION

This paper presented a novel energy-efficient and secure data transmission framework for Wireless Sensor Networks based on trust-aware hybrid optimization and learning. By jointly considering energy efficiency and security requirements, the proposed approach achieves significant improvements in network lifetime, data confidentiality, and data integrity. The results demonstrate the potential of hybrid optimization and adaptive trust evaluation for sustainable and secure WSN deployments. Future work will focus on real-world implementation and reinforcement learning-based adaptive routing strategies.

REFERENCES

1. P. Narayana, K. Keerthi, O. I. Khalaf, P. Chithaluru, M. A. Patil, S. Tumula, D. Jayaram, and M. S. Sharif, "Energy-efficient and secure routing strategy for opportunistic data transmission in WSNs," J. Cyber Secur. Technol., 2024, doi: 10.1080/23742917.2024.2431355.
2. S. N. Bhukya and C. S. R. Annavarapu, "Hybrid reliable clustering algorithm with heterogeneous traffic routing for wireless sensor networks," Sensors, vol. 25, no. 3, Art. no. 864, 2025, doi: 10.3390/s25030864.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

3. M. A. Tawfeek, I. Alrashdi, M. Alruwaili, L. Jamel, G. F. Elhady, and H. Elwahsh, "Improving energy efficiency and routing reliability in wireless sensor networks using modified ant colony optimization," EURASIP J. Wirel. Commun. Netw., vol. 2025, no. 22, 2025. doi: 10.1186/s13638-025-02449-w.
4. G. Siamantas, A. F. Kandris, D. G. Visvardis, and P. Kokkinos, "Energy saving in wireless sensor networks via T-LEACH_SAS protocol," Electronics, vol. 15, no. 2, p. 19, 2025, doi: 10.3390/electronics15020019.
5. L. Yang, A. Lu, S. X. Yang, T. Guo, and Z. Liang, "EDSSR: a secured energy-efficient opportunistic routing scheme for WSNs," Sci. Rep., 2024, doi: 10.1038/s41598-024-77852-2.
6. K. Shekar, P. S. Raman, and R. M. Ameer, "Implementation of novel learning based energy efficient routing methods for WSN," Pers. Ubiquitous Comput., 2025, doi: 10.1007/s10791-025-09718-8.
7. D. Priya and A. S. Raj, "Energy-efficient routing protocols in wireless sensor networks," ITM Conf. Proc., 2025. doi: 10.1051/itmconf/20250703007.
8. Y. P. Makimaa, "Secured routing protocol for improving the energy efficiency of WSNs," IET Cyber-Secur. Technol., 2024, doi: 10.1049/2024/6675822.
9. N. Gupta, "Analysis of energy-efficient smart path optimization routing in wireless sensor networks," Sci. Direct, 2025, doi: 10.1016/j.suscom.2025.03.017.
10. S. Thakur, "AI-driven energy-efficient routing in IoT-based wireless sensor networks," Sensors, vol. 25, no. 24, 2025, doi: 10.3390/s25247408.
11. S. S. Babu and N. Geethanjali, "Lifetime improvement of wireless sensor networks by employing trust index optimized cluster head routing (TIOCHR)," Meas. Sens., 2024, doi: 10.1016/j.measen.2024.101068.
12. S. Kaur, T. Kour, and M. Singh, "Hybrid reliable clustering protocol performance evaluation for WSNs," Eng. Res. Express, vol. 7, no. 1, 2025, doi: 10.1088/2516-1067/ac03f2.
13. R. S. Razooqi, M. Al-Asfoor, and M. Hamzah Abed, "Optimize energy consumption of WSNs using modified ant colony optimization," arXiv, 2024. doi: 10.48550/arXiv.2402.12526.