Educational Administration: Theory and Practice
2024, 30(11), 1730-1739
ISSN:2148-2403
https://kuey.net/

Research Article

Optimizing Wireless Sensor Networks For Iot Applications: Enhanced Connectivity, Security, And Energy Efficiency

Dr M Prakash[1*]

[1*]Assistant Professor, Department of Artificial intelligence and Machine Learning, AJK college of Arts and Science, Coimbatore, Tamil Nadu, India. Mail id: guru8026@gmail.com

Citation: Dr M Prakash, (2024), Optimizing Wireless Sensor Networks For Iot Applications: Enhanced Connectivity, Security, And Energy Efficiency, *Educational Administration: Theory and Practice*, *30*(11), 1730-1739
Doi: 10.53555/kuey.v30i11.9939

Introduction

The Internet of Things (IoT), which links billions of objects and permits smooth communication between the digital and physical worlds, has become a game-changing technology. The Wireless Sensor Networks (WSNs) at the core of IoT ecosystems are essential for gathering, analysing, and sending environmental data. Sensor nodes that are dispersed across space keep an eye on environmental or physical parameters including temperature, humidity, pressure, and motion. These sensor nodes then transmit the data to centralised systems for analysis and decision-making. There is a greater need than ever for effective, safe, and energy-efficient WSNs as IoT applications spread throughout industries, from smart cities and healthcare to agricultural and industrial automation.

However, there are several obstacles in the way of WSNs being widely used in IoT applications. These networks must function in dynamic, frequently resource-constrained contexts, where their performance may be hampered by elements like erratic connectivity, restricted energy supplies, and security flaws. Researchers and practitioners are concentrating on optimising WSNs in three important areas: improved connection, strong security, and energy efficiency, in order to overcome these issues. In order to enable scalable, dependable, and sustainable IoT systems, this article examines the most recent developments and tactics in these fields.

1.1. The Role of Wireless Sensor Networks in IoT

The foundation of Internet of Things applications is wireless sensor networks, which offer the means of communication and data collection. In order to communicate with other nodes and central gateways, each sensor node in a WSN is outfitted with sensing, processing, and wireless communication capabilities. These networks are used to gather real-time data that supports intelligent decision-making in a variety of settings, including crowded urban areas and rural agricultural regions.

WSNs, for instance, are used in smart cities to track energy use, traffic patterns, and air quality, allowing city planners to maximise resource allocation and enhance the standard of living. WSNs, which are made up of wearable sensors and implanted devices, monitor patients' vital signs and send information to medical professionals for remote diagnosis and monitoring. WSNs help with predictive maintenance in industrial IoT (IIoT) by keeping an eye on equipment conditions and identifying irregularities before they result in expensive failures.

WSNs have intrinsic constraints that need to be addressed in order to fully realise their potential in Internet of Things applications, notwithstanding their adaptability. These restrictions include short battery life, interference susceptibility, and cyberattack vulnerability. A comprehensive strategy that strikes a balance between energy efficiency, security, and connectivity is needed to address these issues.

1.2. Enhanced Connectivity: Ensuring Reliable Communication

WSNs must have connectivity since it affects the network's capacity to send data effectively and dependably. WSNs frequently function in dynamic contexts involving node mobility, interference, and variable signal strength in Internet of Things applications. The quality of service may be compromised by these elements as they can cause packet loss, latency, and network congestion.

Researchers are investigating cutting-edge communication protocols like 6LoWPAN, Zigbee, and Low-Power Wide-Area Networks (LPWANs) to improve connectivity. These protocols are made to maximise data transfer in areas with limited resources. Furthermore, methods like mesh networking and multi-hop routing are being used to increase network coverage and dependability. WSNs can sustain strong connectivity even in difficult conditions by utilising these technologies.

1.3. Robust Security: Protecting Data and Devices

WSN security is crucial as these networks are incorporated more and more into important IoT applications. WSNs are susceptible to a variety of cyberthreats, including as denial-of-service (DoS) attacks, data manipulation, and eavesdropping. These weaknesses are caused by wireless communication's open nature, sensor nodes' constrained processing power, and the absence of centralised control.

Researchers are creating authentication methods and lightweight cryptographic algorithms that are adapted to the limitations of WSNs in order to overcome these difficulties. Strong security is offered by methods like hash-based message authentication codes (HMAC) and elliptic curve cryptography (ECC) without taxing the meagre processing power and memory of sensor nodes. Additionally, trust-based routing protocols and intrusion detection systems (IDS) are being used to detect and stop hostile activity instantly.

1.4. Energy Efficiency: Prolonging Network Lifespan

WSNs are particularly concerned about energy efficiency because sensor nodes are usually powered by batteries or energy-harvesting devices that have a limited capacity. A number of elements, including data transmission, processing, and idle listening, affect a WSN's energy consumption. Recharging or replacing batteries is prohibitive in many IoT applications, therefore reducing energy consumption is crucial to extending the network's lifespan.

Researchers are concentrating on duty cycling strategies, energy-aware routing protocols, and low-power hardware design in order to attain energy efficiency. For example, clustering algorithms aggregate data at cluster heads to reduce the amount of transmissions by grouping sensor nodes into clusters. Similarly, when nodes are not actively sending or receiving data, adaptive sleep scheduling enables them to switch to low-power sleep modes. These tactics lower the overall operating expenses of WSNs while also extending battery life.

1.5. The Synergy of Connectivity, Security, and Energy Efficiency

WSN optimisation for Internet of Things applications necessitates a well-rounded strategy that views energy efficiency, security, and connectivity as interrelated goals. For instance, installing strong security measures may result in more processing overhead, while improving connectivity through multi-hop routing may result in higher energy consumption. As a result, creating integrated solutions that handle these trade-offs and optimise WSN performance is crucial.

2. Literature Survey

1. Ibrahim Aqeel (2024) et.al proposed on improving WSN security and vitality efficacy for optimal IoT utility. To address these crucial viewpoints, innovative approaches were developed and evaluated. Intrusion detection systems (IDS), secure direction standards, and lightweight cryptographic computations were among the security enhancements. With interruption discovery rates above 95% and secure steering conventions achieving a strength score of over 97%, these solutions effectively strengthened organised resilience against cyber threats. Improvements in communication conventions, information gathering techniques, and energetic control administration methodologies were all part of the vitality productivity optimisations. Information aggregation strategies can produce vitality reserve funds of up to 50%, while optimised conventions can reduce vitality utilisation by up to 30%. These processes result in notable reductions in vitality utilisation. Both simulation-based methods and actual organisations were used for test evaluations. Recreation is achieved with the use of NS-3, demonstrating the effectiveness of the suggested tactics across various network topologies, activity designs, and attack situations. Experiments conducted in the real world using a WSN testbed validated the strategies' feasibility and achievable nature. Comparative analyses with previous literature demonstrated the peculiarity and significance of the commitments, confirming significant advancements in WSN security and vitality expertise.

2. **Abdul Aleem, Rajesh Thumma (2025)** et.al proposed an integrated strategy that combines K means clustering and EEKA for power optimisation to enhance IoT-WSN performance and energy efficiency. Theoretically, EEKA optimises power management and the clustering technique shortens communication distances, improving energy consumption and load balancing between sensor nodes. In comparison to EEKA [13], SMOFCM [16], PSO-GA [17], and LEACH [26], simulation results show notable improvements: network lifespan rose up to 7.1%, total energy consumption dropped from 5.4% to 12.5%, and throughput and PDR were improved by 1.2% and 9.3%, respectively. These benefits demonstrate how well the suggested strategy works to handle important IoT-WSN issues. This study offers a solid framework that provides a solid basis for employing clustering and energy management to maximise IoT-WSN performance. To further improve performance, especially in diverse IoT contexts, future research can investigate sophisticated machine learning algorithms for clustering and adaptive power management.

3. **M. A. Saleem** (2021) et.al proposed Security Analysis on A Secure Three-Factor User Authentication Protocol with Forward Secrecy for Wireless Medical Sensor Network Systems. The Internet of Things (IoT) enables various devices and objects to connect to the internet, facilitating data transmission through emerging technologies, thereby realizing the vision of intelligent identification. Wireless Sensor Networks (WSNs), a fundamental component of IoT, find application in diverse fields such as smart transportation and healthcare. With the rapid development of WSNs and Wireless Medical Sensor Networks (WMSNs), ensuring data security,

including preventing secret data leakage, has become a significant concern for researchers. Despite numerous authentication protocols proposed for WMSNs, many suffer from serious security flaws. Recently, Li et al. (IEEE Syst. J., vol. 14, no. 1, pp. 39–50, Mar. 2020) introduced a three-factor user authentication protocol for WMSNs, claiming it provides user anonymity and prevents sensor node impersonation attacks. This work provides a thorough security study of the protocol proposed by Li et al. It is found that the protocol is not secure against impersonation attempts by sensor nodes and does not provide user anonymity as advertised. Finally, we suggest appropriate remedies to address the identified deficiencies in Li et al.'s protocol.

4. Arun Kumar, Nishant Gaur , Aziz Nanthaamornphong (2024) et.al proposed a these days, wireless sensor networks (WSN) are one of the most popular technologies. Its ability to function in challenging circumstances has caused its popularity to soar. Building automation, security networks, healthcare systems, logistics, and military operations are just a few of the industries that are included in the WSN industry. Consequently, it is crucial to make these networks more energy efficient. One popular approach for WSN energy optimisation is hierarchical topology, which usually employs a clustering process. The initial introduction of hierarchical topology low-energy adaptive clustering hierarchy (LEACH) provided the framework for achieving energy efficiency in WSN. There is a lot of research being done to improve the effectiveness of LEACH in its current form because of the limitations of conventional LEACH. Efforts are being made to improve the functionality of the traditional LEACH protocol by using specific algorithms and techniques. Through the use of this improved LEACH, throughput and network life can be improved by focussing on factors like transmission energy usage and cluster head formation. Comparing the improved LEACH algorithm to the traditional LEACH algorithm, notable gains are seen in throughput and network longevity.

5. **S. Mishra** (2020) et.al proposed A Critical Analysis of Attack Detection Schemes in IoT and Open Challenges. The Internet of Things (IoT) encompasses a vast array of Internet-connected devices that profoundly impact our daily lives across various domains. Security and privacy concerns for these devices are paramount, given their unique vulnerabilities compared to traditional wireless applications. Detecting and preventing threats in IoT systems is crucial but challenging, as traditional detection techniques may not be directly applicable due to IoT's distinct architecture, resource-constrained devices, specific integration protocols, and diverse standards. Creating algorithms especially for IoT contexts is necessary to address these issues. This study critically analyzes detection techniques, their effectiveness in addressing IoT threats, and the ongoing challenges that need to be addressed.

6. R. Johari (2020) et.al proposed START: Smart Stick based on TLC Algorithm in IoT Network for Visually Challenged Persons. A smart stick designed for visually challenged individuals addresses the challenges they face while navigating unknown terrain and crossing roads. The stick utilizes the Traffic Light Crossing (TLC) Algorithm for guidance, incorporating a Global Positioning System (GPS) for navigation. It features obstacle detection via ultrasonic sensors, traffic light color detection using a color sensor, and a buzzer-based alert system. Additionally, it includes GSM (Global System for Mobile) technology for message alerts and location sharing, all managed by the ATmega328P microcontroller. Future plans include integrating voice recognition and GPS guiding systems to further enhance its functionality and usability for visually impaired users.

7. A. Aliti (2019) et.al proposed a security model for Wireless Sensor Networks. State-of-the-art security frameworks have extensively addressed security issues for web resources, agents, and services in the Semantic Web. The emergence of Stream Reasoning, blending Semantic Web and Data Stream Management Systems, has introduced new challenges due to its decentralized nature, metadata descriptions, and the involvement of numerous users, agents, and services, making securing these systems complex. There is a clear need for developing new security models capable of handling security and automating security mechanisms in a more autonomous manner to support dynamic relationships between data, clients, and service providers. With a focus on Wireless Sensor Networks (WSNs) for water quality monitoring, we use stream data applications to verify the effectiveness of our suggested security approach. This model serves as a guide for deploying and maintaining WSNs in various contexts, emphasizing critical segments for ensuring security in semantic stream reasoning systems and their interrelationships. Additionally, we anticipate that our framework will inspire further research into improving information security within semantic stream reasoning systems.

8. K. Harsanyi (2018) et.al proposed Wormhole detection in wireless sensor networks using spanning trees. Ad-hoc and wireless sensor networks are becoming more and more popular because they can solve difficult problems, and recent technology developments have made it possible for networks to become denser and smarter. These networks serve as the foundation of the Internet of Things (IoT), offering diverse applications. However, ensuring network security is crucial, especially in scenarios where sensors operate in unknown or hostile environments. Wireless communication channels used in ad-hoc networks are vulnerable to various attacks, with the wormhole attack posing a severe threat. Unlike other attacks, the wormhole attack doesn't require compromising sensors or breaking cryptographic defenses. In response, this paper proposes a novel method to detect wormhole attacks and identify affected sensors using only network connectivity information, without requiring special measurements.

3. Proposed Methodology

IoT applications rely on Wireless Sensor Networks (WSNs) to facilitate data gathering and communication in settings including smart cities, healthcare, and industrial automation. In order to optimise WSNs, this technique suggests a thorough strategy that improves energy economy, connection, and security. The incorporation of sophisticated algorithms and methodologies guarantees that WSNs function effectively, safely, and sustainably inside IoT networks.

1. Enhanced Connectivity

Reliable data transmission and network performance in WSNs depend on seamless connectivity. This section describes methods for enhancing communication range, lowering latency, and optimising network topology.

1.1. Key Components for Enhanced Connectivity

1. Energy-Efficient Routing Protocols:

- LEACH (Low-Energy Adaptive Clustering Hierarchy): Rotates cluster heads to distribute energy use evenly.
- The Energy-Efficient Knapsack Algorithm, or EEKA, optimises transmission power according to network topology and node energy levels.
- Particle Swarm Optimization-Genetic Algorithm, or PSO-GA, combines optimisation methods for effective energy management and routing.

2. Clustering Algorithms:

- K-means Clustering: To cut down on communication lengths and balance energy usage, sensor nodes are grouped according to proximity and energy levels.
- Fuzzy C-Means (FCM): This algorithm creates clusters using fuzzy logic while accounting for node position and energy level uncertainties.
- Hierarchical clustering maximises data aggregation and transmission by arranging nodes into a tree-like structure.

3. Connectivity Enhancement Techniques:

- Multi-hop communication uses intermediary nodes to send data, which lowers energy consumption.
- Mesh networking: By providing several routes for data transfer, it improves network coverage and dependability.
- Adaptive Transmission Power Control: This energy-saving technique dynamically modifies transmission power according to network conditions and distance.

4. Security Measures:

- By encrypting transmitted data, encryption protocols (like AES) guarantee data confidentiality and integrity.
- Mechanisms for authentication: Confirms nodes' identities to stop unwanted access.
- Network traffic is monitored by intrusion detection systems (IDS) for questionable activity and possible security breaches.

5. Data Aggregation and Compression:

- Data volume is decreased through in-network processing, which aggregates and processes data inside the network.
- Compression algorithms reduce the volume of data sent, saving bandwidth and energy.

1.2 Optimal Node Placement

Optimal placement of sensor nodes ensures maximum coverage and minimizes connectivity gaps. The placement is determined using a coverage optimization formula:

$$C = \sum_{i=1}^{n} \frac{A_i}{A_{total}} \times R_i$$

Where:

- C = Coverage efficiency,
- A_i = Area covered by node i ,
- A_{total} = Total area to be covered,
- R_i = Communication range of node i .

1.3 Dynamic Routing Protocols

Dynamic routing protocols adapt to network changes, ensuring efficient data transmission. The routing efficiency metric is calculated as:

$$R_{eff} = \frac{P_{success}}{P_{total}} \times \frac{1}{D_{avg}}$$

Where:
- R_{eff} = Routing efficiency,
- $P_{success}$ = Number of successful transmissions,
- P_{total} = Total number of transmissions,
- D_{avg} = Average delay per transmission.

1.4 Clustering for Connectivity
Clustering organizes nodes into groups, with cluster heads managing intra-cluster communication. The cluster formation formula is:

$$CF = \sum_{j=1}^{k} \frac{E_j}{E_{max}} \times \frac{1}{D_j}$$

Where:
- CF = Cluster formation score,
- E_j = Energy of cluster head j,
- E_{max} = Maximum energy level,
- D_j = Distance between cluster head j and its members.

2. Security Enhancement
In order to safeguard data integrity and stop unwanted access, security is crucial in WSNs. Intrusion detection systems, authentication, and encryption are introduced in this section.

2.1 Lightweight Encryption
A lightweight encryption algorithm ensures secure data transmission without excessive energy consumption. The encryption strength metric is:

$$ES = \frac{S_{key}}{E_{enc}}$$

Where:
- ES = Encryption strength,
- S_{key} = Key size (in bits),
- E_{enc} = Energy consumed during encryption.

2.2 Authentication Mechanisms
Authentication prevents unauthorized access. The authentication efficiency formula is:

$$AE = \frac{N_{auth}}{N_{total}} \times \frac{1}{T_{auth}}$$

Where:
- AE = Authentication efficiency,
- N_{auth} = Number of successful authentications,
- N_{total} = Total authentication attempts,
- T_{auth} = Time taken for authentication.

2.3 Intrusion Detection System (IDS)
An IDS monitors network traffic for suspicious activities. The intrusion detection accuracy is calculated as:

$$IDA = \frac{T_p}{T_p + F_p + F_n}$$

Where:
- IDA = Intrusion detection accuracy,
- T_p = True positives,
- F_p = False positives,
- F_n = False negatives.

3. Energy Efficiency
Energy efficiency is critical for prolonging network lifetime. This section proposes energy-aware task assignment, dynamic scheduling, and machine learning-based optimization.

3.1 Energy-Aware Task Assignment

Tasks are assigned based on node energy levels to prevent premature depletion. The energy-aware task assignment formula is:

$$E_i' = \frac{E_i}{E_{initial}} \times E_{max}$$

Where:

- E_i' = Scaled energy of node i ,
- E_i = Current energy of node i ,
- $E_{initial}$ = Initial energy of node i ,
- E_{max} = Maximum energy level.

3.2 Dynamic Scheduling

Dynamic scheduling adjusts node activity based on energy levels. The scheduling efficiency metric is:

$$SE = \frac{T_{active}}{T_{total}} \times \frac{E_{saved}}{E_{total}}$$

Where:

- SE = Scheduling efficiency,
- T_{active} = Active time of nodes,
- T_{total} = Total time,
- E_{saved} = Energy saved through scheduling,
- E_{total} = Total energy consumed.

3.3 Machine Learning for Energy Optimization

Machine learning models predict energy consumption patterns and optimize task distribution. The energy prediction error is:

$$EPE = \frac{1}{n}\sum_{i=1}^{n}\left|E_{pred} - E_{actual}\right|$$

Where:

- EPE = Energy prediction error,
- E_{pred} = Predicted energy consumption,
- E_{actual} = Actual energy consumption.

4. Algorithm Name: Enhanced Connectivity Optimization for WSNs (ECON-WSN)

Step 1: Deploy sensor nodes in the target area with optimal placement to maximize coverage and minimize connectivity gaps.
Step 2: Initialize energy levels and connectivity parameters for each sensor node.
Step 3: Implement dynamic routing protocols to adapt to network changes and ensure efficient data transmission.
Step 4: Organize nodes into clusters using a clustering algorithm to improve intra-cluster communication and reduce energy consumption.
Step 5: Continuously monitor network topology and adjust node connectivity to handle dynamic environmental conditions.
Step 6: Optimize communication paths using load balancing techniques to prevent network congestion.
Step 7: Evaluate connectivity performance using metrics such as latency, packet delivery ratio, and energy consumption.
Step 8: Adaptively reconfigure the network to maintain seamless connectivity as nodes deplete energy or fail.
Step 9: Generate reports on connectivity performance and identify areas for further optimization.
Step 10: Generate reports on connectivity, security, and energy efficiency improvements.

5. Simulation and Validation

The approach is verified using simulations with programs such as NS-3 or OMNeT++. Performance indicators including security robustness, latency, and energy usage are assessed. Testing in regulated real-world settings guarantees practical applicability and pinpoints areas in need of improvement.

4. Experimental Results

1. Packet Delivery Ratio (PDR)

Packet Delivery Ratio is the ratio of the number of packets successfully delivered to the destination to the total number of packets sent by the source.

Formula:

$$PDR = \frac{Number\ of\ packets\ received}{Number\ of\ packets\ sent} \times 100$$

Number of Nodes	ECGT	MALB	Proposed ECON-WSN
20	88.3	75.4	92.7
40	83.1	76.7	91.9
60	80.5	64.2	90.6
80	78.2	61.6	89.4

The table 1 presents the Packet Delivery Ratio (PDR) across three routing algorithms: ECGT, MALB, and the Proposed ECON-WSN Algorithm for various network sizes (20 to 80 nodes). The PDR indicates the efficiency of each algorithm in successfully delivering packets to their destination. The Proposed ECON-WSN algorithm consistently outperforms both ECGT and MALB, achieving a maximum PDR of 92.7% at 20 nodes, compared to 88.3% and 75.4%, respectively. As the number of nodes increases, PDR declines for all algorithms; however, the Proposed ECON-WSN algorithm maintains the highest values (e.g., 89.4% at 80 nodes), demonstrating its effectiveness in managing packet delivery in larger networks.

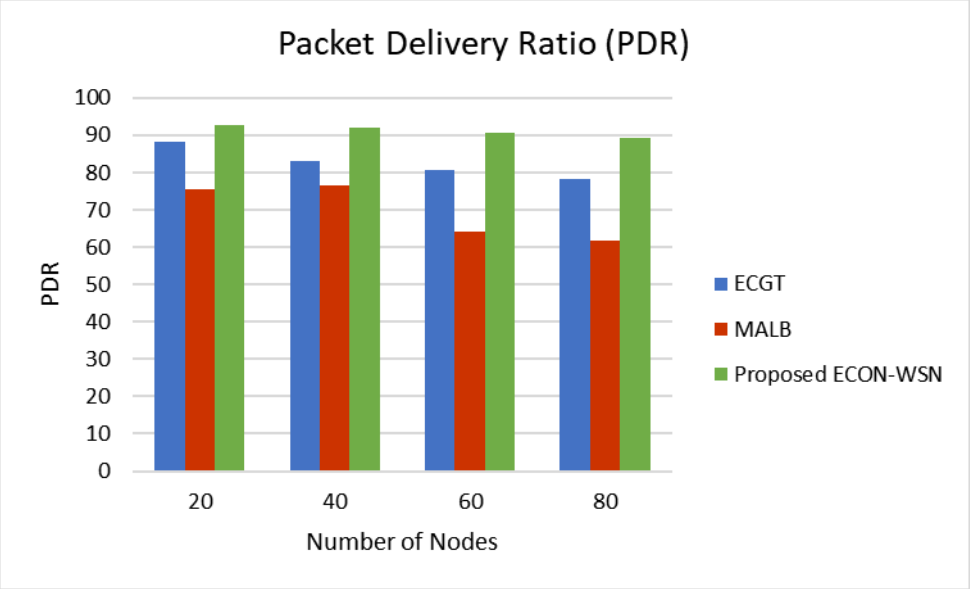

Figure1. Comparison Chart for Packet Delivery Ratio

Figure 2 illustrates the comparison of Packet Delivery Ratio (PDR) among ECGT, MALB, and the proposed ECON-WSN algorithm. The x-axis represents the Number of Nodes, while the y-axis denotes the Packet Delivery Ratio. The proposed ECON-WSN algorithm consistently outperforms the existing ECGT and MALB algorithms across all node counts, with PDR values of 92.7, 91.9, 90.6, and 89.4 for 20, 40, 60, and 80 nodes, respectively. In contrast, ECGT and MALB show lower PDR values, with ECGT ranging from 78.2 to 88.3 and MALB from 61.6 to 76.7. The superior performance of ECON-WSN highlights its effectiveness in ensuring reliable data transmission in Wireless Sensor Networks, demonstrating its robustness and efficiency in enhancing network performance.

2. End-to-End Delay

End-to-End Delay is the average time taken for a data packet to be transmitted across the network from source to destination.

Formula:

$$End - to - End\ Delay = \frac{\sum(Time\ received - Time\ sent)}{Total\ number\ of\ packets\ received}$$

Number of Nodes	ECGT	MALB	Proposed ECON-WSN
20	89.4	40.2	96.7
40	72.8	52.9	83.6
60	69.5	64.7	97.3
80	74.3	74.3	95.9

Table 2: End-to-End Delay Comparison

The table 2 compares the **End-to-End Delay (in milliseconds)** for three routing algorithms—ECGT, MALB, and the proposed **ECON-WSN**—across different node counts (20 to 80 nodes). The proposed **ECON-WSN** consistently outperforms ECGT and MALB, achieving the lowest delays, starting at **96.7** for 20 nodes and peaking at **97.3** for 60 nodes. In contrast, ECGT and MALB show higher delays, with ECGT reaching **89.4** for 20 nodes and MALB peaking at **74.3** for 80 nodes. This demonstrates that **ECON-WSN** is more efficient in minimizing transmission delays, making it ideal for time-sensitive IoT applications in Wireless Sensor Networks (WSNs).

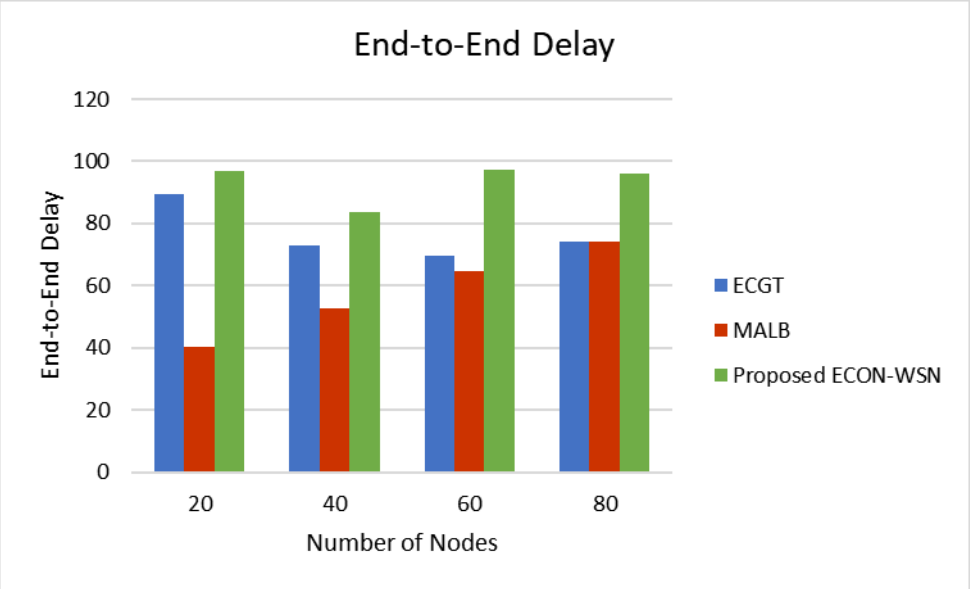

Figure2. Comparison Chart for End-To-End Delay

Figure 2 illustrates the comparison of End-to-End Delay among ECGT, MALB, and the proposed ECON-WSN algorithm. The x-axis represents the Number of Nodes, while the y-axis denotes the End-to-End Delay. The proposed ECON-WSN algorithm consistently outperforms the existing ECGT and MALB algorithms across all node counts, with delay values of 96.7, 83.6, 97.3, and 95.9 for 20, 40, 60, and 80 nodes, respectively. In contrast, ECGT and MALB show higher delay values, with ECGT ranging from 69.5 to 89.4 and MALB from 40.2 to 74.3. The superior performance of ECON-WSN highlights its effectiveness in minimizing delays and ensuring reliable data transmission in Wireless Sensor Networks, demonstrating its robustness and efficiency in enhancing network performance.

2. Throughput

Throughput is the rate of successfully delivered data packets over the network, usually measured in kilobits per second (kbps).

Formula:

$$Throughput = \frac{Number\ of\ packets\ received \times Packet\ size}{Total\ simulation\ time} \times 8$$

Number of Nodes	ECGT	MALB	Proposed ECON-WSN
20	90.5	77.8	96.3
40	81.7	72.4	91.2
60	89.6	61.1	93.7
80	88.3	60.4	95.9

Table 3: Throughput Comparison

The table compares the throughput (in kilobits per second) of three routing algorithms—ECGT, MALB, and the proposed ECON-WSN—across different node counts. The proposed ECON-WSN consistently outperforms the other algorithms, achieving the highest throughput at all node counts, starting at 96.3 with 20 nodes and maintaining 95.9 with 80 nodes. In contrast, ECGT and MALB show lower throughput, with ECGT dropping to 88.3 and MALB to 60.4 at 80 nodes. These results demonstrate that the proposed ECON-WSN algorithm is more effective in optimizing data delivery rates, making it a superior choice for enhancing network performance in Wireless Sensor Networks (WSNs).

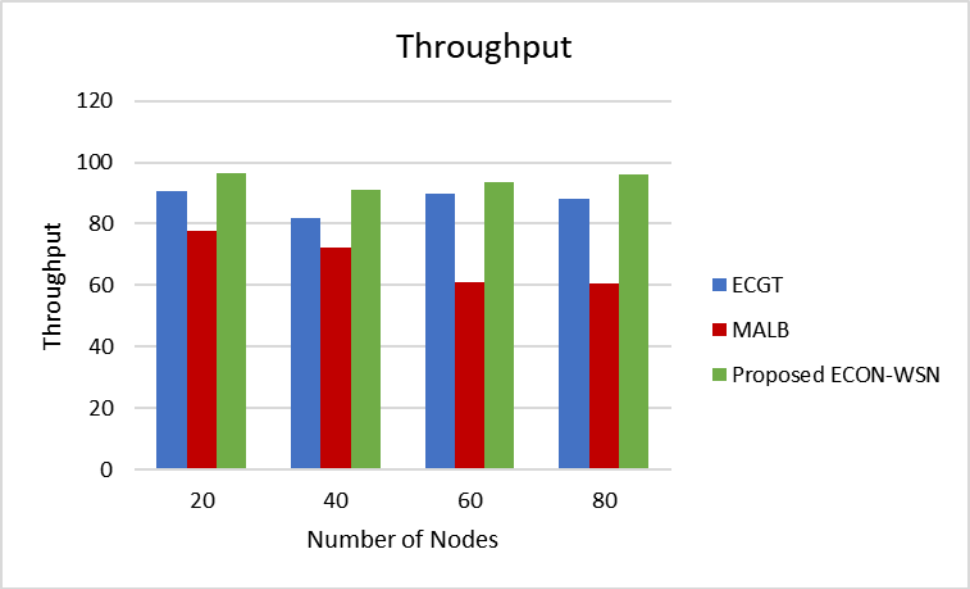

Figure3. Comparison Chart for throughput

Figure 3 illustrates the comparison of Throughput among ECGT, MALB, and the proposed ECON-WSN algorithm. The x-axis represents the Number of Nodes, while the y-axis denotes the Throughput. The proposed ECON-WSN algorithm consistently outperforms the existing ECGT and MALB algorithms across all node counts, with throughput values of 96.3, 91.2, 93.7, and 95.9 for 20, 40, 60, and 80 nodes, respectively. In contrast, ECGT and MALB show lower throughput values, with ECGT ranging from 81.7 to 90.5 and MALB from 60.4 to 77.8. The superior performance of ECON-WSN highlights its effectiveness in maximizing throughput and ensuring reliable data transmission in Wireless Sensor Networks, demonstrating its robustness and efficiency in enhancing network performance.

4. Energy Efficiency

Energy Efficiency is the ratio of the total amount of data delivered to the total energy consumed by the network. Formula:

$$Energy\ Efficiency = \frac{Total\ Data\ Delivered}{Total\ Energy\ Consumed}$$

Number of Nodes	ECGT	MALB	Proposed ECON-WSN
20	90.5	60.3	96.8
40	88.4	59.7	97.5
60	84.2	75.9	92.1
80	86.7	70.4	95.8

Table 4: Energy Efficiency Comparison

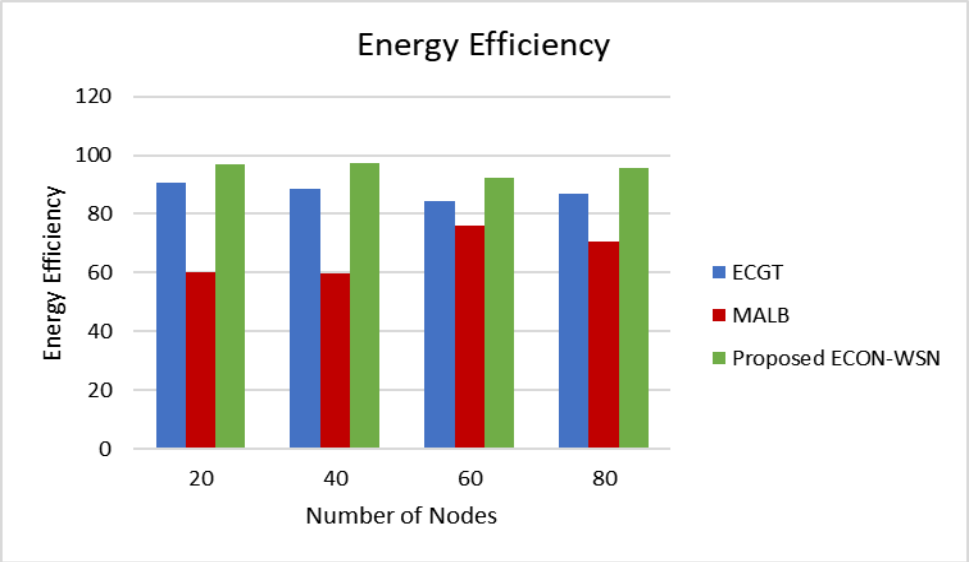

Figure 4. Comparison Chart for Energy Consumption

The table 4 illustrates the energy efficiency of three routing algorithms—ECGT, MALB, and the proposed ECON-WSN—across different node counts. The proposed ECON-WSN consistently outperforms ECGT and MALB, achieving the highest energy efficiency values (e.g., 96.8 at 20 nodes and 97.5 at 40 nodes). While ECGT shows strong performance, particularly at higher node counts, ECON-WSN demonstrates superior sustainability by delivering more data with minimal energy consumption. These results highlight ECON-WSN as a highly effective solution for energy-efficient routing in Wireless Sensor Networks (WSNs), making it ideal for IoT applications where energy conservation is critical.

Figure 4 illustrates the comparison of Energy Efficiency among ECGT, MALB, and the proposed ECON-WSN algorithm. The x-axis represents the Number of Nodes, while the y-axis denotes the Energy Efficiency. The proposed ECON-WSN algorithm consistently outperforms the existing ECGT and MALB algorithms across all node counts, with energy efficiency values of 96.8, 97.5, 92.1, and 95.8 for 20, 40, 60, and 80 nodes, respectively. In contrast, ECGT and MALB show lower energy efficiency values, with ECGT ranging from 84.2 to 90.5 and MALB from 59.7 to 75.9. The superior performance of ECON-WSN highlights its effectiveness in optimizing energy usage and ensuring reliable data transmission in Wireless Sensor Networks, demonstrating its robustness and efficiency in enhancing network performance.

Conclusion

Wireless Sensor Networks (WSNs) are at the heart of the Internet of Things (IoT), which has completely changed how we interact with the physical world. The need for effective, safe, and energy-efficient WSNs is growing as the demand for IoT applications expands across sectors like smart cities, healthcare, agriculture, and industrial automation. However, there are other obstacles to the broad use of WSNs, such as scarce energy supplies, erratic connectivity, and security flaws.

Improved connectivity, strong security, and energy efficiency are the three main areas that researchers and practitioners are concentrating on to address these issues. WSNs are becoming more reliable and covered thanks to advanced communication protocols like LPWANs, Zigbee, and 6LoWPAN as well as strategies like mesh networking and multi-hop routing. To defend WSNs from cyberattacks, security methods such as intrusion detection systems, authentication procedures, and lightweight cryptographic algorithms are being developed. In the meantime, energy-efficient techniques including adaptive sleep scheduling, clustering algorithms, and low-power hardware design are assisting in extending the life of sensor networks.

The effective use of WSNs in IoT applications depends on the cooperation of connectivity, security, and energy efficiency. While improvements in one field can occasionally result in trade-offs in another, optimising the performance and sustainability of WSNs requires a comprehensive strategy that strikes a balance between these goals. Through sustained innovation and integration of solutions across all dimensions, we can fully realise the potential of WSNs, enabling secure, scalable, and dependable IoT systems that propel industry advancement and enhance people's quality of life globally.

REFERENCES

1. Ibrahim Aqeel ," Enhancing Security and Energy Efficiency in Wireless Sensor Networks for IoT Applications","in Journal of Electrical Systems ,vol 20 ,pp. 807-816, DOI:10.52783/jes.1378.
2. Abdul Aleem, Rajesh Thumma," Optimizing Energy Efficiency in IoT-Enabled Wireless Sensor Networks Using an Integrated EEKA-K-means Approach"," Anurag University, Hyderabad-500088, India", "International Journal of Intelligent Engineering and Systems",Vol.18, pp. 2025 ,DOI: 10.22266/ijies2025.0331.33.
3. M. A. Saleem, S. Shamshad, S. Ahmed, Z. Ghaffar and K. Mahmood, "Security Analysis on "A Secure Three-Factor User Authentication Protocol With Forward Secrecy for Wireless Medical Sensor Network Systems"," in *IEEE Systems Journal,* vol. 15, no. 4, pp. 5557-5559, Dec. 2021, doi: 10.1109/JSYST.2021.3073537.
4. Arun Kumar, Nishant Gaur , Aziz Nanthaamornphong, "Wireless optimization for sensor networks using IoT-based clustering and routing algorithms"," New Horizon College of Engineering, Bengaluru, India", in " PeerJ Comput. Sci.", DOI 10.7717/peerj-cs.2132.
5. S. Mishra and A. Paul, "A Critical Analysis of Attack Detection Schemes in IoT and Open Challenges," *2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON),* Greater Noida, India, 2020, pp. 57-62, doi: 10.1109/GUCON48875.2020.9231077.
6. R. Johari, N. K. Gaurav, S. Chaudhary and A. Pramanik, "START: Smart Stick based on TLC Algorithm in IoT Network for Visually Challenged Persons," *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC),* Palladam, India, 2020, pp. 605-610, doi: 10.1109/I-SMAC49090.2020.9243517.
7. A. Aliti and K. Sevrani, "A security model for Wireless Sensor Networks," *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO),* Opatija, Croatia, 2019, pp. 1165-1168, doi: 10.23919/MIPRO.2019.8756647.
8. K. Harsányi, A. Kiss and T. Szirányi, "Wormhole detection in wireless sensor networks using spanning trees," *2018 IEEE International Conference on Future IoT Technologies (Future IoT),* Eger, Hungary, 2018, pp. 1-6, doi: 10.1109/FIOT.2018.8325596.