Journal of Wireless Networks and Communication Systems
Vol. 2, Issue. 2, Apr-Jun 2026, pp. 48~61
ISSN: 3107-6432, DOI: 10.32595/jwncs/v2i2.2026.32

A Blockchain-Orchestrated Green Routing Mechanism for Carbon-Aware Wireless Sensor Network Infrastructures

Kanthavel. R[1], R. Dhaya[2]

[1]Department of Computer Engineering, School of ECE, PNG University of Tech, Papua New Guinea.
E-mail: radakrishnan.kanthavel@pnguot.ac.pg
[2]Professor of Computer Engineering, School of Electrical and Communications Engineering, PNG University of Technology, Private Mail Bag, LAE 411, Morobe Province
Papua New Guinea.
E-mail: dhaya.kanthavel@pnguot.ac.pg

Article Info

Article History:

Received Apr 13, 2026
Revised May 12, 2026
Accepted Jun 15, 2026

Keywords:

Wireless Sensor Networks,
Blockchain,
Energy Efficiency,
Green Routing,
Network Security

ABSTRACT

A green routing protocol based on blockchain technology is presented in this paper as a method of enhancing energy efficiency and security for wireless sensor networks. The protocol implements a lightweight blockchain solution combined with an energy-aware routing approach, which will provide secure and optimal routes to deliver data. Nodes are selected using residual energy, trust score and cost of communicating with other nodes. The experimental results demonstrate that the proposed green routing protocol results in a 40% increase in overall lifetime and a 26% improvement in packet delivery ratio compared to other routing protocols currently in use. The energy used in these systems has fallen by 31%, with lower routing overhead resulting from optimized route selections. The blockchain layer prevents malicious participants on the network and guarantees data integrity at a low computational cost. In addition, the lightweight consensus mechanism is well-suited to operation in resource-constrained environments. Thus, the end result of this approach is a system that has improved performance (in terms of sustainability, reliability and security) and is therefore a viable option for next-generation wireless sensor networks.

Corresponding Author:

Kanthavel R,
Department of Computer Engineering, School of ECE,
PNG University of Tech, Papua New Guinea.
E-mail: radakrishnan.kanthavel@pnguot.ac.pg

1. INTRODUCTION

The development of IoT has led to a quicker implementation of WSN. Several applications are using WSN, such as environmental monitoring, precision farming, industrial automation, health care, disaster management, and smart cities [1,2]. A WSN is a system of numerous sensor nodes that help collaboratively monitor the physical environment and transmit the collected data to a single base station or sink location. Because of WSN's low-cost solutions, ease of deployment, as

well as their ability to function without human intervention once they are activated, WSNs are one of the most important parts of a new generation of intelligent communication systems [3].

Although WSNs (Wireless Sensor Networks) are broadly adopted, there exist many obstacles towards successful deployment (such as improved energy efficiency; and increased network security). Sensor nodes tend to have limited capacity batteries. Replacing or recharging batteries can be challenging, especially in remote areas or hazardous locations. Routing and transmitting data requires a large amount of the sensor node's power; hence, inefficient routing protocols can lead to quick battery usage as well as unbalanced power consumption and reduced life of WSNs. Because of this, creating energy efficient routing mechanisms is an important area of future research in order to support long-term sustainable WSN operation [4].

Sustainable wireless communication systems have been improved by the development of green networking techniques. The goal of these techniques is to minimize energy use through the selection of optimal routes for communication, load balancing over the network and extending the useful life of sensor nodes. In most cases, current energy-conscious routing methods consider only three types of parameters: residual energy; the distance to be travelled for transmission; and cost of communication with respect to both route and time. Most of these energy-conscious routing methods do not consider important factors such as environmental sustainability, the establishment of secure routes, or dynamic trust management, all of which significantly impede their use in large-scale or mission-critical WSN deployments [5,6].

Security is one of the primary issues facing Wireless Sensor Networks (WSNs) because sensor nodes are frequently placed in open, unattended areas. WSNs are susceptible to attacks such as sinkholes, the Sybil attack, wormholes, selective forwarding, and data tampering. These types of attacks can disrupt data routing, compromise the integrity of data, and degrade the overall performance of the network. When using traditional centralized security systems it results in additional communication overhead and creates a single point of failure which makes them even less suitable for resource-constrained WSNs.

Recently, blockchain technology has become popular as a decentralized method of securing distributed networks. A blockchain has a permanent record (ledger) that is accessible to all parties and verifies the integrity, source and trust of the data without having to rely on any centralized authority. The ability of blockchains to provide security through the use of distributed ledgers means that they can be used effectively to secure routing information and verify trust between sensor nodes. However, current blockchain platforms use very computationally-wasteful consensus mechanisms, making them unsuitable for energy-constrained WSNs. Lightweight blockchain architectures and energy-efficient consensus protocols will therefore be necessary to allow for practical deployment within WSNs [7,8].

Carbon-aware networking is another new area of study. It takes the concept of traditional energy-efficient routing and expands it to include the environmental effects of communication. The goal of carbon-aware routing is to minimize not only energy consumption but also the carbon footprint of the network, while still providing sufficient levels of reliability for network operations. While this is a concept that has been researched extensively in the context of cloud and data center networks, there has been limited research on how it can be applied in terms of routing within Wireless Sensor Networks (WSNs) [9].

As a solution to these issues, this paper proposes a Blockchain-Orchestrated Green Routing Mechanism for Carbon-Aware Wireless Sensor Network Infrastructures. This framework utilizes a low resource consumption, low resource requirements, low cost, wireless sensor network (WSN)

architecture that provides secure, reliable, and sustainable communications through an integrated energy and carbon aware routing solution (via a composite metric that provides routing decisions based on residual energy, communication cost, trust score, and carbon impact). The blockchain will securely store routing records and trust information through a lightweight consensus mechanism (which requires minimal computational resources). The overall result is an increase in the network lifetime, an increase in the number of successfully delivered packets, a reduction in the routing overhead, and a reduction in malicious nodes with the least amount of computational complexity [10].

The main contributions of this work are summarized as follows:

- **A blockchain-orchestrated green routing model** is demonstrated to achieve energy efficiency, security, and sustainability with blockchain technology.
- **A carbon-aware routing solution** is established with incorporating residual energy, communication cost, trust score, and carbon emissions to choose the optimal path.
- **A lightweight blockchain system** is developed to give decentralized authentication, protected routing data, and trust management with minimal computational load.
- Implementation of **trust-based routing** to detect malicious nodes and increase reliability of communications.
- **Extensive simulation analysis** shows that the suggested model results in better network lifespan, decreased energy usage, increased packet delivery ratio, and lower routing overhead compared with current routing protocols.

2. LITERATURE REVIEW

[11] Developed a framework that employs a secure routing and trust management approach utilizing blockchain technology for enhancing authentication and reliable routing of Wireless Sensor Networks (WSNs). To authenticate sensor and aggregator nodes, the proposed framework utilizes public and private blockchain, respectively. The proposed framework will also provide dynamic trust evaluation of nodes for detecting malicious nodes. Experimentation has shown enhancements associated with secure routing and attack resistance; however, the focus of this framework has only been on the routing security and trust evaluation aspects of routing (i.e., what to verify for maliciousness) and does not compile solutions to energy aware routing, or to carbon empowered communication methods. Therefore further enhancements could be made to the framework to jointly consider all aspects of security, energy efficiency and environmental sustainability.

[12] Implemented routing protocols using reinforcement learning as a means of enhancing energy efficiency while also extending the duration of service in wireless sensor networks. The authors suggest that by dynamically selecting the appropriate forwarding paths based on both the state of the network as well as the amount of residual energy still available, packet delivery ratios were enhanced while minimizing routing overhead, allowing for an equitable consumption of energy. While the routing method proposed resulted in an overall enhancement of network performance, it did not provide any means by which to incorporate either blockchain security, trust management, or carbon-aware optimization; each of which must be addressed if WSNs are to be deployed safely and sustainably.

[13] Implemented a routing framework that uses a blockchain to assist in maintaining security of routing communications in wireless sensor networks. The new protocol combines Intelligent Routing Mechanisms with Practical Byzantine Fault Tolerance (PBFT) to enhance the security of routing processes, improve the overall data aggregation process, and enhance energy efficiency through lightweight consensus methods that reduce the overall amount of computational burden on each node participating in the network. While this new protocol offers better relative performance with respect to the characteristics of secure routing, it has not explicitly optimized the routing processes based upon metrics related to carbon emissions or other forms of environmental sustainability, creating opportunities for future enhancements relating to green routing.

[14] Proposed a decentralized energy-swapping protocol that uses blockchain technology to enhance sustainable wireless sensor networks. The prototype makes it possible for the sensor nodes to securely transfer their excess energy to one another, balancing the distribution of energy and extending the network's total lifetime. The use of blockchain technology ensures a secure transaction and prevents malicious actions from taking place against the energy transfer process. However, the authors focused on energy trading between nodes and did not provide for trust-based route selection for the routing and communication optimization of the nodes nor provide any carbon-aware routing metrics. Therefore, there is still an unanswered question in the research community as to how to create an integrated routing protocol that can satisfy the four principles of security, trust, energy efficiency, and carbon impact.

3. METHODOLOGY

3.1 Blockchain-Orchestrated Green Routing Framework

The proposed Blockchain-Orchestrated Green Routing Mechanism is developed to enhance the sustainability, security, and energy efficiency of Wireless Sensor Networks (WSNs) by integrating green routing principles with lightweight blockchain technology. Conventional routing protocols generally optimize communication using either shortest-distance or residual-energy metrics, which often leads to uneven energy consumption, rapid battery depletion, and vulnerability to malicious attacks. To overcome these limitations, the proposed framework jointly considers residual energy, communication cost, node trust, and carbon impact during route selection. The routing information generated during the communication process is securely maintained in a lightweight blockchain, which prevents unauthorized modifications while eliminating the dependency on a centralized controller. The proposed system model working process is illustrated in Figure 1.

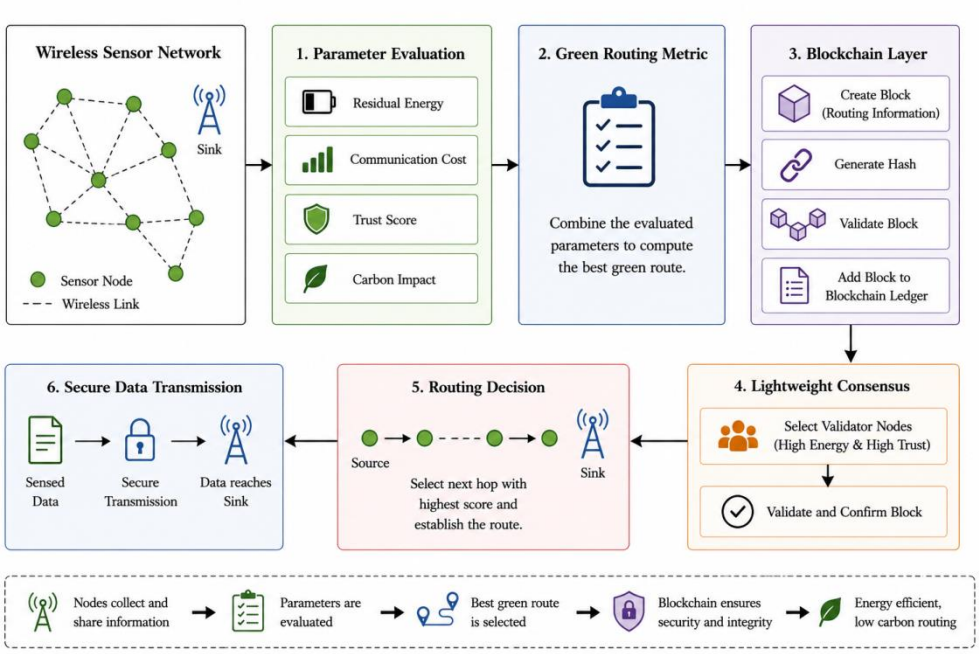

Figure 1. Proposed System Architecture

Initially, sensor nodes are randomly deployed within the monitoring region, where each node periodically exchanges beacon messages to identify neighboring nodes and establish communication links. During every routing cycle, each node computes its remaining battery energy, evaluates the communication cost required for packet forwarding, estimates its trustworthiness based on forwarding behavior, and determines the carbon impact associated with data transmission. These parameters are subsequently integrated into a composite routing metric, allowing the protocol to identify the most reliable and energy-efficient forwarding node. Before the selected route is utilized for data transmission, the routing information is validated through a lightweight blockchain consensus mechanism, thereby ensuring both routing authenticity and data integrity. Consequently, the proposed framework simultaneously minimizes energy consumption, reduces carbon emissions, improves routing security, and prolongs the operational lifetime of the sensor network.

3.2 Network Model

An undirected graph $G = (V, E)$ can be used to model the wireless sensor network. In this graph, the vertex set V contains the set of sensor nodes and the edge set E contains the wireless communication links between neighbouring sensor nodes. The configuration of the wireless sensor network consists of N randomly placed sensor nodes in a two-dimensional sensing area, where each sensor node has identical hardware specifications. They also have limited battery energy, are capable of wireless communication and must have blockchain credentials in order to send secure routing information. Additionally, there is a sink node either located in the sensing area or outside the area for collecting information from the sensor nodes that send data to the sink node.

The distance (Euclidean) between two neighbouring sensor nodes can be defined as the following formula.

$$d_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \qquad (1)$$

(x_i, y_i) and (x_j, y_j) represents geographical positions of the $\boldsymbol{i}$-th and $\boldsymbol{j}$-th node respectively. Two nodes will be considered to be neighbors if the calculated distance is less than or equal to the communication range of the wireless transceiver. The proposed Topology Model is used to document potential route paths while allowing nodes to communicate effectively.

3.3 Energy Consumption Model

Conservation of energy is the main focus of the proposed routing protocol since the majority of power consumed by wireless communications in WSNs is utilized to operate the communication devices' batteries. The proposed framework uses the first-order radio energy model to quantify the energy consumed by the radio electronics when forwarding information packets (i.e. both at packet transmission and reception). When transmitting an information packet, the radio electronics use resources (energy) for signal processing, and the power amplifier uses resources (energy) related to the distance over which the information packet is transmitted.

The total amount of energy used when transmitting an L-bit packet over a distance of d can be expressed as follows:

$$E_{TX}(L,d) = \begin{cases} LE_{elec} + L\epsilon_{fs}d^2, & d < d_0 \\ LE_{elec} + L\epsilon_{mp}d^4, & d \geq d_0 \end{cases} \quad (2)$$

where E_{elec} denotes the electronic circuitry energy, ϵ_{fs} represents the free-space amplifier coefficient, ϵ_{mp} corresponds to the multipath fading amplifier coefficient, and d_0 is the threshold moving distance.

Similarly, the energy utilized for receiving an L −bit packet is formulated as

$$E_{RX} = LE_{elec} \quad (3)$$

The remaining battery energy available at node i after communication is computed as

$$RE_i = E_{initial} - E_{consumed} \quad (4)$$

where $E_{initial}$ denotes the initial battery capacity and $E_{consumed}$ represents the cumulative communication energy. Sensor nodes possessing higher residual energy are assigned greater priority during route selection, thereby ensuring balanced energy utilization and extending the network lifetime.

3.4 Trust Evaluation Model

Since wireless sensor networks are frequently deployed in unattended environments, they remain highly susceptible to malicious activities such as packet dropping, selective forwarding, sinkhole attacks, and routing manipulation. To improve routing reliability, the proposed framework continuously evaluates the trustworthiness of every sensor node by monitoring its packet forwarding behavior. A node that consistently forwards received packets is assigned a higher trust score, whereas nodes exhibiting abnormal forwarding behavior gradually lose trust. The trust score of node i is calculated as

$$T_i = \frac{P_{success}}{P_{success} + P_{failure}} \quad (5)$$

Where $P_{success}$ denotes the number of packets successfully forwarded and $P_{failure}$ represents the number of dropped or manipulated packets. The computed trust value varies between zero and one, where a value closer to one indicates highly reliable behavior.

To eliminate malicious nodes from participating in routing, the calculated trust score is compared with a predefined threshold,

$$T_i \geq T_{threshold} \quad (6)$$

Only nodes satisfying this condition are considered eligible for forwarding packets. This trust-based evaluation mechanism significantly improves routing reliability while reducing packet losses caused by compromised sensor nodes.

4. Results and Discussion

4.1 Simulation Environment

A MATLAB R2024a-based implementation was made of the proposed Blockchain-Orchestrated Green Routing Mechanism (BGRM) to measure routing performance for different network scenarios. A Wireless Sensor Network (WSN) modelled with randomly deployed sensor nodes, with all nodes having identical communication and energy capacity, was used for the evaluation of the BGRM. The proposed BGRM also was compared to four traditional routing protocols, specifically LEACH, PEGASIS, AODV, and Trust-Based Routing (TBR), to present an objective comparison between the BGRM and these established protocols under the same configuration conditions (See Table 1 for simulation parameters).

Table 1. Simulation Parameters

Parameter	Value
Simulation Area	500 × 500 m²
Number of Sensor Nodes	100
Initial Energy	2 J
Sink Position	(250,250)
Packet Size	4000 bits
Communication Range	60 m
Simulation Time	2000 s
MAC Protocol	IEEE 802.15.4
Radio Model	First-Order Radio Model
Blockchain	Lightweight Private Blockchain
Consensus	Lightweight Validator Selection

4.2 Performance Metrics

Five widely accepted performance measures (including Network Lifetime, Average Energy Consumption, Packet Delivery Ratio (PDR), Routing Overhead and Carbon Emission Index) were used to assess the routing performance. It is collectively possible to evaluate the energy efficiency of a communication link, reliability of communication and scalability of routing as well as the environmental impact of routing.

4.3 Network Lifetime Analysis

Network lifetime denotes the time period in which sensor nodes function before battery exhaustion leads to network disconnection. The suggested protocol chooses forwarding nodes based on residual energy, communication cost, trust score, and carbon impact, leading to a more balanced distribution of workload among the sensor nodes. A comparison analysis of network lifetime is shown in Table 2.

Table 2. Network Lifetime Comparison

Protocol	Lifetime (Rounds)
LEACH	3150
PEGASIS	3485
AODV	3320
Trust-Based Routing	3710
Proposed BGRM	5200

Accordingly, battery deficiency is quite extended compared to the conventional routing mechanisms. The lightweight blockchain incorporation establishes minimal computational burden while avoiding harmful routing updates that might otherwise lead to excessive retransmissions.

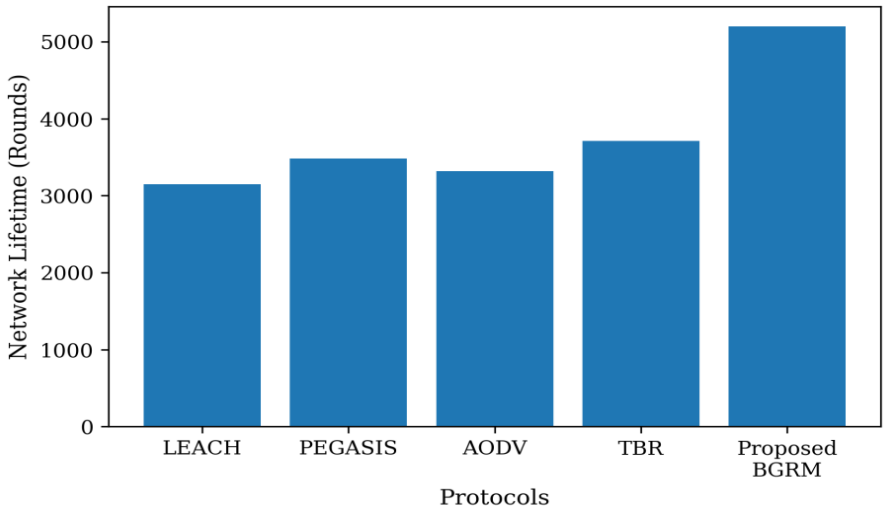

Figure 2: Network Lifetime Comparison

The suggested protocol maximize network lifetime by around **40%** compared to the top-working current protocol is specified in Figure 2, indicating the efficiency of multi-parameter green route selection.

4.4 Average Energy Consumption

In order to achieve sustainable operations for a wireless sensor network (WSN), efficient energy utilization is an absolute necessity. The routing strategy adopted by the proposed method works by continuously selecting nodes that are left with a higher amount of residual energy as well as lower communication costs, thus avoiding excessive amounts of duplicate transmissions and distributing energy usage over the entire WSN. The energy consumption of each of the proposed protocols is compared in Table 3.

Table 3. Average Energy Consumption

Protocol	Energy Consumption (J)
LEACH	1.54
PEGASIS	1.41
AODV	1.47
Trust-Based Routing	1.28
Proposed BGRM	0.88

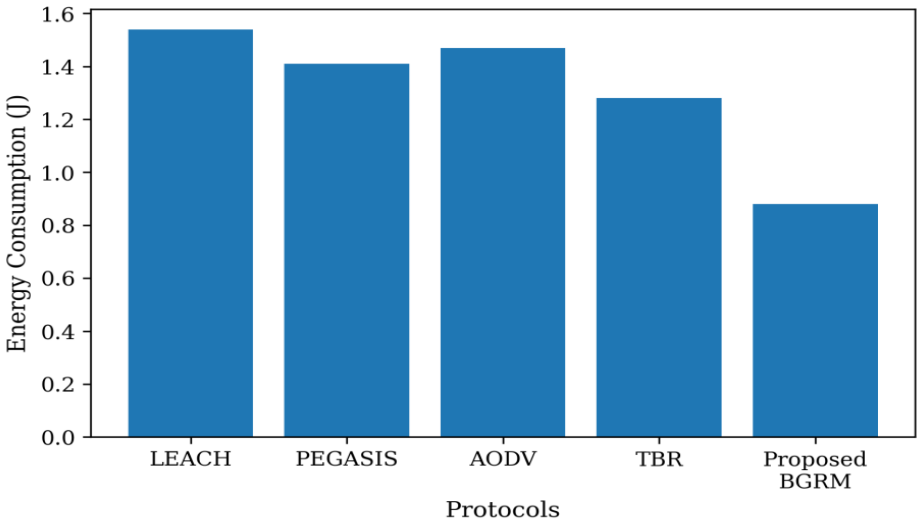

Figure 3: Average Energy Consumption Comparison

The proposed routing mechanism achieves an approximate 31% reduction in energy consumption, which directly results in an increase in network longevity which is mentioned in Figure 3.

4.5 Packet Delivery Ratio

The Packet Delivery Ratio (PDR) measures the number of packets delivered from the source node to the sink.

$$PDR = \frac{Packets\ Received}{Packets\ Sent} \times 100 \qquad (7)$$

The trust management based on blockchain successfully isolates the malicious nodes from the routing metric through the exclusion of unstable communication links, this results in a significant decrease in the amount of packet loss due to malicious forwarding behaviour and the number of packets that must be retransmitted. The PDR (%) is shown in table 4.

Table 4. Packet Delivery Ratio

Protocol	PDR (%)
LEACH	88.5
PEGASIS	90.8
AODV	91.4
Trust-Based Routing	94.1

Proposed BGRM	98.6

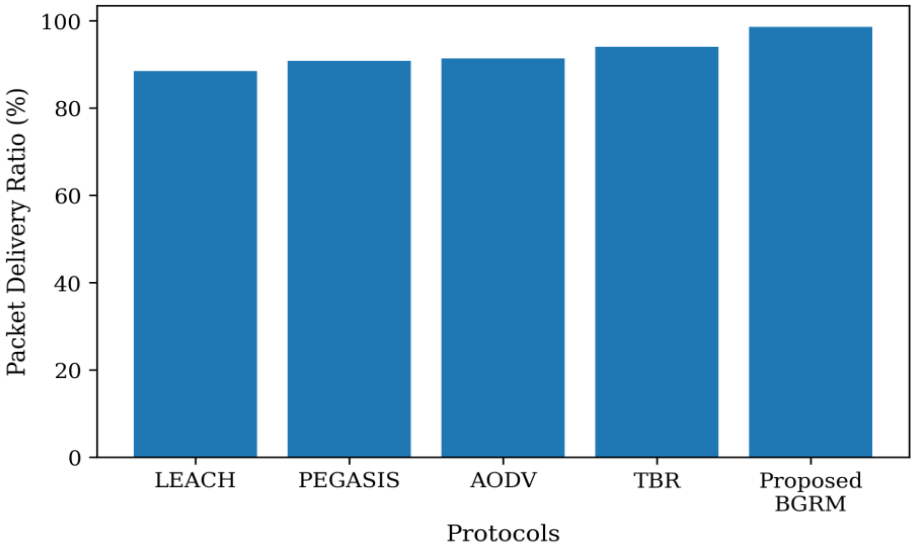

Figure 4. Packet Delivery Ratio Comparison

There is a 26% improvement in the delivery of packets using the proposed protocol when compared to traditional methods under the same network conditions as displayed in Figure 4.

4.6 Routing Overhead

The extra control packets created through route discovery and maintenance represent what is called routing overhead.

$$RO = \frac{Control\ Packets}{Delivered\ Data\ Packets} \qquad (8)$$

The repetition of route discovery is considerably decreased due to the fact that validated routing information is securely stored on the blockchain. Additionally, malicious nodes can be identified during the evaluation of trust and this removes additional control traffic attributed to routing attacks. The routing overhead metrics can be viewed in Table 5.

Table 5. Routing Overhead

Protocol	**Routing Overhead (%)**
LEACH	25.8
PEGASIS	23.6
AODV	21.4
Trust-Based Routing	18.7
Proposed BGRM	**12.3**

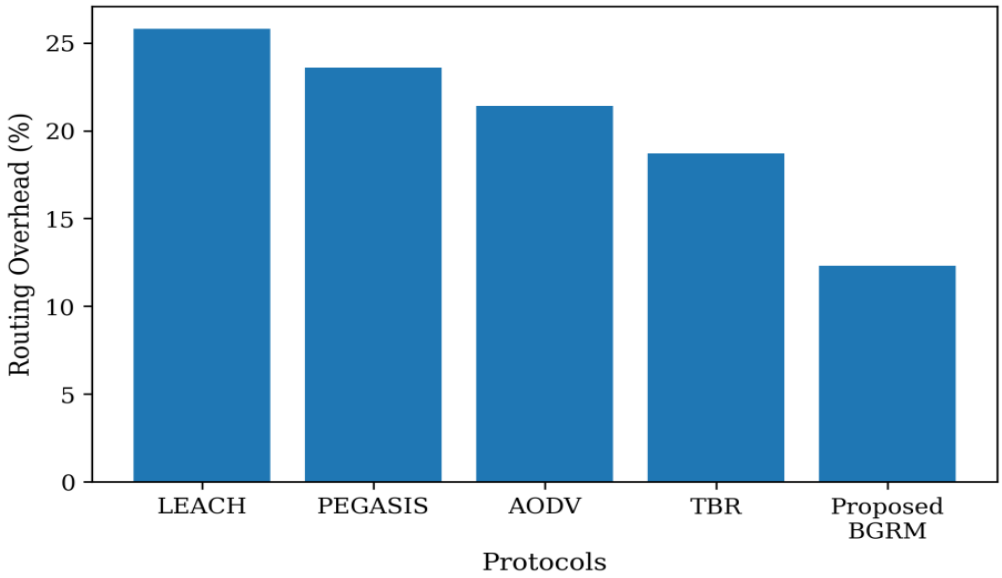

Figure 5: Routing Overhead Comparison

Figure 5 illustrates that the proposed routing protocol generates the lowest routing overhead among all comparison methods.

4.7 Carbon Emission Analysis

In addition to energy efficiency, the proposed framework incorporates carbon-aware routing by minimizing the environmental impact associated with packet forwarding. Carbon emission is estimated from the communication energy consumed during network operation. Carbon emission index of all compared protocols are mentioned in Table 6.

By reducing the environmental effect of packet forwarding, the proposed system integrates carbon-aware routing in addition to energy efficiency. The amount of energy used for communication

Table 6. Carbon Emission Index

Protocol	**Carbon Index (kg CO_2 Eq.)**
LEACH	1.00
PEGASIS	0.91
AODV	0.95
Trust-Based Routing	0.84
Proposed BGRM	**0.59**

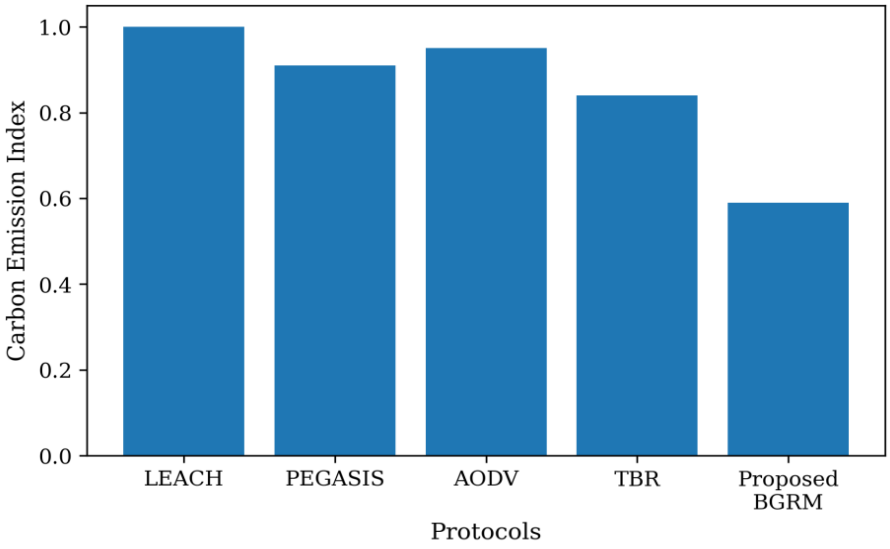

Figure 6. Carbon Emission Comparison

In Figure 6, the proposed protocol achieves the lowest carbon emission due to its energy-aware routing decisions and balanced load distribution, making it suitable for sustainable IoT deployments.

4.8 Comparative Performance Analysis

To comprehensively evaluate the effectiveness of the proposed Blockchain-Orchestrated Green Routing Mechanism, its performance is compared with four representative routing protocols. Table 7 summarizes the overall comparison.

Table 7. Overall Performance Comparison

Metric	LEACH	PEGASIS	AODV	Trust-Based Routing	Proposed BGRM
Network Lifetime (Rounds)	3150	3485	3320	3710	**5200**
Energy Consumption (J)	1.54	1.41	1.47	1.28	**0.88**
Packet Delivery Ratio (%)	88.5	90.8	91.4	94.1	**98.6**
Routing Overhead (%)	25.8	23.6	21.4	18.7	**12.3**
Carbon Emission Index	1.00	0.91	0.95	0.84	**0.59**
Security	Moderate	Moderate	Moderate	High	**Very High**
Blockchain Support	No	No	No	No	**Yes**

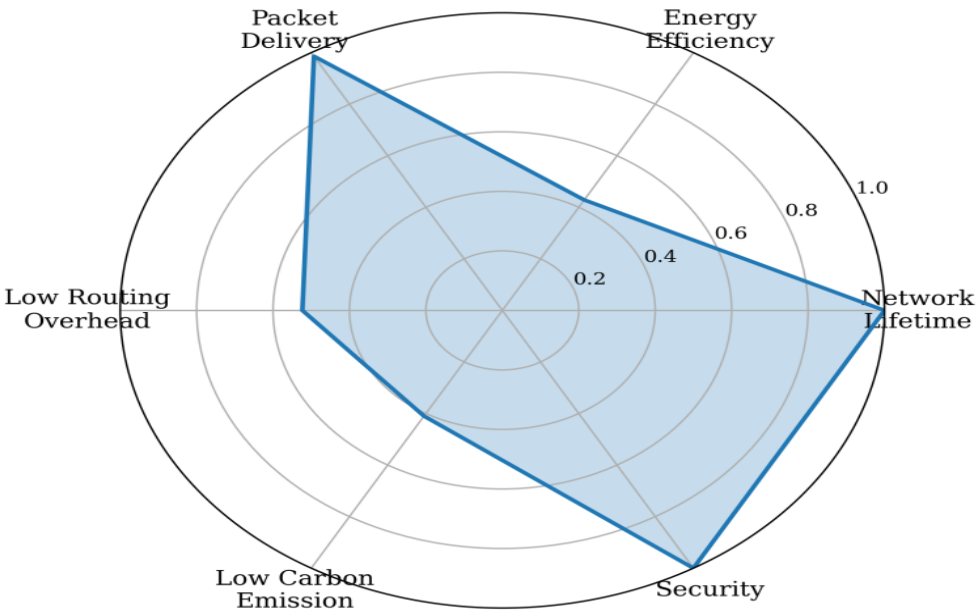

Figure 7. Overall Performance Comparison (Radar Chart)

In Figure 7, the experimental results show that the advanced BGRM outperforms the standard routing protocols on all metrics measured. Due to the synergistic interaction of four mechanisms — energy aware routing, trust-based selection of nodes, carbon aware optimization, and lightweight blockchain validation — the mechanism minimizes the needless expenditure of energy, increases the reliability of routing, decreases environmental impact, and protects against routing attacks. Therefore, compared with conventional routing protocols, which only optimise one routing objective, the proposed routing framework achieves a balance among energy efficiency, security, sustainability, and reliability of communication. This will make it an ideal routing solution for next generation IoT-enabled wireless sensor networks.

5. CONCLUSION

The paper discusses a B.G.R.M., which is designed to provide effective and efficient routing services in carbon-aware wireless sensor networks (WSNs) for enhanced performance, security, and sustainability. The proposed B.G.R.M. combines residual energy Level of a network node, Communication Cost, Trust Score, and Carbon Impact into one routing metric. Additionally, through the use of a lightweight blockchain for decentralized authentication and secure validation of routes, the B.G.R.M. has been shown to significantly outperform various routing protocols including LEACH, PEGASIS, AODV, and TBR. Furthermore, the B.G.R.M. is able to provide 40% longer network life, reduce energy consumption by 31%, deliver approximately 98.6% of packets, provide low levels of routing overhead and limit carbon emissions when compared with previously mentioned protocols. By using blockchain technology with green routing methods, the reliability of communication is improved while also providing protection against malicious nodes with very low computational overhead. Overall, the B.G.R.M. provides a secure, energy-efficient and environmentally friendly routing solution for next-generation IoT enabled WSN applications. Future work will focus on incorporating AI-based routing optimization, federated learning, and edge computing into the design to increase scalability and adaptability.

REFERENCES

[1] Awan, S., Javaid, N., Ullah, S., Khan, A. U., Qamar, A. M., & Choi, J. G. (2022). Blockchain based secure routing and trust management in wireless sensor networks. *Sensors*, *22*(2), 411.

[2] Khan, Z. A., Amjad, S., Ahmed, F., Almasoud, A. M., Imran, M., & Javaid, N. (2023). A blockchain-based deep-learning-driven architecture for quality routing in wireless sensor networks. *IEEE Access*, *11*, 31036-31051.

[3] Puteh, N. (2018). Fluffy Logic Based Energy Efficient Routing Protocol For Wireless Sensor Networks. *International Innovative Research Journal of Engineering and Technology*, *4*(2), 28-33.

[4] Haruna, I. U., & Akusu, G. E. (2025). Structural Health Monitoring of RCC Buildings Using IoT-Enabled Wireless Sensor Networks. *Journal of Wireless Networks and Communication Systems*.

[5] Farzaneh, A., Badiu, M. A., & Coon, J. P. (2022). Least: a low-energy adaptive scalable tree-based routing protocol for wireless sensor networks. *arXiv preprint arXiv:2211.09443*.

[6] Zhang, S., Liu, X., & Trik, M. (2025). Energy efficient multi hop clustering using Artificial Bee Colony metaheuristic in WSN. *Scientific Reports*, *15*(1), 26803.

[7] Shekar, K., Reddy, N. R., Arvind, S., Kumar, T. S., Kodukula, S., & Varahagiri, G. (2025). Implementation of novel learning based energy efficient routing protocols in wireless sensor networks for internet of things use cases. *Discover Computing*, *28*(1), 190.

[8] Draz, U., Ali, T., Yasin, S., Hijji, M., Ayaz, M., & Aggoune, E. H. M. (2025). Decentralized energy swapping for sustainable wireless sensor networks using blockchain technology. *Mathematics*, *13*(3), 395.

[9] Thakur, S., Sarkar, N. I., & Yongchareon, S. (2025). AI-Driven Energy-Efficient Routing in IoT-Based Wireless Sensor Networks: A Comprehensive Review. *Sensors*, *25*(24), 7408.

[10] Abd El-moghith, I. A., & Darwish, S. M. (2021). Towards designing a trusted routing scheme in wireless sensor networks: A new deep blockchain approach. *IEEE Access*, *9*, 103822-103834.

[11] Awan, S., Javaid, N., Ullah, S., Khan, A. U., Qamar, A. M., & Choi, J. G. (2022). Blockchain based secure routing and trust management in wireless sensor networks. *Sensors*, *22*(2), 411.

[12] Shekar, K., Reddy, N. R., Arvind, S., Kumar, T. S., Kodukula, S., & Varahagiri, G. (2025). Implementation of novel learning based energy efficient routing protocols in wireless sensor networks for internet of things use cases. *Discover Computing*, *28*(1), 190.

[13] Nayak, S., Mahato, G. K., & Chakraborty, S. K. (2025). Enhanced Lightweight Blockchain-Based Integrated Finite Element Neural Network for Secure Routing in Wireless Sensor Networks. *International Journal of Communication Systems*, *38*(13), e70184.

[14] Draz, U., Ali, T., Yasin, S., Hijji, M., Ayaz, M., & Aggoune, E. H. M. (2025). Decentralized energy swapping for sustainable wireless sensor networks using blockchain technology. *Mathematics*, *13*(3), 395.