iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67415

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

An Analysis of Data Dribble in IoT Devices Using Fuzzy Networks

Anjali Gujar[1], Ruchi Kulshrestha[2]
JECRC University

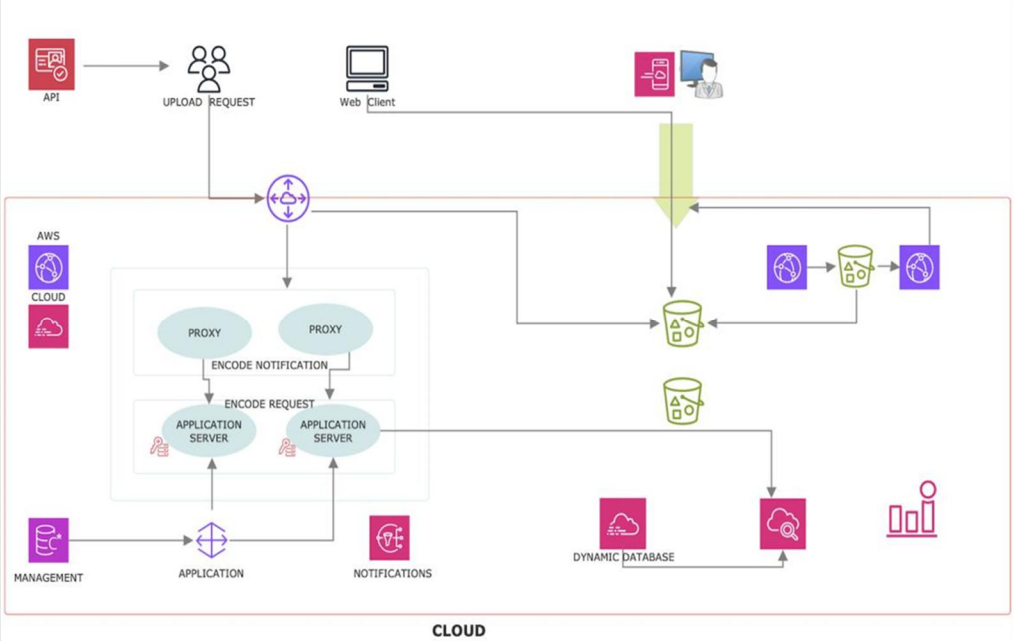
Abstract: ***It is impossible to ignore this information centre segment because it is closely related to the Web of Material. Wireless sensor networks, which operate in a variety of situations, are essential to the web of Contents. They serve as the fundamental framework for the Internet of Things network in many important domains, including manufacturing operations, environmental tracking, as well as the artificially intelligent neighbourhood. Nevertheless, a multitude of obstacles which are for instance, security and technical issues arise alongside such integrated sensor networks, particularly when trying to scale them up and deploy them seamlessly. The inherent challenges of WSNs largely arise as a result of their constrained and defective nodes which can be attributed to power and computation while the bandwidth is limited. Included among the main technology challenges in WSNs guided by IoT bartered with the weighty data transmission with an energy concern cost the balance with the longevity of the deployment, as well as the security robustness against future threats. Most importantly, such issues need to be solved to eliminate any constraints for the integration of low-powered IoT devices. Energy efficiency remains an important design consideration in IoT-enabled WSNs as sensor nodes are for the most part powered by batteries with limited capacities. Network Layer Global Unique VLAN ID Confabulating features which are typical for uniform WSNs do deliver part of the answer, but few can cope with issues related to the complexity of heterogeneous.***

I. INTRODUCTION

As Internet of Things (IoT) devices are becoming commonplace, routing data in a secure as well as energy-capable nature is of great concern. The networks of IoT are extensive, varied and resource-constrained and therefore, new strategies for data management are needed while ensuring higher levels of security. In particular, the paper looks into different approaches aimed at ensuring the security and energy aspects of data routing over IoT-based networks. As Internet of Things (IoT) devices are becoming commonplace, routing data in a secure and energy-efficient manner is of great concern. The networks of IoT are extensive, varied and resource-constrained and therefore, new strategies for data management are needed while ensuring higher levels of security. In particular, the paper focuses on several techniques that can allow better secure and energy-efficient routing of data in IoT-based frameworks. A lot of the traditional routing protocols prescribed for IoT networks tend to emphasize hop count or shortest path-based routing; however, they tend to ignore the fact that IoT is a dynamic and diverse setting. Consequently, they do not fully exploit the energy consumption of the network or perform well under modified network states. Furthermore, enhancing confidence in the network is of utmost importance to safeguard sensitive data and guarantee reliability in the context of IoT applications. This introduction ushers one into discussing an innovative concept, Trust-related Energy Efficient Routing policy for IoT-based Sensor Networks (TERP). TERP Trust is developed to resolve the weaknesses of previous paradigms by providing routing protocols that focus on trust that models the history of influence nodes and interactions about the routes[1]. In trust-centric networks, TERP will be able to dynamically determine routes that will provide not only energy-saving means but will also improve reliable and secure transmission of data. This document discusses the basic principles of energy efficiency and trust-based routing in the context of IoT networks. It describes the troubles linked by the use of standard routing protocols and explains the necessity of implementing trust-based principles. In addition, the paper presents the aims, methods, and expected outcome of TERP for the improvement and robustness of sensor networks for IoT applications[2]. Through this inquiry, we seek to add to the existing attempts to make strong and sustainable IoT frameworks that can handle various tasks with relevant levels of efficiency, preservation of data confidentiality, and security. Several challenges and threats are based on the web which must be resolved to ensure safe adjustments of wireless web and help in making secure and efficient information routing. The great challenges in good and prompt information routing involve the certificate of net force use and net throughput. Sensor nodes (SNS) are liable for finding the atmospheric parameters including force temperature, humidity acoustics and wet levels which use arsenic indicators of important environmental changes. After the task of sensing is finished, the data gathered by every sensor node is transmitted to an underpinning base station (BS).

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Notwithstanding the energy-intensive world of both the perception and communicating subsystems inside the SNS leads to fast depletion. Once a node exhausts its energy reserves it is deemed "dead" and becomes non-functional making it unsuitable for recharging or replacement with an alternative power source. Hence optimising employment sensor nodes is dominant to ensuring net seniority. To mitigate these energy constraints various clustering processes have been applied [3]. It is very important for extending the web lifespan and to improve the worthlessness of the entire system. The toughness of a wireless sensor network (WSN) is intrinsically related to the green management of its strength sources, making strength optimisation a crucial requirement for sustaining community operations. The choice of the ideal routing protocol, a key determinant in ensuring efficient information transmission, must be completed judiciously.



WORKING ARCHITECTURE OF IoT

Figure 1

It needs to facilitate the secure delivery of information packets to the intended destination with minimum overhead, an important consideration given the inherent boundaries of sensor nodes (SNs), inclusive of restrained electricity components and confined verbal exchange range. Despite big improvements in optimising WAN's overall performance, the quest for more progressive and robust answers remains an ongoing challenge [4]. The advantages of an urban IoT architecture are multifaceted. It permits the clever control and optimisation of vital public services, which include transportation and parking systems, smart lighting fixtures, surveillance and preservation of public spaces, cultural history conservation, waste control, and public fitness offerings encompassing hospitals and academic establishments. Moreover, the aggregation of numerous records streams, whether saved in cloud platforms or centralised records warehouses inside the city IoT environment, enhances governmental transparency. This, in turn, facilitates data-driven governance by municipalities and local authorities, fostering civic engagement and elevating public awareness about the current state of urban infrastructure and overall lifestyle quality.

II. LITERATURE REVIEW

The design, growth, as well as evaluation of IoT products as well as policies require robust testing using specialised research tools before they are deployed in real-world environments. IoT simulators play an important role in this process by providing an environment where Controls are available for testing and analysis[5]. An effective IoT simulator must have important features such as high fidelity. Scalability Energy modelling capabilities and the ability to expand to support custom needs... IoT simulators are generally divided into 3 levels: Full-stack simulators. Big data processing simulator as well as network simulator This thesis focuses on network simulators. This helps in evaluating communication protocols and network behaviour in IoT systems.

Below are some of the most widely used network simulators: -

1) Cooja =Cooja + Contiki The Contiki operating system, an integrated modelling engine designed for Internet of Things sensor nodes, is included alongside Cooja. It complies with popular app-level mechanisms. CoAP In contrast to conventional training simulators, Cooja is a kind of computer that can generate directives for different hardware levels when a wireless context is present. The programming language, C, is mostly used in the tool's development.
2) OMNeT++ = (Tests objective modular networks in C++): OMNeT++ is a versatile and widely accepted network simulation framework. Widely used for wireless sensor networks. It has a modular architecture and supports external expansion. For example, it is used to create Veins, a vehicle network simulation. To evaluate intelligent transportation systems, however, OMNeT++ IoT-specific radio types and app protocol stacks which ought to be used are not supported by default.
3) Network Simulator 3 (NS-3):= NS-2, the successor to NS-2, focuses on IoT simulation at the cognitive level. As shown in the IoT architecture model, like OMNeT++, C++ is used as the primary programming language. It also includes support for IoT-specific radio models. However, it does not natively support application layer protocols. Therefore, such functionality requires further development efforts. -
4) Qualnet= QualNet is a commercial network simulator known for its high-fidelity simulation. Especially in IoT-specific situations, unlike open-source alternatives, QualNet provides strong support for simulating different types of cyberattacks. Including eavesdropping radio interference Distributed Denial of Service (DDoS), transmission and intelligence attack Proprietary tools It provides advanced features that enable high-performance IoT network simulation. These network simulation tools are critical to managing the complexity of IoT environments, allowing researchers to test and fine-tune protocols before deploying them into production.The suggested method for forwarding In addition to memory considerations To guarantee reliable and efficient in terms of energy content transfer and storage in Internet of Things-based sensors, it is developed along with executed in the 3 main processes.

- Phase I focuses on secure data routing using Multi-path Link Routing Protocol (MLRP) which ensures efficient communication between sensor nodes while protecting against potential threats..
- Phase II includes the H-TEEN protocol which is specifically designed to achieve load balancing between sensor nodes. This method enhances energy consumption across the network. Helps extend the life of each node and the network as a whole.
- Phase III has mainly focused on storing the data along with managing the capacity and extensive data storage protocol. This phase is very important in the transmission of data as it focuses on the storage of data while managing the reliability of the data as well. It ensures the transmitted data is stored safely by providing reliability to the network.

The MLRP framework works through five different step:

- Neighbour Discovery: Identify and establish connections with neighbouring nodes.
- Topology Creation: Create a flexible network topology to support multi-path communication.
- Pairwise Key Distribution: Secure key allocation to create an encrypted communication channel.
- Clustering: Arranging nodes into groups to enable hierarchical management and energy-efficient communication.
- Data Communication:Transmit data securely while increasing energy efficiency and maintaining data integrity. By combining these steps and phases The proposed protocol thus guarantees comprehensive energy efficiency enhancement. Secure communication and reliable data storage within IoT-based sensor networks... One of the most important challenges in IoT-WSN is to achieve efficient data routing between source nodes (S) and destination nodes (D) and reduce energy consumption.

A proposed solution to this problem is a new routing protocol called
Energy-Efficient Geographic Routing (EGE). It suggests six items designed to optimise performance based on the primary objective function: Delay, distance, power consumption Quality of Service (QoS), Cost, and Trust The EEG protocol identifies the most efficient path using improved fuzzy logic with improved membership functions. [6]This makes it possible to accurately estimate routing metrics. Optimal route selection is further improved through algorithms. *Harris Hawks Optimisation (HHO),* which estimates possible routes against a six-fold objective, parameter f, provides high performance in route optimisation in IoT-WSN, ensuring reliable communication with decreased energy and improving overall network performance.
One major task in IoT-WSN is to achieve efficient data routing between source nodes (S) and destination nodes (D) and reduce energy consumption. A proposed solution to this problem is a new routing protocol called Energy-Efficient Geographic Routing (EEG). It suggests six items designed to optimize performance based on the primary objective function: *Delay, distance, power consumption Quality of Service (QoS), Cost, and Trust :* The EEG protocol identifies the most efficient path using improved fuzzy

logic with improved membership functions. This makes it possible to accurately estimate routing metrics. Optimal route selection is further improved through algorithms.

Harris Hawks Optimisation (HH0), which estimates possible routes against a six-fold objective, parameter f, provides high performance in route optimisation in IoT-WSN, ensuring reliable communication with Reduced energy consumption and improving overall network performance.

Internet of Things (IoT) efficient in terms of energy georouting utilising improved flexible reason:

In Internet of Things (IoT) networks, where devices or nodes are often distributed over a large area and operate on limited power sources (such as batteries), data routing efficiency is critical.

The challenge is to ensure that data is transmitted over the network with minimal power consumption while maintaining communication reliability. Using fuzzy logic to optimize energy-efficient geo-routing protocols is one such approach. Here's an outline of how. Energy efficient geo data routing based on optimised fuzzy logic can work in the context of IoT:

- Overview of geo-routing in IoT Geo-routing protocols use the physical location (coordinates) of IoT nodes for routing data. This is different from traditional protocols that rely on routing tables. This is useful in dynamic environments such as IoT, where devices move. And network topology can change frequently. In geographic routing, A node typically sends data to its next-hop neighbour closest to the destination. However several factors must be considered to ensure energy efficiency and reliable delivery. These include: - residual energy of the node - Distance to destination - Link quality (e.g. signal strength) - Network congestion[7].
- Challenges in energy-efficient geographic routing Some of the challenges in energy-efficient geographic routing include: - Power consumption: Nodes are normally powered by batteries. Therefore, excessive power consumption can lead to node failure and network disruption. - Dynamic Topology: In IoT, nodes can enter or leave the network in many ways. Or moving around It requires an adaptive routing protocol. - Data reliability: Routing decisions need to be reliable in the face of varying network conditions. - Scalability: As the network size increases Managing decisions regarding routing and energy efficiency has thus become more complex.
- The role of Fuzzy Logic in increasing efficiency Fuzzy logic is a method for modelling uncertainty and imprecision. This makes it a good candidate for optimising routing decisions in IoT networks. Fuzzy logic map member functions feed data to output in a way that reflects real-world fuzziness. [8]Using fuzzy logic Routing algorithms can make decisions based on several factors with continuous values rather than discrete values. The main elements of fuzzy reasoning include: - obfuscation: Translating sharp inputs (e.g. power level, distance) into ambiguous values. - Fuzzy Inference System (FIS): A set of rules that control how fuzzy values are combined to create an output (i.e. next-hop node). - Devoicing: Convert fuzzy output back to a sharp value, e.g. selecting a specific next-hop neighbour.
- 4. Proposed optimisation framework An optimised fuzzy logic routing protocol must consider several factors to ensure energy efficiency. Here's how to do it:

Input to a fuzzy logic system:

- Remaining capacity of a node: If the energy of a node is low Participation in routing should be avoided. This information can be expressed as fuzzy information with the words "low", "medium" and "high".
- Distance to destination: Geographic distance to the destination node. Ambiguous words may include "short," "medium," and "long."
- Link Quality: A measure of the signal strength or reliability of the link to the next hop node. Unclear terms can include "weak," "moderate," and "strong."
- Network traffic/congestion: A measure of network congestion. Vague terms can include low, medium, and high.
- Node speed (In the case of mobile): The speed of nodes in a mobile IoT network may affect the selection of nodes as relays. Vague terms such as "slow," "medium," and "fast" may be used. Fuzzy inference rules: From these inputs Fuzzy inference rules are formulated to determine the best next hop for routing. Example rules might include: -

Rule 1: If the power level is 'High' the distance to the destination is 'Short' and the link quality is 'Strong', then select this node as the next hop with 'High' priority. ' -

Rule 2: If the energy level is "low", prioritise routes through nodes with "high" energy, even if the distance is "medium". -

Rule 3: If traffic is "high", route data to nodes with less traffic. Even if those nodes are far away.

Explosion: When fuzzy rules produce output (fuzzy decision) Fuzzy rules are translated into explicit values, such as a decision about the next hop node with the highest priority. This node then forwards the data to the destination[8].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

III. INTERNET OF THINGS WITH DIZZY LOGIC-BASED FORWARDING SYSTEM

In FLEA-RPL, the ETX method as well as demand statistics take place throughout reduction, whilst the rate of return navigation meter takes place during maximisation. This aids in the complicated route metrics calculation of the suggested protocol. In order to choose parenting according to the standard of the selected DODAG pyramidal master node, it presents a novel objective function (OF). In order to find the best DODAG parent node to send information coming from the network clients to the DODAG foundation, FLEA-RPL uses DODAG OF.

$$\text{Load Pqg DoDAG root)} = \sum_{x=1}^{Z} \text{load (x)} \quad (1)$$

A fuzzy-based routing protocol called FLEA-RPL is used to evaluate routing metrics to evaluate the parent node's quality. 3 vague source variables—RER, EXX, as well as Load—as well as a vague output term that aggregates the primary node's performance metrics are used. To choose the best course of action, this procedure entails converting input variables into fuzzy values and reversed.

$$\text{Load (x)} = \sum_{m=1}^{\text{child\_count (m)}} \quad (2)$$

The amount of network data sent over a given time known as the traffic load, is handled by a load-balancing feature. This feature makes sure traffic is spread among network nodes by tweaking the load to match the number of child nodes. To improve data flow, experts figure out the traffic load on a specific path (P) between a source node (Q) and the DODAG root.

A. Estimated Number of Transmissions

The amount of effective broadcasts needed to send material to the base node determines the calibre of the link between a DODAG participating node to the DODAG root.

ETX (Expected Transmission Count) : It affects the reliability of a link between two DODAG nodes. This includes the ratio of forward delivery, whereby we can know about number the of data packets received by the destination node, and the ratio of reverse delivery, that we can know about the number of acknowledgement packets returned back to the source[9].

In this case, \(the variables x\) denotes a single node, while \(n\) denotes the total number of nodes along a specified path \(the P\). The forward delivery ratio is called FD, and the opposite delivery ratio is called RD. The quality of the end-to-end communication between a source node and the DODAG root is indicated by the ETX of a route. Determine the total ETX on the path \(P\) that transmits information generated by the receiving node \(q\) to the root using equation (3). This gives an accurate representation of how reliable and efficient the method is.

$$\text{ETX (x)} = 1/\text{FD x } | \text{ RD} \quad (3)$$

B. Fuzzification

The system converts specific (crisp) input statistics into fuzzy enter values for processing inside a fuzzy logic framework. The inputs required for this method encompass important information about DODAG hyperlinks and nodes. Key components of the fuzzy good judgment device, specifically linguistic variables and club features, are mentioned beneath.

C. Linguistic Variable

The linguistic variable is an essential thing of fuzzy logic systems.

LOAD	*Low, standard, heavy*
ETX	*Small, standard, extended*
RER	*Quite low, average, packed*
QUALITY OF NEIGHBOUR	*Terrible, very poor, poor, excellent, favourable, brillant*

Table 1: Linguistic variable

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

It represents values through the use of descriptive terms or phrases, allowing the machine to handle qualitative statistics successfully. Table 1 illustrates the linguistic variables employed for both enter and output routing metrics, showcasing their position in encapsulating the network's dynamic characteristics inside the fuzzy common sense framework[10].

D. Membership Function

Within the fuzzier good judgement framework, language parameters are essential because they function as non-numerical identifiers that use language rather than exact numerical data to express values. The linguistic variables utilized for input and output routing metrics, primarily (h_1), (i_1), and (j_1), are listed in Table 1. The fundamental components for the device's assessment system are shaped by (h_1) and (j_1).

$$\mu_{c1}(z) = \begin{cases} 0, & z \le h_1, \\ \dfrac{Z - h_1}{i_1 - h_1}, & h_1 < z \le i_1, \\ \dfrac{j_1 - z}{j_1 - i_1}, & i_1 < z < j_1, \\ 0, & j_1 \ge z. \end{cases} \quad (4)$$

4 scalars parameters—h_2, i_2, j_2, and k_2—are used to characterise the serpentine curve, which is expressed as a reality value vector (y). Here, the bottom as well as higher boundaries of the arc are indicated by (h_2) and (k_2), respectively, while the middle as well as greater guide restrictions are specified by (i_2) and (j_2). This property, which is frequently used to illustrate version membership possibilities in computational systems, is frequently described in terms of those properties.

$$\mu_{c2}(y) = \begin{cases} 0, & y \le h_2, \\ \dfrac{y - h_2}{i_2 - h_2}, & h_2 < z < i2, \\ 1, & i_2 < z \le j_2, \\ \dfrac{j_2 - y}{j_2 - k_2}, & j_2 < z < k_2, \\ 0, & k_2 \ge z, \end{cases} \quad (5)$$

$$\text{Light (Load)} = \begin{cases} 1, & \text{if Load} \le 2, \\ \dfrac{\text{Load} - 3}{6 - 3}, & 3 < \text{Load} < 5, \\ 0, & \text{if Load} \ge 5. \end{cases} \quad (6)$$

The load premium-ship function showcases the site visitors' load skills using network nodes. Traffic load can be described using linguistic variables including "Heavy," "Normal," and "Light," as mentioned with the aid of Z. Latib et al. [20]. The club characteristic for "Light" site visitors load is described in Equation (6). Similarly, club features for other linguistic variables representing traffic load also can be derived[11].

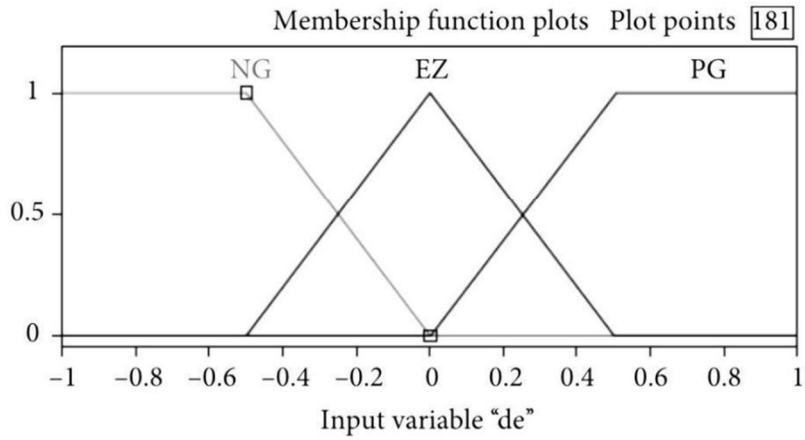


Figure 2: Given membership function of Load

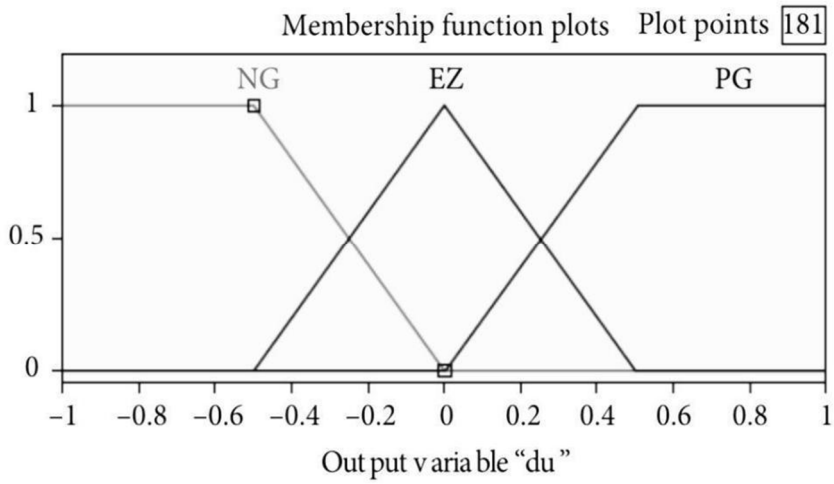


Figure 3: Membership function of RER

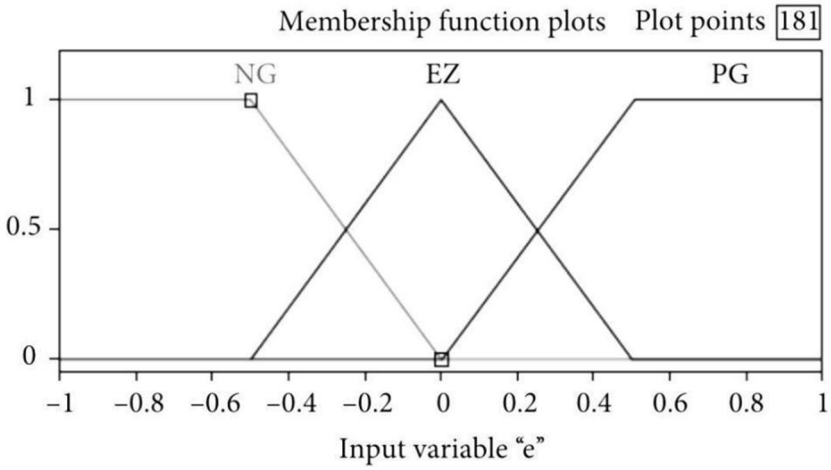


Figure 4: Membership function of ETX

In addition to load, club functions may be formulated for different metrics including ETX, RER, and neighbouring nodes exceptional. Figure 2 illustrates the burden club feature. The RER membership characteristic, then again, reflects the modern-day energy levels of the RPL router, providing insights into strength performance inside the community[12].

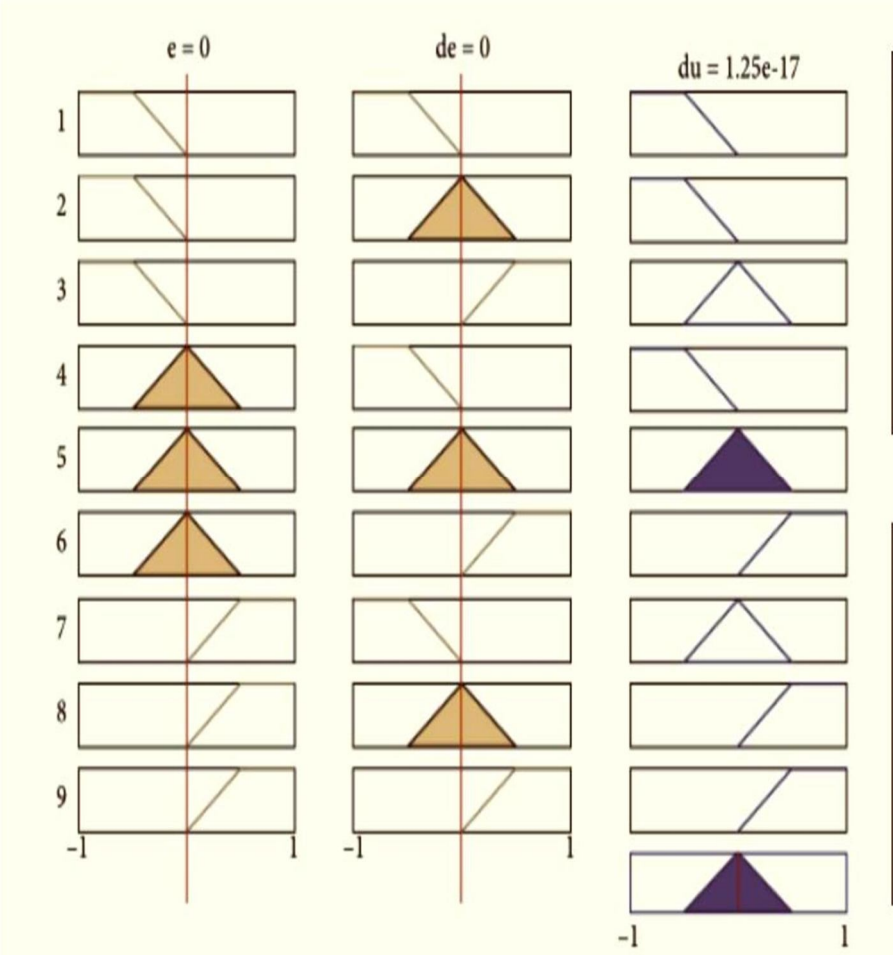


Figure 5: Membership function of neighbour quality

E. Fuzzy Rule

In FLEA-RPL, the machine makes use of a fuzzy inference mechanism to manage input and output variables. The input fuzzy variables—RER (Residual Energy Ratio), ETX (Expected Transmission Count), and Load—are mapped to their respective membership functions, which constitute them in a linguistic shape (e.G., "Low," "Medium," "High"). The output fuzzy variable represents the neighbour node quality, indicating how nicely a node within the community may be selected as the figure for routing.

Fuzzy Rule Base: Define a set of IF-THEN rules for connecting inputs and determining outputs (Routing Priority, RP):

If the remaining power is high and the distance is similar and the connection quality is good, then the Routing Priority is high.

If the remaining power is low or the connection quality is poor The routing priority is low.

If the remaining energy is moderate the distance is moderate and the connection quality is moderate The routing priority is moderate.

The fuzzy rule base in FLEA-RPL includes 27 awesome rules, derived from the 3 input variables. Each of these input variables has its own set of membership features that correspond to specific linguistic phrases. The number of policies is calculated using multiplying the feasible states of every entered variable, wherein each variable has three membership functions (e.g., Low, Medium, High). The output of those rules is determined with the aid of evaluating the aggregate of fuzzy inputs through a procedure known as fuzzy inference, resulting in the dedication of the neighbour node[13].

	Residual energy	Load	Neighbour quality	ETX
1	Packed	Low	Brillant	Short
2	Packed	Low	Excellent	Preferable
3	Packed	Low	Preferable	Long
4	Lower	Low	Preferable	Short
5	Lower	Low	Poor	Preferable
6	Lower	Low	Very poor	Long
7	Standard	Low	excellent	Short
8	Standard	Low	Preferable	Preferable
9	Standard	Average	Preferable	Short
10	Packed	Average	Excellent	Short
11	Packed	Average	Preferable	Preferable
12	Packed	Average	Poor	Long
13	Lower	Average	Poor	Short
14	Lower	Average	Very poor	Preferable
15	Lower	Average	Poor	Long
16	Standard	Average	Preferable	Short
17	Standard	Average	Less preferable	Preferable
18	Standard	High	Less poor	Long
19	Packed	High	Preferable	Short
20	Packed	High	Poor	Preferable
21	Packed	High	Preferable	Long
22	Lower	High	Less poor	Short
23	Lower	High	Poor	Preferable
24	Lower	High	terrible	Long
25	Standard	High	Poor	Short
26	Standard	High	Less poor	Preferable
27	Standard	High	Poor	Long

Table 2: fuzzy rules

However, the fuzzy rule base can be updated with more accurate utility preference when given. FLEA-RPL can thus be adapted to different network conditions and needs [14].

For fuzzy rules evaluation, FLEA-RPL uses the Mamdani type fuzzy inference. This model applies If-Then statements to analyse situations solely based on the fuzzy inputs. A max-min composition operation is used to unify fuzzy enter values of the Mamdani model, followed by a defuzzification technique to translate the bushy output proper into a crisp worth which implies the class of the neighbour node. This crisp cost releases the routing choice in deciding on the nice describe node for the switch of information[15].

In short, the FLEA-RPL dynamically assesses different network situations via fuzzy common sense and thus makes optimal routing decisions. This end device makes sure that the conversation inside the community is efficient and adjusts to changing visitors, the nature of the hyperlinks and their energy levels. The fuzzy regulations valuable to this decision-making process are shown in Table 2.

F. Defuzzification

Defuzzification is a critical step in a fuzzy inference gadget [24], wherein the bushy output is transformed right into an unmarried crisp fee. This fee usually falls within a defined range, which includes 0 to one hundred. In the FLEA-RPL protocol, the weighted average approach is hired for the defuzzification technique. This technique computes the crisp output by calculating the weighted average of the club function outputs, with weights similar to the degree of membership of each fuzzy set. The mathematical representation of this defuzzification approach is provided in [16].

Fuzzy output transformation (path priority) to a sharp value using methods such as the Centroid method:

RP= ∑i μ(xi)·xi

∑i μ(xi)

$$S = \frac{\sum_{j=1}^{N} W_j \times \mu_c(W_j)}{\sum_{j=1}^{N} \mu_c(W_j)}. \quad (7)$$

In the defuzzification technique, **S** shows the sharp output value, and **c** denotes a fuzzy location. **N** suggests the total wide variety of fuzzy regulations, even as **μc** represents the predicate fact fee within a specific domain **W**, with **Wj** similar to the domain value for rule **j.**

$$S = \frac{(0.5 \times 70 + 0.5 \times 86)}{(0.5 + 0.5)} = 78.$$

For instance, whilst considering the determined node choices in FLEA-RPL, the metrics concerned are **Load, RER, and ETX,** with their values being 2, hundred seventy-five, and 10, respectively. The linguistic variables used to describe those metrics are "Light" and "Standard" for Load, "Full" for RER, and "Short" for ETX. In this case, the club values for those linguistic terms are as follows: Light (0.5), Normal (0.5), Full (1), and Short (1).

During the fuzzification technique, FLEA-RPL generates policies, which can be based totally on the fuzzy rule base [25]. For the given instance, Rule 1 and Rule 4 are activated consistent with the bushy enter values. Both regulations yield an output of zero.5. Consequently, the qualitative assessments of the neighbouring nodes, based totally on their association to the "Very Good" and "Excellent" categories, bring about corresponding values of 70 and 86[17].

Rank (x) = rank increase + rank (parent node) (8)

rankIncrease= minHopRankIncrease+ step (9)

The spiky reasoning manipulation, which collects the outcomes from the operational regulations plus calculates the defuzzification number in accordance with the weighted average or another chosen defuzzification methodology, is used in calculating the finalised uncertain reasoning price. This produces a clear output that highlights the network's adjoining nodes' remarkable performance.

Similarly, the FLEA-RPL evaluated the best quality of parent node in the participant node and selected the discern with the highest crisp cost [25].

The participant's node x then calculates its rank in the DODAG by considering its ranking augmentation along with each rank of the observer node. The stage cost as well as the minHopRankIncrease are the two rules that determine the rank adjustment. The aim function, which takes into account several traffic gauges, is used to calculate the step cost.The minHopRankIncrease is a predefined regular, generally set to 256. The final rank calculation is primarily based on those elements, ensuring that the participant node selects the highest quality determined node for routing, with the rank increment reflecting the node's role within the DODAG hierarchy. The rank computation is designated in [18].

In FLEA-RPL, path advent occurs via primary methods. First, the participant node proactively transmits a DIO (DODAG Information Object) message to the DODAG root. Second, the DODAG root periodically pronounces DIO messages to its neighbouring nodes. For information transmission, the protocol performs figure selection with the use of fuzzy common sense to determine the maximum finest discern node for the player [19]. The parent selection node is selected in figure 6.

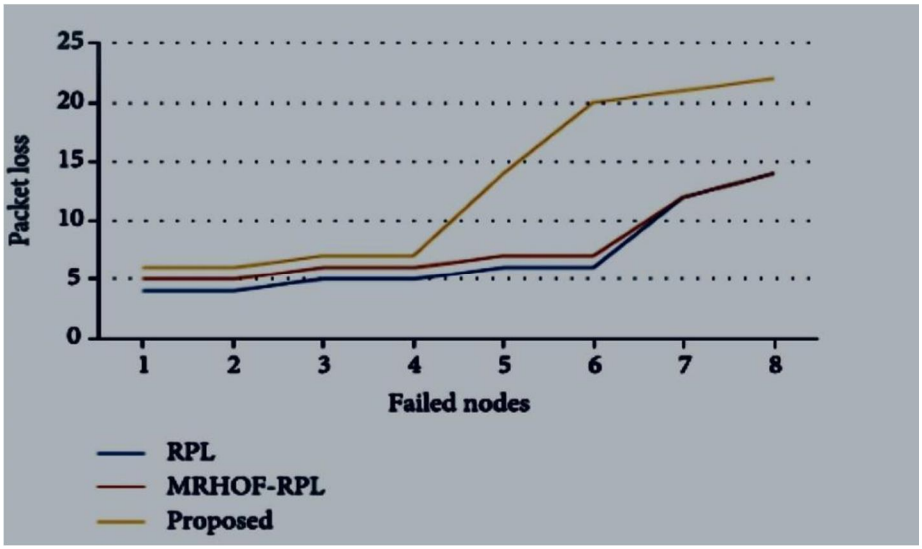


Figure 6: Average calculated packet loss ratio in the node failure scenario.

The DODAG triggers a Trickle timer (indicated with the utilization of I) in order to maintain the network topology throughout the nodes. At C, the preliminary counter begins from zero and timer intervals are ranging from Imin to Imax. These durations are known in RPL as Imin (normally 12 ms) and Imax (normally 10 ms). In this Trickle c language, the participant node sends response message to its decided parent node inside the domain of directed acyclic graph (DODAG). Then the discern node obtains the reception of the message by sending a DAO-ACK (Destination Advertisement Object Acknowledgment) message back to the participant [20]

The parent choice set of rules is in addition distinct within the pseudocode, while Figure 7 offers the flowchart of the Optimisation Algorithm. This optimisation set of rules is accountable for selecting the first-class features inside the machine, ensuring that the routing technique is both green and adaptable to dynamic network conditions[21].

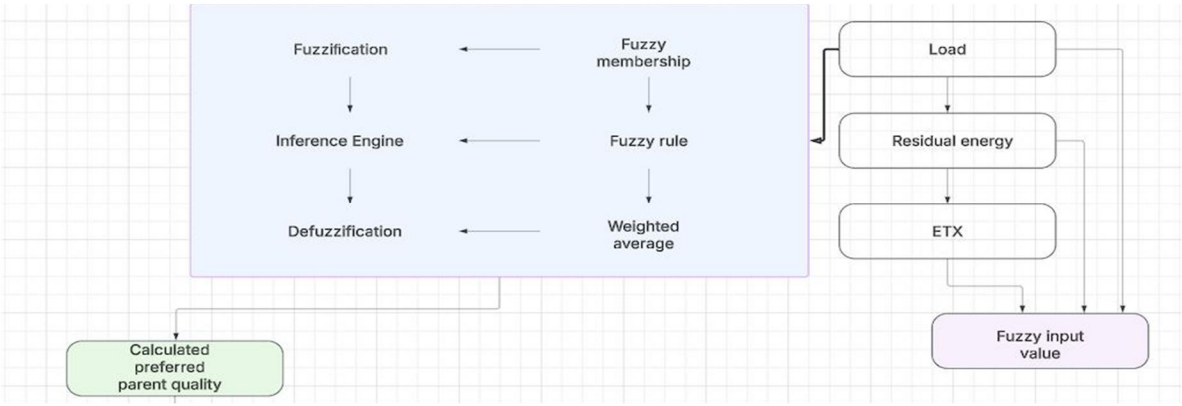


Figure 7: Parent selection mechanism

Algorithm 1: Selection method for parents.

Input: parentNodeList
Output: bestPreferredParentNode
1: method SELECTING PARENTS
2: start:
3: optimal ParentNodeRank is infinite
4: for preferredParentNodeId in parentNodeList do
5: rank(participant) = rank(parentNode) + rankIncrease;
6: rankIncrease = step + min HopRankBoost
7: Develop a linguistic variable and define the membership for Load, ETX, and RER
8: Create a fuzzy rule set
9: Assess the produced guidelines using a fuzzy rule framework
10: Execute the defuzzification procedure
11: if optimal If ParentNodeRank exceeds preferredParentNodeRank, then
12: optimal ParentNodeRank equals preferredParentRank
13: conclude if
14: conclude loop
15: continue while condition is met ParentNodeRank is at its peak ParentNodeRank do
16: participantNodeId=preferredParentNodeId
17: conclude loop
18: Return optimal PreferredParentNode
19: conclude process

The Directed Acyclic Graph, or DODAG, is started with inter-cluster routing [28]. Selecting the optimal figure node for data transfer within the cluster is the responsibility of the Cluster Head (CH) node. Every Cluster Member node in the cluster receives the DIOC message. After that, the CH node waits for the CM nodes to respond. The CH node sends a CH-ACK (Cluster Head Acknowledgement) message to the designated CM nodes within the cluster once it has compiled all of the responses [22]. During the upward routing process in MCEA-RPL (Modified Constructed Energy-Aware Routing Protocol), the CH node may sustain 2 different types of discern nodes: the inadequate form plus the distinctive parent.

The inefficient discern gathers information from all CM nodes and performs statistical aggregation. The primary entity processes and subsequently transmits the compiled information to the appropriate CH figure node situated in the upper tier of the network. Furthermore, the less-than-ideal identification is equipped with DIOC management messages, which include pertinent established data to aid in the routing selection process[23]. In the specified selection process, the less-than-ideal figure assesses the capability of CH parent nodes relying on key routing metrics: ETX (Expected Transmission Count) and RER (Residual Energy Ratio). These metrics are employed to identify the optimal method for transmitting data, ensuring effective routing throughout the cluster. The Fuzzy Inference System (FIS) plays a crucial role in the fuzzy logic framework by transforming input values into output values through the application of fuzzy logic principles [24].

Within the FIS framework, the main operations involve fuzzification, which transforms precise inputs into fuzzy values; the inference engine, which utilizes logical rules to process the fuzzy inputs; fuzzy rules, which establish the connections between inputs and outputs; and defuzzification, which translates the fuzzy output into a clear value for decision-making. This methodical approach facilitates flexible and responsive routing choices in MCEA-RPL by considering uncertainties and fluctuations in community conditions.

IV. EXPERIMENTAL ANALYSIS AND RESULT

A. Simulation Setup

The performance of the FLEA-RPL protocol changed into evaluating the usage of the COOJA network simulator, where it became tested and compared towards well-known protocols including RPL, FL-RPL, and MRHOF-RPL. The simulation environment utilized Tmote Sky nodes, which had been randomly dispersed throughout a 600m x 600m network vicinity. The simulation covered a DODAG root node and a set of 100 RPL routers, efficiently representing an ordinary community configuration in a low-power and lossy community (LLN).

The simulation was conducted under 3 awesome conditions, with various information transmission quotes: 1 packet in step with minute, 6 packets in step with minute, and 10 packets consistent with minute [25]. These configurations allowed for the evaluation of protocol performance under distinctive network site visitors hundreds. The results furnished insights into the common performance metrics received from the simulation runs.

The setup, inclusive of the community configuration and simulation parameters, is summarized in Table 3. This table outlines key simulation info, inclusive of node placement, network length, and traffic patterns, providing a clear overview of the experimental situations used to evaluate the protocols' performance and overall performance under numerous community situations.

B. Performance Metrics

The overall performance of the FLEA-RPL protocol is evaluated using the following metrics [26]:

1) Residual Energy: This represents the ultimate strength to be had in a node, imparting insights into the energy performance and sturdiness of the network.

2) Packet Loss Ratio (PLR): It refers to a proportion of the total broad spectrum of knowledge messages received to the total extensive diversity of messages that were ignored. This indicator measures how consistently the audience delivers reports.

3) End-to-End Delay: Measures the average time taken to efficiently transmit records from the supply node to the vacation spot. It displays the general latency in the network.

4) Parent Change Frequency: Tracks the range of figure node adjustments that occur in the course of the simulation. This metric shows the steadiness of the routing topology and the responsiveness of the protocol to dynamic network conditions[27].

Parameters used for simulation	Values
OS	Contiki 2.7
Total number of nodes	100 RPL routers and 1 DODAG root
Timer for data packet	60 sec
Duration of simulation	1 hour
MAC/adaptation layer	ContikiMAC/6LowPAN
Battery level full	1500 mA
Area of network	600 × 600 m2
Environment of radio	Unit disk graph medium
Simulator	COOJA
Minimum DIO interval	12
Type of node	Tmote sky
DIO interval doubling	10
Routing protocol	RPL

Table 3: settings of simulation and all parameters

C. Results after Evaluating Performance

The overall performance of the FLEA-RPL protocol was analyzed through simulations, specializing in key evaluation metrics such as manage overhead, end-to-end latency, residual energy, energy consumption, and packet loss ratio. The outcomes have been in comparison towards installed routing protocols, consisting of well-known RPL and MRHOF-RPL [28].

1) Scenario 1

Data Transmission Rate of One Packet in line with Minute

Figure eight illustrates the parent change frequency across specific RPL protocols for a transmission fee of 1 packet according to minute. The parent trade metric for FLEA-RPL was assessed as a degree of community stability and benchmarked towards trendy RPL, FL-RPL, and MRHOF-RPL. The discovered determined exchange values have been:

- Standard RPL: 0.20
- FL-RPL: 0.28
- MRHOF-RPL: 0.25
- FLEA-RPL: 0.17

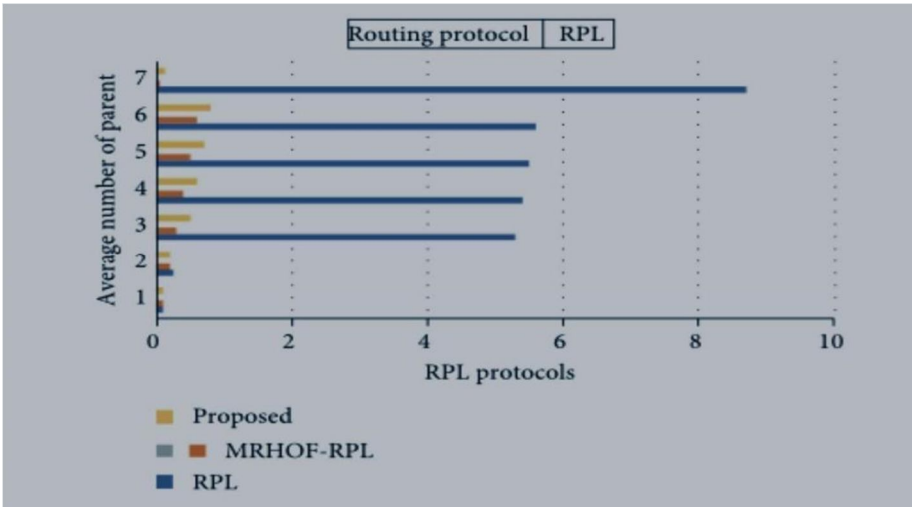


Figure 8: Different RPL protocols with changes in parental data.

The effects imply that FLEA-RPL exhibited a decrease in discerning trade frequency as compared to the other protocols. This reduced parent switching is attributed to the incorporation of the load metric in figure selection, which allows FLEA-RPL to always select the maximum optimal figure inside the DODAG. Consequently, this complements community stability and contributes to an extended community lifespan. The latency values for RPL, FL-RPL, MRHOF-RPL, and FLEA-RPL protocols are three. Eight seconds, 3.2 seconds, 3.7 seconds, and 2.9 seconds, respectively. These effects display that FLEA-RPL achieves the lowest latency in many of the protocols, emphasising its performance in parent node selection and traffic distribution across the community[29].

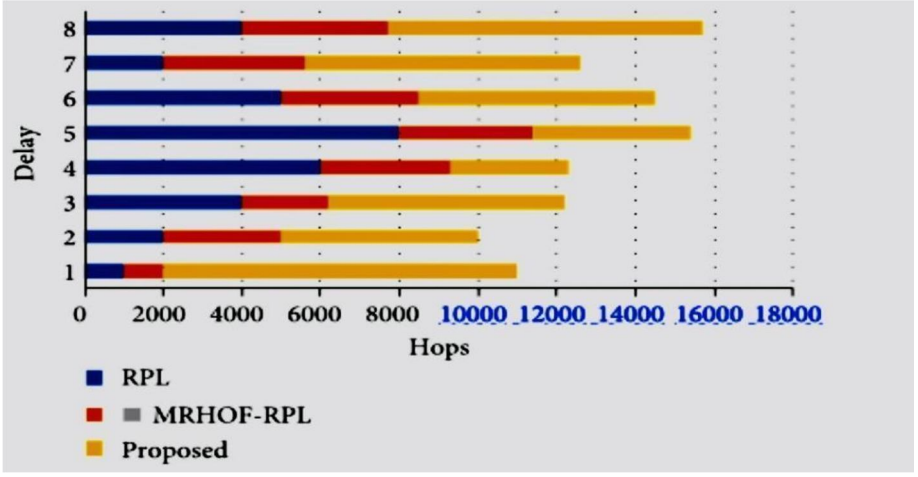


Figure 9: Delay (end to end) vs no. of hops

The residual strength tiers of community nodes with a data transmission rate of one packet per minute are shown in Figure 9. The final 10% of nodes in the FLEA-RPL protocol maintain power stages between 90% and 92%, whereas 90% of nodes retain residual electricity stages between around 84% and 87%. In contrast to the conventional RPL, FL-RPL, and MRHOF-RPL protocols, FLEA-RPL significantly improves the strength and lifespan of networks. The use of the Residual Energy Ratio (RER) to choose the most beneficial node for transmitting records to the DODAG root is responsible for this breakthrough.

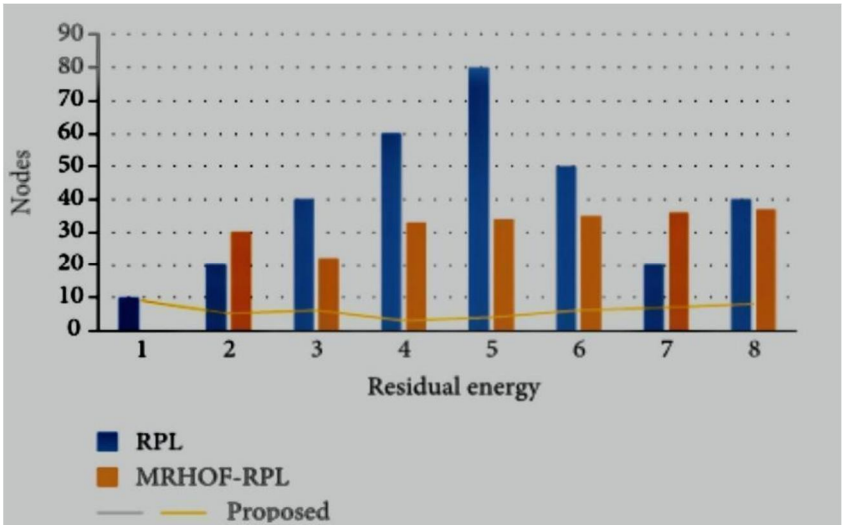


Figure 10: The residual energy of network nodes.

Figure 10 affords the packet loss ratios for RPL, FL-RPL, MRHOF-RPL, and FLEA-RPL protocols because the network length will increase, with a hard and fast information transmission rate of 1 packet per minute. The conventional RPL protocol exhibits a high packet loss ratio because of its reliance solely on the variety of hops for parent node selection, as cited in [32]. In assessment, MRHOF-RPL considers only the Expected Transmission Count (ETX) metric, which accelerates battery depletion and contributes to big packet loss[30].

For a network size of 100 nodes, the packet loss ratios are observed to be 6% for RPL, 4% for FL-RPL, 5.8% for MRHOF-RPL, and 3.8% for FLEA-RPL. These results highlight FLEA-RPL's advanced overall performance in minimizing packet loss. The experiments similarly indicate that as the range of nodes in the network increases, the packet loss ratio tends to upward thrust across all protocols[31].

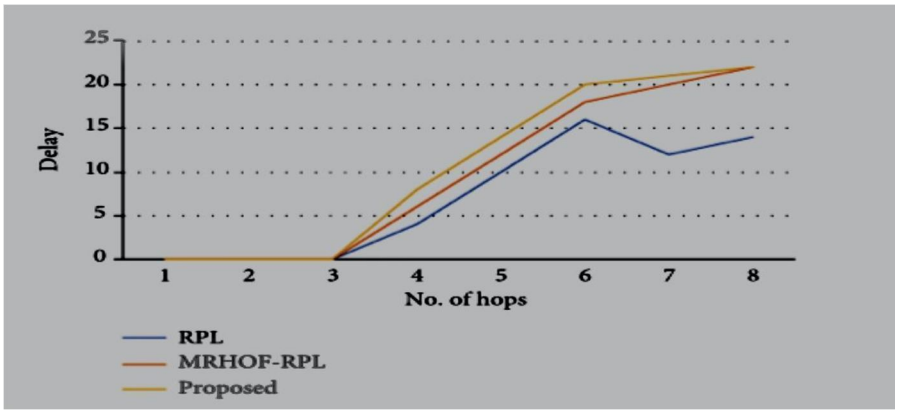


Figure 11: Given ratio of network size and packet delivery.

Figure 11 illustrates the impact of node screw-ups on packet loss, with the range of failed nodes varying from zero to 30. The analysis exhibits that because the number of failing nodes increases, the packet loss ratio also rises, as noted in [33]. Among the evaluated protocols, FLEA-RPL demonstrates superior resilience, decreasing the packet loss ratio to 2%–4% for a network with 30 failed nodes. In comparison, RPL, FL-RPL, and MRHOF-RPL revel in extensively higher packet loss ratios, achieving as much as eleven[32].

This development in FLEA-RPL is attributed to its integration of the Expected Transmission Count (ETX) and Residual Energy Ratio (RER) metrics in parent selection, which allows the distribution of the traffic load extra correctly. However, as node failures grow, the chance of DODAG root instability grows because of the immoderate trade of manipulated packets required for route reconstruction and renovation. This highlights the importance of sturdy mechanisms to handle network disruptions and maintain reliable conversation[33].

2) Scenario 2

Figure 6 illustrates the discern exchange values for diverse RPL protocols. To evaluate community stability, the figure of alternate cost of FLEA-RPL is recorded and compared with the ones of popular RPL, FL-RPL, and MRHOF-RPL. The determined trade values for well-known RPL, FL-RPL, MRHOF-RPL, and FLEA-RPL are 0.3, 04, 035, and 0.28, respectively. It can be discovered that FLEA-RPL reveals a decrease in determined trade value as compared to RPL, FL-RPL, and MRHOF-RPL. Figure 12 suggests the common variety of facts worries, which is by and large influenced by the aid of the burden metric utilised in selecting the figure node.

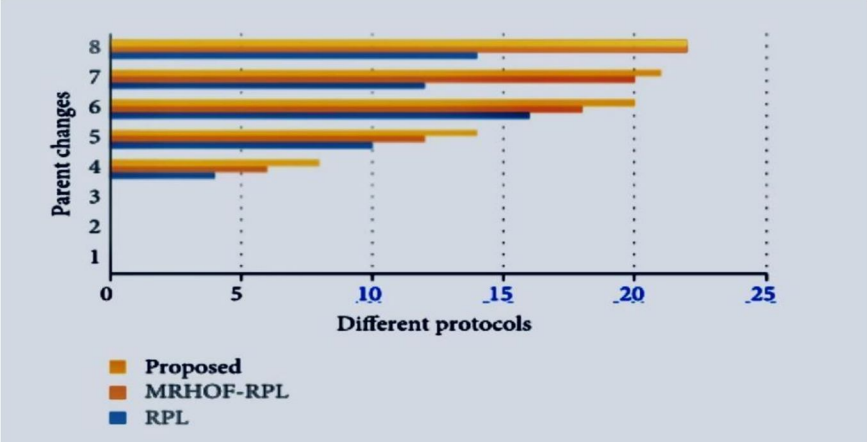


Figure 12: The average number of data that concerns various protocols.

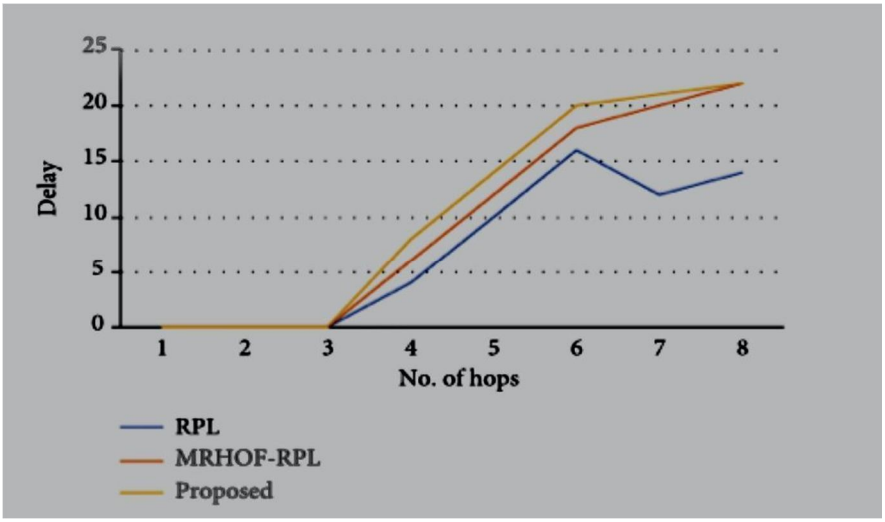


Figure 13: Delay (end- to -end) vs total number of hops.

Figure 13 presents the common cease-to-quit latency as a characteristic of the range of hops. The stop-to-stop put-off for standard RPL, FL-RPL, MRHOF-RPL, and FLEA-RPL is measured at 5. 5, 5, 4.8, and 4.2 seconds, respectively. These results reveal that FLEA-RPL well-known shows a decrease in give-up-to-cease delay as compared to traditional RPL, FL-RPL, and MRHOF-RPL. This discount in put-off can be attributed to the more green distribution of network traffic at some stage in the discern choice procedure, which minimises routing inefficiencies[34].

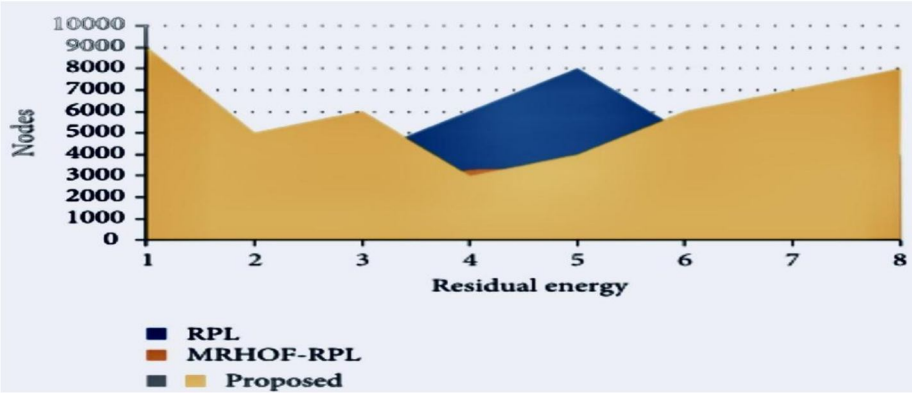


Figure 14: The residual energy of network nodes.

Figure 14 depicts the residual strength of network nodes below a facts transmission fee of six packets according to minute. In the case of FLEA-RPL, approximately 90% of the network nodes preserve residual electricity between 62% and 66%, whilst the last 10% show residual energy levels starting from 70% to 72%. This shows that FLEA-RPL now does not best enhance community MRHOF-RPL in terms of residual strength retention and average network lifetime.

Figure 14 illustrates the packet loss behaviour of the RPL, FL-RPL, FLEA-RPL, and MRHOF-RPL protocols as a feature of network length, with a regular statistics transmission fee of six packets in step per minute. The wide variety of failed nodes is varied from 0 to 30. It is evident that packet loss escalates because the range of malfunctioning nodes will increase. Standard RPL, which does not contain hyperlink first-class metrics in its figure selection technique, reviews better packet loss. In evaluation, MRHOF-RPL selects figure nodes primarily based completely on hyperlink satisfaction, which improves reliability but speeds up node strength depletion, resulting in a multiplied packet loss fee. FLEA-RPL, alternatively, considers each link exceptional (ETX) and traffic load during discerning node selection, leading to a greater balanced method that reduces packet loss. For a community inclusive of a hundred nodes, the packet loss quotes for popular RPL, FL-RPL, MRHOF-RPL, and FLEA-RPL are thirteen%, 8%, 12%, and seven%, respectively, with FLEA-RPL demonstrating the most efficient performance in terms of packet retention.

Figure 15 depicts the packet corruption fees as a characteristic of the number of failed nodes, with the records switch price maintained at six packets according to minute. As the variety of failed nodes increases from 0 to 30, there's a proportional rise in packet damage. Since RPL does not forget hyperlink best metrics in its discerning selection, it reveals an excessive degree of packet damage. In assessment, FLEA-RPL achieves a large discount in packet corruption. When the range of failed nodes reaches 30, FLEA-RPL reduces packet harm by 7%, 2%, and 4% compared to RPL, FL-RPL, and MRHOF-RPL, respectively. This reduction is attributed to FLEA-RPL's twin approach to figure choice, which incorporates each the Expected Transmission Count (ETX) and the community's traffic load, consequently optimising the change-off between power consumption and network reliability. This technique notably mitigates packet corruption, especially in scenarios with higher node failures.

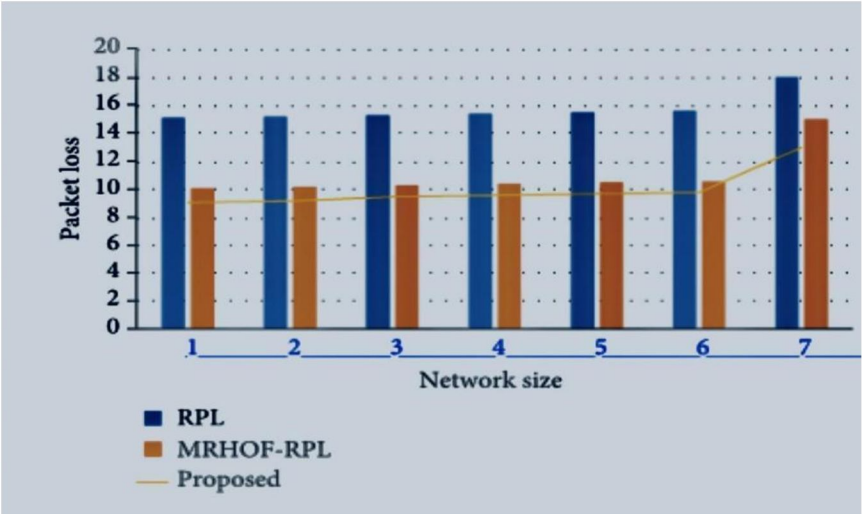


Figure 15: Represents packet loss in network.

3) Scenario 3

Figure 16 illustrates the determined switch frequency for one-of-a-kind RPL protocols, with an information transmission charge of ten packets per minute. To examine network balance and resilience [35], the determined trade charge of FLEA-RPL is measured and compared in opposition to that of fashionable RPL, FL-RPL, and MRHOF-RPL. The figure trade charges for popular RPL, FL-RPL, MRHOF-RPL, and FLEA-RPL are 0.4, 0.5, 0.45, and 0.35, respectively.

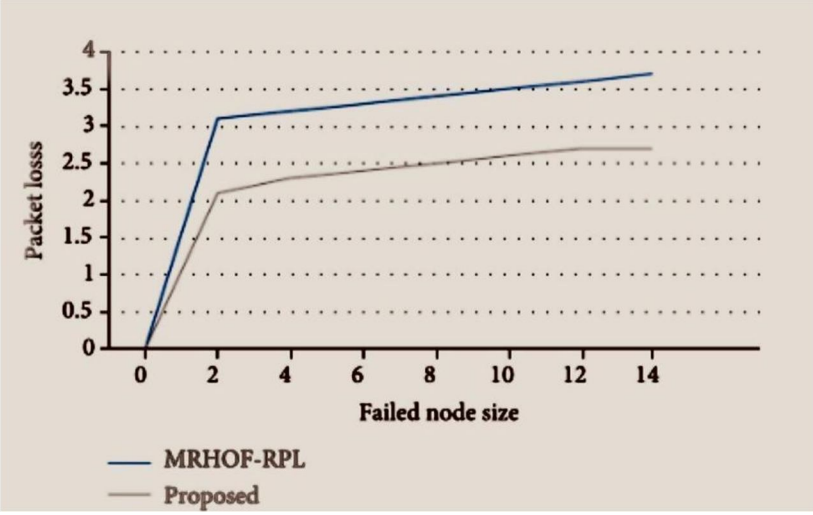


Figure 16: The node failure scenario with less packet loss.

The results suggest that FLEA-RPL has a lower figure alternate fee compared to RPL, FL-RPL, and MRHOF-RPL. This is usually attributed to FLEA-RPL's incorporation of the burden metric in its figure choice algorithm. By factoring in community visitors' load at the side of hyperlink best (ETX), FLEA-RPL ensures extra solid discern node assignments, leading to fewer topology changes. This strategy enhances the robustness of the Directed Acyclic Graph (DODAG) and contributes to a prolonged community lifetime by minimising common parent reassignment and enhancing common routing performance.

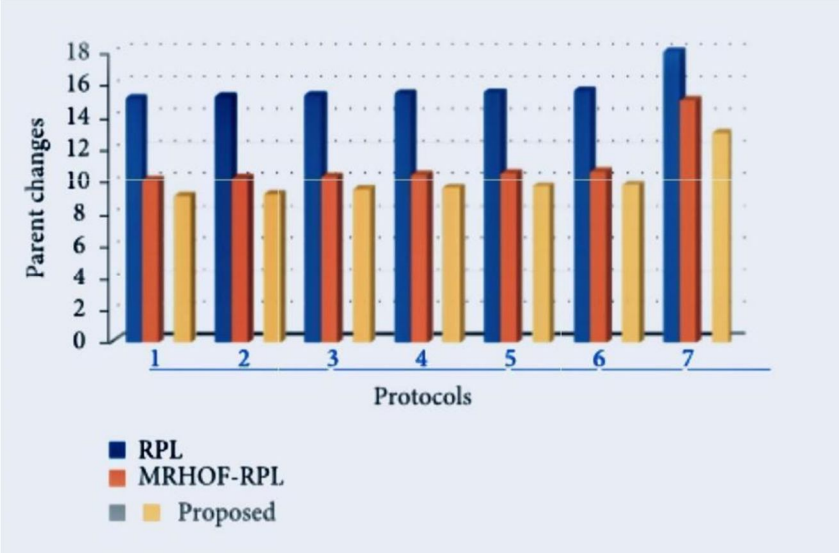


Figure 17: Average comparison in the given system.

Figure 17 illustrates the end-to-cease latency as a feature of the hop count number. The discovered latency values for popular RPL, FL-RPL, MRHOF-RPL, and FLEA-RPL are 6. Five, 6, 5.Five, and 5 seconds, respectively. These effects indicate that FLEA-RPL achieves decreased latency compared to conventional RPL, FL-RPL, and MRHOF-RPL. This reduction in put-off is attributed to the more efficient distribution of network visitors throughout the parent selection technique, which helps to optimize routing paths and reduce the overall transmission postponed throughout the community.

Figure 18 illustrates the residual power levels of network nodes at some stage in records transmission at a charge of ten packets according to minute. Notably, in FLEA-RPL, the residual energy of the community nodes ranges between 51% and 56%. In comparison to standard RPL, FL-RPL, and MRHOF-RPL, FLEA-RPL demonstrates improved community sturdiness and extra-efficient energy retention. This development can be attributed to the assessment of the Residual Energy Ratio (RER) in FLEA-RPL, which enables the optimal choice of parent nodes for forwarding information in the direction of the DODAG root. By integrating RER into the parent selection manner, FLEA-RPL guarantees greater balanced energy intake across the community thereby prolonging the operational lifetime of the nodes and enhancing the general energy performance of the gadget.

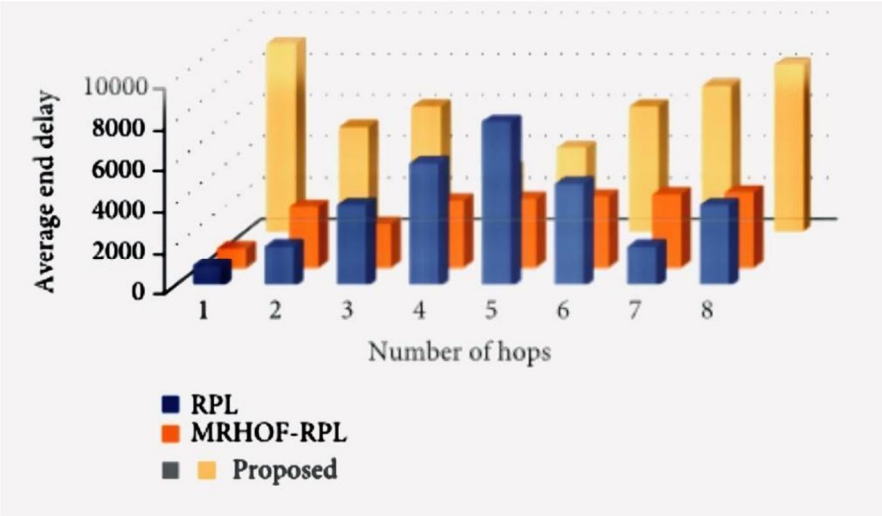


Figure 18: The time delay between the nodes.

Figure 19 illustrates the packet loss ratio for RPL, FL-RPL, MRHOF-RPL, and FLEA-RPL as a function of community length throughout the 4 RPL variants. For a community of one hundred nodes, the packet loss ratios for popular RPL, FL-RPL, MRHOF-RPL, and FLEA-RPL are 17%, 16%, 13%, and 10%, respectively, as proven within the packet loss ratio table. It is found that because the network size will increase, the packet loss ratio also rises. This growth in packet loss may be attributed to the developing network site visitors and the following congestion, which might be exacerbated by using the larger scale. However, FLEA-RPL mitigates this effect by incorporating each visitor's load and Expected Transmission Count (ETX) into its parent choice process. This dual consideration allows greater green routing decisions, lowering packet loss while the network length expands.

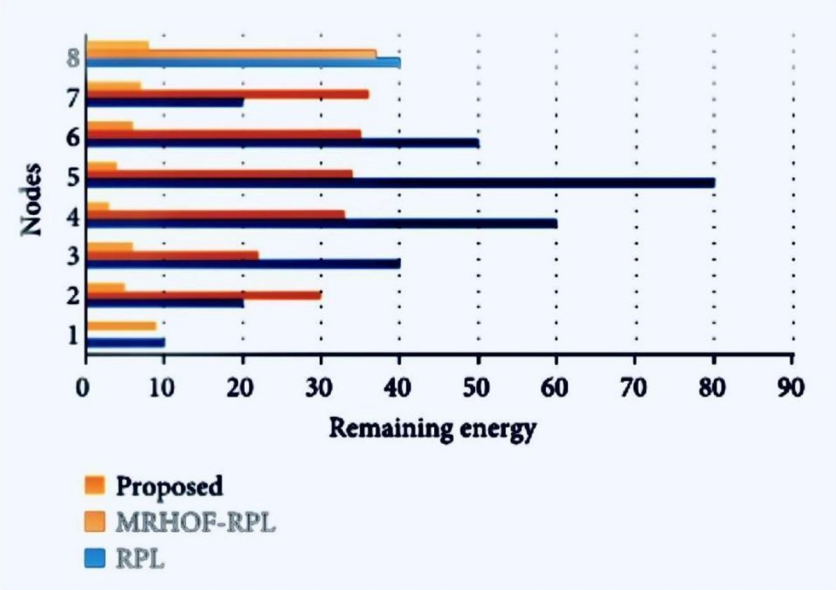


Figure 19: The network nodes and remaining energy

Figure 20 illustrates the device-degree packet loss in the presence of failed nodes, with the variety of faulty nodes ranging from 0 to 30. As anticipated, an increase in packet loss is located because the quantity of faulty nodes rises. This is by and large due to RPL's failure to include link first-class metrics into its discern choice process, leading to suboptimal routing choices and, consequently, better packet loss. In assessment, FLEA-RPL demonstrates a great reduction in packet loss. When the range of failed nodes reaches 30, FLEA-RPL reduces the packet loss ratio using 15%, eight, and 10%, respectively, as compared to RPL, FL-RPL, and MRHOF-RPL. This development is a result of FLEA-RPL's twin method to determine selection, which integrates each hyperlink fine and network traffic load, allowing extra resilient and green routing underneath node failure conditions.

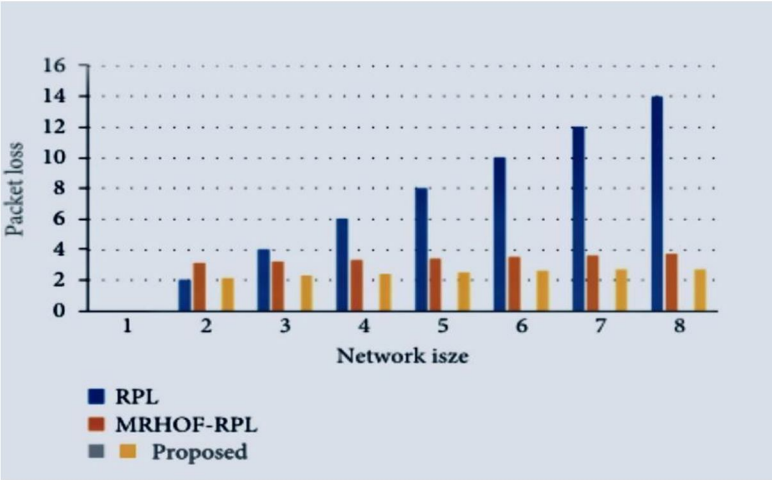


Figure 20: The ratio between packets and network inside the given system.

Figure 21 offers the relationship between packet loss and the wide variety of tried nodes in the routing protocol, highlighting the efficiency of different RPL variations in managing congestion and node failures for the duration of packet forwarding.

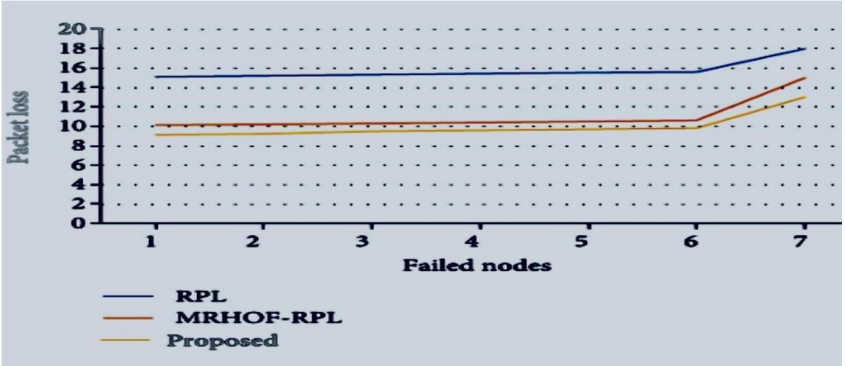


Figure 21: The ratio between packet loss and the attempted nodes in protocol.

V. CONCLUSION

This study uses the conventional RPL custom to deal with the difficulties of IoT networking protocols. The initial change that is suggested is the Fuzzy Logic-based Energy-Aware RPL (FLEA-RPL) protocol, which uses fuzzy good judgement to optimize advice selection based on ETX, Load, and RER metrics. Simulation results indicate that FLEA-RPL greatly increases solidarity in their lives. The next protocol that is presented is the IoT Multilayer Energy-Aware RPL (MCEA-RPL), in which the ecosystem is divide. By utilising fuzzy logic in conjunction with RSSI and PER data to determine the transition value, the 0.33 protocol, IoT Enhanced Mobility Support RPL (EM-RPL), enhances connectivity overall. EM-RPL rapidly identifies change channels to minimise path breakdowns along with improving data transfer when the transfer of information cost surpasses a certain amount. The outcomes of the experiment show that EM-RPL enhances node movement. Future studies should build on the current examination, particularly by tackling the usage of a limited number of sink nodes for data succession, which streamlines the neighbourhood structure, even though those standards enhance the IoT organisation lifetime.

It is crucial to control energy use across nodes as internet of things gadgets proliferate. The primary objective of this research is to enhance the RPL standard (Routing Protocol for Low-Power, Lossy Networks) by tackling issues in the IoT routing protocols. system that assesses important indicators including network load along with projected message count (ETX). Additionally, the residual energy ratio (RER) is used to identify the best data transmission method. According to the simulation results, FLEA-RPL increases energy efficiency, which enhances overall performance. Energy Awareness at Several Levels RPL (MCEA-RPL): This protocol groups networks into comparable-sized groups. It optimises path selection using fuzzy logic in accordance with RER and ETX parameters.

The data collected by the cluster head node is aggregated and sent to the sink node. Simulation results indicate that MCEA-RPL significantly extends the network lifetime compared to traditional RPL protocols by balancing power consumption among nodes.

Advanced Movement Support RPL (EM-RPL):. EM-RPL addresses mobility challenges in IoT networks by applying fuzzy logic to measures such as received signal strength indicator (RSSI) and packet error rate (PER) to Calculate delivery value. Simulations show that EM-RPL reduces interference and improves data transfer efficiency. Added support for moving nodes. Summary of participation: These proposed protocols share the goal of extending the lifetime of IoT networks, and increasing energy efficiency. And increasing the ability to adapt to dynamic conditions such as node movement, etc., although current research reduces the complexity of the network architecture by using a limited number of sink nodes for data collection. But future work could expand on this matter. A framework to explore various IoT applications. These findings highlight the effectiveness of combining fuzzy logic with routing protocols to address key IoT challenges, paving the way for further innovation in this area.

VI. FUTURE WORK

Although this research presents important advances in agile and energy-efficient routing protocols for IoT networks, many areas are still open for further investigation to increase scalability. Adaptability and the efficiency of the proposed solution... Dynamic sink node integration: Current methods use a fixed number of sink nodes, which makes the network architecture simpler. Future research could explore dynamic or mobile sink nodes to balance energy consumption. And reduce hotspot problems Especially in large IoT networks. Supports different IoT devices: IoT networks often consist of devices with different capabilities. Including processing power Energy processing and detection range Future protocols should address the challenges posed by this diversity. To ensure equal energy consumption and maintain consistent grid performance... Integrated with machine learning: Advanced machine learning models can complement fuzzy logic by providing predictive capabilities, such as predicting a node's power loss or modelling traffic. This integration can enable proactive decision-making and further optimize routing.

Security mechanism improvements: While this work focuses on energy efficiency and mobility support, Future protocols may include improved security features to protect against common IoT threats such as eavesdropping, data tampering, and tampering. and denial-of-service attacks without compromising energy efficiency… Micro-encryption techniques can be integrated. Real-World Deployment and Validation: The proposed protocol is validated through simulation. Future efforts may focus on real-world applications and testing in various IoT scenarios, such as industrial automation. Smart agriculture and inspections in the city To check efficiency beyond practical limitations... Multi-hop communication in the mobile scenario: Extending EM-RPL's ability to support multi-hop communications in highly dynamic environments, such as vehicular networks or drone-based IoT systems, can address the additional challenges of mobility and topology changes.

Power capacity: Future studies could investigate the integration of energy harvesting technologies such as solar energy or RF energy to extend the life of the electric grid. The protocol can be optimised to prioritise nodes with energy harvesting capabilities.

QoS optimisation for various applications: As IoT applications vary greatly in their quality of service (QoS) requirements (e.g., latency-sensitive smart healthcare vs. throughput-intensive industrial IoT), future work can focus on this. Developing adaptive protocols to suit the needs of specific applications... When discussing these issues Future research will be able to build on the foundation laid by this work. Create a strong routing protocol that is effective and more versatile. It meets the changing needs of the IoT ecosystem.

REFERENCES

[1] Gaddour, O., Koubaa, A., & Abid, M. (2015). Quality-of-service-aware routing for static and mobile IPv6-based low-power and lossy sensor networks using RPL. Ad Hoc Networks, 33(1), 233–256.

[2] Gara, F., Saad, L. B., Hamida, E. B., Tourancheau, B., & Ayed, R. B. (2016). An adaptive timer for RPL to handle mobility in wireless sensor networks. In 2016 International Wireless Communications and Mobile Computing Conference (IWCMC) (pp. 678–683). Paphos, Cyprus. https://doi.org/[Insert DOI if available]

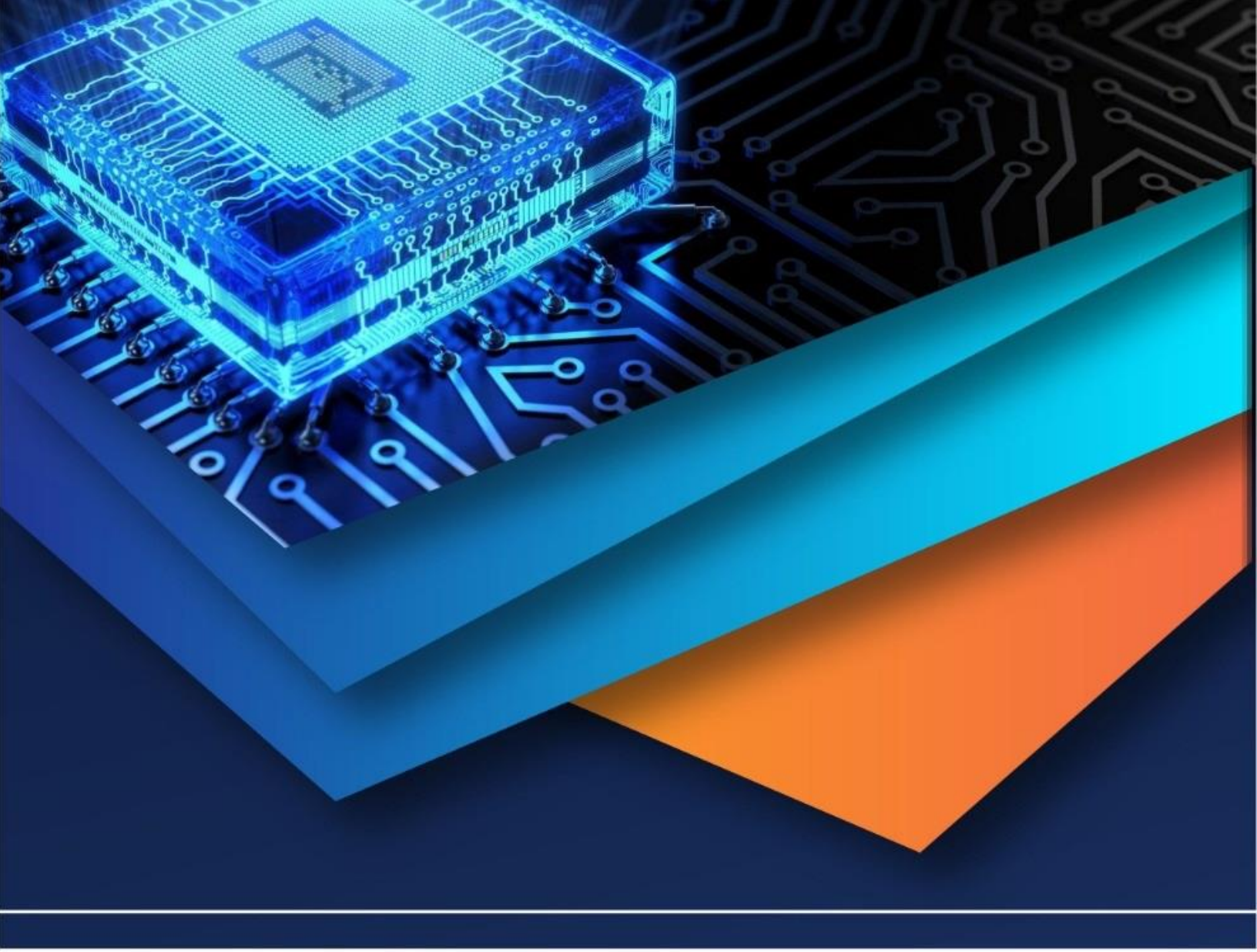
[3] Ghaleb, B., Al-Dubai, A. Y., Ekonomou, E., Romdhani, I., Nasser, Y., & Boukerche, A. (2018). A novel adaptive and efficient routing update scheme for low-power lossy networks in IoT. IEEE Internet of Things Journal, 5(6), 5177–5189. https://doi.org/[Insert DOI if available]

[4] Latib, Z., Jamil, A., Alduais, N., Abdullah, J., Audah, L., & Alias, R. (2017). Strategies for a better performance of RPL under mobility in wireless sensor networks. AIP Conference Proceedings, 1883, Article 020002. https://doi.org/[InsertDOI if available]
[5] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660. https://doi.org/[Insert DOI if available]
[6] Hassan, A., Alshomrani, S., Altalhi, A., & Ahsan, S. (2016). Improved routing metrics for energy-constrained interconnected devices in low-power and lossy networks. Journal of Communications and Networks, 18(3), 327–332. https://doi.org/[Insert DOI if available]
[7] Goyal, S., & Chand, T. (2018). Improved trickle algorithm for routing protocol for low power and lossy networks. IEEE Sensors Journal, 18(5), 2178–2183. https://doi.org/[Insert DOI if available]
[8] Heinzelman, W. B., Chandrakasan, A. P., & Balakrishnan, H. (2002). An application-specific protocol architecture for wireless microsensor networks. IEEE Transactions on Wireless Communications, 1(4), 660–670. https://doi.org/[InsertDOI if available]
[9] Tomar, M. S., & Shukla, P. K. (2019). Energy-efficient gravitational search algorithm and fuzzy-based clustering with hop count-based routing for wireless sensor networks. Multimedia Tools and Applications, 78(19), 27849–27870. https://doi.org/[Insert DOI if available]
[10] Iova, O., Theoleyre, F., & Noel, T. (2015). Using multiparent routing in RPL to increase the stability and the lifetime of the network. Ad Hoc Networks, 29(1), 45–62. https://doi.org/[Insert DOI if available]
[11] Izquierdo, S., & Izquierdo, L. R. (2017). Mamdani fuzzy systems for modelling and simulation: A critical assessment. [Journal Name], 21(3), 1–15. https://doi.org/[Insert DOI if available]
[12] Karagiannis, V., Chatzimisios, P., Vazquez-Gallego, F., & Alonso-Zarate, J. (2015). A survey on application layer protocols for the Internet of Things. Transactions on IoT and Cloud Computing, 3(1), 11–17. https://doi.org/[Insert DOI if available]
[13] Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: The Internet of Things architecture, possible applications, and key challenges. In 2012 10th International Conference on Frontiers of Information Technology (pp. 257–260). Islamabad, Pakistan. https://doi.org/[Insert DOI if available]
[14] Harshavardhana, T., Vineeth, B., Anand, S., & Hegde, M. (2018). Power control and cross-layer design of RPL objective function for low power and lossy networks. In 2018 10th International Conference on Communication Systems and Networks (COMSNETS) (pp. 214–219). Bengaluru, India. https://doi.org/[Insert DOI if available]
[15] Kharrufa, H., Al-Kashoash, H., & Kemp, A. H. (2018). A game-theoretic optimization of RPL for mobile Internet of Things applications. IEEE Sensors Journal, 18(6), 2520–2530. https://doi.org/[Insert DOI if available]
[16] Kim, H.-S., Cho, H., Kim, H., & Bahk, S. (2017). DT-RPL: Diverse bidirectional traffic delivery through RPL routing protocol in low-power and lossy networks. Computer Networks, 126(1), 150–161. https://doi.org/[Insert DOI if available]
[17] Kim, H.-S., Paek, J., & Bahk, S. (2015). QU-RPL: Queue utilization-based RPL for load balancing in large-scale industrial applications. In 2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON) (pp. 265–273). Seattle, WA, USA. https://doi.org/[Insert DOI if available]
[18] Ko, J., & Chang, M. (2015). MoMoRo: Providing mobility support for low-power wireless applications. IEEE Systems Journal, 9(2), 585–594. https://doi.org/[Insert DOI if available]
[19] Lamazi, H., Benamar, N., & Jara, A. J. (2018). RPL-based networks in static and mobile environments: A performance assessment analysis. Journal of King Saud University - Computer and Information Sciences, 30(3), 320–333. https://doi.org/[Insert DOI if available]
[20] Rao, U. P., Shukla, P. K., Trivedi, C., & Gupta, S. (2021). Blockchain for information security and privacy (Z. S. Shibeshi, Ed.; 1st ed.). Auerbach Publications.
[21] Lamaazi, H., & Benamar, N. (2018). OF-EC: A novel energy consumption-aware objective function for RPL based on fuzzy logic. Journal of Network and Computer Applications, 117(1), 42–58. https://doi.org/[Insert DOI if available]
[22] Kautoo, P., Shukla, P. K., & Silakari, S. (2014). Trust formulization in dynamic source routing protocol using SVM. International Journal of Information Technology and Computer Science (IJITCS, 6), 43–50. https://doi.org/[Insert DOI if available]
[23] Butani, B., Shukla, P. K., & Silakari, S. (2014). An exhaustive survey on physical node capture attacks in WSN. International Journal of Computer Applications, 95(3), 32–39. https://doi.org/[Insert DOI if available]
[24] Bhatt, R., Maheshwary, P., Shukla, P., Shukla, P., Shrivastava, M., & Changlani, S. (2020). Implementation of Fruit Fly Optimization Algorithm (FFOA) to escalate the attacking efficiency of node capture attack in Wireless Sensor Networks (WSN). Computer Communications, 149, 134–145. https://doi.org/[Insert DOI if available]
[25] Gupta, R., & Shukla, P. K. (2015). Performance analysis of anti-phishing tools and study of classification data mining algorithms for a novel anti-phishing system. International Journal of Computer Network and Information Security (IJCNIS, 7)(12), 70–77. https://doi.org/[Insert DOI if available]
[26] Rajawat, A. S., Bedi, P., Goyal, S. B., et al. (2021). Securing 5G-IoT device connectivity and coverage using Boltzmann machine keys generation. Mathematical Problems in Engineering, 2021, Article ID 2330049, 10 pages. https://doi.org/[Insert DOI if available]
[27] Ahirwar, M. K., Shukla, P. K., & Singhai, R. (2021). CBO-IE: A data mining approach for healthcare IoT dataset using chaotic biogeography-based optimization and information entropy. Wireless Communications and Mobile Computing, 2021, Article ID 8715668, 14 pages. https://doi.org/[Insert DOI if available]
[28] Gupta, M., Gupta, K. K., Khosravi, M. R., Shukla, P. K., Kautish, S., & Shankar, A. (2021). An intelligent session key-based hybrid lightweight image encryption algorithm using logistic-tent map and crossover operator for Internet of Multimedia Things. Wireless Personal Communications, 121. https://doi.org/[Insert DOI if available]
[29] Khare, A., Gupta, R., & Shukla, P. K. (2022). Improving the protection of wireless sensor networks using a black hole optimization algorithm (BHOA) on the best possible node capture attack. In P. Nayak, S. Pal, & S. L. Peng (Eds.), IoT and Analytics for Sensor Networks (Vol. 244). Springer, Singapore. https://doi.org/[Insert DOI if available]
[30] Gupta, M., Gupta, K. K., & Shukla, P. K. (2021). Session key-based novel lightweight image encryption algorithm using a hybrid of Chebyshev chaotic map and crossover. Multimedia Tools and Applications, 80(25), 33843–33863. https://doi.org/[Insert DOI if available]
[31] Saxena, A. K., Sinha, S., & Shukla, P. (2018). Design and development of image security technique by using cryptography and steganography: A combined approach. International Journal of Image, Graphics and Signal Processing (IJIGSP, 10)(4), 13–21. https://doi.org/[Insert DOI if available]

[32] Tarwani, N., Chourasia, U., & Shukla, P. K. (2017). Survey of cyberbullying detection on social media big data. International Journal of Advanced Research in Computer Science, 8(5), 831–835. https://doi.org/[Insert DOI if available]

[33] Parwani, D., Dutta, A., Shukla, P. K., & Tahiliyani, M. (2015). Various techniques of DDoS attacks detection and prevention at cloud: A survey. Oriental Journal of Computer Science & Technology, 8, 110–120. https://doi.org/[InsertDOI if available]

[34] Mahatpure, J., Motwani, M., & Shukla, P. K. (2019). An electronic prescription system powered by speech recognition, natural language processing, and blockchain technology. International Journal of Scientific & Technology Research, 8(8), 1454–1462. https://doi.org/[Insert DOI if available]



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY