

ARTICLE

A Novel Reliable and Trust Objective Function for RPL-Based IoT Routing Protocol

Mariam A. Alotaibi^{1,2,*}, Sami S. Alwakeel^{1,*} and Aasem N. Alyahya¹

¹Department of Computer Engineering, College of Computer Science, King Saud University, Riyadh, 11543, Saudi Arabia

²Department of Computer Science and Information Technology, Shaqra University, Shaqra, 11961, Saudi Arabia

*Corresponding Authors: Mariam A. Alotaibi. Email: mariam_a@su.edu.sa; Sami S. Alwakeel. Email: swakeel@ksu.edu.sa

Received: 05 November 2024; Accepted: 24 December 2024; Published: 17 February 2025

ABSTRACT: The Internet of Things (IoT) integrates diverse devices into the Internet infrastructure, including sensors, meters, and wearable devices. Designing efficient IoT networks with these heterogeneous devices requires the selection of appropriate routing protocols, which is crucial for maintaining high Quality of Service (QoS). The Internet Engineering Task Force's Routing Over Low Power and Lossy Networks (IETF ROLL) working group developed the IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) to meet these needs. While the initial RPL standard focused on single-metric route selection, ongoing research explores enhancing RPL by incorporating multiple routing metrics and developing new Objective Functions (OFs). This paper introduces a novel Objective Function (OF), the Reliable and Secure Objective Function (RSOF), designed to enhance the reliability and trustworthiness of parent selection at both the node and link levels within IoT and RPL routing protocols. The RSOF employs an adaptive parent node selection mechanism that incorporates multiple metrics, including Residual Energy (RE), Expected Transmission Count (ETX), Extended RPL Node Trustworthiness (ERNT), and a novel metric that measures node failure rate (NFR). In this mechanism, nodes with a high NFR are excluded from the parent selection process to improve network reliability and stability. The proposed RSOF was evaluated using random and grid topologies in the Cooja Simulator, with tests conducted across small, medium, and large-scale networks to examine the impact of varying node densities. The simulation results indicate a significant improvement in network performance, particularly in terms of average latency, packet acknowledgment ratio (PAR), packet delivery ratio (PDR), and Control Message Overhead (CMO), compared to the standard Minimum Rank with Hysteresis Objective Function (MRHOF).

KEYWORDS: IoT; LLNs; RPL; objective function OF; MRHOF; OF0; routing metrics; reliability; trustworthiness

1 Introduction

Recently, many devices have seamlessly integrated into the Internet infrastructure, giving rise to the expansive and interconnected network known as the Internet of Things (IoT). The number of connected devices has exceeded the worldwide population and has exponentially increased [1]. Wireless sensors, smartphones, embedded systems, and other electronic devices are now linked to the Internet or local networks, heralding a new era of IoT. The number of IoT devices is anticipated to grow in the coming years. For instance, in 2023, Cisco projected over 500 billion IoT devices would exist [2]. IoT will significantly change areas such as weather tracking, smart cities, healthcare, factory operations, and homes, becoming more intelligent [3]. However, network management challenges have also increased, especially regarding selecting the appropriate



routing protocol to improve network performance and maintain significant security, reliability, and energy efficiency. IoT is classified as a Low Power Lossy Network (LLN) due to the limitations and restrictions of resources such as battery-powered sensors with limited data storage [4–6]. LLNs are a subset of Wireless Sensor Networks (WSNs) with limited resources in their routers and nodes, such as processing capability, battery capacity, and memory size. The instability and unreliability of links between nodes and security issues lead to high loss rates, low data rates, and reduced packet delivery rates. As a result, routing in LLNs presents a significant challenge, and any routing protocols developed for LLNs must consider and address these constraints. Recently, there has been increasing interest in LLN applications, leading to a demand for effective routing solutions for numerous low-cost and low-power embedded devices. Many organizations, as well as research studies, have made efforts to improve the routing protocol in several aspects, including security, reliability, energy efficiency, and others [7–10].

The Internet Engineering Task Force (IETF) accomplished a significant feat by creating the 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) specification, which offers guidelines for sending IPv6 data over LLNs. To improve routing in LLNs, the IETF formed the Routing over Low Power and Lossy Networks (ROLL) working group. This group was tasked with developing a better routing solution. They examined existing protocols such as DSR (Dynamic Source Routing), AODV (Ad hoc On-demand Distance Vector), OLSR (Optimized Link State Routing Protocol), and OSPF (Open Shortest Path First). Still, they found them ineffective for LLNs due to power usage, delay, excessive data, and reliability. Recognizing these challenges, the IETF meticulously designed the IPv6 routing protocol for LLNs, known as RPL [11]. This protocol was suggested as the primary routing standard for such networks. RPL provides IPv6 connectivity for battery-operated wireless devices that communicate using low-power radios. Although RPL is based on popular routing protocols such as CTP and Hydro used in the WSN domain, it has been developed and expanded to include IPv6 support. Over time, RPL has grown in sophistication. It is now the established routing protocol due to its versatility, support for different traffic patterns, and ability to deliver data with low overhead efficiently.

The fundamentals of RPL operation involve an objective function (OF) that uses one or more metrics to establish links between nodes, forming a network topology consisting of a root node, intermediate nodes, and leaf nodes. Based on the criteria defined by the OF, each node in the network transmits data until it reaches the root node. RPL has defined two standard objective functions, each relying on a single metric: Objective Function Zero (OF0), which uses hop count (HC) as its metric, and the Minimum Rank with Hysteresis Objective Function (MRHOF), which uses Expected Transmission Count (ETX) as its metric. Each OF is distinguished by its use of specific quantitative and qualitative metrics. The flexibility of RPL allows for easy switching between different OFs, making it a highly adaptable protocol. Moreover, new OFs can be integrated into RPL regardless of the metrics they utilize. As a result, RPL has become a vibrant area of research, with numerous OFs being proposed and their performances evaluated against the standard OFs. RPL also features local and global repair mechanisms, resilience to changes in the wireless medium, and loop prevention. These qualities make RPL popular for various LLN applications [12]. Although RPL has successfully resolved significant issues, some limitations, such as security and reliability, still require attention. RPL constructs a destination-oriented directed acyclic graph (DODAG) topology without considering the parent node's security and reliability. Consequently, issues such as insecure and unreliable nodes result in network vulnerabilities. In the standard RPL protocol, when constructing an RPL topology, a node selects its parent based on ETX or HC values without considering other aspects such as security, reliability, and energy efficiency.

This paper addresses the shortcomings above by proposing a novel objective function, the Reliable and Secure Objective Function (RSOF), which considers node and link reliability, security, stability, and

efficient resource use during the parent selection procedure in the RPL routing protocol. The proposed RSOF enhances the parent selection process, in which the node evaluates potential parent candidates based on their remaining energy, security level, and reliability, ultimately selecting the most optimal parent. This approach aims to enhance overall network performance while ensuring high security and reliability within the network topology. The proposed RSOF is evaluated and compared to the standard MRHOF in terms of Packet Delivery Ratio (PDR), Packet Acknowledgment Ratio (PAR), Control Message Overhead (CMO), and End-to-End (E2E) delay, demonstrating overall superior performance. Additionally, simulations are conducted across different network sizes 25, 50, 70, and 90 to examine the impact of both OFs on network performance. This work's contributions to the field are summarized as implementing the RPL routing protocol with a novel objective function, RSOF. This implementation incorporates new metrics, including residual energy (RE), Node Failure Rate (NFR), Extended RPL Node Trustworthiness (ERNT), Expected Transmission Count (ETX), and rank, which collectively enhance security, reliability, stability, and resource efficiency. Establishing a mechanism for communicating and broadcasting these new metrics within the DODAG Information Object (DIO) message is crucial for the system's efficient functioning and for implementing a parent selection process that leverages the newly introduced metrics.

The rest of the paper is organized as follows: [Section 2](#) provides a comprehensive background on RPL, covering its fundamental concepts, control messages, routing metrics, and objective functions (OFs). [Section 3](#) of the Literature Review covers related work on improving RPL OF to improve network performance. This section reviews studies proposing modifications and new OFs to address limitations in the standard RPL protocol and presents an in-depth analysis of recent efforts to refine RPL OF. It highlights the advancements and challenges these approaches address to achieve more robust and efficient network performance in various deployment scenarios. [Section 4](#) introduces the proposed RSOF and provides a detailed explanation of its design. The motivation behind developing the proposed RSOF stems from the limitations of existing OFs, and this section includes its mathematical formulation and operational description. [Section 5](#) presents the results obtained from evaluating the proposed RSOF and provides an in-depth discussion of these findings. This section details the performance improvements achieved by the new OF compared to existing ones, particularly MRHOF, under various network conditions and configurations. [Section 6](#) concludes the paper by summarizing the key contributions and the effectiveness of the proposed RSOF. It emphasizes how incorporating additional metrics such as Residual Energy (RE), Node Failure Rate (NFR), Extended RPL Node Trustworthiness (ERNT), and Expected Transmission Count (ETX) into the parent selection process can significantly enhance network performance and longevity.

2 Routing Protocol for Low-Power and Lossy Networks (RPL)

RPL is a proactive source routing protocol designed for LLNs, maintaining up-to-date routing information by establishing routes before data transmission is needed. This is achieved through the continuous exchange of control messages, ensuring that routes remain pre-established even when data transmission is not occurring. RPL operates as a distance vector and source routing protocol and is compatible with various link-layer technologies, such as IEEE 802.15.4 PHY and media access control (MAC) layers [13,14]. It is particularly well-suited for networks with many routers (nodes) and limited resources, addressing these networks' constraints and challenges. The protocol supports three types of traffic patterns: point-to-point (P2P) communication between nodes, point-to-multipoint (P2MP) communication for network configuration, and multipoint-to-point (MP2P) communication for data collection [15]. RPL's versatility in handling various traffic patterns, its efficiency in data delivery, and its low overhead make it an attractive option for LLNs. Additionally, RPL includes robust features such as local and global repair mechanisms and the ability to adapt to changes in the wireless medium, further enhancing its suitability for diverse LLN applications [12]. [Table 1](#) provides additional details on RPL's features.

Table 1: RPL protocol features

Feature	Description
Loop avoidance and detection	In RPL, the rank of any node must exceed that of its parent, which ensures the acyclic structure of the DODAG. RPL incorporates local and global recovery mechanisms for loop detection and topology recovery.
Self-configuration	Network pathways are generally identified dynamically by IPv6 neighbor discovery procedures.
Target networks	LLNs; 6LowPAN networks; other IPv6 networks.
Protocol type	Infrastructure protocol with distance vector and source routing capabilities
Link-layer mechanisms	Built on top of IEEE 802.15.4 PHY and MAC layers
Network size	Suitable for collection networks with up to thousands of routers (nodes)
Traffic flow support	Supports three traffic patterns: P2P, P2MP, MP2P
Network topology	Organizes the network as a Direct Acyclic Graph (DAG) rooted at the sink node (Mesh/hierarchical based on DAGs)
Objective function	Minimizes the cost to reach the sink node from any node in the network using an objective function
Mode of operation (MOP)	MOP (0): No downward routes MOP (1): Non-storing MOP (2): Storing MOP(3): Storing with multicast.

The fundamental concept of RPL involves structuring the network as a DAG with the sink node as the root [13]. The purpose is to minimize the cost of reaching the sink node from any given node in the network by employing an OF. The principle of DAGs dictates that it is not feasible for a path to exist where node X leads back to itself, thus ensuring no loops are formed. The RPL protocol establishes a network that follows a tree topology, representing the network structure as a DODAG. The DODAG serves as the central component of the RPL protocol and is rooted at a singular destination, commonly referred to as the sink node. This sink node is characterized by its lack of outbound edges, as shown in Fig. 1. In RPL, the formation of the DODAG is influenced by link costs and node attributes, collectively used to calculate the path costs. Link costs and node attributes may encompass several aspects, such as energy resources, throughput, latency, hop count, and dependability. In essence, the primary purpose of RPL is to reduce the expenses associated with traversing a given path, namely the path from the source node to the sink node, which is achieved by utilizing an objective function [13]. The RPL protocol establishes and describes its topology using four identifiers or instance values. These identifiers include the instance ID, DODAG ID, DODAG version number, and rank. Specifically, each node in the RPL protocol can be distinctly recognized using four instance variables. The RPL instance is utilized to identify the DODAGs with a standard service type, also known as an objective function. Nodes with a common root are associated with the same DODAG identifier. The version number of the DODAG is modified whenever there is a modification in the topology of the DODAG. The rank parameter is utilized to denote the relative distance between a node and the root in the RPL protocol. It is of significant importance to the nodes within the network. Nodes with lower ranks are indicative of their

proximity to the root. A certain DODAG is distinguished in the network by combining the RPLInstanceID and DODAGID [12].

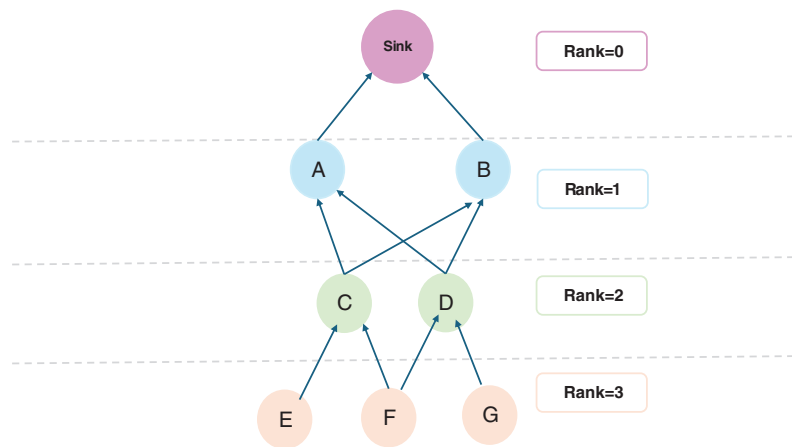


Figure 1: RPL DODAG

RPL employs four distinct control messages, transmitted to maintain the routing topology and update routing information; Table 2 shows the types of control messages in the RPL protocol. A specific code identifies each RPL control message and consists of a base structure that depends on the message type, along with optional fields that will be used to include the new metrics of the proposed RSOF. The structure of an RPL control message consists of an ICMPv6 header, followed by a message body, which contains the base message and potentially several options, as shown in Fig. 2. These control messages are classified as ICMPv6 informational messages, with a designated Type of 155 [11].

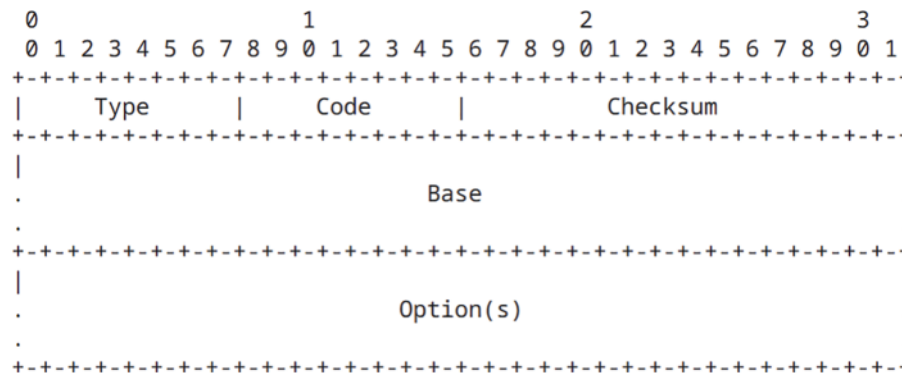
Table 2: Control messages in the RPL protocol

Control message	Description
DODAG Information Object (DIO)	-Abbreviation: DIO - Code: 0x01 - Sending time: Periodically - The DIO message contains critical information, including an RPL Instance, configuration settings, and a DODAG parent set for the maintenance or reconstruction of the DODAG.
DODAG Information Solicitation (DIS)	- Abbreviation: DIS - Code: 0x00 - Sending time: Joint event - A node seeking to join a DAG uses a DIS message to request a DIO from an RPL node.
Destination Advertisement Object (DAO)	- Abbreviation: DAO - Code: 0x02 - Sending time: Event base

(Continued)

Table 2 (continued)

Control message	Description
Destination Advertisement Object	- A DAO message facilitates the upward transmission of destination information via the DODAG to the sink node. It serves to indicate the distance to the sink. - Abbreviation: DAO-ACK - Code: 0x03 - Sending time: DAO reply
Acknowledgment	- A DAO recipient sends a unicast packet in response to a unicast DAO message.

**Figure 2:** RPL control messages format

The performance of RPL heavily depends on routing metrics, which play a crucial role in evaluating the cost of paths and determining the most efficient route within the network. RPL can employ either a single metric or a combination of metrics and constraints, depending on the specific implementation [15,16]. These routing metrics vary in characteristics, including link or node factors, qualitative or quantitative nature, and static or dynamic behavior. It is essential to differentiate between routing metrics and constraints: while metrics help select paths based on specified conditions like reliability, constraints are used to avoid undesirable paths, such as those with unreliable links. The selection of metrics or constraints is based on the requirements of the specific RPL deployment.

Given the dynamic nature of LLNs, routing metrics must adapt to changing conditions. For instance, node-based metrics such as RE evolve during network operation as nodes continuously deplete their energy reserves. Consequently, RPL's path selection must account for these dynamic changes to maintain efficiency and stability [16]. Table 3 summarizes the routing metrics used in RPL.

Table 3: Summarizes the routing metrics used in RPL

Metric type	Metrics	Description	Application
Link metrics	RSSI (Received Signal Strength Indicator)	Evaluates signal strength, frequency, and voltage in the physical layer.	Determines signal availability before data transmission.
	LQI (Link Quality Indicator)	Measures link reliability on a scale of 0 to 7.	Indicates link quality level.
	ETX (Expected Transmission Count)	Calculates transmissions needed for acknowledgment.	Indicates network reliability; lower value signifies optimal path.
Node metrics	Energy	Quantifies energy consumption during node operations.	Important for designing energy-efficient networks; considers residual energy.
	HC (Hop Count)	Measures path length based on the number of hops.	Commonly used but disregards link quality.
	End-to-end Delay	Determines time for packets to travel sender to sink.	Critical for real-time applications; ensures timely data transmission.

One of the significant challenges in RPL is constructing the network topology as a DODAG. RPL forms this topology based on the OF, which guides each node in selecting the optimal parent from a set of potential candidates. The OF incorporates factors such as the spatial placement of nodes, link characteristics, and other constraints to determine each node's rank within the DODAG. The selection of an OF plays a critical role in shaping the network topology and significantly influences the performance of RPL. As the network evolves, the path cost is periodically recalculated to reflect changes, such as updates in the selected metrics or the reception of new metric advertisements. The effectiveness of the routing protocol in RPL is rooted in three key components [15]:

1. The selected metric, which determines the path choice,
2. The path cost, which measures the quality of the path, and
3. The best parent is the node offering the most optimal path.

The IETF ROLL working group has standardized two primary OFs for RPL: Objective Function Zero (OF0) and the Minimum Rank with Hysteresis Objective Function (MRHOF) [17]. OF0 selects the nearest parent node to the root within the DODAG, using HC as its routing metric to minimize latency by reducing the number of intermediate nodes. However, this simplicity comes with limitations, as OF0 does not consider link quality, which can lead to packet loss, nor does it account for load balancing in RPL networks. In contrast, MRHOF reduces network instability by incorporating the ETX metric alongside the number of intermediate nodes. ETX calculates the number of transmissions required for a sender to receive an acknowledgment from the recipient successfully. Each node tracks ETX values for its neighboring nodes and selects paths that minimize the total ETX across links, optimizing route efficiency. Despite its advantages in improving path reliability, MRHOF may overload nodes with higher link quality during periods of heavy traffic.

3 Literature Review

Researchers have made significant advancements in the Routing Protocol for Low-Power and Lossy Networks (RPL) by incorporating suitable routing metrics and developing new Objective Functions (OFs) to meet the diverse requirements of Internet of Things (IoT) applications. These enhancements are crucial for optimizing network performance and reliability in various IoT contexts. An in-depth examination of these developments is captured in the literature review presented in [Table 4](#), which summarizes the efforts to create new OFs for RPL, highlighting their objectives and key outcomes.

Most of the existing literature attempts to overcome the single metric limitation of RPL. In 2013, Kamgueu et al. [18] was among the first to propose a routing approach that overcame single metrics with three key metrics: ETX, delay, and energy, to determine the most suitable route by generating a quality measure for candidate parents. Building on this pioneering work, Olfa Gaddour et al. [19] advanced the concept by introducing OF-FL (Objective Function based on Fuzzy Logic). This objective function considered four metrics, HC, E2E delay, link quality, and energy, employing fuzzy logic to compute the quality of the optimal parent node. Simulation comparisons against standard RPL OF demonstrated notable enhancements in network lifetime, PDR, and reduced parent change frequency with OF-FL. To optimize routing decisions, [20] proposed an opportunistic fuzzy logic-based objective function, introducing a novel metric called Children Number through fuzzy logic. This new metric combines HC and ETX metrics. Additionally, [21] introduced OF-FZ, employing four metrics, ETX, HC, RE, and delay, to achieve superior PDR, reduced latency, power consumption, and traffic overhead. Further innovations in objective functions came with [22,23], who proposed OF-EC, a novel approach that fuses three metrics, EC, ETX, and HC, using fuzzy logic. The composite metric derived from OF-EC was employed for routing decisions, resulting in notable improvements in network convergence time, energy consumption, latency, routing overhead, PDR, and network lifetime within RPL implementations. In [24], the authors endeavored to identify an optimal approach for mitigating energy consumption in mobile base stations. They employed a fuzzy clustering technique that considers three crucial parameters: energy sensor, distance sensor from the sink, and cluster-centric priorities. The investigation outcomes demonstrate a notable enhancement in the base station's lifetime due to its mobility. In [25], the paper introduces a novel approach called OFRRT-FUZZY, an enhanced objective function for WSNs that combines multiple metrics for more effective routing decisions. The metrics utilized in OFRRT-FUZZY include RSSI, RE, and throughput (TH). Simulation results demonstrated the superiority of OFRRT-FUZZY over OF0, highlighting its promising performance in enhancing the routing efficiency in WSNs. In [26], the authors introduce a novel Fuzzification with a Machine Learning (FML) algorithm designed to select the most suitable parent nodes in MP2P topology. Through simulations, they demonstrate that the algorithm achieves an impressive 89% accuracy in prediction using the Random Forest (RF) classifier, outperforming other classifiers such as SVM (Support Vector Machine) and kNNs (k-Nearest Neighbors).

In [27], a novel RPL-CGA approach is proposed, which employs a chaotic genetic algorithm to determine the optimal weighting factors in the composite metric. This method considers five metrics: queue length, delay, RE, HC, and ETX, resulting in reduced power consumption. Similarly, authors in [28] introduce the EEOPS-RPL version of RPL, leveraging the firefly optimization algorithm to enhance performance. The attractiveness parameters ETX and RE, along with the movement parameter of the distance between nodes, are used to select the optimal parent in the DODAG. EEOPS-RPL offers faster convergence and extended network lifetime. In [29], Preeth et al. propose E-RPL, an ant colony optimization-based RPL implementation. This method incorporates the number of children, RE, ETX, and rank value as heuristic and pheromone factors. The child-parent relationship signifies the pheromone evaporation factor. By combining these factors using weights, an objective function is derived to optimize the routing process and detect

rank attacks in RPL. In a recent approach [30], the Equilibrium Optimizer-RPL (EO-RPL) protocol is provided, which picks the preferred parent using an optimization technique known as the Equilibrium Optimizer (EO) algorithm, which is based on composite metrics, EC, ETX, and HC, through a DIO control message. Simulation results show that EO-RPL outperforms other protocols, such as Energy-based Path Cost-RPL (EPC-RPL), Energy Efficient RPL (E-RPL), and Energy Efficient Optimal Parent Selection-RPL (EEOPS-RPL), in terms of PDR, CMO, E2E delay, and EC.

A new objective function called EEQ is presented in [31]. EEQ uses ETX, EC, and queue length metrics to achieve its primary goal: to keep bottlenecked nodes in the network running smoothly and directly sending data to their destination. When evaluated in different network densities, EEQ reduces overhead communication compared to standard methods. However, more than relying on one factor (traffic loads) to assess the entire process is required. Other important factors like energy consumption, network lifetime, and network stability should also be considered. In [32], researchers proposed a new protocol called EL-RPL to make the network last longer. They used three criteria, load, battery depletion index (BDI), and ETX, and combined them. The goal was to find the best parent node for routing based on these three metrics. EL-RPL improved the PDR and increased the network's lifetime compared to the OF-FL RPL protocol, which uses fuzzy logic. However, the comparison between EL-RPL and OF-FL is limited because they use different methods, and the fuzzy logic approach requires more calculations. In the research presented in [33], the authors propose an enhancement to the RPL protocol specifically designed for innovative grid applications, incorporating both parent-oriented (PO) and interface-oriented (IO) solutions. They introduce a hybrid metric that takes into account three critical parameters for rank computation: the rank of the potential parent node ($R(p)$), the link quality level (LQL), and the expected transmission time (ETT). Through the additive combination of these metrics, the PO and IO solutions outperform the single interface approach, demonstrating improved performance regarding reduced parent changes, decreased E2E delay, and increased PDR. However, it is worth noting that while these solutions offer benefits, they may only partially guarantee reliability and low latency, as they need to consider the presence of duplicated packets that may be transmitted in the network. In [17], they introduce a method to enable multi-criteria-based routing in the RPL. They employ the widely recognized VIKOR Multi-Criteria Decision Making (MCDM) technique to achieve this. Using the VIKOR method, each route link identifies the most suitable parent for routing purposes. Through simulations, they demonstrate that the approach improves QoS in various aspects, including average energy consumption, E2E delay, PDR, and throughput.

In [34], they introduce a novel objective function named Time OF (T-OF) to enhance the network lifetime by achieving a balance in node energy. The T-OF utilizes a weighted combination of three metrics: energy, ETX, and Number of Children and Siblings (NOCS). Comparative analysis with MRHOF, OF0, and Energy Objective Function (EN-OF) demonstrates that the proposed T-OF significantly improves network lifetime and energy balancing. The experimental results show lower delay and a PDR. The authors in [35] introduce a modified routing protocol named Maximum Number of Parent Objective Function (MNP-OF). The MNP-OF utilizes a novel node metric called the Neighboring metric (N-metric). The proposed protocol, MNP based on Remaining Energy (MRE), combines N-metric with the node's remaining energy metric for all nodes to the root node, aiding in selecting the preferred path. The experimental results demonstrate that MRE achieved significant energy savings of up to 94% compared to the RPL protocol in medium- and large-scale networks. Additionally, in small-scale networks, MRE exhibited a reduction of approximately 33% in average remaining energy. Moreover, MRE showed notable reductions in average delay and dead nodes, coupled with improved throughput, control messages, and switching parents in large-scale networks.

In a study [36], the researchers introduce a novel objective function that aims to balance the number of children nodes for heavily burdened nodes, ultimately maximizing their lifetime. To implement this OF,

they made modifications to the DIO message format. They also utilized a new technique to reduce any potential additional overhead. A new RPL metric was introduced to distribute the traffic load evenly across the network. Simulation experiments were conducted to evaluate the performance of this new approach. The collected results confirm that the proposed objective function outperforms existing ones in terms of node lifetime, power consumption, and PDR. In the same context of loading balance, the author in [37] proposed the Load Balanced Minimum Rank with Hysteresis Objective Function (LB_MRHOFF) improves RPL-based networks by optimizing parent selection using a new metric, Composite ETX, and Number of Children (CENOC), which combines ETX and the number of children to estimate node load. By avoiding nodes with high CENOC, LB_MRHOFF ensures a more balanced network. It outperforms existing Objective Functions like MRHOFF, OF_FUZZY, and OF-EC in PDR and HC, especially in large-scale networks, without increasing energy consumption. In research [38], the authors introduced two new objective functions: the Weighted Combined Metrics Objective Function (WCM-OF) and the Non-Weighted Combined Metrics Objective Function (NWCM-OF). These functions consider both link quality ETX and the current node's energy consumption as metrics, and they can be weighted equally or not to find a balance between reliability and energy savings. The procedure to implement these new objective functions is as follows: when a node receives a DIO message from its parent, it updates the link quality metric and power consumption. Then, it calculates a new combined metric using these values and forwards this information to its neighbors through DIO messages. The goal is to find paths to the root node with the lowest sum of combined metrics. The researchers tested these new objective functions using the Contiki operating system and the Cooja emulator. The results showed that the proposed objective functions improved the network's overall performance compared to the default objective functions.

Other research efforts have focused on enhancing parent selection in RPL through machine learning. In [39], the authors introduced ML-RPL for Wireless Smart Grid Networks. This model employs machine learning to predict successful delivery probabilities based on metrics such as ETX, HC, and RSSI. It has shown significant improvements in PDR and reductions in E2E delays, though it faces challenges with system overload. Additionally, in [40], the authors utilized Random Forest analysis to enhance parent selection by assessing the importance of features like ETX and throughput, aiding in the selection among equally ranked candidates. While this approach has improved PDR, it has struggled with adaptability under varying load conditions due to static weight assignments in its scoring function.

In further developments, Kuwelkar et al. [41] enhanced RPL performance by integrating multiple criteria metrics such as HC, delay, RE, and ETX using the k-Nearest Neighbor technique. This method assigns quality scores to neighboring nodes, facilitating optimal parent node selection. The results demonstrated marked improvements in energy efficiency, PDR, delay, and CMO.

Table 4: A summary of literature review developing new OFs for RPL

Reference	Routing approach	Objective	Routing metrics	Key outcomes
[18]	Fuzzy logic	Determine the most suitable route	ETX, Delay, Energy	Improved network energy distribution and packet reception rates compared to the ETX scenario

(Continued)

Table 4 (continued)

Reference	Routing approach	Objective	Routing metrics	Key outcomes
[19]	Fuzzy logic	OF-FL to compute the quality of the optimal parent node	HC, E2E Delay, Link Quality, Energy	Improved Network Lifetime, PDR, Reduced parent change frequency
[20]	Opportunistic fuzzy logic	Novel metric: Children number	HC, ETX	Enhanced routing decisions
[21]	Fuzzy logic	Propose a novel objective function OF-FZ	ETX, HC, RE, Delay	Improved PDR, Reduced latency, Lower power consumption, Reduced traffic overhead
[22,23]	Fuzzy logic	New objective function OF-EC	EC, ETX, HC	Enhanced network convergence time, Reduced EC, Lower latency, Reduced routing overhead, Improved PDR, Extended network lifetime
[24]	Fuzzy clustering	Approach for mitigating energy consumption in mobile base stations	Energy Sensor, Distance Sensor from Sink, Cluster-Centric Priorities	Enhanced Base Station Lifetime due to mobility
[25]	Fuzzy logic	OFRRT-FUZZY, an enhanced Objective Function for WSNs	RSSI, RE, TH	Superior routing efficiency demonstrated over OF0
[26]	Fuzzification with machine learning	FML Algorithm to select the most suitable parent nodes in MP2P topology	RSSI, Expected Lifetime (ELT)	Accuracy in parent node selection using RF classifier Outperformed SVM and kNNs

(Continued)

Table 4 (continued)

Reference	Routing approach	Objective	Routing metrics	Key outcomes
[27]	Chaotic Genetic Algorithm (CGA)	A novel approach (RPL-CGA) to determine optimal weighting factors in the composition metric	Queue length, Delay, RE, HC, ETX	Reduced power consumption
[28]	Firefly optimization	Proposes energy efficient optimal parent selection in RPL (EEOPS-RPL)	ETX, RE, Distance between nodes	Improves the packet transmission ratio and lifespan of the network
[29]	Ant colony optimization	Proposes an energy efficient RPL (E-RPL)	Children Number, RE, ETX, Rank Value	Optimized routing process by Improving packet delivery ratio and energy consumption
[30]	A novel optimization method known as an EO algorithm	Propose an equilibrium optimizer-RPL (EO-RPL) protocol that selects the preferred parent	ETX, EC, HC	Optimized routing process by PDR, CMO, E2E delay and EC
[31]	Calculus-based	Proposed an OF (EEQ) to protect the node that has already excessively consumed its energy	ETX, EC, Queue length	Reduced overhead communication compared to standard methods
[32]	Calculated based	Propose Energy and Load aware RPL (EL-RPL) protocol	Load, BDI, ETX	Improved PDR and increased network lifetime compared to OF-FL

(Continued)

Table 4 (continued)

Reference	Routing approach	Objective	Routing metrics	Key outcomes
[33]	Additive combination	Propose an enhancement to the RPL protocol specifically designed for smart grid applications	LQL, ETT	reduce parent changes, decrease E2E delay, and increase PDR, but do not account for duplicated packets
[17]	VIKOR multi-criteria decision making	Propose a novel MC-RPL to improve RPL	ETX, HC, delay and energy	Improved QoS in terms of average EC, E2E delay, PDR, and throughput
[37]	Additive combination based.	Design of a load balancing Objective Function for RPL (LB_MRHOF)	ETX and Number of Children (CENOC)	outperforms MRHOF, OF_FUZZY, and OF-EC in PDR and HC, especially in large-scale networks, without increasing energy consumption
[38]	Additive combination based.	Propose two objective functions, WCM-OF and NWCM-OF, to improve RPL	ETX, EC	Improved overall network performance compared to default OFs
[39]	ML-based	Optimize parent selection in RPL	ETX, HC, Mac losses, Channel utilization, Queue utilization, Density, RSSI, Throughput	Significant improvement in PDR and end-to-end delay
[40]	ML-based	Novel parent selection strategy for RPL	ETX, Mac losses, Channel utilization, Throughput	Significant improvement in PDR compared to standard RPL across networks of various sizes
[41]	ML-based	Enhance RPL performance	HC, Delay, RE, ETX	Improved EC, PDR, delay, and control overhead

4 Proposed Reliable and Secure Objective Function (RSOF)

This section outlines the motivation behind this paper and highlights the features of the proposed OF. The novel Reliable and Secure Objective Function (RSOF) aims to improve network performance by extending network lifetime and enhancing average latency, PAR, PDR, and CMO. This is achieved by

selecting an optimal parent node based on optimal remaining energy, security level, and reliability compared to other nodes.

4.1 Motivation

The primary objective of this paper is to propose a novel Objective Function (RSOF) that considers multiple aspects of the parent selection process in RPL networks to optimize network performance. As illustrated in Fig. 3a, DAG is constructed based on metrics such as rank and ETX. For example, nodes C and D have two potential parent candidates, A and B. If only rank and ETX are considered, both nodes might select Node B as the optimal parent. However, this could lead to suboptimal results if other critical metrics, like RE and ERNT, are ignored. If Node B has significantly lower RE and ERNT than Node A, the communication between Node B and its children, C and D, could fail due to Node B's depleted energy and reduced security level. Similarly, if Node B has a higher NFR than Node A, packet loss would increase, and overall network reliability would decrease. When Node B frequently fails, nodes may consume more energy to reroute packets or maintain connectivity. This also results in increased CMO in the network due to repeated route recalculations, which can reduce the available bandwidth for data transmission. These challenges highlight the necessity of a more comprehensive approach to parent selection. Rather than basing the selection solely on rank and ETX, incorporating additional metrics such as RE, NFR, ERNT, and ETX can lead to more robust parent selection and, consequently, better overall network performance.

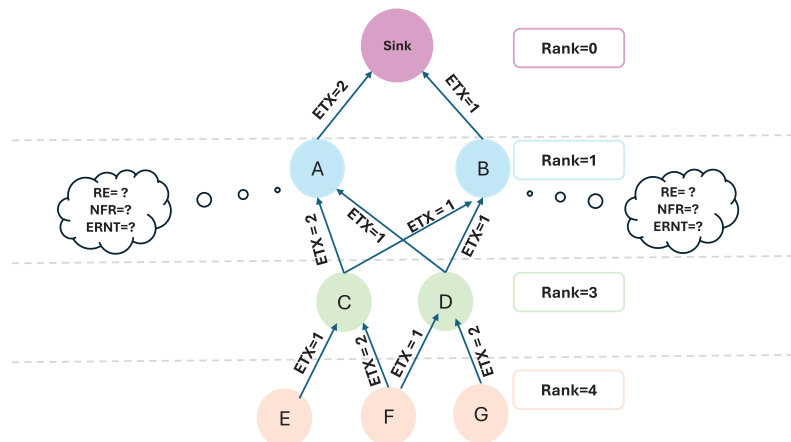


Figure 3: DODAG construction and parent selection

4.2 Proposed RSOF Formulation and Description

The proposed RSOF implementation procedure includes many steps: First, implement the RPL routing protocol with a new objective function to include the new metrics. RE, NFR, ERNT, ETX, and rank. As explained in Table 3, RPL metrics are categorized mainly into node-based and Link-based Metrics. RSOF is designed to enhance the reliability and trustworthiness of parent selection at both node and link levels within IoT, where ETX measures link transmission reliability, our novel metric NFR measures the node reliability, and ERNT evaluates the trustworthiness of each node within the network. Table 5 summarizes the new metrics introduced in the RSOF. Second, the next step is to implement the communication and broadcast of the new metrics within the DIO message, a pivotal element for the system's effective operation. Third, implement the parent selection process, which uses the new metric as a key factor in decision-making.

In the following scenario, nodes must select the best parent based on various metrics related to network protocols RPL. A decision-making process in which the algorithm evaluates potential parent nodes based on their acceptability and specific thresholds (RE, NFR, and ERNT). It compares two parents (p1 and p2) at a time, considering factors like ETX and other thresholds (RE, NFR, ERNT), and then selects the best parent node to ensure optimal routing or connectivity. During the first phase of network setup, the border router broadcasts DIO messages that include details such as rank, the identity of the DODAG, version number, and the OF. Upon receiving DIO messages from the border router, each node computes a rank based on the Eq. (1) and Eq. (2).

$$\text{Rank (K)} = \text{Rank}(\text{parent}) + \text{Rank_increase} \quad (1)$$

where the rank for each node is calculated based on the parent's rank plus the rank increase that is calculated as Eq. (3).

$$\text{Rank_increase} = \text{MinHopRankIncrease} \times \text{steps} \quad (2)$$

Table 5: Summary of new metrics introduced in RSOF

Metric	Description	Application
Expected Transmission Count (ETX)	link-based metric, calculated for the link between a node and its parent using Eq $\frac{1}{d_f \times d_r}$, where d_f and d_r are the probabilities of successful forward and reverse transmissions, respectively.	Indicates network reliability.
Extended RPL Node Trustworthiness (ERNT)	Node-based metric, Evaluate the trustworthiness of each node within the network, ERNT is calculated using nodes behaviors components: selfishness, energy Eq. (10)	Indicates network security
Node Failure Rate (NFR)	Node-based metric, Calculates and evaluates the reliability of node, NFR for a node is given by Eq. (8).	Indicates node Reliability
Residual Energy (RE)	Node-based metric, Calculates and evaluates the amount of energy remaining in a device's battery at any given point in time, RE is calculated from Eq. (6)	To manage and optimize the energy consumption

The standard value of MinHopRankIncrease is 256, totaling three steps. The DODAG root facilitates the MinHopRankIncrease for the construction of the DAG. The rank's integer portion identifies loop detection or establishes the child-parent node relationship. The integer portion of the rank can be calculated using DAGRank(), as defined in Eq. (3).

$$\text{DAGRank}(\text{Rank}) = \left\lfloor \frac{\text{Rank}}{\text{MinHopRankIncrease}} \right\rfloor \quad (3)$$

where $\text{floor}(x)$ denotes the function that identifies the greatest integer less than or equal to x . The topology can be designed such that the root node must possess a minimum rank, and all parent nodes must have a rank lower than that of their child nodes.

Using routing metrics and constraints, RPL generates DAGs. The DIO message is used to advertise these metrics and constraints, as outlined in [11]. The options field of the RPL DIO packet carries these routing metrics and constraints. Multiple metrics and constraints can be included in the option field, allowing an OF to define the best path for routing. The proposed RSOF defines various metrics, such as RE, HC, ETX, NFR, and ERNT. The Options field of the conventional DIO packet is utilized to carry information about these new metrics, as outlined in RFC 6550 [11]. The process of the proposed RSOF is illustrated in the accompanying flowchart in Fig. 4, with a detailed step-by-step description provided below.

Upon the construction of the topology, each node will regularly broadcast DIO messages containing their Rank, NFR, ERNT, RE, ETX, HC, and the identity of the DODAG:

- **Step 1.** Each node identifies its neighboring nodes by frequently received DIO messages, which include information about Rank, NFR, ERNT, RE, ETX, HC, and the identity of the DODAG.
- **Step 2.** A node produces a parent candidate set from its neighboring nodes.
- **Step 3.** Each node conducts a parent node selection procedure initially, and if there is a modification in its knowledge of the parent candidate.
- **Step 4.** In the first case, the process begins with initializing a variable that is best to null.
- **Step 5.** The process checks if more neighboring nodes are available to evaluate as potential parents.
- **Step 6.** The process checks if p1 and p2 meet the criteria to be considered an acceptable parent according to Eq. (4).

$$\text{link_metric} \leq \text{MAX_LINKd_METRIC} \&\& \text{path_cost} \leq \text{MAX_PATH_COST} \quad (4)$$

- **Step 7.** The process checks whether both p1 and p2 have acceptable thresholds(RE,NFR,ERNT), or if neither does. The RE threshold represents the minimum acceptable energy level required for the parent node to be considered viable, according to Eq. (5).

$$RE(pk) < RE_{TH} \quad (5)$$

where $RE(pk)$ is the residual energy of the parent node pk . RE can be calculated from Eq. (6).

$$RE = \text{Initial}_{\text{Energy}} - \text{Consumed}_{\text{Energy}} \quad (6)$$

The NFR threshold represents the maximum acceptable failure rate for the parent node to be considered viable. If $p \rightarrow \text{NFR}$ is less than NFR_TH , it indicates that the parent node's failure rate is within acceptable limits according to Eq. (7).

$$NFR(pk) < NFR_{TH} \quad (7)$$

where $NFR(pk)$ is the node failure rate of the current parent and a threshold value for deciding when to perform parent switching. The NFR for a node pk is given by Eq. (8).

$$NFR = \frac{N_{\text{failed Packet}}}{N_{\text{total Packet}}} \quad (8)$$

where $N_{\text{failed Packet}}$ is the number of packets that failed to be transmitted successfully, and $N_{\text{total Packet}}$ is the total number of packets transmitted.

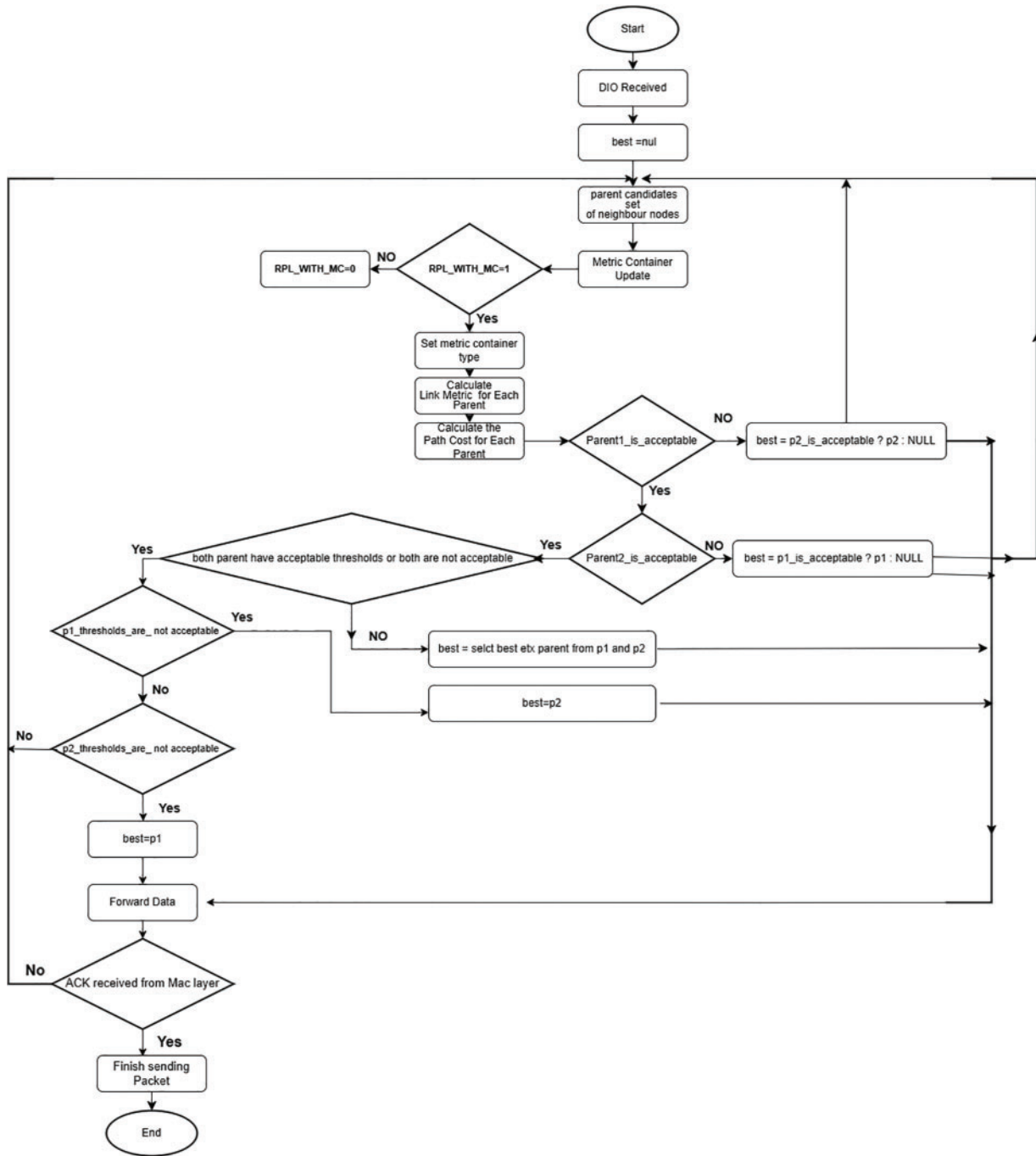


Figure 4: Process of the proposed RSOF

The ERNT threshold represents the minimum acceptable security level for the parent node to be viable. If $p \rightarrow \text{ERNT}$ is more than ERNT_{TH} , it indicates that the parent level of security is within acceptable limits according to Eq. (9).

$$\text{ERNT}(pk) > \text{ERNT}_{\text{TH}} \quad (9)$$

ERNT(pk) is the Extended Node Trustworthiness of a current parent and a threshold value for deciding when to perform parent switching. The ERNT for a node pk as evaluated by node k at time t is given by Eq. (10).

$$ENTR = w1(RemainingEnergy) + w2(1 - Selfishness) \quad (10)$$

The process will evaluate the thresholds of p1 and p2 according to Eq. (11).

$$IFRE(pk) < RE_{TH} \text{ and } NFR(pk) < NFR_{TH} \text{ and } ERNT(pk) > ERNT_{TH}; \text{ THEN Minimize } ETX(K, pk) \quad (11)$$

- **Step 8.** After comparing p1 and p2 based on their acceptability and thresholds, the process selects the best parent node accordingly.
- **Step 9.** The process loops back to check if more neighbors are available for evaluation. If no more neighbors are left, the process terminates, with the best being the selected parent.
- **Step 10.** After selecting the parent node, the data will be sent to the chosen parent node.
- **Step 11.** The receipt of an acknowledgment packet from the MAC layer indicates that the parent node has successfully received the packet.
- **Step 12.** If the MAC layer does not provide acknowledgment, the packet may be lost, necessitating retransmission. Consequently, the procedure will be repeated by returning to step 2.

5 Performance Evaluation and Criteria

5.1 Simulation Environment

To evaluate the proposed RSOF, we conducted experiments using the Cooja Simulator running on the Contiki-NG operating system (OS). For benchmarking purposes, the standard MRHOF, which employs the ETX metric, was used as a reference to compare the proposed RSOF's performance. This setup allowed for a thorough assessment of the improvements introduced by the RSOF compared to the conventional MRHOF.

We used the Cooja Unit Disk Graph Medium (UDGM) channel model, which accounts for lossiness based on the relative distances between nodes in the radio medium. The simulations were run for 60 min. Two different topologies were considered: a random topology and a grid topology consisting of one DODAG root and multiple client nodes.

In both topologies, the number of client nodes varied from 25 to 50, 70, and 90. The packet reception ratio (RX) was set to 100%; RX means the rate of successful packet reception at the receiver. Table 6 outlines the parameter values and configurations used for these simulations, ensuring consistency and reliability in performance comparison.

5.2 Performance Evaluation Criteria

This section discusses the evaluation performance criteria and parameters that are considered indications for evaluating the performance of the proposed RSOF. This paper focuses on the most significant parameters of network performance: PDR, PAR, E2E delay, and CMO. Table 7 summarizes the key metrics definition and formula.

Table 6: Simulation configurations and parameters

Parameter	Value
Simulator	Cooja Contiki-ng
Radio medium	UDGM
TX ratio	100%
TX range	50 m
INT range	60 m
RX ratio	100%
Number of nodes	25, 50, 70, 90
Area (m × m)	300 × 300
Simulation time	1 h (7200s)
MAC	802.15.4
OF	RSOF, MRHOF
Routing protocol	RPL
RPL example	RPL UDP
Topology	Random, Grid

Table 7: Summarizing evaluation performance key metrics definition and formula

Metric	Description	Equation
Packet Delivery Ratio (PDR)	The ratio of packets received by the sink to packets transmitted by source nodes.	$PDR(\%) = \left(\frac{\sum \text{Pkt}_{\text{received}}}{\sum \text{Pkt}_{\text{Sent}}} \right) \times 100$
Packet Acknowledgment Ratio (PAR)	is a networking metric to evaluate data transmission reliability. It refers to the ratio of packets successfully acknowledged by the receiver to the total number of packets sent by the sender.	$PAR(\%) = \left(\frac{\text{Pkt}_{\text{ack}}}{\text{Pkt}_{\text{Sent}}} \right)$
End-to-end delay	Average delay for each packet transmitted from a source node to the root.	$Avg_delay(\text{ms}) = \frac{\sum (T_r - T_s)}{R}$ where: T_s: The sent time of the packets by the source nodes, T_r: The received time of the packets at the sink, and R: The number of received packets.
Control Message Overhead (CMO)	Total number of control messages (DAO, DIO, and DIS) produced by the nodes.	$\text{Control overhead} = \sum_{k=1}^N DIO_k + \sum_{k=1}^N DAO_k + \sum_{k=1}^N DIS_k$ where, N is the number of nodes.

5.3 Result and Discussion

The proposed RSOF was assessed against the standard MRHOF, highlighting enhancements in reliability, trustworthiness, and critical evaluation metrics such as PDR, PAR, delay, and CMO. This section

compares RSOF and MRHOF across different network sizes and topologies to assess their efficiency under light—and heavy-load network conditions. Fig. 5a illustrates the network model featuring various deployed nodes arranged in a random distribution, and Fig. 5b illustrates nodes arranged in a grid topology. The following subsections present an analysis of the results and extract significant insights from each OF according to the evaluation metrics.

5.3.1 Random Topology Evaluation

Packet Delivery Ratio (PDR)

The data in Table 8 and Fig. 6 indicate notable variations in the performance of RSOF and MRHOF regarding PDR across different node groups. PDR repeatedly declines with increasing network density. The consequence is consistent with expectations, as increased network density tends to increase communication distances between nodes and the root, subsequently raising the probability of congestion, contention, and packet collisions. The main factor contributing to this issue is the increased transmission of control packets, resulting in a higher data packet loss rate. As a result, there is a significant decrease in the quantity of data packets successfully transmitted to the DODAG root.

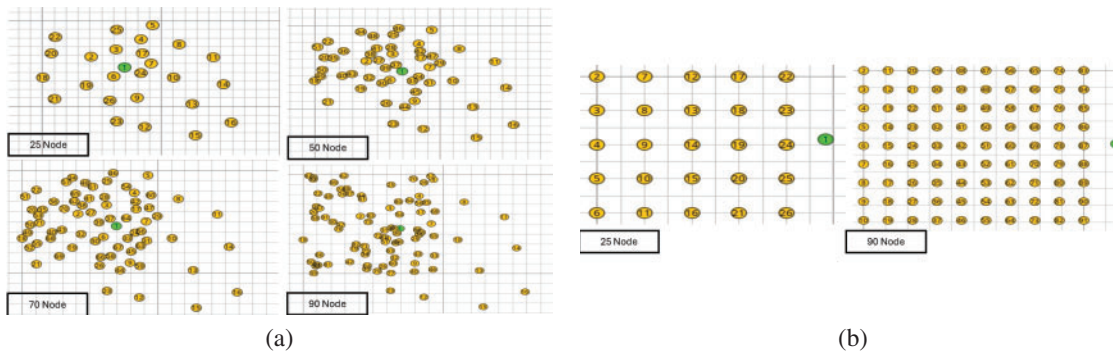


Figure 5: IoT topology with varying node densities: (a) Random topology with 25, 50, 70 and 90 nodes. (b) Grid topology with 25 and 90 nodes

Table 8: PDR for RSOF and MRHOF in different node density

Node density	RSOF	MRHOF
25	100	99
50	99	99
70	99	99
90	98	97
Avg	99	98

In the smallest group of 25 nodes, RSOF demonstrates a PDR of 100%, surpassing MRHOF's 99%. This suggests RSOF may be marginally more effective at sustaining PDR in low-density networks. Furthermore, as the number of nodes increases, RSOF continues outperforming MRHOF. For the group of 90 nodes, RSOF achieves a PDR of 98%, while MRHOF achieves 97%. This suggests that RSOF demonstrates superior capability in managing elevated network densities while ensuring reliable data transmission amidst increased network load.

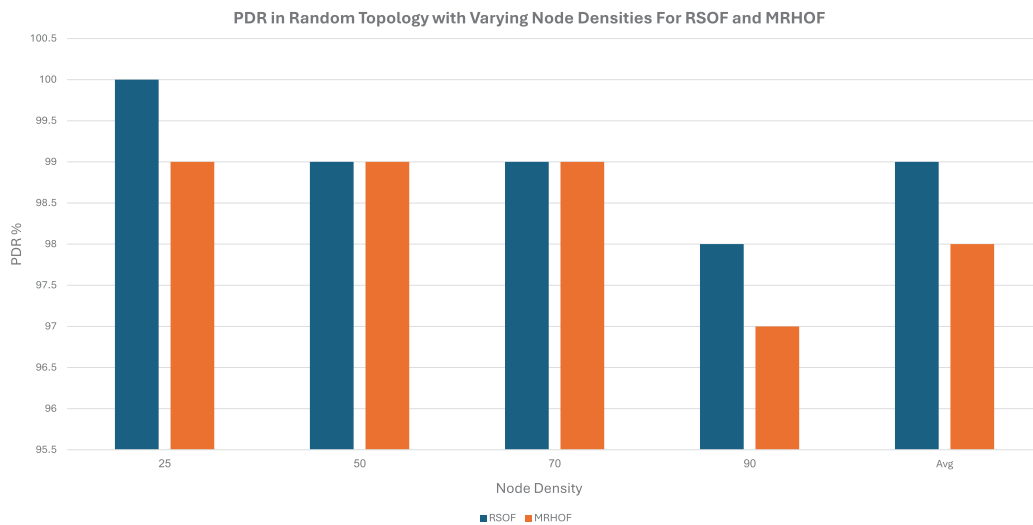


Figure 6: PDR Performance in random topology with varying node densities

In networks comprising 50 to 70 nodes, RSOF and MRHOF exhibit equivalent performance, achieving a PDR of 99%. This indicates that in moderately dense environments, both protocols demonstrate comparable efficiency in packet delivery. In evaluating the average PDR across all node groups, RSOF demonstrates superiority with an average PDR of 99%, in contrast to MRHOF's 98%. This indicates that RSOF provides a more uniform performance across various network sizes.

The analysis indicates that RSOF exhibits superior scalability compared to MRHOF, especially in denser network conditions. RSOF's capacity to sustain elevated PDR with increasing node counts underscores its efficacy in optimizing parent selection, load balancing, and mitigating potential bottlenecks, which is essential in large-scale deployments. MRHOF demonstrates effective performance in small to medium-scale scenarios; however, RSOF exhibits superior performance under more challenging network conditions, rendering it a more robust option for dynamic and dense IoT environments. Therefore, the average improvement ratio of RSOF over MRHOF across all node densities is approximately 1%, indicating a slight overall advantage of RSOF regarding PDR under the conditions tested.

Packet Acknowledgment Ratio (PAR)

The PAR for RSOF and MRHOF is analyzed across different node densities as [Fig. 7](#) demonstrating RSOF's consistent superiority over MRHOF in the majority of scenarios; this is obviously due to our proposed RSOF focused on considering node and link reliability and trustworthiness by including NFR metrics and ERNT in selecting best parent algorithm.

[Table 9](#) demonstrates that, at lower and moderst node densities (25, 50, and 70 nodes), RSOF consistently surpasses MRHOF in performance. At 25 nodes, RSOF achieves a PAR of 98%, slightly surpassing MRHOF's 97%. This trend continues at 50 and 70 nodes, with RSOF attaining a PAR of 96% and 95%, respectively, compared to MRHOF's 95% and 94%. The consistent advantage, though minor, suggests that RSOF is more effective in ensuring reliable packet acknowledgment under moderate network loads, demonstrating its capability to manage various network scenarios. At the node density of 90 nodes, MRHOF exhibits a notable decrease in PAR with 89%. While RSOF exhibits an advantage at this density by approximately a 3.37% improvement over MRHOF, The significant disparity underscored the difficulties encountered by the MRHOF protocol in conditions of high network contention. Nevertheless, the minor

decrease in PAR at RSOF in high density compared with minor and moderate does not undermine the overall superiority of RSOF, which consistently attains a higher PAR across various density levels. RSOF demonstrates an average performance with a PAR of 95.25%, significantly exceeding MRHOF's 93.75%. This average further underscores the efficacy of RSOF in sustaining elevated packet acknowledgment rates across various network sizes. RSOF exhibits a more extraordinary ability for reliable packet delivery, establishing it as the more robust option for different network conditions. The results demonstrate that RSOF is superior in maintaining performance and reliability, particularly under challenging network conditions, providing a consistent advantage over MRHOF.

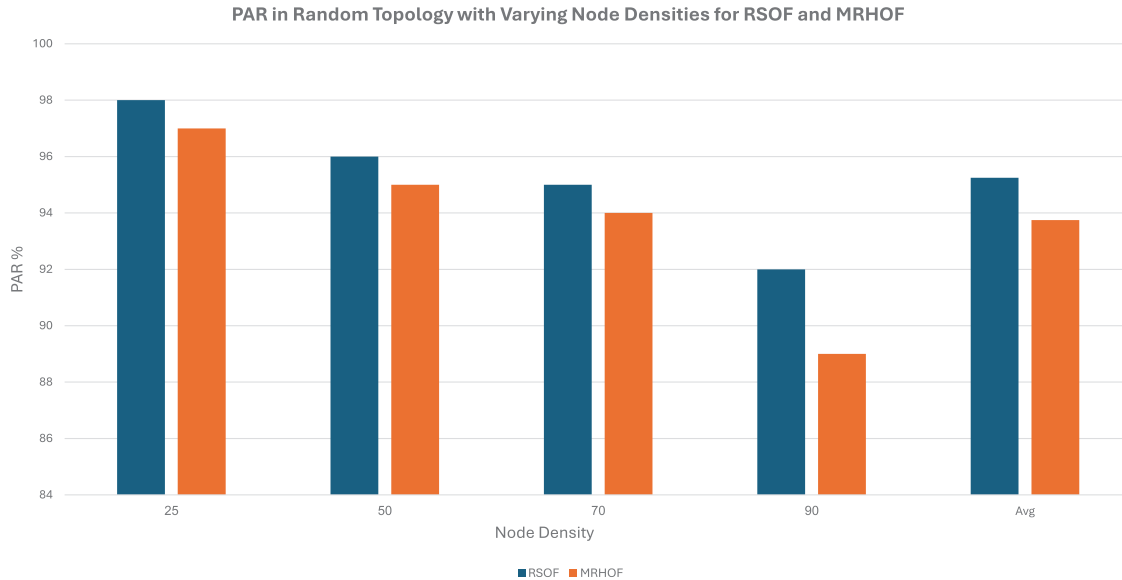


Figure 7: PAR Performance in random topology with varying node densities

Table 9: PAR for RSOF and MRHOF in different node density

Node density	RSOF	MRHOF
25	98	97
50	96	95
70	95	94
90	92	89
Avg	95.25	93.75

The examination of the PAR for RSOF and MRHOF is further substantiated by the trends illustrated in Fig. 8. The figure presents a comparative analysis of the performance of RSOF and MRHOF over time across various network sizes of 25, 50, 70, and 90 nodes. Consistent with the data from the previous Table 9, RSOF exhibits a distinct advantage in PAR, consistently achieving higher values than MRHOF throughout the simulation period. This is attributed to NFR metrics and ERNT, where nodes with lower reliability and higher probability of failure are avoided when selecting the best parent. In the 25-node scenario, RSOF exhibits a high PAR, beginning at 96% and increasing to 97% by the end of the experiment. In contrast, MRHOF begins at approximately 95% and concludes slightly below RSOF, indicating that the proposed

RSOF demonstrates greater efficiency, even in a relatively low-density environment. A comparable trend is observed for 50 and 70 nodes, with RSOF consistently attaining superior PARs relative to MRHOF as time progresses. RSOF achieves 95% and 94% for 50 and 70 nodes, respectively, while MRHOF attains only 94% and 91% under comparable conditions. The figure indicates that RSOF exhibits superior overall performance and a more stable trend in PAR over time, particularly at higher node densities. MRHOF demonstrates a slower enhancement in PAR, indicating its difficulty adapting to rising network loads compared to RSOF, which achieves over-performance MRHOF by approximately 4%.

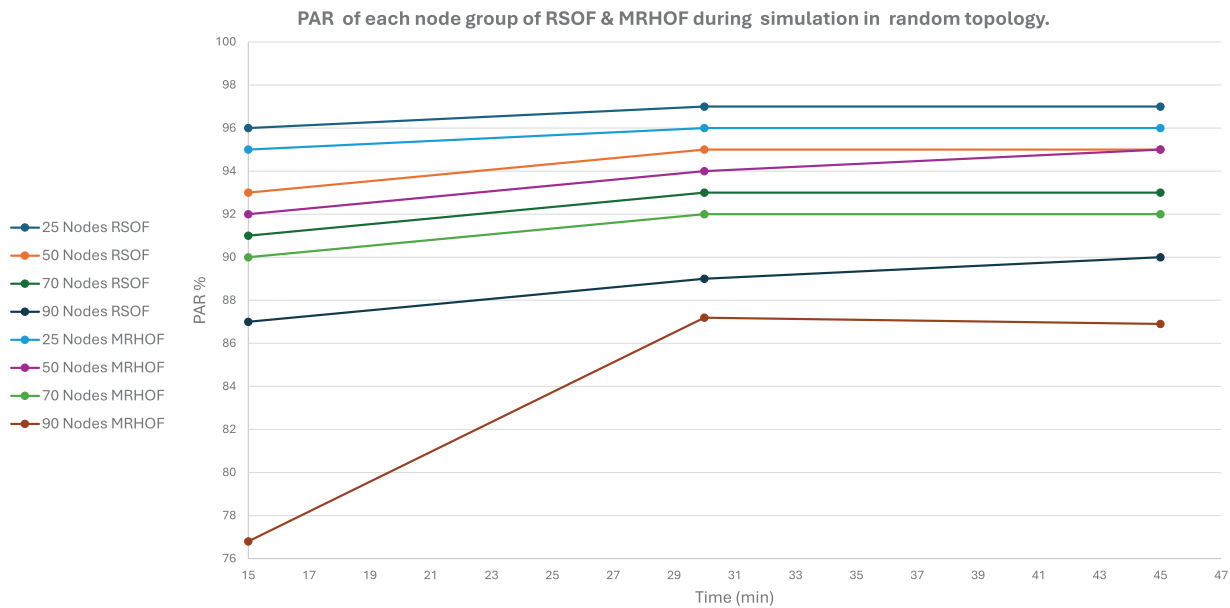


Figure 8: The PAR of every node group in RSOF and MRHOF varies throughout the simulation in random topology

The analysis results indicate that RSOF consistently outperforms MRHOF in achieving higher PAR across various network densities and throughout the experiment. RSOF demonstrates a notable performance advantage in moderate to high-density scenarios, achieving superior packet acknowledgment in the context of increasing network complexity. The persistent increase in PAR associated with RSOF highlights its enhanced ability to sustain reliability and efficient parent selection over time, rendering it a more robust alternative to MRHOF.

End to End Delay

The E2E delay is calculated by the average time required for packets to transmit from each node to the DODAG root across different time intervals. Fig. 9 illustrates and analyses the average E2E delay in milliseconds between the proposed RSOF and standard MRHOF protocols in various node densities. Fig. 9 illustrates significant insights into their performance under varying network loads. Several interconnected factors can explain the increase in E2E delays correlating with network density. In dense networks, congestion typically rises due to the increased number of nodes, leading to packet queuing.

Furthermore, in such networks, packets must traverse more hops between the sender and receiver (root), significantly increasing the E2E delay. Additionally, contentions and collisions increase in dense networks, resulting in packet losses and requiring packet retransmission, extending the end-to-end delay. The combined factors contribute to the rising trend of E2E delay in these scenarios.

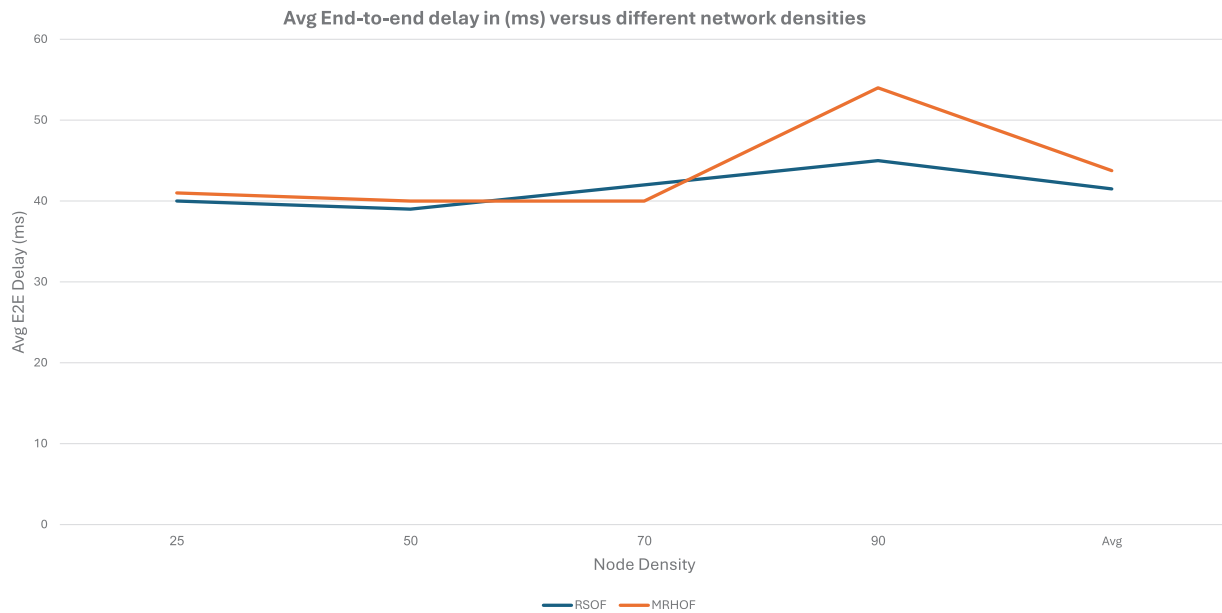


Figure 9: Average E2E delay for RSOF and MRHOF

In scenarios with lower and moderate node densities (25, 50, and 70), RSOF outperforms MRHOF since MRHOF relies only on the single measure ETX to assess the rank of nodes in its pursuit of the DODAG root node. Consequently, some nodes lacking enough trustworthy and reliable nodes, linkages, and energy are selected as preferable parents because of their elevated ETX scores. This thus results in poor routes and inefficient data transfer, adversely affecting packet delivery latency, as Fig. 9 illustrates. At 25 nodes, RSOF shows a delay of 40 ms compared to MRHOF's 41 ms. This trend continues at 50 nodes where RSOF records a slightly shorter delay of 39 ms vs. MRHOF's 40 ms. At 70 nodes, however, RSOF shows a slight increase to 42 ms, equating MRHOF's performance at the exact node count. These results suggest that both protocols effectively manage low to moderate network densities, with RSOF offering slight improvements in reducing delay. However, The most significant differences are observed at a node density of 90, where MRHOF protocols exhibit a sharp increase in delay because of node density, as elaborated earlier. RSOF records a delay of approximately 44 ms, while MRHOF shows a higher delay of roughly 57 ms. This substantial rise indicates that MRHOF struggles with high network congestion as a round 750 packets queue was dropped as Fig. 10 while RSOF performs better under these conditions. Overall, the average delay of 40 ms across all node densities for RSOF is approximately 2% lower than MRHOF's average of 44 ms. This indicates that RSOF generally performs better in managing network delays across diverse scenarios. RSOF shows robust performance in managing delays across varying network densities and consistently offers improvements. Particularly at higher node densities, RSOF's ability to sustain lower delays could be significant for applications where minimal latency is critical. These findings suggest that RSOF could be more effective in scenarios prone to congestion and high network traffic, potentially leading to more reliable network operations.

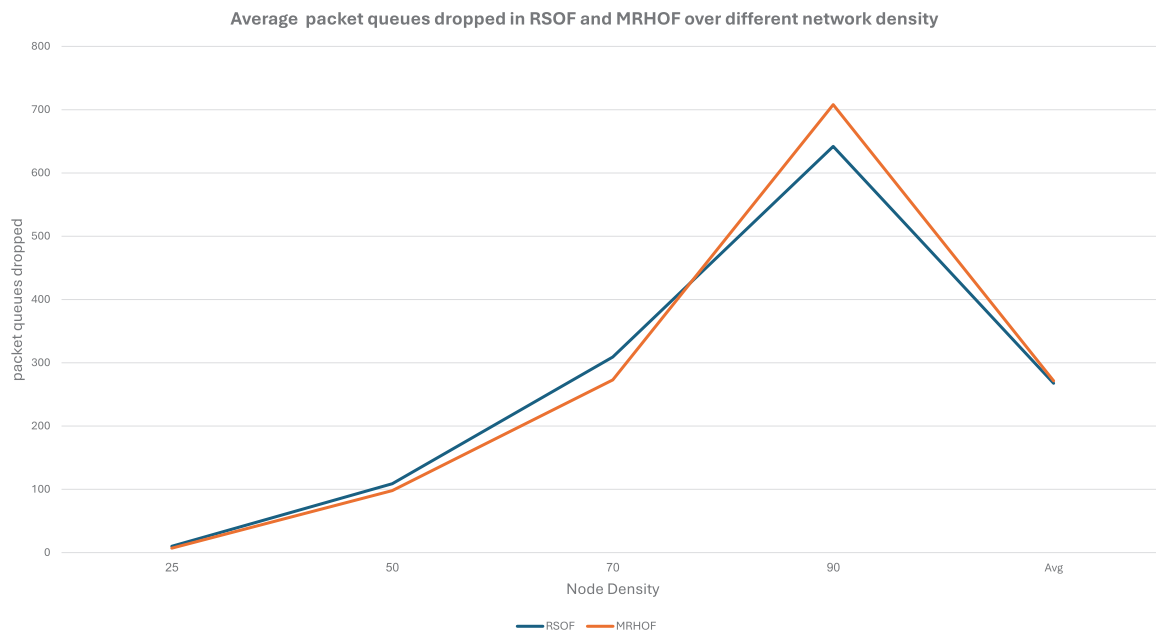


Figure 10: Average packets queue dropped for RSOF and MRHOF

Control Message Overhead (CMO)

During IoT and restricted resource networks such as LLNs, minimizing control overhead is a significant task that requires consideration. Minimizing message control overhead (DIO, DIS, and DAO) decreases the node's limited resource burden, leading to improved energy efficiency and overall network performance. In constructing the DODAG, nodes employ the trickle timer algorithm to ensure network consistency by propagating control messages and adjusting the frequency of DIO messages. If the network is consistent, the rate of produced messages is minimal. Inconsistencies within the network prompt both local and global repairs, leading to an increase in the transmission of control messages. Unfortunately, as the network grows, the level of control overhead correspondingly increases. This leads to increased energy depletion in the nodes and heightens the likelihood of congestion and collisions, thereby elevating the packet loss probability. This detrimentally affects both end-to-end latency and PDR, thereby impairing network performance.

To help explain further, [Fig. 11](#) shows the extra work needed to control messages for RSOF and MRHOF when the network has 25, 50, 70, or 90 nodes. The graph shows that the CMO for both routing protocols increases as network density increases. However, the overhead trends between RSOF and MRHOF present some notable differences. At lower densities (25 nodes), the CMO for RSOF is consistently lower than MRHOF's by approximately 13%, showcasing more efficient management in RSOF.

RSOF consistently maintains a significantly lower overhead than MRHOF at all node densities. [Table 10](#) presents the improvement ratios for RSOF in different network densities to more effectively examine its potency in contrast to MRHOF. The differences are particularly striking at medium densities (50 and 70 nodes), where RSOF shows nearly 50% and over 59% less overhead, respectively. These significant discrepancies highlight the efficiency of RSOF in managing network communication, particularly in more populated environments where message overhead can significantly impact network performance and resource utilization. Overall, RSOF's efficiency in managing message overhead suggests better scalability and potential for improved network performance in dense and complex environments than MRHOF. This

advantage might contribute significantly to network stability and efficiency, particularly under conditions that strain network resources.

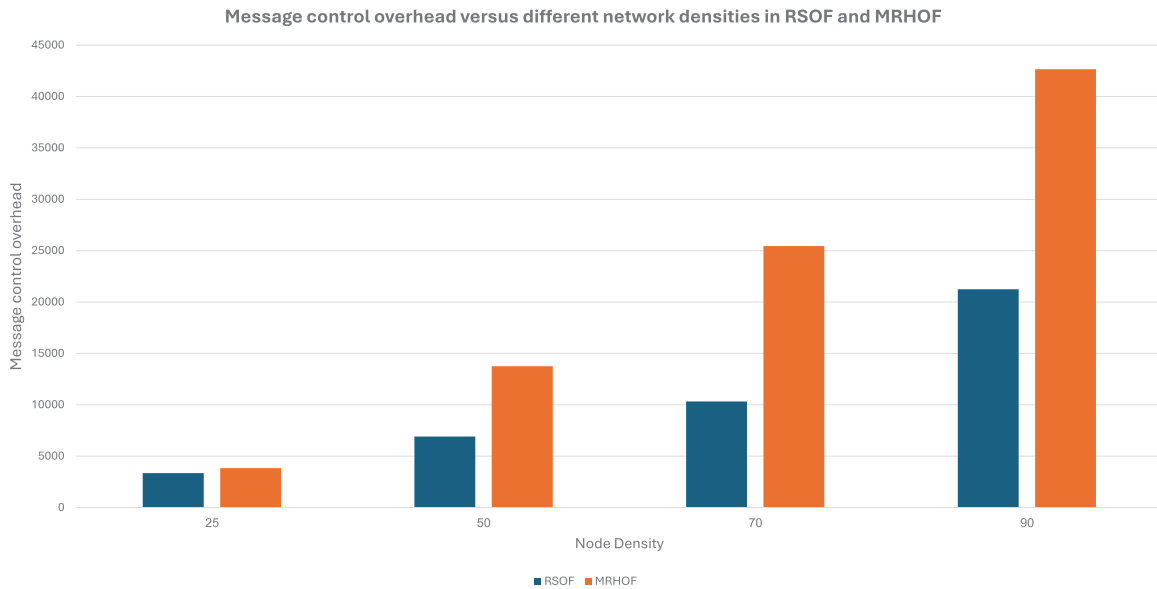


Figure 11: Message control overhead vs. different network densities

Table 10: Control message overhead improvement ratios of RSOF

Node density	RSOF	MRHOF	Improvement ratios
25	3349	3832	12.6%
50	6913	13748	49.72%
70	10324	25454	59.44%
90	21246	42666	50.20%
Avg			42.99%

5.3.2 Grid Topology Evaluation

The bar chart in Fig. 12 presents a comparative analysis of PDR and PAR across two network densities (25 and 70 nodes) for both RSOF and MRHOF in a grid topology. PDR remains consistently high for RSOF and MRHOF, with only minor variations. For instance, at 25 nodes, the PDR for RSOF is slightly higher than MRHOF, but the difference is minimal. Both protocols achieve near-perfect PDR values, indicating robust performance in delivering packets to the DODAG root, even as network density increases.

However, the most significant contrast appears in the PAR metric. RSOF exhibits a considerable improvement in PAR, especially at lower node densities. At 25 nodes, RSOF outperforms MRHOF, showing a more efficient packet acceptance process, while the gap narrows slightly as node density increases to 70 nodes. This difference can be attributed to the more optimized routing decision-making process in RSOF, which handles congestion and contention more effectively, leading to fewer packet losses and retransmissions. RSOF shows a notable enhancement over MRHOF in terms of PAR, particularly at lower network densities.

Showcasing RSOF's superiority in handling packet acceptance in less congested scenarios. This performance gap reduces as the network becomes denser (70 nodes), but RSOF still maintains an edge over MRHOF. The results demonstrate that RSOF generally outperforms MRHOF, especially in scenarios with lower node densities, due to its more efficient handling of packet overhead and network control traffic.

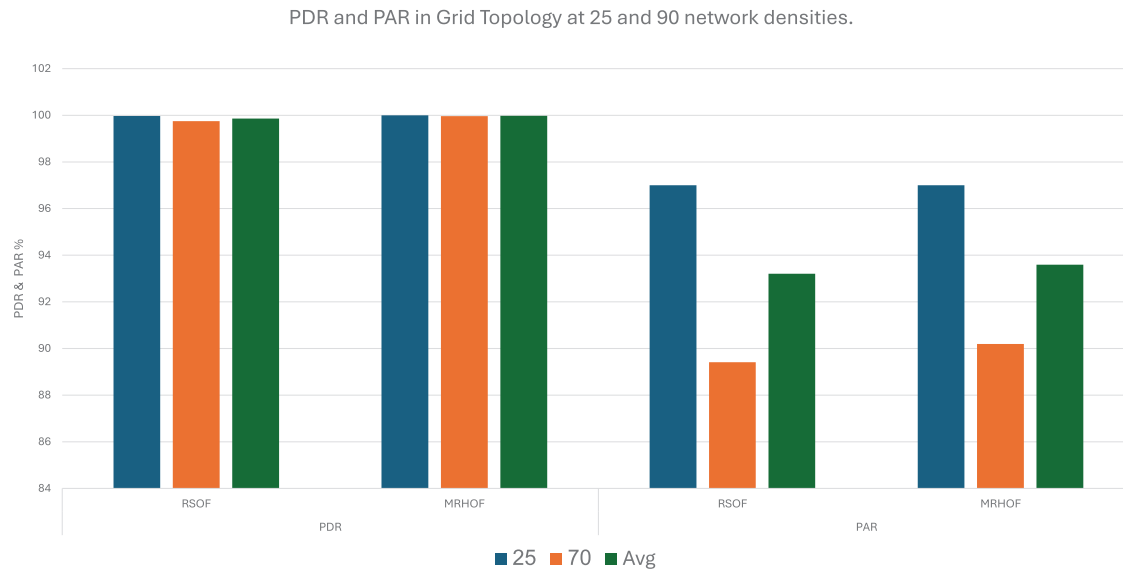


Figure 12: PDR and PAR in grid topology across two node densities 25 and 70

Fig. 13 compares the CMO of RSOF and MRHOF protocols in grid topology at two network densities, 25 and 70 nodes, and the average. MRHOF incurs significantly higher control overhead than RSOF, especially as the network density increases. At 25 nodes, RSOF and MRHOF exhibit relatively low control message overhead (CMO). However, as the network density rises to 70 nodes, the CMO in MRHOF dramatically increases, nearly doubling its value compared to RSOF. This trend is consistent in the average results, where MRHOF's CMO remains significantly higher than RSOF's. The increased CMO in MRHOF can be attributed to the protocol's reliance on frequent control messages to maintain route stability, especially in denser networks. This results in more network congestion and higher resource usage. RSOF, on the other hand, manages CMO more efficiently, which may be due to its more adaptive decision-making process, resulting in fewer control messages and reduced network congestion. This performance difference highlights RSOF's efficiency in managing control traffic, particularly in denser networks, making it more suitable for scenarios where minimizing overhead is crucial. **Table 11** shows the superiority of the RSOF and the improvement ratio compared to MRHOF.

Fig. 14 illustrates the average delay (in milliseconds) for RSOF and MRHOF across two network densities of 25 and 70 nodes within a grid topology. The comparison provides valuable insights into the performance and scalability of these routing protocols under varying network conditions. **Fig. 4** shows that RSOF increases delay from approximately 40 ms at 25 nodes to about 60 ms at 70 nodes. This trend indicates a substantial impact on performance due to increased network density, likely due to longer path lengths and heightened congestion within the network. This is normal as the density of the network increases. The same pattern happens in MRHOF, demonstrating a more gradual increase in delay under similar conditions, starting just above 40 ms at 25 nodes and reaching around 60 ms at 70 nodes. This suggests that both OFs may have effective mechanisms for managing routing paths or control messages, contributing to more consistent

delay times even as network density increases. When averaged across both network densities, RSOF records a mean delay of approximately 58 ms, while MRHOF records a slightly lower average of around 57 ms.

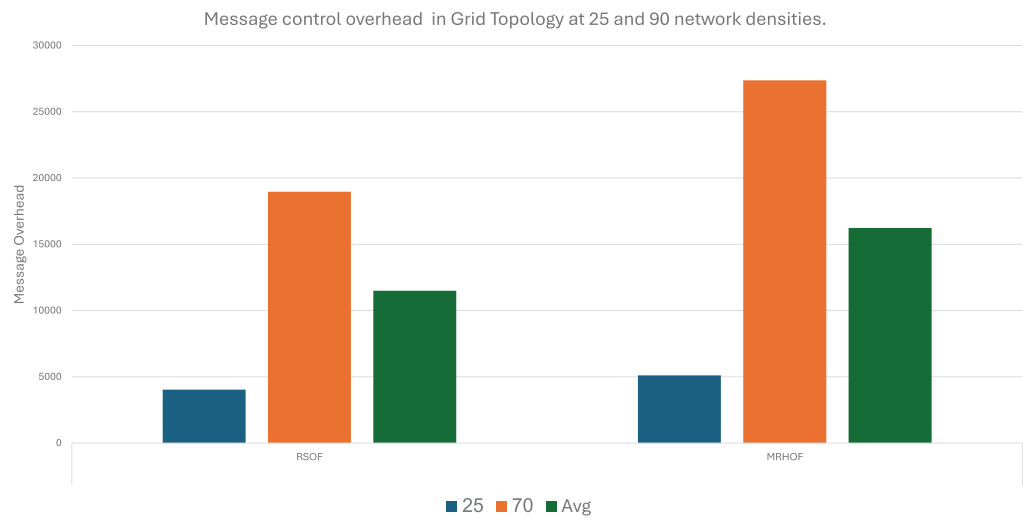


Figure 13: Control Message Overhead in grid topology at 25 and 70 network densities

Table 11: Control message overhead improvement ratios of RSOF in grid topology

Node density	RSOF	MRHOF	Improvement ratios
25	4031	5103	21.01%
70	18964	27377	30.73%
Avg			25.87%

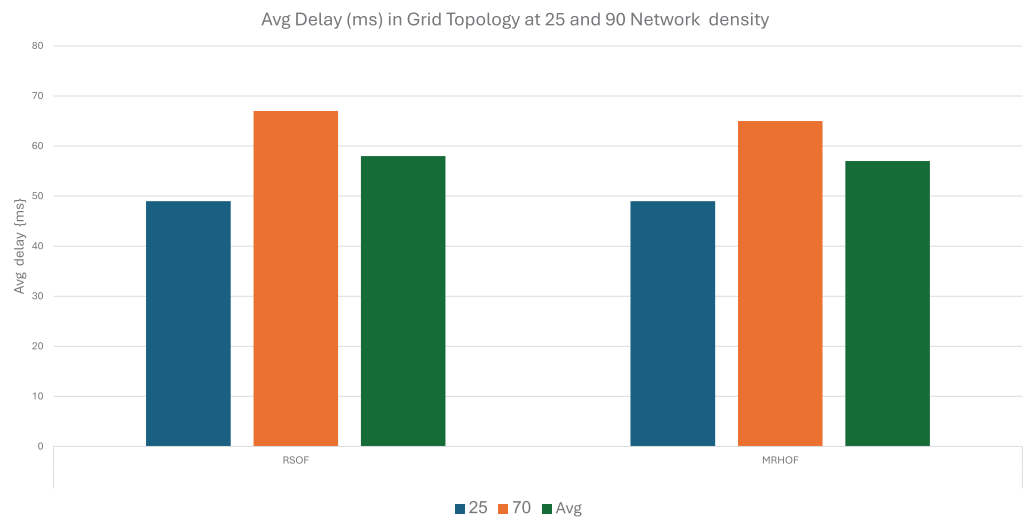


Figure 14: Average E2E delay comparison in grid topology at 25, 70 network densities

6 Conclusion and Future Work

IoT has emerged as a technology that improves diverse aspects of life. LLNs are vital for connecting resource-constrained wireless devices in IoT. The IPv6 RPL has been designated as a standard routing protocol for IoT. Designing routing protocols tailored to IoT environments is challenging, with RPL's use of two OFs limited by a single metric for various IoT applications. This paper proposes a reliable and trusted OF to enhance network performance while ensuring high security and reliability and overcoming RPL's restrictions. The proposed RSOF constructs the RPL topology considering composed metrics during the parent selection, where each node evaluates potential parent candidates based on their remaining energy, security level, and reliability, ultimately selecting the most optimal parent. The proposed RSOF is assessed and compared to the standard MRHOF regarding the PDR, PAR, CMO, and E2E delay across different network sizes and random and grid topology. The results have proven that the proposed RSOF improves network performance regarding reliability and security and efficiently uses resources that increase the network's lifetime under small to large-density networks compared to the standard MRHOF. Future work intends to use ML in the parent selection process and integrate it into Contiki OS.

Acknowledgement: The authors would like to thank the reviewers for their observations, comments, and suggestions for improving the manuscript content.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm their contribution to the paper as follows: study conception and design: Mariam A. Alotaibi; data collection: Mariam A. Alotaibi; analysis and interpretation of results: Mariam A. Alotaibi; draft manuscript preparation: Mariam A. Alotaibi; supervision Sami S. Alwakeel and Aasem N. Alyahya. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data supporting this study's findings are available from the corresponding author, Mariam A. Alotaibi, upon reasonable request.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study

References

1. Swan M. Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0. *J Sens Actuator Netw.* 2012;1(3):217–53. doi:10.3390/jsan1030217.
2. Evans D. The internet of things how the next evolution of the internet is changing everything. CISCO White Paper. 2011;1:1–11.
3. Atzori L, Iera A, Morabito G. The internet of things: a survey. *Comput Netw.* 2010;54(15):2787–805. doi:10.1016/j.comnet.2010.05.010.
4. Clausen T, Herberg U, Philipp M. A critical evaluation of the IPv6 routing protocol for low power and lossy networks (RPL). In: 2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob); 2011; Shanghai, China. p. 365–72. doi:10.1109/WiMOB.2011.6085374.
5. Hui JW, Culler DE. Extending ip to low-power, wireless personal area networks. *IEEE Internet Comput.* 2008;12(4):37–45. doi:10.1109/MIC.2008.79.
6. Hui J, Vasseur J, Culler D, Manral V. An IPv6 routing header for source routes with the routing protocol for low-power and lossy networks (RPL). RFC 6554. 2012 [cited 2024 Nov 30]. Retrieved from: <https://www.rfc-editor.org/rfc/rfc6554.html>.
7. Haseeb K, Almogren A, Islam N, Din IUd, Jan Z. An energy-efficient and secure routing protocol for intrusion avoidance in IoT-based WSN. *Energies.* 2019;12(21):4174. doi:10.3390/en12214174.

8. Othman SO, Bahattab AA, Trad A, Youssef H. PEERP: an priority-based energy-efficient routing protocol for reliable data transmission in healthcare using the IoT. *Procedia Comput Sci.* 2020;175:373–8. doi:10.1016/j.procs.2020.07.053.
9. Conti M, Kaliyar P, Lal C. REMI: a reliable and secure multicast routing protocol for iot networks. In: *Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES '17)* 2017 Aug; Reggio Calabria, Italy. p. 1–8. doi:10.1145/3098954.3106070.
10. Lenka RK, Rath AK, Sharma S. Building reliable routing infrastructure for green IoT network. *IEEE Access.* 2019;7:129892–909. doi:10.1109/Access.6287639.
11. Brandt A, Hui J, Kelsey R, Levis P, Pister K, Struik R, et al. RPL: IPv6 routing protocol for low-power and lossy networks. *Internet Eng Task Force (IETF).* 2012;6550:1–157.
12. Zhao M, Kumar A, Joo Chong PH, Lu R. A comprehensive study of RPL and p2p-RPL routing protocols: implementation, challenges and opportunities. *Peer Peer Netw Appl.* 2017;10:1232–56. doi:10.1007/s12083-016-0475-y.
13. Aljarrah E, Yassein MB, Aljawarneh S. Routing protocol of low-power and lossy network: survey and open issues. In: *2016 International Conference on Engineering & MIS (ICEMIS).* 2016; Agadir, Morocco. p. 1–6. doi:10.1109/ICEMIS.2016.7745304.
14. Witwit AJ, Idrees AK. A comprehensive review for RPL routing protocol in low power and lossy networks. In: *Proceedings of the 3rd International Conference on New Trends in Information and Communications Technology Applications (NTICT 2018), Communications in Computer and Information Science;* 2018 Oct; Baghdad, Iraq. p. 50–66. doi:10.1007/978-3-030-01653-1_4.
15. Lamaazi H, Benamar N. A comprehensive survey on enhancements and limitations of the RPL protocol: a focus on the objective function. *Ad Hoc Netw.* 2020;96:102001. doi:10.1016/j.adhoc.2019.102001.
16. Vasseur J-P, Kim M, Pister K, Dejean N, Barthel D. Routing metrics used for path calculation in low-power and lossy networks. *Tech Rep.* 2012.
17. Farzaneh B, Ahmed AK, Alizadeh E. MC-RPL: a new routing approach based on multi-criteria RPL for the internet of things. In: *2019 9th International Conference on Computer and Knowledge Engineering (ICCKE).* Mashhad, Iran; 2019. p. 420–5. doi:10.1109/ICCKE48569.2019.8964675.
18. Kamgueu PO, Nataf E, Djotio T, Festor O. Fuzzy-based routing metrics combination for RPL. In: *Doctoral Consortium SensorNets. Centre pour la Communication Scientifique Directe (CCSD).* Lyon, France: French National Open Access Repository, HAL; 2014 [cited 2024 Nov 30]. Available from: <https://inria.hal.science/hal-01093965v1/document>.
19. Gaddour O, Koubâa A, Abid M. Quality-of-service aware routing for static and mobile IPv6-based low-power and lossy sensor networks using RPL. *Ad Hoc Netw.* 2015;33:233–56. doi:10.1016/j.adhoc.2015.05.009.
20. Kechiche I, Bousnina I, Samet A. A novel opportunistic fuzzy logic based objective function for the routing protocol for low-power and lossy networks. In: *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC);* 2019; Tangier, Morocco. p. 698–703.
21. Kuwelkar S, Virani HG. OF-FZ: An Optimized Objective Function for the Ipv6 Routing Protocol for LLNs. *IETE J Res.* 2023;69(9):6101–19. doi:10.1080/03772063.2021.1990139.
22. Lamaazi H, Benamar N. Of-ec: a novel energy consumption aware objective function for RPL based on fuzzy logic. *J Netw Comput Appl.* 2018;117:42–58. doi:10.1016/j.jnca.2018.05.015.
23. Lamaazi H, Benamar N. RPL enhancement using a new objective function based on combined metrics. In: *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC);* 2017; Valencia, Spain. p. 1459–64. doi:10.1109/IWCMC.2017.7986499.
24. Toulabi M, Javadi S. Energy-saving in wireless sensor networks based on sink movement control using fuzzy logic. *J Wirel Sensor Network.* 2015;1(1).
25. Saaidah A, Almomani O, Al-Qaisi L, Kamel M. An efficient design of RPL objective function for routing in internet of things using fuzzy logic. *Int J Adv Comput Sci Appl.* 2019;10(8):184–90.

26. Gopika D, Majumder P, Kumar P. FML: Fuzzification with machine learning based parent node selection in RPL/6LoWPAN. In: 2020 2nd PhD Colloquium on Ethically Driven Innovation and Technology for Society (PhD EDITS) 2020; Bangalore, India. p. 1–2. doi:10.1109/PhDEDITS51180.2020.9315313.
27. Cao Y, Wu M. A novel RPL algorithm based on chaotic genetic algorithm. *Sensors*. 2018;18(11):3647. doi:10.3390/s18113647.
28. Sennan S, Somula R, Luhach AK, Deverajan GG, Alnumay W, Jhanjhi N, et al. Energy efficient optimal parent selection based routing protocol for internet of things using firefly optimization algorithm. *Trans Emerg Telecomm Technol*. 2021;32(8):e4171. doi:10.1002/ett.4171.
29. Preeth SSL, Dhanalakshmi R, Kumar R, Si S. Efficient parent selection for RPL using aco and coverage based dynamic trickle techniques. *J Ambient Intell Humaniz Comput*. 2020;11:4377–91. doi:10.1007/s12652-019-01181-w.
30. Darabkh KA, AlAdwan HH, Al-Akhras M, Jubair F, Rahamneh S. A revolutionary RPL-based iot routing protocol for monitoring building structural health in smart city domain utilizing equilibrium optimizer algorithm. *Soft Comput*. 2024;1–40. doi:10.1007/s00500-024-09677-0.
31. Sarwar S, Rauf S, Rasheed R, Aslam L. Energy-aware routing in internet of things (IoT). In: 2019 2nd International Conference on Communication, Computing and Digital systems (C-CODE); 2019; Islamabad, Pakistan. p. 81–6. doi:10.1109/C-CODE.2019.8680974.
32. Sankar S, Srinivasan P. Energy and load aware routing protocol for internet of things. *Int J Adv Appl Sci (IJAAS)*. 2018;7(3):255–64. doi:10.11591/ijaas.v7.i3.pp255-264.
33. Lemercier F, Montavont N. Performance evaluation of a RPL hybrid objective function for the smart grid network. In: Ad-hoc, Mobile, and Wireless Networks: 17th International Conference on Ad Hoc Networks and Wireless, ADHOC-NOW 2018; 2018 Sep 5–7; Saint-Malo, France: Springer. p. 27–38.
34. Moradi S, Javidan R. A new objective function for RPL routing protocol in IoT to increase network lifetime. *Int J Wirel Mob Comput*. 2020;19(1):73–9. doi:10.1504/IJWMC.2020.109270.
35. Hamodi ZA, Kadhim AA. Performance of RPL protocol based on new objective function for iot-wsn. *Iraqi J Inform Commun Technol*. 2020;3(2):21–34. doi:10.31987/ijict.vol3.issue2.
36. Qasem M, Al-Dubai A, Romdhani I, Ghaleb B, Gharibi W. A new efficient objective function for routing in internet of things paradigm. In: 2016 IEEE Conference on Standards For Communications and Networking (CSCN); 2016; Berlin, Germany. p. 1–6. doi:10.1109/CSCN.2016.7785168.
37. Elmahi M, Osman N. Design of a load balancing objective function for RPL. *J High Speed Netw*. 2024;30(3):1–23.
38. Hassani AE, Sahel A, Badri A. A new objective function based on additive combination of node and link metrics as a mechanism path selection for RPL protocol. *Int J Commun Networks Inf Secur*. 2020;12(1):63–8.
39. Santos CLD, Mezher AM, León JPA, Barrera JC, Guerra EC, Meng J. ML-RPL: machine learning-based routing protocol for wireless smart grid networks. *IEEE Access*. 2023;11:57401–14.
40. Duenas Santos CL, Astudillo León JP, Mezher AM, Cardenas Barrera J, Meng J, Castillo Guerra E. RPL+: an improved parent selection strategy for RPL in wireless smart grid networks. In: Proceedings of the 19th ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks (PE-WASUN '22); 2000 Oct 24–28; Montreal, QC, Canada. p. 75–82. doi:10.1145/3551663.3558677.
41. Kuwelkar S, Virani HG. RPL protocol enhancement using k-nearest neighbor machine learning approach for IoT application. 2023 Apr 2. doi:10.21203/rs.3.rs-2392682/v1.