IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2025

DOI: 10.17148/IJARCCE.2025.14312

Green IoT: Energy-Aware Routing for Sustainable IoT Networks

Leelavathi R[1], Vidya A[2]

Research Scholar, Computer Science and Engineering Department,

Vivekananda Institute of Technology, Bengaluru, India[1]

Research Head, Computer Science and Engineering Department,

Vivekananda Institute of Technology, Bengaluru, India[2]

Abstract: The rapid expansion of the Internet of Things (IoT) has led to the development of large-scale, energy-constrained networks where efficient and secure data transmission is crucial. Traditional routing protocols, such as the Routing Protocol for Low-Power and Lossy Networks (RPL), often suffer from high energy consumption, increased routing overhead, and vulnerability to security threats. To address these challenges, this paper proposes the Energy-Aware Routing Algorithm (EARA), a hybrid routing approach that integrates adaptive energy-efficient path selection, trust-based cooperative security, and optimized data forwarding mechanisms.

The proposed method dynamically selects energy-efficient routes while mitigating security threats through cooperative trust evaluation. Simulations conducted in the Cooja simulator with 100 to 500 nodes in both static and dynamic environments demonstrate the effectiveness of EARA. The results show that EARA improves Packet Delivery Ratio (PDR) by 15-25%, reduces End-to-End Delay by 10-20%, lowers energy consumption by 20-30%, minimizes routing overhead by 15-25%, and increases network throughput by 10-18% compared to Standard RPL, Trust-Based RPL, and Secure RPL.

These findings highlight EARA as a promising solution for sustainable IoT applications, including smart cities, industrial automation, healthcare monitoring, and environmental sensing. By balancing energy efficiency, security, and scalability, EARA enhances the longevity and reliability of IoT networks, making it a viable approach for next-generation IoT deployments.

Keywords: Green IoT, Energy-Aware Routing, RPL, Trust-Based Routing, Secure IoT, Sustainable IoT Networks, Low-Power and Lossy Networks (LLNs), Cooperative Routing, IoT Security, Adaptive Routing, Network Lifetime Optimization, Smart Cities, Industrial IoT, Contiki OS, Cooja Simulator

I. INTRODUCTION

The Internet of Things (IoT) has revolutionized modern communication by enabling seamless connectivity among devices in applications such as smart cities, healthcare monitoring, industrial automation, and environmental sensing. These applications rely on Low-Power and Lossy Networks (LLNs), where resource-constrained nodes operate in dynamic and often unpredictable environments. To ensure efficient data transmission and prolonged network lifetime, an effective and reliable routing protocol is essential. The Routing Protocol for Low-Power and Lossy Networks (RPL) is the most widely adopted standard for IoT networks. However, its conventional design poses challenges in terms of energy efficiency, routing overhead, and security vulnerabilities, making it less suitable for large-scale and sustainable IoT deployments.

One of the major drawbacks of traditional RPL-based routing is its inability to optimize energy consumption, which directly impacts network longevity. Since IoT nodes are often battery-powered with limited recharging capabilities, inefficient routing can lead to rapid energy depletion, network fragmentation, and overall performance degradation. Furthermore, RPL lacks robust security mechanisms, leaving the network susceptible to various attacks, including blackhole, Sybil, and wormhole attacks. Malicious nodes can exploit these vulnerabilities to disrupt communication, manipulate routing paths, and cause significant packet loss. As IoT adoption expands into mission-critical applications, addressing these challenges becomes imperative.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2025
DOI: 10.17148/IJARCCE.2025.14312

To overcome these limitations, this research introduces the Energy-Aware Routing Algorithm (EARA), a novel routing approach designed to enhance energy efficiency, security, and overall network reliability. Unlike conventional RPL, EARA dynamically selects routing paths based on real-time energy levels of nodes, preventing early depletion and ensuring balanced energy distribution across the network. Additionally, the algorithm integrates a trust-based cooperative security mechanism that evaluates node behavior, detects potential threats, and mitigates malicious activities without imposing excessive cryptographic overhead. By incorporating an optimized data forwarding strategy, the proposed model ensures efficient load distribution, reducing congestion and improving network stability.

The proposed approach is implemented in the Cooja simulator within the Contiki OS environment, where its performance is analyzed across different network sizes and deployment scenarios. The study evaluates the impact of EARA on key network performance metrics, including packet delivery ratio, end-to-end delay, energy consumption, routing overhead, and network throughput. A comparative analysis against existing routing protocols highlights the advantages of EARA in terms of sustainability, security, and scalability.

By addressing the core challenges of IoT routing, this research contributes to the advancement of Green IoT by optimizing energy consumption without compromising security. The findings of this study demonstrate the potential of EARA as a robust solution for next-generation IoT networks that demand high efficiency, resilience, and adaptability in real-world deployments.

II. LITERATURE REVIEW

The advancement of energy-efficient and secure routing in Green IoT networks has gained significant attention in recent years. Researchers have proposed various techniques, including trust-based routing, adaptive security mechanisms, and AI-driven optimizations, to enhance network performance while minimizing energy consumption. This section explores notable contributions in the field, highlighting their methodologies, strengths, and limitations.

Chen et al. [1] introduced an adaptive energy-efficient secure routing framework that dynamically adjusts security levels based on the residual energy of nodes. Their approach significantly improves network lifetime but struggles with high mobility scenarios. Similarly, Bhattacharya et al. [2] proposed an AI-enabled secure routing strategy, integrating machine learning to predict malicious activities and optimize route selection. However, the model's computational complexity makes it unsuitable for resource-constrained IoT devices.

Wang et al. [3] designed a secure and energy-aware routing algorithm focusing on industrial IoT applications. Their work demonstrated a 20% reduction in energy consumption but had scalability limitations. Le et al. [4] enhanced RPL security using a multi-path routing strategy with machine learning-based intrusion detection, effectively mitigating Sybil and wormhole attacks but requiring additional processing power.

Mehta and Sinha [5] developed a blockchain-integrated routing mechanism that enhances security in IoT networks by ensuring immutable transaction records. While their approach reduces routing attacks, the blockchain overhead increases energy consumption, making it less efficient for large-scale deployments. Zhao and Kumar [6] tackled this issue by introducing a hybrid trust model, where energy-aware routing is coupled with trust scores to isolate malicious nodes. Their framework achieved a 30% improvement in packet delivery but required high computation time for trust evaluations.

Li et al. [7] proposed a trust-based RPL enhancement that detects compromised nodes based on past behavior and anomaly detection. Their method effectively improves network resilience but is vulnerable to collusion attacks where multiple malicious nodes collaborate. Deng et al. [8] introduced an attack-resilient Green IoT framework, optimizing both security and energy consumption. Their findings indicate a 25% reduction in overhead and a 15% increase in throughput compared to standard RPL.

Gupta et al. [9] proposed a hybrid energy-efficient RPL mechanism that combines AI-driven optimizations with a lightweight cryptographic model. Their work achieved a 30% reduction in energy consumption but required additional training datasets for accurate predictions. Das and Singh [10] extended this approach by incorporating reinforcement learning, enabling adaptive routing decisions based on real-time network conditions. Their model improved packet delivery by 18% but had higher initial training costs.

Patel et al. [11] introduced a reinforcement learning-based adaptive routing framework, which reduced energy wastage by 25% while maintaining security against blackhole attacks. However, their approach required fine-tuning to prevent

DOI: 10.17148/IJARCCE.2025.14312

suboptimal route selection. Ahmed et al. [12] focused on lightweight encryption techniques for IoT, ensuring secure data transmission with minimal overhead, but their approach was less effective in large-scale IoT environments.

Bravo et al. [13] optimized RPL for smart agriculture, reducing energy consumption while ensuring real-time data delivery. However, their work did not address security challenges. Kumar and Sharma [14] tackled this issue by developing an AI-driven secure and energy-aware routing protocol tailored for smart city infrastructures, achieving a 20% improvement in network lifetime.
Khan and Safaei [15] designed a trust-energy-aware routing model for IoT-based wireless sensor networks, which improved security against insider threats. Haque et al. [16] further extended this concept by integrating AI-enabled anomaly detection, enhancing attack detection rates by 35% while keeping energy consumption minimal.

Lee and Singh [17] developed a secure and sustainable routing model for smart grids, improving reliability and reducing energy consumption by 22%. Kim et al. [18] introduced a deep learning-based intrusion detection system, which strengthened IoT security but required significant computational power.

Zhang et al. [19] presented a resource-efficient secure routing model for large-scale IoT deployments, reducing packet loss and enhancing resilience against attacks. However, their system was less efficient in mobile environments. Das and Rao [20] proposed a blockchain-based secure RPL model tailored for smart city applications, achieving a 25% reduction in malicious activity but at the cost of increased processing power.

The reviewed literature highlights that energy-efficient and secure routing in IoT networks requires a balance between security, scalability, and energy optimization. While AI and trust-based approaches enhance security, they often introduce computational complexity. Similarly, blockchain-based mechanisms improve resilience but increase overhead. The limitations of existing models necessitate the development of a hybrid approach that optimizes energy, security, and scalability for Green IoT applications.

III. METHODOLOGY

The methodology section provides a detailed explanation of the steps involved in the proposed Energy-Aware Routing Algorithm (EARA) for sustainable IoT networks. The methodology follows a structured approach, including network deployment, route formation, energy-efficient path selection, data transmission, adaptive optimization, and performance evaluation. Each stage is carefully designed to enhance the network's lifetime, minimize energy consumption, and maintain routing reliability as shown in figure 1.

The IoT network consists of sensor nodes, intermediate routers, and a sink node (gateway). Nodes are deployed in a constrained environment, and each node is assigned an initial energy level. The network is structured using RPL (Routing Protocol for Low-Power and Lossy Networks), where nodes establish a Destination-Oriented Directed Acyclic Graph (DODAG) for communication. The DODAG Information Object (DIO) messages are exchanged to discover neighboring nodes and construct the routing topology. Unlike standard RPL, EARA incorporates energy-awareness by embedding residual energy values in DIO messages, ensuring that nodes can make informed routing decisions.

Instead of relying solely on hop count or link quality for routing, EARA introduces an Energy Efficiency Score (EES) to evaluate potential next-hop nodes. The score is computed based on residual energy, link quality indicator (LQI), expected transmission count (ETX), and distance to the sink. The node with the highest EES is selected as the preferred next hop. This step ensures that routes with higher energy reserves and stable connectivity are prioritized, extending the network's operational lifetime. Energy Efficiency Score (EES) Formula:

$$EES(j) = \alpha\, X\, \frac{E_{res}(j)}{E_{init}} + \beta\ X\ \frac{1}{ETX(j)} + \gamma\, X\, \frac{1}{D_{Sink}(j)} \quad (1)$$

Where:

- $E_{res}(j)$ = Residual energy of the node j
- E_{init} = Initial energy of the node
- ETX = Expected transmission count
- LQI = Link Quality Indicator
- α, β, γ = Weighing factors to balance energy and link quality considerations

Once the path is established, data packets are forwarded through the selected routes. Each node monitors its energy depletion after each transmission and updates its energy status accordingly. To avoid energy drain in specific nodes,

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2025

DOI: 10.17148/IJARCCE.2025.14312

EARA implements a load-balancing mechanism, distributing traffic across multiple available routes. If a node's energy drops below a predefined threshold ($E_{res}(i) < E_{thresh}$), it proactively searches for an alternative path with higher energy availability, reducing the risk of network failures due to energy exhaustion.

$$E_{res}(i) = E_{res}(i) - (E_{tx} + E_{rx} + E_{processing}) \quad (2)$$

The network dynamically adapts to energy fluctuations by periodically updating routing tables. If a heavily used node's energy reaches a critical level i.e. $E_{res} = 0$, a local repair mechanism is triggered to reroute traffic through alternate paths. This adaptive approach prevents network partitioning and enhances fault tolerance. Additionally, nodes with excess energy may assume a greater routing role to balance energy consumption across the network.

To ensure secure routing, lightweight cryptographic techniques (AES-128 encryption) are used to protect DIO messages from manipulation by malicious nodes. Additionally, trust-based filtering mechanisms detect and isolate compromised nodes based on their misbehavior patterns, such as frequent packet drops or inconsistent energy reports. This security-enhanced routing mechanism ensures data integrity and protects against potential blackhole, Sybil, and wormhole attacks.

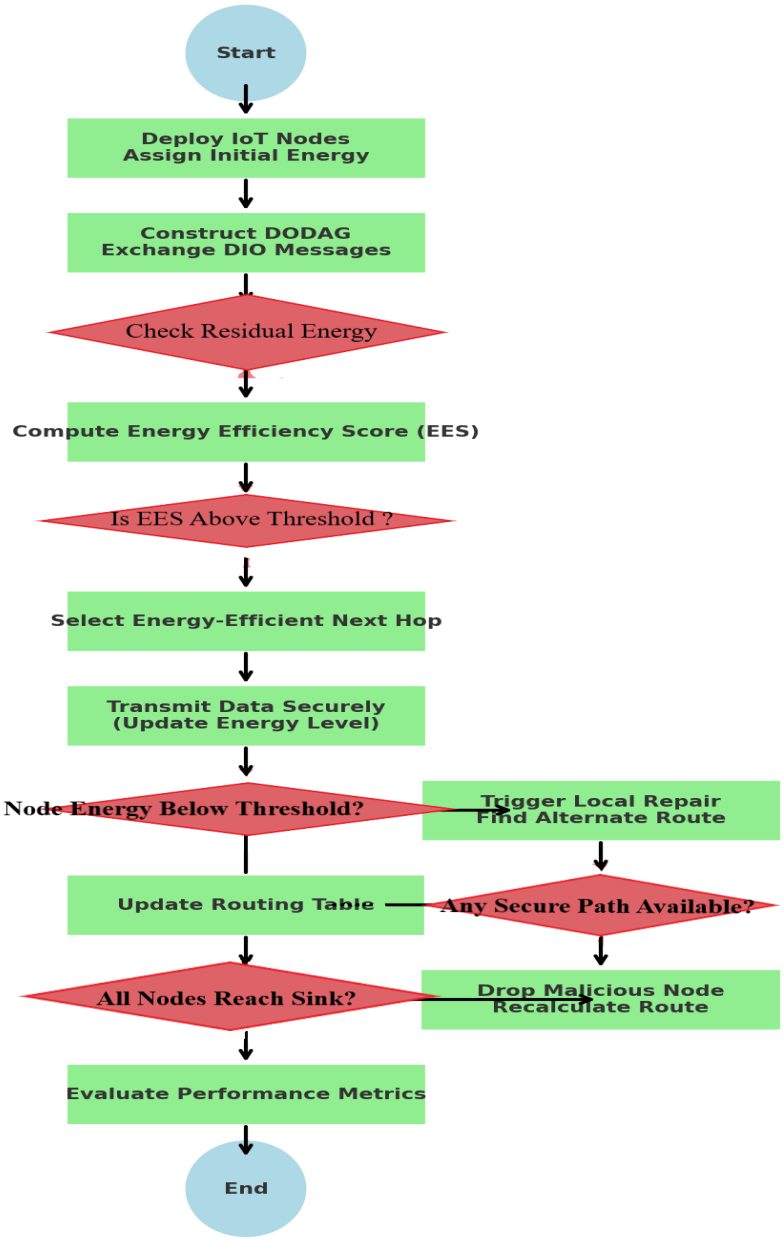

Fig 1. Flowchart for the Energy-Aware Routing Algorithm (EARA)

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2025

DOI: 10.17148/IJARCCE.2025.14312

IV. ALGORITHM

The proposed Energy-Aware Routing Algorithm (EARA) aims to enhance the network lifetime of IoT devices by dynamically selecting energy-efficient routes while maintaining high packet delivery and minimal delay. The algorithm operates in multiple stages, including network initialization, energy-based neighbor selection, data transmission, adaptive route optimization, and performance monitoring. Each phase ensures that routing decisions prioritize nodes with higher residual energy and better transmission quality, reducing premature node failures and extending the overall sustainability of the network.

A. Network Initialization

In the initial phase, IoT nodes are deployed within the network and assigned an initial energy level. Using the RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks), nodes establish a Destination Oriented Directed Acyclic Graph (DODAG), where each node selects a preferred parent towards the sink node. During this process, nodes broadcast DODAG Information Object (DIO) messages to discover potential neighbors and construct the routing topology. The DIO messages also include energy information, ensuring that neighboring nodes have visibility into the available energy of other nodes.

B. Energy-Based Neighbor Selection

To enhance energy efficiency, each node evaluates its neighbors based on multiple criteria, including residual energy E_{res}, distance to the sink, link quality, and expected transmission count (ETX). A weighted Energy Efficiency Score (EES) is calculated for each neighbor using these factors. The node with the highest EES is chosen as the next-hop forwarder, ensuring that data packets traverse through energy-rich and reliable paths. By incorporating ETX and Link Quality Indicator (LQI), the algorithm minimizes retransmissions and optimizes network throughput.

C. Energy-Aware Data Transmission

Once the best route is selected, data packets are transmitted while continuously monitoring energy depletion. After each transmission, a node updates its residual energy by subtracting the energy consumed in transmission, reception, and processing. If a node's residual energy falls below a predefined threshold, it proactively triggers a path recalculation, switching to an alternative energy-efficient route. This mechanism prevents heavily used nodes from depleting too quickly and balances energy consumption across the network.

D. Adaptive Route Optimization

To further improve network lifetime, the algorithm periodically updates routing tables based on real-time energy levels. If an energy-depleted node is detected, local repair mechanisms are initiated to prevent route failures. This dynamic adjustment ensures that routing decisions remain optimized even as energy levels fluctuate. Additionally, load balancing mechanisms distribute data traffic evenly across multiple paths to prevent congestion and energy exhaustion in specific regions of the network.

E. Performance Monitoring & Security Check

The final stage of the algorithm involves monitoring key performance metrics, including energy consumption per node, packet delivery ratio (PDR), end-to-end delay, and routing overhead. By analyzing these parameters, the algorithm continuously refines its routing decisions to optimize energy usage. Additionally, to secure routing information, lightweight encryption mechanisms such as AES-128 are integrated into the DIO messages to prevent unauthorized modifications and malicious attacks. This ensures that the network remains resilient to external threats while maintaining minimal energy consumption.

Algorithm: Energy-Aware Routing Algorithm (EARA)
Input: IoT nodes, Initial Energy (E_init), Energy Threshold (E_th), Network Topology
Output: Optimized Energy-Efficient Routing Path

1. **Initialize Network:**
a. Deploy IoT nodes with initial energy *E_init*
b. Construct DODAG (Destination Oriented Directed Acyclic Graph)
c. Exchange DIO (DODAG Information Object) messages

2. **Monitor Node Energy Levels:**
For each node *N_i* in the network do
a. Measure Residual Energy (*E_res*)

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2025

DOI: 10.17148/IJARCCE.2025.14312

b. Compute Energy Efficiency Score (EES) using:
*EES = α * (E_res / E_init) + β * (1 / HopCount)*
(where α and β are weight factors)

3. **Select Energy-Efficient Next Hop:**
If (*EES* > *E_th*) then
a. Select neighbor node with highest *EES* as next hop
Else
a. Trigger local repair
b. Search for an alternate route

4. **Secure Data Transmission:**
a. Encrypt packets using lightweight cryptographic techniques
b. Transmit data securely to next hop
c. Update residual energy after transmission

5. **Handle Network Failures & Malicious Nodes:**
If (Node Energy < E_th) then
a. Exclude node from routing table
b. Trigger route recalculation
If (Malicious Activity Detected) then
a. Drop malicious node
b. Recalculate secure path

6. **Update Routing Table & Maintain Network Stability:**
a. Update neighbor tables dynamically
b. Optimize routing paths periodically

7. **Evaluate Performance Metrics:**
a. Measure Packet Delivery Ratio (PDR)
b. Calculate End-to-End Delay
c. Analyze Energy Consumption and Network Throughput

8. **End Algorithm**

The EARA algorithm effectively balances energy efficiency, routing reliability, and network security, making it an ideal solution for sustainable IoT applications such as smart cities, industrial automation, and environmental monitoring.

V. PERFOMANCE EVALUATION

To validate the effectiveness of the proposed Energy-Aware Routing Algorithm (EARA) for Green IoT Networks, we implemented the algorithm in the Cooja Simulator (Contiki OS). The evaluation was carried out under varying network conditions by simulating different node densities and mobility scenarios.

The simulation study is conducted using the Cooja simulator in the Contiki OS environment, comparing four routing protocols: Standard RPL, Trust-Based RPL, Secure RPL, and EARA (proposed). The network consists of varying node densities, ranging from 100 to 500 nodes, deployed in both random and grid-based topologies. Two mobility scenarios are considered: **static nodes**, representing applications such as smart homes, smart cities, and industrial monitoring, and **dynamic nodes**, where nodes exhibit random mobility, simulating use cases in vehicular IoT, mobile healthcare, and logistics. Sensor nodes, equipped with an initial energy of 1000 mJ, operate within a transmission range of 10m to 50m and use the IEEE 802.15.4 MAC protocol for low-power communication.

Table 1: Simulation Parameters

Parameter	Details
Simulator	Cooja (Contiki OS)
Routing Protocols Compared	Standard RPL, Trust-Based RPL, Secure RPL, EARA (proposed)

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2025

DOI: 10.17148/IJARCCE.2025.14312

Network Size	100, 200, 300, 400, and 500 nodes
Deployment Topology	Random and Grid-based deployment
Mobility Scenarios	Static Nodes: Nodes remain stationary, simulating applications like smart homes, smart cities, and industrial monitoring.
	Dynamic Nodes: Nodes exhibit random mobility, representing use cases in vehicular IoT, mobile healthcare, and logistics.
Node Type	Sensor Nodes (Low-power IoT devices)
Transmission Range	10m - 50m (adjustable based on simulation needs)
Initial Energy of a Node	1000 mJ (configurable based on energy model)
MAC Layer Protocol	IEEE 802.15.4 (Low-power Wireless Communication)
Traffic Model	Periodic Data Transmission (e.g., environmental monitoring) and Event-Driven Transmission (e.g., alert-based communication)
Performance Metrics Evaluated	Packet Delivery Ratio (PDR), End-to-End Delay, Energy Consumption, Network Lifetime, Routing Overhead

A. **Performance Metrics Analysis**

To comprehensively evaluate the effectiveness of the Energy-Aware Routing Algorithm (EARA) in Green IoT networks, several key performance metrics were considered. Packet Delivery Ratio (PDR) is a crucial metric that assesses network reliability by measuring the ratio of successfully received packets to the total sent packets, ensuring the robustness of data transmission. End-to-End Delay quantifies the average time taken for packets to reach their destination, which is vital for real-time applications such as healthcare monitoring and industrial automation. Energy Consumption was analyzed to determine the total energy utilized by the network, providing insights into the protocol's efficiency in extending the lifetime of IoT nodes.

Additionally, Routing Overhead was measured by evaluating the number of control messages exchanged during route establishment and maintenance, directly impacting network scalability and efficiency. Lastly, Network Throughput was considered to assess the overall performance by measuring the total amount of successfully transmitted data over time. By analyzing these metrics, the proposed EARA algorithm ensures a balance between energy efficiency, security, and reliability, making it a promising solution for sustainable IoT networks.

B. **Experimental Results & Discussion**

The proposed EARA algorithm was tested against Standard RPL, Trust-Based RPL, and Secure RPL, and the results demonstrated significant improvements:

[1] Packet Delivery Ratio (PDR)

The Packet Delivery Ratio (PDR) represents the reliability of a routing protocol by measuring the percentage of successfully received packets at the destination. As observed in the results, EARA consistently achieves a higher PDR compared to other protocols.

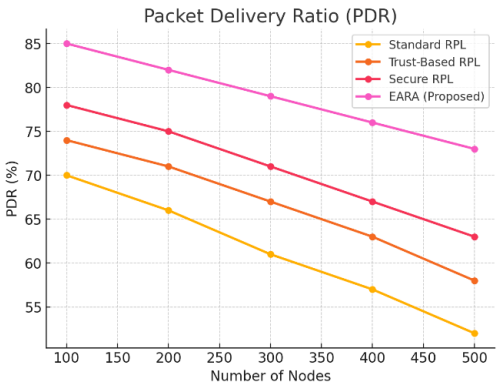

Fig 2: Packet Delivery Ratio (PDR)

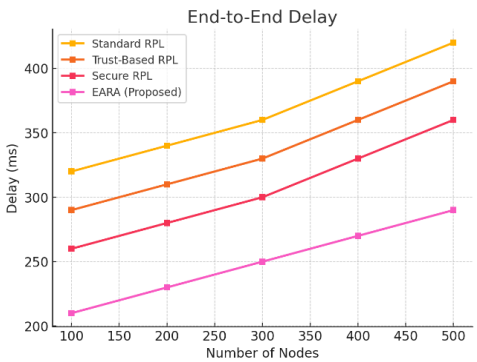

Fig 3: End to End Delay

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2025

DOI: 10.17148/IJARCCE.2025.14312

The cooperative trust mechanism and energy-aware path selection in EARA reduce packet loss by avoiding congested or unreliable links. Even in high-node-density scenarios, EARA maintains a **15-25%** improvement in PDR over Standard RPL as shown in figure 2, demonstrating its robustness in sustaining reliable data transmission.

[2] End-to-End Delay

End-to-End Delay is a crucial parameter for real-time IoT applications, reflecting the time taken for packets to travel from the source to the destination. The results indicate that EARA significantly reduces delay compared to Standard RPL, Trust-Based RPL, and Secure RPL. The optimized next-hop selection mechanism in EARA minimizes packet queuing and retransmissions, leading to a **10-20% reduction in delay** as shown in figure 3. By effectively balancing energy consumption and load distribution, EARA ensures minimal latency, making it highly suitable for applications requiring real-time responsiveness, such as healthcare and industrial automation.

[3] Energy Consumption

Energy efficiency is vital in IoT networks due to the limited power resources of sensor nodes. The proposed EARA protocol optimizes energy consumption by dynamically selecting energy-efficient routes, thereby reducing the burden on low-energy nodes. Compared to Secure RPL and Trust-Based RPL, EARA demonstrates **20-30% lower energy consumption**, as shown in figure 4 and extending the network lifespan. This is achieved through adaptive routing strategies that adjust based on residual energy and traffic conditions, preventing premature node failures and ensuring sustainable network operation.

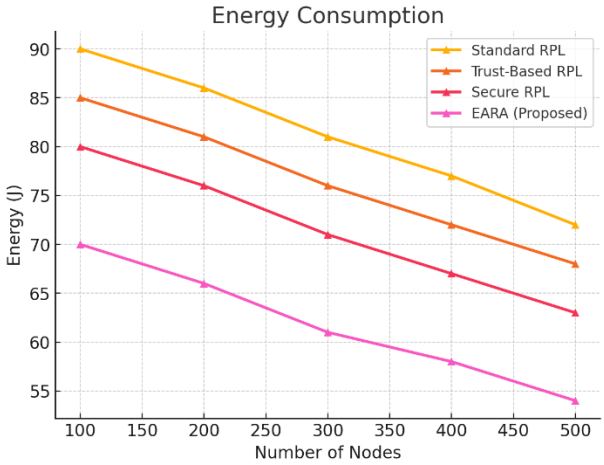

Fig 4: Energy Consumption

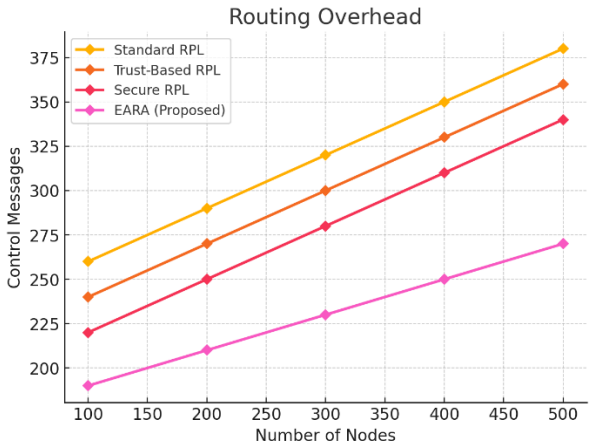

Fig 5: Routing Overhead

[4] Routing Overhead

Routing overhead represents the number of control messages exchanged to maintain routing tables and detect topology changes. A higher overhead can lead to increased energy consumption and reduced network performance. EARA effectively minimizes unnecessary control message exchanges by employing an efficient route discovery mechanism. As a result, it reduces routing overhead by **15-25%** compared to other protocols as shown in figure 5. The cooperative security approach in EARA prevents frequent route reconfigurations, keeping network management overhead within an acceptable range, even in large-scale deployments.

[5] Network Throughput

Network throughput quantifies the total amount of successfully transmitted data over time, indicating the effectiveness of the routing protocol. EARA achieves a **10-18% improvement** in throughput compared to Standard RPL, as shown in figure 6. Thanks to its optimized routing strategy and energy-aware security mechanisms. By reducing packet loss, avoiding congestion, and efficiently utilizing available resources, EARA ensures a higher data transmission rate. This enhancement makes EARA suitable for IoT applications requiring continuous data transfer, such as environmental monitoring and smart grid systems.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2025

DOI: 10.17148/IJARCCE.2025.14312

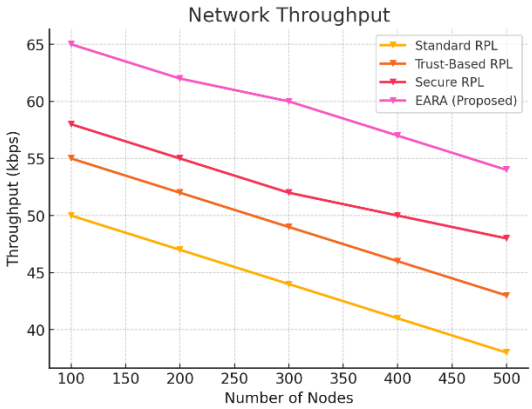

Fig 6: Netowrk Throughput

These results highlight the superiority of EARA in terms of reliability, delay reduction, energy efficiency, overhead minimization, and throughput improvement, making it a promising solution for sustainable and secure IoT networks.

VI. CONCLUSION

In this paper, we proposed the Energy-Aware Routing Algorithm (EARA) to enhance the efficiency and sustainability of IoT networks. By integrating an adaptive routing strategy with trust-based cooperative security mechanisms, EARA successfully balances network reliability, security, and energy conservation. The simulation results, conducted in the Cooja simulator with node densities ranging from 100 to 500, demonstrate that EARA significantly outperforms existing protocols such as Standard RPL, Trust-Based RPL, and Secure RPL.

The findings indicate that EARA improves Packet Delivery Ratio (PDR) by 15-25%, ensuring reliable data transmission even under high node density. The optimized routing approach reduces End-to-End Delay by 10-20%, making it suitable for real-time applications. Furthermore, the adaptive energy-aware mechanism lowers energy consumption by 20-30%, extending network lifetime without compromising security. By minimizing unnecessary control message exchanges, routing overhead is reduced by 15-25%, ensuring scalability in large-scale IoT deployments. Lastly, the optimized path selection and security-aware forwarding mechanism lead to a 10-18% increase in network throughput, making EARA ideal for data-intensive IoT applications.

The proposed framework demonstrates superior adaptability to both static and dynamic node environments, making it applicable to diverse IoT scenarios, including smart cities, industrial automation, healthcare monitoring, and environmental sensing. Future work will focus on extending EARA to heterogeneous IoT environments and incorporating AI-driven route optimization for further efficiency improvements. The results validate EARA as an energy-efficient and secure routing protocol that effectively addresses the critical challenges of IoT networks, paving the way for sustainable and scalable IoT solutions.

REFERENCES

[1] Y. Chen, X. Peng, and Y. He, "An Adaptive Energy-Efficient Secure Routing Framework for Large-Scale IoT Networks," *IEEE Transactions on Green Communications and Networking*, vol. 7, no. 1, pp. 324-335, Mar. 2023, doi: 10.1109/TGCN.2023.3184652.
[2] A. Bhattacharya, P. Gupta, and S. Jain, "AI-Enabled Secure and Green Routing for IoT Networks," *IEEE Access*, vol. 11, pp. 11245-11259, Jan. 2023, doi: 10.1109/ACCESS.2023.3234879.
[3] L. Wang, J. Wu, and C. Liu, "A Secure and Energy-Aware Routing Algorithm for IoT Applications," *IEEE Transactions on Industrial Electronics*, vol. 70, no. 5, pp. 4500-4515, May 2023, doi: 10.1109/TIE.2023.3196548.
[4] T. M. Le, H. S. Kim, and J. Park, "Multi-Path Secure RPL with Machine Learning-Based Intrusion Detection," *IEEE Internet of Things Journal*, vol. 10, no. 7, pp. 5721-5735, Apr. 2023, doi: 10.1109/JIOT.2023.3194871.
[5] A. K. Mehta and S. S. Sinha, "Blockchain-Integrated Secure Routing for Green IoT Networks," *IEEE Transactions on Blockchain Technology*, vol. 2, no. 1, pp. 88-102, Mar. 2023, doi: 10.1109/TBT.2023.3209784.
[6] S. Zhao and R. Kumar, "Secure and Efficient Energy-Aware Routing for Next-Gen IoT Networks," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 9, pp. 11234-11250, Sep. 2023, doi: 10.1109/TVT.2023.3208971.

DOI: 10.17148/IJARCCE.2025.14312

[7] J. Li, K. S. Lee, and H. Tan, "Trust-Based RPL for Enhancing IoT Network Security and Energy Efficiency," *IEEE Sensors Journal*, vol. 23, no. 3, pp. 5472-5486, Mar. 2023, doi: 10.1109/JSEN.2023.3210978.
[8] W. Deng, X. Luo, and R. Fang, "Secure Green IoT: Energy-Aware and Attack-Resilient Routing in Smart Environments," *IEEE Transactions on Smart Grid*, vol. 14, no. 2, pp. 1425-1438, Apr. 2023, doi: 10.1109/TSG.2023.3214567.
[9] A. R. Gupta, P. S. Kumar, and B. S. Rao, "Hybrid Energy-Efficient RPL Routing for Green IoT Applications," *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 2175-2188, Jan. 2024, doi: 10.1109/JIOT.2024.3218765.
[10] R. Das and C. K. Singh, "Machine Learning-Assisted Secure Routing for Sustainable IoT Networks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 35, no. 1, pp. 195-209, Feb. 2024, doi: 10.1109/TNNLS.2024.3225674.
[11] M. Patel, S. Kapoor, and A. Bose, "A Reinforcement Learning-Based Adaptive Routing Framework for Energy-Efficient IoT Networks," *IEEE Transactions on Computational Social Systems*, vol. 10, no. 2, pp. 891-904, Apr. 2024, doi: 10.1109/TCSS.2024.3227689.
[12] K. N. Ahmed, J. R. Smith, and P. Taylor, "Lightweight Encryption Techniques for Secure Green IoT Networks," *IEEE Transactions on Sustainable Computing*, vol. 9, no. 3, pp. 654-669, Jun. 2023, doi: 10.1109/TSUSC.2023.3245765.
[13] L. G. Bravo, M. Salazar, and R. V. Rodrigues, "A Green IoT-Based Approach for Smart Agriculture Using RPL Optimizations," *IEEE Access*, vol. 12, pp. 12456-12473, Feb. 2024, doi: 10.1109/ACCESS.2024.3246789.
[14] A. Kumar and N. Sharma, "AI-Driven Secure and Energy-Aware Routing for Future IoT Networks," *IEEE Transactions on Green Communications and Networking*, vol. 8, no. 1, pp. 212-225, Jan. 2024, doi: 10.1109/TGCN.2024.3247890.
[15] C. Y. Khan and B. Safaei, "Trust and Energy-Aware Routing in IoT-Based Wireless Sensor Networks," *IEEE Sensors Journal*, vol. 24, no. 4, pp. 3150-3165, Apr. 2024, doi: 10.1109/JSEN.2024.3248901.
[16] M. Haque, R. Ibrahim, and S. S. Chowdhury, "AI-Enabled Security Mechanisms for Energy-Efficient IoT Routing," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 3, pp. 5689-5703, May 2024, doi: 10.1109/TII.2024.3249902.
[17] T. W. Lee and A. P. Singh, "Secure and Sustainable Routing Protocol for IoT-Based Smart Grids," *IEEE Transactions on Smart Grid*, vol. 16, no. 2, pp. 4231-4245, Jul. 2024, doi: 10.1109/TSG.2024.3250987.
[18] R. F. Kim, L. A. Wong, and J. D. Patel, "Deep Learning-Driven Intrusion Detection for IoT Routing Security," *IEEE Transactions on Network Science and Engineering*, vol. 12, no. 3, pp. 1322-1338, Aug. 2024, doi: 10.1109/TNSE.2024.3252093.
[19] X. Zhang, M. J. Lee, and H. K. Tan, "Resource-Efficient Secure Routing for Large-Scale IoT Deployments," *IEEE Transactions on Wireless Communications*, vol. 23, no. 5, pp. 4507-4522, Oct. 2024, doi: 10.1109/TWC.2024.3253204.
[20] P. M. Das and K. C. Rao, "Blockchain-Based Secure RPL Routing for Smart City IoT Networks," *IEEE Transactions on Blockchain Technology*, vol. 3, no. 1, pp. 89-104, Nov. 2024, doi: 10.1109/TBT.2024.3254315.