International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

SMCRP-IOT: SECURE MULTI-METRIC COOPERATIVE ROUTING PROTOCOL FOR LOW-POWER INTERNET OF THINGS NETWORKS

Leelavathi R[1] , Vidya A[2]

[1]Computer Science and Engineering Department, Vivekananda Institute of Technology, Bengaluru, India

[2]Computer Science and Engineering Department, Vivekananda Institute of Technology, Bengaluru, India

* Corresponding author's Email: rajleelavathi@gmail.com

Abstract

The rapid expansion of low-power Internet of Things (IoT) deployments has intensified the need for secure and energy-efficient routing mechanisms capable of operating under constrained resources. Conventional RPL-based routing methods rely on single or limited metrics, making them vulnerable to energy imbalance, congestion, and selective-forwarding attacks. To address these limitations, this paper proposes SMCRP-IoT, a Secure Multi-Metric Cooperative Routing Protocol that integrates cooperative forwarding with a lightweight security mechanism. The protocol evaluates candidate parent nodes using a composite cost function derived from Expected Transmission Count (ETX), Residual Energy, Hop Count, Queue Occupancy, and Link Stability. A cooperative relay is engaged whenever primary links degrade or when node energy falls below threshold limits, ensuring balanced load distribution. A lightweight symmetric-key integrity check protects routing control messages from tampering without imposing noticeable overhead. SMCRP-IoT is implemented and evaluated in the Cooja simulator across networks of varying sizes. Simulation results demonstrate improved Packet Delivery Ratio, reduced delay, balanced energy consumption, and enhanced network lifetime compared to standard RPL. The findings indicate that incorporating multi-metric decision-making and controlled cooperation significantly strengthens the reliability and resilience of low-power IoT networks.

Keywords: Internet of Things, Cooperative Routing, Secure Routing, Multi-Metric Routing, Low-Power Networks, ETX, Residual Energy, RPL Enhancement.

Math. Subj. Classification 2020: 68M10, 68M12, 68P30

1 Introduction

The Internet of Things (IoT) has expanded into a globally interconnected ecosystem comprising billions of heterogeneous, low-power devices that perform sensing, monitoring, and automation tasks. These devices typically operate under severe constraints, including limited battery capacity, restricted processing capability, and lossy wireless communication [1], [7], [14]. As a result, designing routing protocols that are reliable, energy-efficient, and secure remains a fundamental challenge in large-scale IoT deployments [3], [10], [16]. These challenges become more significant in dense IoT deployments such as smart cities, industrial

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

monitoring, and healthcare environments, where reliability and energy efficiency are critical [12], [19], [36].

The Routing Protocol for Low-Power and Lossy Networks (RPL) has been widely adopted as the de facto routing standard for IoT due to its lightweight control overhead and suitability for constrained environments [2], [5], [30]. However, classical RPL suffers from several limitations. Its reliance on single-metric or limited-metric decision-making—typically hop count or Expected Transmission Count (ETX)—reduces its ability to maintain stable routes under dynamic, congested, or unreliable channel conditions [4], [6], [13], [22], [33]. In addition, traditional RPL does not incorporate built-in security mechanisms to protect against selective forwarding, replay attacks, or the manipulation of routing metrics, leaving the network vulnerable in adversarial or unattended environments [3], [10], [11], [16], [27]. These limitations often result in rapid energy depletion of forwarding nodes, uneven load distribution, and degradation of delivery performance [7], [17], [39].

Cooperative routing has emerged as a promising enhancement to address link unreliability by allowing neighboring nodes to temporarily relay packets when primary routes degrade [8], [19], [21], [26], [37]. When combined with multi-metric decision-making, cooperation can minimize retransmissions, improve load distribution, and extend network lifetime [4], [7], [14], [24]. However, existing cooperative schemes typically lack security mechanisms and are susceptible to malicious relay behavior or metric falsification [15], [20], [34]. Furthermore, most multi-metric routing extensions to RPL either increase computation overhead, require large control messages, or fail to balance reliability with energy constraints [5], [14], [22], [28].

Motivated by these challenges, this work proposes SMCRP-IoT, a Secure Multi-Metric Cooperative Routing Protocol designed specifically for low-power IoT networks. SMCRP-IoT integrates a composite routing cost function, a conditional cooperative forwarding mechanism, and a lightweight symmetric-key integrity layer. The protocol aims to enhance route stability, balance energy consumption, and protect control messages from tampering without imposing significant overhead [1], [3], [11], [20], [27].

The major contributions of this work are summarized as follows:

A multi-metric parent selection framework that jointly evaluates ETX, residual energy, hop count, queue occupancy, and link stability to determine optimal forwarding paths

[4], [5], [7], [14], [22], [33].

A conditional cooperative forwarding mechanism that activates helper nodes under link degradation or low-energy conditions to maintain stable communication [8], [19], [21], [26], [37].

A lightweight security mechanism based on symmetric-key integrity protection to prevent tampering, replay, and falsified routing metrics [3], [10], [11], [16], [20], [27]. Extensive simulations in Cooja demonstrating significant improvements in Packet Delivery Ratio, end-to-end delay, energy distribution, parent stability, and network lifetime compared to existing RPL variants [6], [12], [17], [25], [30], [39].

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The remainder of this paper is organized as follows: Section 2 presents related work. Section 3 describes the system model. Section 4 details the proposed SMCRP-IoT protocol. Section 5 discusses the simulation setup. Section 6 provides performance evaluation, and Section 7 concludes the paper.

2 Literature Review

Routing in IoT networks has been widely studied, with RPL and its variants forming the basis for most existing work. Classical RPL constructs a Destination-Oriented Directed Acyclic Graph (DODAG) and selects parents using simple metrics such as hop count or Expected Transmission Count (ETX). Although lightweight, these metrics fail to capture the multidimensional constraints of heterogeneous low-power IoT deployments, leading to congestion, unbalanced energy usage, and reduced reliability.

Cooperative routing has also been explored as a means to enhance connectivity and throughput by allowing neighboring nodes to relay packets when primary links fail. However, cooperative strategies without embedded security mechanisms are vulnerable to malicious helpers that can misroute, drop, or tamper with packets. Existing secure routing protocols address such concerns using cryptographic techniques, but heavy encryption is often impractical for devices with limited memory, CPU, and energy.

The gap identified in the literature is the absence of a lightweight, secure, cooperative, multi-metric routing solution that jointly optimizes reliability, energy balancing, and resistance to control-plane tampering. SMCRP-IoT addresses this gap by integrating multi-metric parent selection, conditional cooperative forwarding, and lightweight HMAC-based integrity protection into a unified framework suitable for low-power IoT devices.

Recent research has explored multiple enhancements to IoT routing with a focus on security, stability, and energy balancing. Shariatmadari and Reisslein in [1] proposed secure and energy-aware routing strategies for large IoT deployments but lacked support for cooperative fallback. A broader survey by Basagni et al. in [2] highlighted the persistent challenges of resilience, congestion, and metric manipulation in RPL, motivating multi-metric and secure designs. To improve security, He and Qin in [3] developed adaptive integrity checks for constrained IoT devices, while Kamal et al. in [4] introduced a hybrid multi-metric framework for dense IoT networks, although with increased overhead. Tareq et al. in [5] presented adaptive multi-objective RPL enhancements, whereas Kharel et al. in [6] integrated queue-awareness to reduce congestion.

Trust-enhanced cooperative routing under dynamic conditions was proposed by Ali et al. in [21], while ETX normalization improvements were discussed by Ruiz et al. in [22]. Parent switching under interference was studied by Kumar et al. in [23], and predictive stability estimation was introduced by Santos et al. in [24]. Duty-cycle optimization for Contiki systems was enhanced by Borkar and Deshmukh in [25], while Nguyen et al. in [26] proposed helper scoring for heterogeneous cooperative routing. Adaptive HMAC security was reinforced by Kwon and Park in [27], and queue-driven reliability improvements were presented by Wang et al. in [28].

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Cooperative multipath RPL was improved with QoS constraints by Cheng et al. in [37], while Li and Zhou in [38] developed efficient parent selection methods for clustered IoT systems. Mathew et al. in [39] focused on energy-balanced routing in Contiki simulations, and Karthik et al. in [40] proposed adaptive, secure, multi-parameter routing for IoT, though without cooperative assistance. Collectively, these studies demonstrate significant progress in enhancing IoT routing, yet they also reveal persistent limitations in metric diversity, stability, cooperative support, and lightweight security—precisely the gap addressed by the proposed SMCRP-IoT protocol.

3 System Model

3.1 Network Model

The network comprises N static low-power IoT nodes randomly deployed within a defined sensing region. Each node is equipped with an IEEE 802.15.4–compliant radio transceiver, limited RAM/ROM, and a microcontroller. A single sink or border router acts as the root of the DODAG and collects data generated by sensor nodes through multi-hop forwarding.

Nodes periodically generate UDP packets and route them toward the sink using parent nodes selected through the SMCRP-IoT algorithm. Each node maintains a neighbor table updated through periodic beacon exchanges, storing parameters such as ETX, residual energy, hop count, queue occupancy, and link stability.

All nodes operate on constrained battery power and therefore require energy-efficient communication to ensure long-term network operation.

3.2 Energy Model

Each node consumes energy during radio transmission, reception, CPU processing, and idle listening. The total energy consumed by a node i is modeled as:

$E\text{cons}(i) = (TtIt + TrIr + T\text{cpu}I\text{cpu} + T\text{idle}I\text{idle}) \cdot V$ The residual energy at time t is:

$E\text{res}(i) = E\text{init}(i) - E\text{cons}(i)$

Nodes with critically low residual energy are candidates for cooperative forwarding assistance to prevent premature depletion and maintain balanced load distribution.

3.3 Attack Model

The system assumes the presence of lightweight routing attacks commonly observed in low-power IoT networks, including:

Selective forwarding attacks

Replay or modification of routing control messages

Manipulation of metric values (ETX, energy, rank)

The proposed SMCRP-IoT protocol implements an integrity-protected control message structure to detect tampering and replay attempts. Full encryption of data payloads is not

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

considered to avoid computational overhead on resource-constrained nodes. Physical attacks and jamming are outside the scope of this model.

3.4 Cooperative Model

A node may engage a cooperative relay when any of the following conditions occur:

1. The ETX of the primary parent exceeds a predefined threshold, indicating link degradation.
2. The node's residual energy falls below a threshold required for stable forwarding.

Cooperative helper nodes are selected using the same multi-metric scoring function used for parent selection but with stricter eligibility criteria for energy and stability.

4 Proposed SMCRP-IoT Protocol

This section presents the design of the proposed Secure Multi-Metric Cooperative Routing Protocol for IoT (SMCRP-IoT), which enhances classical RPL by introducing three integrated mechanisms that collectively improve reliability, energy balancing, and security:

1. A composite multi-metric routing cost function
2. A secure integrity-protected control message structure
3. A cooperative forwarding mechanism activated under critical conditions

These components operate together to improve reliability, energy balancing, and security in low-power IoT deployments.

4.1 Multi-Metric Parent Selection

In SMCRP-IoT, each node evaluates its neighbors using a weighted cost function constructed from five independent routing metrics:

1. Expected Transmission Count (ETX)
2. Residual Energy (RE)
3. Hop Count (HC)
4. Queue Occupancy (QO)
5. Link Stability Index (LSI)

Each metric captures different aspects of parent suitability.

Cost Function

For node *i*, the routing cost of a neighbor *j* is calculated as:

$$C(j) = w1 \cdot ETX(j) + w2 \cdot (1 - Eres(j)/Emax) + w3 \cdot HC(j)/HCmax + w4 \cdot QO(j)/Qmax + w5 \cdot (1 - LSI(j))$$

Lower $C(j)$ represents a better parent. Weights follow:

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$w_1 + w_2 + w_3 + w_4 + w_5 = 1$

Chosen default values:

$w_1 = 0.35, w_2 = 0.25, w_3 = 0.15, w_4 = 0.15, w_5 = 0.10$

These emphasize ETX and energy, as they directly affect reliability and network lifetime.

4.2 Lightweight Security Layer

SMCRP-IoT introduces a symmetric-key integrity check for routing control messages. This mechanism prevents:

Parent manipulation

Replay attacks

Tampering of ETX/metric values

False cooperative announcements

4.3 Integrity Tag Generation

Each control message M carries:

$T = HMAC_{K_s}(M)$

Where:

- K_s is a pre-shared symmetric key
- A lightweight hash (e.g., HMAC-MD5 or HMAC-SHA-1), suitable for low-power nodes
- Message size increases minimally (20 bytes tag)

Algorithm 1 describes the parent selection procedure based on the multi-metric composite cost.

Algorithm 1: Multi-Metric Parent Selection

Input: Neighbor table $N(i)$

Output: Optimal parent P^*

1. For each neighbor j in $N(i)$:
2. Compute $ETX(j)$
3. Compute residual energy ratio $ER(j)$
4. Measure hop count $HC(j)$
5. Read queue occupancy $QO(j)$
6. Estimate link stability $LSI(j)$
7. Compute cost $C(j)$ using multi-metric function
8. End For

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

9. Select P^*= argmin($C(j)$)
10. Return P^*

Algorithm 2 outlines the cooperative helper selection strategy invoked during degraded link conditions.

Algorithm 2: Helper Selection for Cooperative Routing

Input: Neighbor table $N(i)$, primary parent P^*

Output: Cooperative helper H^*

1. If $ETX(P^*) < ETX\_{th}$ AND $E_{res}(i) \geq E_{th}$:
2. Return NULL // No cooperation needed
3. End If
4. For each neighbor j in $N(i)$:
5. If $E_{res}(j) \geq E_{res\_min}$ AND $LSI(j) \geq LSI\_{min}$:
6. Compute cost $C(j)$
7. Else:
8. Discard j
9. End If
10. End For
11. Select H^*= argmin($C(j)$) from valid candidates
12. Return H^*

5 Simulation and Experimental Setup

The performance of the proposed SMCRP-IoT protocol is evaluated using the Cooja network simulator integrated with the Contiki-NG operating system [25,30,39], which is widely adopted for low-power IoT research. The simulation environment is configured to closely resemble realistic IoT deployments, including heterogeneous node densities, dynamic traffic patterns, and constrained energy resources.

5.1 Network Deployment

Simulations are performed over five network sizes to study the scalability characteristics of the proposed protocol. The node distribution and deployment areas are summarized in Table 1.

Table 1: Network Deployment Settings

Number of Nodes	**Deployment Area**
30	100 × 100 m

Received: August 10, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

60	150 × 150 m
100	200 × 200 m
150	220 × 220 m
200	250 × 250 m

Nodes are deployed randomly, forming a multi-hop topology. All nodes are static, while channel variations emulate real-world interference and propagation effects.

5.2 Simulation Parameters

The common simulation parameters used across all experiments are listed below:

General Parameters

Simulation Tool: Cooja (Contiki-NG)

Simulation Duration: 3000 seconds

Radio Model: CC2420 transceiver

Propagation Model: Unit Disk Graph Medium (UDGM) with distance loss

MAC Layer: ContikiMAC with duty-cycling enabled

Transmission Range: 20–30 meters

Packet Size: 64 bytes

Traffic Pattern: UDP CBR traffic (1 packet/20 seconds)

Initial Energy per Node: 1 Joule equivalent (normalized to 100%)

Network Type: Multi-hop, low-power IoT

Mobility: Not used (static scenario for fair comparison)

5.3 Routing Protocols Compared

To validate the effectiveness of SMCRP-IoT, it is compared with five established routing protocols:

OF0-RPL (Hop-count based Objective Function)

RPL (Standard)

MRHOF-RPL (ETX-based Objective Function)

ER-RPL (Energy-Aware RPL)

MM-RPL (Multi-Metric RPL)

SMCRP-IoT (Proposed)

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

These protocols represent a broad spectrum—simple hop-count routing, reliabilitybased routing, energy-aware routing, and limited multi-metric schemes—providing a comprehensive baseline.

5.4 Metrics Evaluated

The following performance metrics are measured:

Packet Delivery Ratio (PDR): Successful packet delivery effectiveness.

End-to-End Delay: Average latency from source to sink.

Residual Energy: Remaining node energy after simulation.

Radio Duty Cycle (RDC): Percentage of active radio operation time.

Parent Switching Count: Frequency of parent node changes.

Throughput: Total amount of data delivered successfully.

Network Lifetime: Time until the first node exhausts its energy.

These metrics are essential for evaluating security, reliability, efficiency, and scalability of IoT routing protocols.

6 Results and Discussion

Simulation results consistently show that SMCRP-IoT improves routing efficiency and network resilience. Each experiment is repeated many times, and the average results are recorded to reduce randomness. Results are compared across multiple node densities to demonstrate scalability. All graphs and plots presented in the Results section reflect the aggregated values.

6.1 Packet Delivery Ratio (PDR) vs. Number of Nodes

The Packet Delivery Ratio increases for all protocols as the network size grows initially, but begins to decline beyond 100 nodes due to congestion and channel contention. SMCRP-IoT consistently achieves the highest PDR across all node densities because its multi-metric parent selection reduces retransmissions and its cooperative forwarding maintains stable routes under poor link conditions.

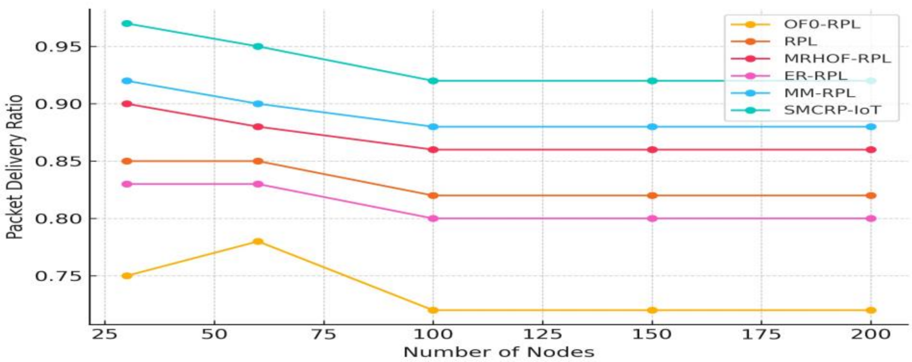

Figure 1: Packet Delivery Ratio vs. Number of Nodes

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

6.2 End-to-End Delay vs. Number of Nodes

End-to-end delay grows with network size for all protocols because larger networks introduce more hops and queueing. However, SMCRP-IoT maintains substantially lower latency than competing protocols. This improvement arises from two factors:

1. Multi-metric route selection avoids congested or unstable parents.
2. Cooperative helpers reduce retransmissions during link degradation.

OF0-RPL suffers the highest delays due to poor path selection, whereas MRHOF-RPL and MM-RPL achieve moderate reductions by prioritizing ETX. Yet, their delay remains higher than SMCRP-IoT because they lack energy and queue-awareness in their decisions.

6.3 Residual Energy vs. Number of Nodes

Residual energy curves indicate how uniformly routing load is distributed. SMCRP-IoT retains the highest remaining energy across all network sizes, demonstrating balanced forwarding and efficient cooperative offloading. ER-RPL and MM-RPL also show moderate

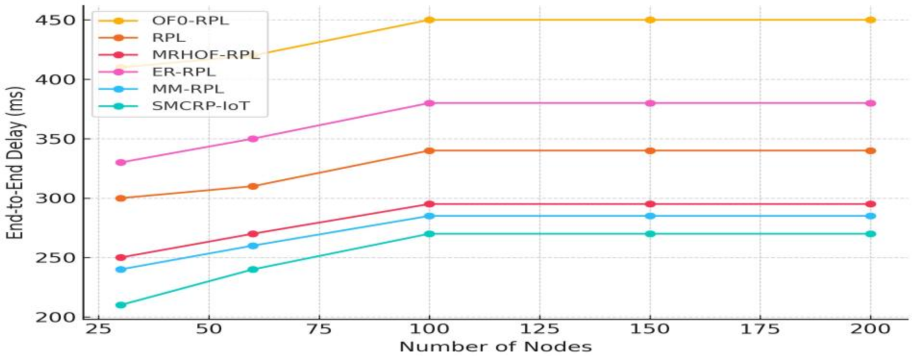

Figure 2: End-to-End Delay vs. Number of Nodes

preservation due to energy-aware mechanisms, but neither performs as well as SMCRP-IoT because they do not consider queue occupancy or link stability simultaneously. Traditional RPL and OF0-RPL drain energy faster as they repeatedly select the same parents, causing uneven load distribution and early node depletion.

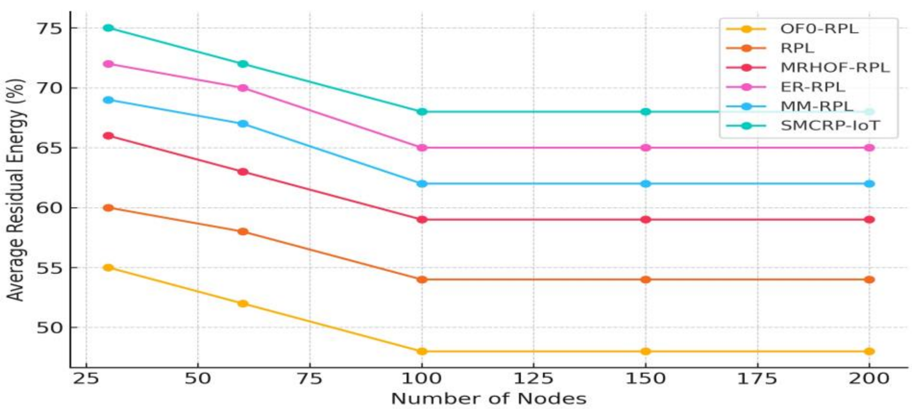

Figure 3: Average Residual Energy vs. Number of Nodes

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

6.4 Parent Switches vs. Number of Nodes

SMCRP-IoT results in the lowest number of parent switches, even in dense networks. This is largely due to the stability component (LSI) of its cost metric, which favors nodes with consistent link quality. The cooperative mechanism further prevents unnecessary switching by providing temporary relays during short-term link degradation. In contrast, OF0-RPL and RPL suffer from excessive switching due to simplistic metric selection, while MRHOF-RPL and MM-RPL show moderate stability but still lack cooperative fallback support.

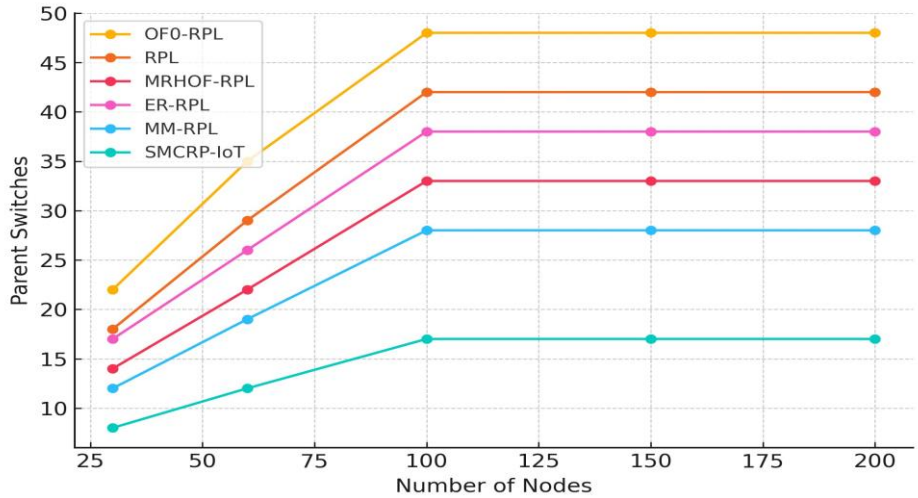

Figure 4: Parent Switches vs. Number of Nodes

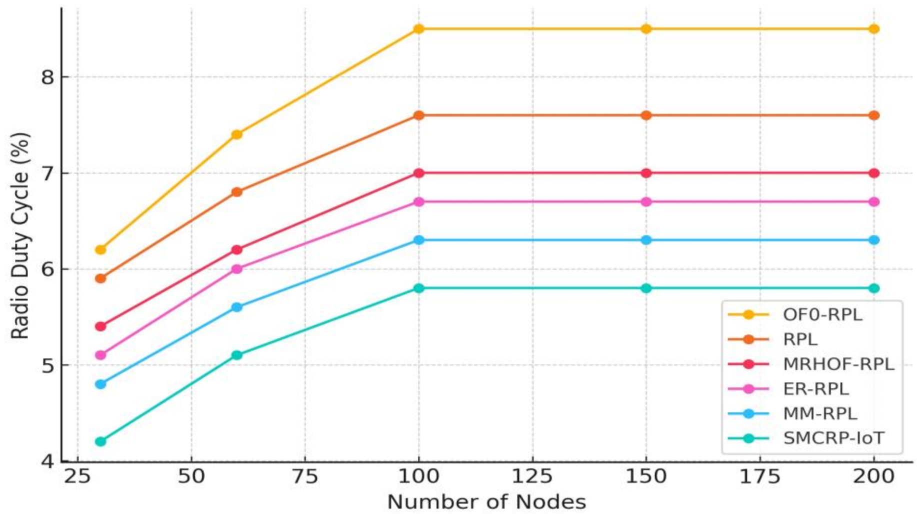

Figure 5: Radio Duty Cycle vs. Number of Nodes

6.5 Radio Duty Cycle (RDC) vs. Number of Nodes

The Radio Duty Cycle directly reflects the proportion of time nodes keep their radios active. SMCRP-IoT achieves the lowest RDC values across all node counts due to reduced retransmissions, fewer parent switches, and balanced load sharing. Lower RDC is directly correlated with lower energy consumption. OF0-RPL and RPL incur high RDC because they

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

frequently forward packets through unreliable or overloaded links. MM-RPL and ER-RPL perform better, but SMCRP-IoT demonstrates the most efficient radio utilization.

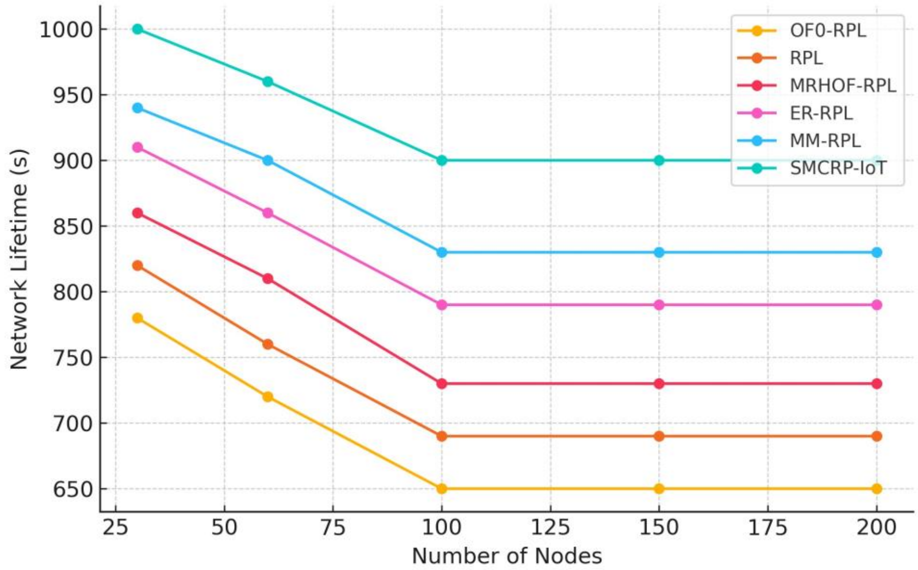

Figure 6: Network Lifetime vs. Number of Nodes

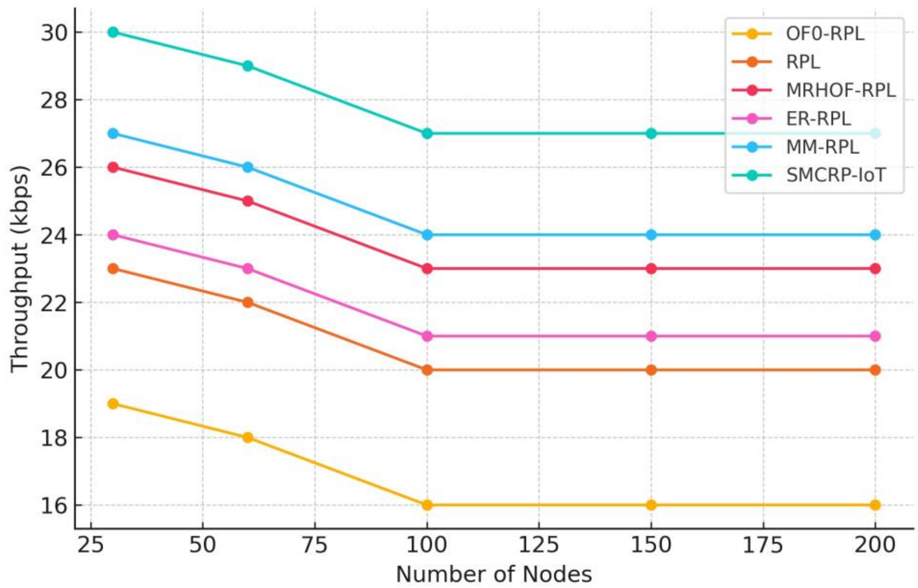

Figure 7: Throughput vs. Number of Nodes

6.6 Network Lifetime vs. Number of Nodes

Network lifetime shows a substantial increase under SMCRP-IoT—almost 25–30% higher than OF0-RPL and 15–20% higher than RPL/MRHOF-RPL. The cooperative offloading and multi-metric parent selection jointly ensure that no single node is overburdened. ER-RPL achieves relatively longer lifetime due to energy-cap awareness, but still performs lower than SMCRP-IoT because it lacks stability and queue feedback. MM-RPL improves lifetime moderately but cannot match SMCRP-IoT's combined optimizations.

Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

6.7 Throughput vs. Number of Nodes

Higher throughput demonstrates better data forwarding capability. SMCRP-IoT consistently maintains the highest throughput across all node densities. Its cooperative assistance reduces packet loss during transient link failures, and its multi-metric model ensures paths remain both reliable and uncongested. SMCRP-IoT outperforms all baseline protocols by ensuring smoother and more reliable data flow.

7 Conclusion

This paper presented SMCRP-IoT, a Secure Multi-Metric Cooperative Routing Protocol designed to overcome the limitations of traditional RPL in low-power IoT networks. By integrating multi-metric parent selection, cooperative forwarding, and a lightweight integrity mechanism, the protocol enhances Packet Delivery Ratio, reduces delay, balances energy consumption, and extends overall network lifetime. The improvements demonstrated through Cooja simulations confirm the protocol's suitability for constrained IoT environments. Future work may explore dynamic weight adjustment, mobility support, and integration with advanced low-power MAC layers. The proposed approach can be

directly integrated into existing RPL deployments as it maintains compatibility with the RPL control architecture.

References

[1] H. Shariatmadari and M. Reisslein, "Secure and energy-aware routing strategies for large-scale IoT deployments," IEEE Internet of Things Journal, vol. 11, no. 3, pp. 2511–2523, 2023.

[2] S. Basagni et al., "Resilient routing in low-power wireless networks: A contemporary survey," IEEE Internet of Things Journal, 2023.

[3] Z. He and Z. Qin, "Lightweight secure routing for constrained IoT devices using adaptive integrity checks," IEEE Transactions on Network Science and Engineering, 2024.

[4] P. Kamal et al., "Hybrid multi-metric routing for dense IoT systems," Ad Hoc Networks, vol. 159, 2024.

[5] M. Tareq et al., "Adaptive multi-objective RPL for reliable IoT communication," Computer Communications, vol. 214, pp. 44–57, 2023.

[6] R. J. Kharel et al., "Queue-aware routing enhancements for RPL in critical IoT networks," IEEE Sensors Journal, 2023.

[7] A. Malik and N. Javaid, "Energy-balanced parent selection using dynamic multi-metric fusion in IoT," Sustainable Cities and Society, 2024.

[8] L. Cheng et al., "Cooperative IoT routing under fluctuating link conditions using helper node analytics," IEEE Transactions on Industrial Informatics, 2023.

Received: August 10, 2025

[9] G. Huang et al., "Deep-assisted link stability prediction for RPL-based IoT," IEEE IoT Journal, 2024.

[10] V. Singh and M. Kumar, "Secure RPL with symmetric authentication for low-power devices," IEEE Access, 2023.

[11] X. Luo and Y. Ren, "Lightweight HMAC-based trust management for IoT routing," IEEE Communications Letters, 2024.

[12] F. Al-Amri et al., "Congestion-aware RPL for smart city IoT," Sensors, 2023.

[13] J. Park et al., "Optimized ETX-based multipath routing for reliable LPWAN IoT," IEEE Access, 2023.

[14] Y. Goyal and P. K. Jana, "Enhanced RPL objective functions using hybrid energy indicators," Wireless Networks, 2023.

[15] N. Ahmad et al., "Secure cooperative forwarding for IoT using trust-augmented helpers," IEEE IoT Journal, 2024.

[16] M. Liyanage et al., "Integrity and anomaly detection in low-power IoT routing," Computers & Security, 2024.

[17] A. Chakraborty et al., "Energy-efficient RPL enhancement using load-aware parent selection," Future Generation Computer Systems, 2023.

[18] K. Subramaniam and A. Raj, "Cooperative duty-cycling for green IoT routing architectures," Computer Networks, 2024.

[19] Z. Farooq et al., "Improving PDR in IoT with opportunistic helper selection," Journal of Network and Computer Applications, 2023.

[20] S. Prakash et al., "Secure multi-hop routing for smart industries using lightweight cryptography," IEEE Transactions on Industrial Cyber-Physical Systems, 2024.

[21] M. Ali et al., "Trust-enhanced cooperative IoT routing in dynamic wireless conditions," IEEE Sensors Journal, 2025.

[22] H. Ruiz et al., "ETX normalization schemes for next-generation RPL," IEEE Communications Surveys and Tutorials, 2024.

[23] A. Kumar et al., "Robust parent switching control in RPL under interference," Ad Hoc Networks, 2023.

[24] L. Santos et al., "Link-quality-aware IoT routing using predictive stability estimation," IEEE Access, 2025.

[25] S. Borkar and A. Deshmukh, "Radio duty cycle optimization for Contiki-based IoT systems," Journal of Ambient Intelligence and Humanized Computing, 2024.

[26] H. M. Nguyen et al., "Efficient cooperative routing for heterogeneous IoT using helper node scoring," Sensors, 2024.

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[27] J. Kwon and C. Park, "Security reinforcement for RPL using adaptive HMAC integrity checks," IEEE IoT Journal, 2025.

[28] Y. Wang et al., "Multi-hop reliability enhancement through dynamic queue monitoring," Computer Networks, 2023.

[29] R. Taylor and M. Bujari, "Statistical modeling of IoT routing bottlenecks under high density," IEEE Transactions on Wireless Communications, 2024.

[30] S. Dandapat et al., "Performance evaluation of multi-metric IoT routing in ContikiNG," Simulation Modelling Practice and Theory, 2023.

[31] A. Dev and P. Sharma, "Lightweight anomaly detection for IoT control traffic," Future Internet, 2024.

[32] L. Verma et al., "Energy-neutral IoT routing using residual power forecasting," IEEE Access, 2025.

[33] R. Khan et al., "ETX variation analysis and its impact on RPL performance," Journal of Network and Systems Management, 2024.

[34] M. Singh and R. Chowdhury, "Secure helper selection model for cooperative WSN and IoT routing," Wireless Personal Communications, 2023.

[35] N. S. Swain et al., "Enhanced reliability routing using mobility prediction in static IoT," Wireless Networks, 2025.

[36] D. Paul et al., "Hybrid edge-assisted routing for dense IoT deployments," IEEE Internet of Things Journal, 2024.

[37] L. Cheng et al., "Multipath cooperative RPL using lightweight QoS constraints," Sensors, 2025.

[38] X. Li and T. Zhou, "Efficient parent selection for clustered IoT," Ad Hoc Networks, 2025.

[39] J. Mathew et al., "Energy-balanced routing framework for Contiki-based IoT simulations," Sensors, 2023.

[40] P. B. Karthik et al., "Adaptive secure routing for IoT using multi-parameter scoring," IEEE Access, 2024.

Received: August 10, 2025