Management Strategies and Engineering Sciences 2025; 7(3):1-15


# An Energy and Load Aware Multipath Routing Protocol in Internet of Things

Roghaye Khaleghnasab[1], Karamolah Bagherifard[1*], Hamid Parvin[2], Samad Nejatian[1], Bahman Ravaei[3]

[1] Department of Computer Engineering, Yasooj Branch, Islamic Azad University, Yasooj, Iran
[2] Department of Computer Engineering, Nourabad Mamasani Branch, Islamic Azad University, Nourabad Mamasani, Iran
[3] Department of Computer Engineering, Yasouj University, Yasouj, Iran

*** Corresponding author email address**: karam.bagherifard@gmail.com

**Received:** 2024-12-23 **Reviewed:** 2025-01-12 **Revised:** 2025-02-03 **Accepted:** 2025-02-12 **Published:** 2025-07-25

**Abstract**

IoT is a network of smart things. This indicates the ability of these physical things to transfer information with other physical things. The characteristics of these networks, such as topology dynamicity and energy constraint, challenges the routing problem in these networks. Previous routing methods could not achieve the required performance in this type of network. One of the routing methods is utilization of multipath protocols which send data to its destination using routes with separate links. One of such protocols is RPL routing protocol. In this paper, this method is improved using composite metrics which chooses the best paths used for separate routes to send packets. the protocol of Energy and Load aware RPL (ELaM-IoT), has been suggested that it has a rise of RPL protocol. It applies a composite metric, estimated based upon the extant energy, hop count, load & battery depletion index, and Link Expiration Time, for the selection of route. In order to evaluate and report the results, the proposed ELaM-IoT method is compared to the ERGID and ADRM-IoT approaches with regard to average remaining energy, and network lifetime. The results demonstrate the superior performance of the proposed ELaM-IoT compared to the ERGID and ADRM-IoT approaches.

***Keywords:*** *Internet of Things, Load Aware, Energy-efficient, Gray System Theory, Multipath Protocol.*

**How to cite this article:**

Khaleghnasab, R., Bagherifard, K., Parvin, H., Nejatian, S., & Ravaei, B. (2025). An Energy and Load Aware Multipath Routing Protocol in Internet of Things. Management Strategies and Engineering Sciences, 7(3), 1-15.

## 1. Introduction

The Internet of Things (IoT) demand has recently increased. Firstly, the wireless sensor network (WSN) empowers pervasive sensing technologies. By the evolution of the WSN technology, the Internet of Things (IoT) was created through the application and proliferation of these sensing devices [1, 2]. IoT, as the next revolution, interconnects smart objects and develops an intelligent space. It is anticipated that there would be 24 billion IoT devices by 2020. By increasing connection and communication among IoT devices, considerable IoT traffic will be created by IoT applications. Given that IoT traffic is due to the communication among objects, the reliability of the transmission is important, particularly in a nearly unstable WSN, in comparison with the wired networks. We employ 500 sensor nodes distributed uniformly over the area of 3000∗3000m:

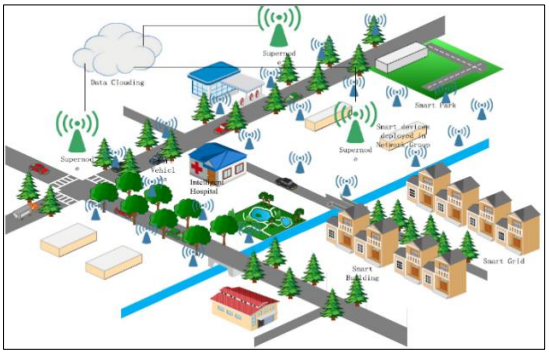



**Figure 1.** The devices deployed in IoT [3].

A routing protocol decides how to send packets to other nodes. Routing protocols have two major divisions including Reactive and Proactive routing protocols. Routes are providing by the reactive protocols when it is needed. When it is necessary, control messages are transmitted by the path of data transfer, using these types of protocols. But, the needed time to find the route is increases. In addition, control messages are periodically exchanged by the proactive routing protocols immediately after start in order to search and propagate the routes. Local control messages together with messages across the entire network are sent by nodes to receive local nearby information and to share the structural information in all nodes of the network.

In this paper, this method is improved using composite metrics which chooses the best paths used for separate routes to send packets. The protocol of Energy and Load aware RPL (ELaM-IoT) is suggested that it has a rise of RPL protocol. It applies a composite metric, estimated based upon the extant energy, hop count, load, battery depletion index (BDI), and Link Expiration Time (LET), for the selection of route.

The increasing demand for the Internet of Things (IoT) has led to the proliferation of wireless sensor networks (WSNs) and the creation of interconnected smart objects. With the growing number of IoT devices and the resulting increase in IoT traffic, ensuring reliable transmission becomes crucial, especially in unstable WSNs compared to wired networks. Therefore, there is a need for an efficient routing protocol that can handle the communication among IoT devices and maintain reliable transmission in such challenging network conditions.

This paper proposes an improved routing protocol, called Energy and Load aware RPL (ELaM-IoT), which addresses the aforementioned challenges. ELaM-IoT incorporates composite metrics that select the best paths for separate routes to send packets. The protocol takes into account factors such as energy levels, hop count, load, battery depletion index (BDI), and Link Expiration Time (LET) to determine the optimal route for transmission. By utilizing these composite metrics, ELaM-IoT aims to enhance the performance and reliability of the routing process in IoT networks.

## 2. Related Works

IoT represents a transformative shift in how devices interact and communicate, leveraging advancements in technology to create interconnected systems. As IoT evolves, its applications span various domains, including urban management, industrial operations, and personal devices. For example, one of its applications is educational activities for children in the Internet of Things environment [4]. Another application is the functioning of the Internet of Things in vehicles [5].

In recent years, there have been many suggested researches on real-time routing protocols. And the central focus of them is divided into two main problems about multipath routing protocols. The first one is the protocol requirement to guarantee the reliability of actual-time packets to decrease the blank regions number created by delay and loss. The other one is the protocol requirement to stabilize the network energy loss and prevent early expiration for a number of nodes.

To maximize the network lifetime through minimization of the consumption of node energy, is the major aim of the suggested work. This study contribution is introducing a mix of BDI based composite metric, Load, and ETX in RPL. That composite metric pursues the property which is minimizable. DIO is sent by DODAG to monitor messages onto all nodes of participant. The node of participant, from DODAG rank chooses the highest parent. In the DODAG, from the composite metric minimized value, the rank estimates. Lastly, participant or sender node, toward the DODAG root, sends the data

to the highest parent into the DODAG. Therefore, it decreases the traffic load, ameliorate network lifetime, and develops the ratio of packet delivery [1].

In LLN, a design guideline was suggested in [2] for the composition of routing metrics and via IETF that document is standardized. In LLN, it is obviously mentioned the requirement, rules and properties of composite metrics. The initial metric composition can be merged lexical and additive manner. For initial metric composition contains of either maximization or minimizable property, additive property is appropriate. For single metric composition contains of both maximization and minimizable, fuzzy logic is appropriate. For single metric composition, lexicographic property is appropriate and the first metric is inspected by it and merely if feasible path has equal value after that from the composition it determines the next metric.

In LLN, the composition of routing metric was assessed in [3] to develop the Quality of Service (QoS). It concentrated upon three things. a). From the single metric, a composite metric was introduced for example Packet forwarding indication (PFI), Expected transmission count (ETX), Remaining energy (RE). b). It produced superior QoS and the efficiency was confirmed employing routing algebra. c). the superior performance was attained and the optimal loop- free paths, provided.

*NLEE Algorithm:* In the paper presented by Vellanki et al. in 2016, the effective energy protocol for improving energy efficiency in internet of things was introduced. The proposed algorithm, makes decisions that minimize upload using shortest paths. This method uses the expected remaining node energy countdown and total number of node transfers as the routing criteria to improve energy efficiency. This method controls the number of transferred and broadcasted packets to discover routes. Furthermore, route discovery is carried out using remaining energies and step counts of the nodes in the routes. Moreover, NLEE algorithm guarantees better utilization of the energy available in the nodes. It also regularizes routing delay while discovering the shortest path in the network [6].

*SCOTRES Method:* SCOTRES is a trust-based system for secure routing in ad-hoc networks which use smart devices to transmit information. The proposed method is described using five criteria. The energy criterion takes into consideration the resource consumption of each node. Trust criterion increases the network lifetime. The topology criterion is aware of the node positions and enhances loading. Chanel's health criterion, due to inappropriate channel conditions, protects the network against harmful attacks. The reputation criterion evaluates each of the participants of specific network operations for the identification of specialized attacks. On the other hand, the trust criterion, general adaptation, evaluate the fulfillment against hybrid attacks. SCOTRES has two types: one is embedded systems, and the other is real systems. The evaluations represented in this paper demonstrated that this system has the highest protection rate while maintaining the performance for setting up real applications [7].

In [8], the authors propose an approach that leverages side-channel information, such as power consumption or electromagnetic radiation, to infer the internal structure and parameters of an AI model running on an IoT device. The paper emphasizes the significance of protecting AI models deployed in IoT devices due to their vulnerability to attacks, which can lead to model theft, privacy breaches, or malicious exploitation. The authors introduce a fuzzy analysis-based framework that combines information theory with side-channel analysis to effectively extract AI models. Fuzzy analysis, based on fuzzy set theory, allows for modelling uncertain and imprecise information, which is particularly relevant in the context of side-channel attacks where noise and variations are present. The proposed method involves three main steps: side-channel data acquisition, fuzzy modelling, and AI model extraction. Side-channel data, such as power consumption traces or electromagnetic radiation signals, are collected while the target AI model is running on the IoT device. Fuzzy sets are then constructed to represent the uncertainty in the side-channel data. These fuzzy sets are used to build fuzzy rules and fuzzy inference systems, which enable the extraction of the AI model parameters. Information-theoretic measures, such as mutual information and channel capacity, are employed to evaluate the quality and relevance of the extracted information.

In [9], the authors address the growing concerns regarding security in IoT systems and propose a solution to detect and classify security threats effectively. The proposed method utilizes a fuzzy optimum-path forest classifier, which combines fuzzy logic and the optimum-path forest algorithm for accurate and efficient threat detection. The approach involves several steps. First, a feature extraction process is applied to the collected data from IoT devices, such as sensor readings or network traffic information. The extracted features are then used to construct fuzzy membership functions, which capture the uncertainty and imprecision in the data. Next, an

optimum-path forest classifier is employed to classify the IoT system's security state based on the fuzzy membership values. The optimum-path forest algorithm utilizes a graph-based representation of the data and determines the optimal paths for classification. By incorporating fuzzy logic, the classifier can handle uncertain and imprecise data effectively. The authors conducted experiments to evaluate the performance of their approach. They used a dataset containing various security-related events in an IoT system and compared the results with other classification methods. The experimental results demonstrated that the fuzzy optimum-path forest classifier outperformed other algorithms in terms of accuracy and efficiency, effectively detecting and classifying security threats in the IoT system.

In [10], the authors address the need for accurate and timely disease prediction and diagnosis, and propose a novel solution that combines IoT, cloud computing, and intelligent techniques. The system aims to provide secure and reliable healthcare services by leveraging the capabilities of IoT devices, cloud infrastructure, and intelligent algorithms. The proposed system consists of three main components: IoT devices, a secure cloud platform, and a hybrid intelligent algorithm. IoT devices, such as wearable sensors or medical devices, collect data related to patients' health conditions. The collected data is securely transmitted to the cloud platform for storage and analysis. The secure cloud platform ensures data privacy and security by employing encryption and access control mechanisms. It provides a centralized infrastructure for data storage and processing, allowing healthcare professionals to access patient information securely. The hybrid intelligent algorithm is applied to the collected data in the cloud platform for disease prediction and diagnosis. The algorithm combines multiple intelligent techniques, such as machine learning, data mining, and expert systems, to analyze the data and generate accurate predictions and diagnoses. The integration of various intelligent techniques enhances the accuracy and reliability of the system. The authors conducted experiments to evaluate the performance of their proposed system. They used real-world healthcare datasets and compared the results with existing methods. The experimental results demonstrated that the hybrid intelligent system achieved higher accuracy and efficiency in disease prediction and diagnosis, showcasing its potential for improving healthcare services.

*ERGID Method:* Based upon Global Information Decision (ERGID), a protocol which is routing called Emergency Response IoT was suggested in the study of Qui et al. in 2016 to increase the reliability of data transmission performance and efficiency of the emergence response to IoT. Especially, in this study a mechanism named delay iterative method (DIM) that is founded upon the approximation of delay was designed to answer the problem of disregarding valid routes. Additionally, a transfer plan named “Remaining Energy Probability Choice” (REPC) was recommended for balancing the network load together with concentrating upon the remained node energy. Consequences and examination of the simulation indicates that ERGID have better performance with respect to SPEED and EA-SPEED approaches regarding delay which is end to end, energy loss and packet dissipation rate. Also, in this study some applied examinations were performed using STM32W108 sensing nodes. It was detected that ERGID can increase the network ability for real-time response [11].

*AOMDV-IOT Technique:* In this study, the suggested technique called AOMDV-IOT is introduced. It is a routing technique and up to the destination, it can perform as the router. The recommended method is not offered just for the node. The enhancements are mostly appropriate in IoT which is a unique technique for it. The principal object in this technique is detecting and generating effective connections between the nodes and the internet using the AOMDV routing protocol in the IoT. The internet connection table (ICT) is added in the suggested routing protocol to every node. Every node has two tables in this method including: routing table and ICT. ICT consists of four units: terminal node number, terminal node IP address, lifecycle, and hop value. Even though ICT uses extra memory, instead it can store connection counts and consequently decreases transmission delay. Comparison of AOMDV, simulating outcomes show that AOMDV-IOT has improved efficiency with respect to delay which is end to end, frequency in IoT, and packet loss. In this research, the multi-objective ad-hoc generated distance vector for the internet of things has been enhanced in such an approach that it can dynamically choose the direct internet transmission route by regular update of internet link table. Simulating effects show that while the AOMDV-IOT routing protocol rises the two routing packets, average end to end delay of the route falls [12].

*Adaptive Distributed Routing Method:* FANET networks are a key part of the IoT and can offer messaging facilities for various devices in the IoT and

cyber-permitted applications. But, moving unmanned aerial vehicles (UAV) in FANETs creates random network link and increases complexity of routing algorithms for these applications, particularly in real-time routing. In this research, an effective opportunistic distributed routing technique is suggested to explain the above-mentioned problem. For data transfer in this process, only the colleague nodes and local information are used by the transmitter. They maximize network use and preserve the end-to-end delay less than a stated threshold in order to care for variations of network and channel by designing and solving an optimization problem. Besides, they guess one stage delay for every communication of the transmitter node and use double parsing to alter the integrated problem into a distributed one. By this method, the transmitter nodes are only permitted to contact with local information and approximate delay in packet routs. Simulation outcomes indicate that the introduced routing technique enhances the network performance regarding its energy efficiency, quantity, and end to end delay [13].

*REL Method:* In the next work, for IoT applications, Machado et al. proposed an energy and link quality-based routing protocol (REL). In order to improve energy efficiency and reliability, REF chooses an estimator mechanism based on the link which is end to end and the remaining energy. Moreover, REL suggests a mechanism which is event-based to maintain the balance of load and avoid the loss of premature energy in the network and nodes. REF provides a plan which has end to end route selection, with minimum overhead based upon cross-layer information. In order to obtain the effectiveness of energy, the nodes deliver the remaining energy of them toward the neighbouring nodes. In this paper, the process of route selection is performed using optimal energy information and the assessment with end to end link quality. A novel approach is used for the calculation of link quality. REL utilizes the wireless link quality and the remaining energy while routing in order to enhance the reliability of system and support QoS for the applications of IoT. REL uses a reactive pattern for discovering routes. This results in reduced signalling overhead and improved scaling capability. Route discovery process consists of diffusing RREQ and RREP messages. With high density of node, in networks which are large scale, the consequences suggest that in REL, lifetime was improved up to %26.6, latency up to %17.9, and the delivery of packet up to %12 whenever they are in comparison with LABILE and AODV [14].

*MLB Method:* In the IoT, large data transfers using wireless sensor networks has caused many problems. However, AODV routing stack in ZigBee protocol has no load balancing mechanism to handle corrupted traffic. Therefore, we develop multipath load balancing (MLB) to replace AODV routing protocol in ZigBee. MLB is proposed for collaboration with ZigBee wireless network in the large scale. In this scenario, ZigBee is used as communication media in wireless sensor networks. In order to create a reliable ZigBee stack, ZigBee network layer is placed in MLB. MLB provides alternative routing service for ZigBee network without altering the existing stack in ZigBee. When a ZigBee router transmits the IoT data forward, MLB guides the ZigBee network layer in selecting the next hop with minimum load towards the IoT gate [15]. Table 1, summarizes the investigated efforts to design multipath routing for IoT.

**Table 1.** Summary of the multipath routing schema for IoT literature.

| Ref | Idea | Advantages | Disadvantages |
|---|---|---|---|
| [6] | Efficient energy protocol for improving energy efficiency in the internet of things | Improved latency – decreased power consumption | Overhead caused by counting the number of sent and control packets, hop count and remaining energy |
| | Secure routing with emphasis on energy consumption of the devices and decreasing it | Increased network lifetime while using trust criterion in order to prevent hybrid attacks | N/A |
| [7] | Routing based on decisions made with general information | Improved data transfer performance and emergency response | The need to estimate delay in order to improve delay and network lifetime |
| | Discovering and establishing efficient link between nodes and the internet based on the AOMDV protocol | Decreased latency and decreased packet loss rate | More overhead because of storing two tables in each node and two extra routing packets |
| [11] | Reducing the complexity of routing algorithms using distributed adaptive routing | Improved energy efficiency, throughput, and end to end latency | The need to carry out exact calculations to calculate delay |
| | Routing protocol based on link quality and energy | Improved reliability and energy efficiency | N/A |

## 3. Proposed ELaM-IoT Schema

The section in succeding, via using the composite metrics, an ELaM-IoT schema has been designed. In Section, 3.1, five phases are included in the schema of ELaM-IoT. The assumptions applied in the proposed ELaM-IoT is discussed, Sect 3.2. presents adding new parameters to RPL, designing the routing packets in ELaM-IoT is discussed in Sect. 3.3. In Sect. 3.4 neighbor discovery step is discussed. And the route discovery step is discussed in Sect. 3.5.

### *3.1. Phase 1: The assumptions applied in the proposed ELaM-IoT*

The assumptions Considered in the proposed approach include:

1. Things existing in the network are not static; they should work independently.
2. Each thing has limited energy and the initial energy of each thing is $EP_N$ where $EP_N \succ 0$
3. Things gather data with a constant rate from the environment.
4. In the proposed approach, energy is consumed to transmit local data among the nodes.
5. To gain spatial data, each node is equipped with a GPS system.

### *3.2. Phase 2: Adding new parameters to RPL*

Because most of the devices are wireless, link stability fluctuation caused by movement or transfer medium characteristics in the internet of things affects the network performance. Efficiency of a dynamic routing protocol can be rated based on its ability to handle link unreliability and its computational and reconfiguration/rerouting overhead. Link stability as the basis of routing can lead to a protocol that has the following capabilities:

**Remaining Energy (Re):** One of the most important elements while choosing a route is the extant energy along that route in the nodes. In the nodes of a route, the higher the extant energy and the lower their consumed energy, the more appropriate that route is to be selected. Remaining energy is calculated using Equation (1).

$$ER_N = \left(EP_N(t) - ECo_N(t)\right) \quad (1)$$

**Hop Count (Hop):** The parameter of Hop count is the number of Hops between the destination node and the origin node. The lower the Hop count of a route, the better that route is because less energy needs to be used in order to transmit the packet.

**Link Expiration Time (LET):** It is the amount of time for which the links stays stable. The longer this time period is, the more stable the link between the nodes will be. This parameter depends on the movement speed of the nodes. The faster the nodes move, the more unstable the route between them will be and the sooner it will be destroyed. By employing Equation (2), link expiration time is estimated based upon the transmitted packets between the nodes.

$$LET(i,j) = \left(\frac{-(ab+cd)+\sqrt{(a^2+c^2)*R^2-(ad-bc)^2}}{a^2+c^2}\right) \quad (2$$

In Eq. (2):

$$\begin{Bmatrix} ER_N(t): \textit{Remaining energy of the node} \\ EP_N(t): \textit{Primary energy of the node} \\ ECo_N(t)\ \textit{Consumed energy of the node} \end{Bmatrix}$$

The nodes are aware of their location using GPS. In the above equation there are two nodes $i$ and $j$ which are at $(x_i, y_i)$ and $(x_j, y_j)$ respectively. Their speeds are $v_i$, $v_j$ and their movement angles are $\theta_i$ and $\theta_j$. In the following section, details for each step are presented.

**Load:** Across the network, at presented amount of time, an amount of data transfer is network data traffic. As a technique, load balance is employed for balancing the traffic across network. It is chiefly focused upon the child number display in every node of parent. In the DODAG, the node of participant chooses the node of parent based upon less number of child collected the node of parent. From Equation (4) and (3), the traffic load estimates. In the DODAG, if the children number enhances into a parent node, the DODAG is constructed by ELaM-IoT.

$$Load\left(path(x)\right) = \left(\sum_{M=1}^{n} Node\_TrafficLoad(M)\right) \quad (3)$$

In Eq. (3): $$\begin{cases} a = v_i * \cos\theta_i - v_j * \cos\theta_j, \\ b = x_i - x_j, \\ d = Y_i - Y_j, \\ C = v_i * \sin\theta_i - v_j * \sin\theta_j \end{cases}$$

**a. Calculating the Load:** In ELaM-IoT, the calculation of path load(x) is based upon the child set or node traffic cumulative.

**b. Calculating the Node Traffic:** The traffic of node, in ELaM-IoT, estimates from children counting of the respective node of parent.

$$Node\_TrafficLoad(M) = \left(\sum_{i=1}^{n} children\_count\right) \quad (4)$$

**Battery Depletion Index (BDI):** How much energy percentage depleted from battery exist in the node, has been indicated by Battery depletion Index (BDI). From the remaining energy of the node and the initial energy, the residual energy estimates [6]. Also, from Equation (5), the residual energy computes.

$$RER(M_i) = \left(\frac{E_{remain}}{E_{initial}}\right) \quad (5)$$

An extant energy in the node Mi, is the residual energy and with regard to 0 to 1, it is indicated. From Equation (6), the BDI computation is estimated.

$$BDI(M_i) = (1 - RER(M_i)) \quad (6)$$

From Equation (7), the BDI pursues the BDI of Path Px and deductive rule computes.

$$BDI(P_x) = \left(\prod_{i=1}^{n} BDI(M_i)\right) \quad (7)$$

**Rank Calculation:** DODAG rank, in EL-RPL, estimates from rank rise value and parent rank. The rank rise estimates from Min-Hop-Rank-Increase and step value. The default value of Min-Hop-Rank-Increase is 256 [12]. In Equation (8), from rank function and objective, the step value computes and it is dedicated.

$$Rank(N) = (W_1 * \mathrm{Re}(p_i)) + (W_2 * HopCount(p_i)) + (W_3 * LET(p_i)) + (W_4 * Load(p_i)) + (W_5 * BDI(p_i)) \quad (8)$$

### *3.3. Phase 3: Designing the routing packets in ELaM-IoT*

In the proposed method, all of the devices need to be equipped with GPS and have maximum initial energy. RPL routing packet format is expanded so that it can be used for ELaM-IoT routing. This is achieved by adding new fields to RPL routing packets. ELaM-IoT routing protocol, just like the base RPL protocol, has four packet formats. However, in the proposed ELaM-IoT method, these formats are altered and required fields are added to these packets. Details of these packets are presented below.

**Table 2.** New format of the HELLO packet.

| | | |
|---|---|---|
| Unused | Reserved | Packet type |
| Origin sequence number | | Origin IP address |
| Node energy | | Time stamp (origin time) |
| Node speed | | Node location |

**HELLO packet:** To find neighboring devices, this packet is employed, in regular intervals. The nodes in nearby alter their location obtained through GPS and remaining energy information using HELLO packets. After exchanging the HELLO packet, each node updates its routing table and the remaining energy of neighboring nodes and also calculates $SINR$ rate based on the received signal from the neighbor and link expiration time ( $LET$ ) with the neighboring node based on its own location and the neighbor's location and also writes them into its table. New format of the $HELLO$ packet is shown in Table 2.

**RREQ packet:** The route request ( $RREQ$ ) packet is the second packet. Each time a node tries for communicating with further nodes in the network, route

discovery process needs to be carried out. Therefore, the node broadcasts the $RREQ$ packet publicly to find an appropriate route to its destination $RREQ$ packets contain an $ID$ to distinguish each packet, the IP address for destination, network time stamp, and sequence number. The number of destination sequence displays the route freshness. We add the remaining node energy, $SINR$ value, and the calculated $LET$ with the last hop based on the $HELLO$ message fields to the $RREQ$ packet. Each node has calculated these parameters based on the Eq. (1) through Eq. (3) upon receiving the $HELLO$ message and saved them in its table. Now, once the $RREQ$ message is received, each node on this route adds this information and along the route transfers to the next node toward the destination. New format of the packet of $RREQ$ is shown in Table 3.

**Table 3.** The packet of RREQ New format.

| Hop count | Reserved | Packet type |
|---|---|---|
| Destination IP address | | ID RREP |
| Origin IP address | | Origin sequence number |
| Battery Depletion Index | | Accumulated route |
| Total hop count along the route | | Total remaining energy of the nodes along the route |
| Total LET along the route | | Total Load along the route |

**RREP packet:** The route reply packet is the third packet. A lot of routes are found from the origin toward the destination, after obtaining the packets of broadcasted $RREQ$. Normally, $RREP$ packet consists of an ID to distinguish unique packets, sequence number, accumulated routes and origin IP address. In the proposed method, we get the destination of every $RREQ$ packet from different routes and calculate the total number of hops, total remaining energy in each route, and total $SINR$ and $LET$ in the links of each route and add them to the $RREP$ packet. Then, this packet is sent to the origin of that route. Therefore, we add the new total remaining energy of the route nodes, hop count, and total $SINR$ and $LET$ fields to the $RREP$ packet. New format of the $RREP$ packet is shown in Table 4.

**Table 4.** The packet of RREP new format.

| Hop count | Reserved | Packet type |
|---|---|---|
| Destination IP address | | ID RREP |
| Origin IP address | | Origin sequence number |
| Battery Depletion Index | | Accumulated route |
| Total hop count along the route | | Total remaining energy of the nodes along the route |
| Total LET along the route | | Total Load along the route |

**RERR packet:** When a node discovers an error, a route error ( $RERR$ ) packet is broadcasted by it with the infinite hop count and the sequence number of destination. The origin node or any other node along the route can reestablish the route through sending a packet of $RREQ$. If the origin node or any other node obtains the packet of $RRER$, it needs to re-execute the route discovery process.

**Table 5.** New format of the TEST packet.

| Hop count | Reserved | Packet type |
|---|---|---|
| IP address of Middle node | | Broadcasting ID the Test packet |
| Source IP address | | Measurement rate |

**Test packet:** after detecting nodes, the origin sends a test message through all routes in the format shown in table 5 to take the responses of all the nodes in the routes. In this way, we can calculate two mentioned parameters namely MER and SCS. New format of the $Test$ packet is shown in Table 5.

### *3.4. Phase 4: Neighbor discovery step*

In the neighbor discovery step, nodes (devices) flood the network with $HELLO$ packets to find their neighbors. The $HELLO$ packet includes the origin IP address, remaining energy of the node, node location, node speed, time stamp, and sequence number. After the step of neighbor discovery, every device, in the network understands all of its neighbors and is conscious of the location of them and remaining energy. The nodes also calculate the $Load$ and $Battery\ Depletion\ Index$ value for their immediate neighbors using the received signal and the noise rate and interference values. Also, using the location and speed of the neighboring node in the last step and their own location and speed, each node calculates the link expiration time ( $LET$ ) of its link with the neighboring node. Each node stores this information for its immediate neighbors.

### *3.5. Phase 5: Route discovery step*

When the origin node decides to send a packet to the destination, it floods the network with $RREQ$ packets to discover the suitable routes. $RREQ$ packet includes the IP address of the origin and destination, sequence number, hop count, remaining energy in the node, accumulated route, LET, load and battery depletion index. IP address of the origin and the destination are used to identify unique nodes in the network. The destination sequence number is used to show the suitable routes toward the destination. After receiving the packet of $RREQ$ packet, each node retrieves its neighbor information and inserts it into its routing table. Then inserts the new information along with its own information into the $RREQ$ packet and sends it to the next node. Figure 2 demonstrates the flooding of $RREQ$ packets in the network in order to find routes leading to the destination.

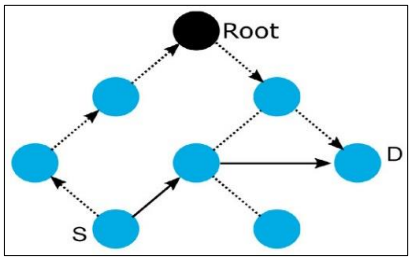



**Figure 2.** From node S to node D, it is a P2P message transmission. The path established via RPL, is displayed by dotted lines with an arrow whereas the path created via P2P-RPL is indicated by the solid lines with an arrow.

The destination node received multiple $RREQ$ packets using different routes. Also, the $RREP$ packet includes the node ID to identify unique packets, lifespan in the network, sequence number, IP address of destination, and accumulated routes. The accumulated routes are a list of separate routes from origin to destination. Moreover, three new fields, namely the total $LET$ of each route, load and battery depletion index, and remaining energy of each route calculated by the destination node using the $RREQ$ packets are added to the $RREP$ packet. After adding these fields, the destination node sends the $RREP$ packet using all of the routes and stores this information in its routing table. The origin node, upon receiving the $RREP$ packets from destination, stores the origin of these multiple routes in its routing table.

The pseudo code related to the proposed method is shown in Algorithm 1:

**Algorithm 1.** Initialize node parameters (energy levels, routing tables, load information)

```
Main loop
While network is operational
 Check for incoming messages
   If messageReceived()
     If messageType is data
        Source_node ← getSourceNode(message)
        Destination_node ← getDestinationNode(message)
        Available_energy ← AvailableEnergy(source_node)
        Load ← Load(destination_node)
        Candidate_paths←CandidatePaths(source_node, destination_node)
        Feasible_paths ← FeasiblePaths(candidate_paths, available_energy, load)
        Best_path ← selectBestPath(feasible_paths)
        ForwardMessage(message, best_path)
     Else If messageType is control
        UpdateRoutingTables()
        UpdateNeighborInformation()
        CheckNodeStatus()
Return feasible_path
```

## 4. Evaluating the Performance

In the following section, the performance of suggested ELaM-IoT will be evaluated for the problem of multipath routing.

### *4.1. The metrics of Performance*

In this section, the efficacy and performance of the suggested ELaM-IoT approach is thoroughly analysed applying simulations which are comprehensive. With ADRM-IoT and ERGID approaches, the attained consequences will be discussed and compared in [12] and [16]. The network lifetime and mean remaining energy will be assessed.

**Average Remaining Energy:** Equation (9) demonstrates that node's unused energy in a time instance which is arbitrary, is the additional energy that after a communicating with receiver is kept in the node. The energy for the reception, fading effects, wasted energy in the system ( $E_{sys}$ ), energy for transmission, etc. are the remaining energy examples. Table 6 presents the list of the parameters that are used for $ARE$ .

**Table 6.** Parameters utilized for average residual energy

| Parameters | Explanation |
|---|---|
| $di_0$ | The distance of reference larger than the Fraunhofer-distance |
| $di$ | The distance that the packet is transferred on it |
| $Lb$ | The bits per packet (BPP) number |
| $di^2$ | The loss of power in the model with free space channel |
| $di^4$ | The loss of power in the multipath model of fading channel |
| $E_{elec}$ | The energy that is dissipated when reception or transmission |
| $lb \in fsi$ | Transmission Efficiency |
| $lb \in mpi$ | The channel Condition |

$$Energy_{residual} = Energy_{initial} - \left\{ ET_X + ER_X + E_{sys} \right\} \quad (9$$

$$ET_X(1b, di) = \left\{ lbE_{elec} + lb\varepsilon_{fs} di^2, di < di_0 \right\} = \left\{ lbE_{elec} + lb\varepsilon_{mpi} di^4, di \geq di_0 \right\} \quad (10$$

$$ER_X = lbE_{elec}. \quad (11)$$

The parameter which is simulated is given as:

$$\left\{ \begin{array}{l} E_{elec} = 100nJ / bit, \\ \varepsilon_{fsi} = 20\,pJ / bit / m^2, \\ \varepsilon_{mpi} = 0.0015\,pJ / bit / m^4 \end{array} \right\}$$

Equations 10 and 11 are used for calculating the amount of energy that is used during the transmission of packet $ET_X(1b, di)$ and reception of packet ( $ER_X$ ).

In case of $di > di_0$, multipath fading impact happens, and energy wasting occurs during transmission. Nevertheless, as the current paper does not

address the fading scheme, it is considered that the distance is fewer than the Fraunhofers distance. In addition, the channel state information will not be taken into account, while it is considered that the efficiency of transmission is 1.

**Lifetime of Network:** By definition, the lifetime of the network is the time that elapses between sensing commencement and communication with the receiver, and the time during it the last communicating link is broken from active node toward the receiver. For the whole nodes, network lifetime that are now active with the receiver in communicating is defined as the lifetime aggregating at any time instance for the whole nodes. In case of clustering the network, the network lifetime is considered as the whole lifetime for all things [17]. Equation (12) calculates the value of $NL$.

$$NL = \left( \sum_{i=1}^{m} Things_i \right) \quad (12)$$

### 4.2. Simulation Setup and Comparing Algorithms

In actual networks, since debugging and implementing IoTs is hard, it is essential to determine simulations as a fundamental design instrument. The simulation initial profit is verification of protocol, and simplification of analysis, particularly in systems which are large. According to this section, the performance of suggested method's is evaluated NS-3 as the instrument of simulation, and after that the consequences will be deliberated. It is worth mentioning that all ERGID, ADRM-IoT, and ELaM-IoT parameters and settings, as equal are determined.

### 4.3. Simulation Analysis and Results

In this part, the performance of ELaM-IoT, under the two programs is investigated (Table 5). Firstly, in the area of network, 500 IoT things in an identical manner are deployed. Some main parameters are indicated in Table 7.

**Table 7.** Setting of simulation parameters.

| Parameters | Value |
|---|---|
| Topology (m x m) | 1000 x 1000 |
| Simulation tool | NS-3 |
| Transport | UDP/IPv6 |
| Communication range of each node | 160 m |
| Channel bandwidth | 2 Mbps |
| Traffic type, rate | CBR, 15 packets/sec |
| Number of things, and Packet size | 500, 128 Kbps |
| Number of connections, and Pause time | 70, 100 sec |
| Full Battery | 2000 mJ |
| Maximum mobility (varying) | 5 m/sec - 25 m/sec |
| Simulation time (in Sec) | 500-2000 |

Table 8 and 9 compares the performance of ELaM-IoT with that of ERGID and ADRM-IoT regarding to throughput, the rate of packet receiving, average residual energy, end to end delay, and network lifetime.

**Table 8.** $ARE$ (in Joule) of various frameworks vs number of CBR sources.

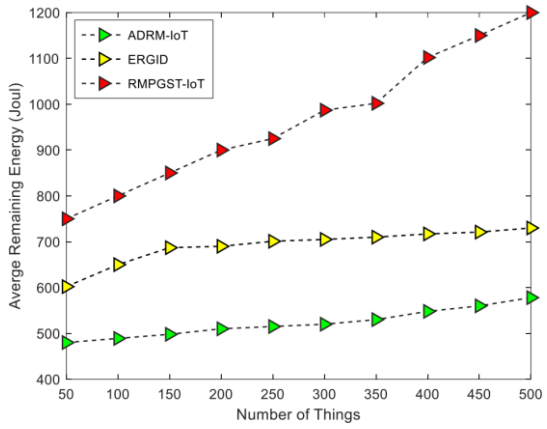
| Rate of Transmission (kb/s) | ARE (Joule) | | |
|---|---|---|---|
| | $ADRM-IoT$ | $ERGID$ | $ELaM-IoT$ |
| 10 | 750 | 830 | 950 |
| 20 | 730 | 814 | 933 |
| 30 | 700 | 801 | 928 |
| 40 | 640 | 789 | 925 |
| 50 | 600 | 780 | 920 |
| 60 | 550 | 773 | 902 |
| 70 | 510 | 770 | 891 |
| 80 | 500 | 762 | 886 |
| 90 | 430 | 757 | 880 |
| 100 | 400 | 752 | 871 |

**Table 9.** $NL$ (in Joule) of various frameworks vs number of CBR sources.

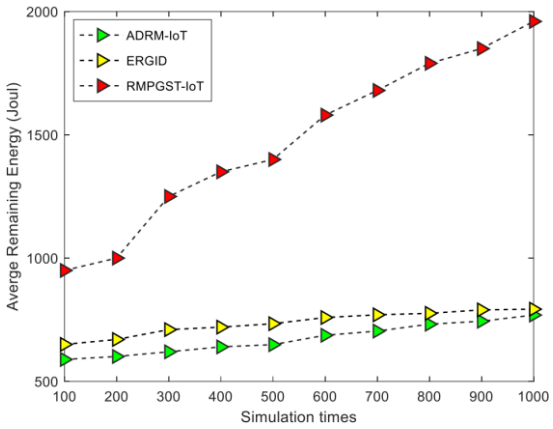
| Rate of Transmission (kb/s) | NL (Sec) | | |
|---|---|---|---|
| | $ADRM-IoT$ | $ERGID$ | $ELaM-IoT$ |
| 10 | 720 | 891 | 1400 |
| 20 | 680 | 800 | 1350 |
| 30 | 640 | 770 | 1300 |
| 40 | 600 | 730 | 1150 |
| 50 | 550 | 714 | 1080 |
| 60 | 503 | 704 | 975 |
| 70 | 475 | 680 | 904 |
| 80 | 430 | 674 | 850 |
| 90 | 410 | 645 | 760 |
| 100 | 400 | 612 | 710 |

Figure 3 indicates the comparing of the suggested scheme of ELaM-IoT, ERGID and the models of ADRM-IoT regarding to $ARE$ . (a) The things number, (b) Simulation time, (c) Speeds, and (d) Number of CBR sources respectively. This criterion presents the $ARE$ in the nodes after routing has been carried out and is calculated using equation 13 which is calculated by subtracting the consumed energy from the initial energy. As seen in figure 3, the $ARE$ in the nodes is calculated at 100 and 1000 seconds in every simulation. The simulation results present that the $ARE$ in the nodes for the proposed ELaM-IoT is higher than the ERGID and ADRM-IoT methods. This is because in the proposed method, routing is carried out using routes which consist of nodes which are better than the nodes in other routes with respect to hop count, noise rate, $ARE$ , and link expiration time criteria. Therefore, taking into account the hop count criterion leads to lower energy consumption, while selecting the route which consists of nodes with higher energy levels controls the network energy and increases the $ARE$ . Therefore, the ELaM-IoT performs better in this regard as well. The $ARE$ in ELaM-IoT, ERGID and ADRM-IoT algorithms is reduced by 700, 600 and 470%, respectively, while the number of things is increased by 940, 690 and 550%, respectively.

(a)




(b)




(c)

(d)

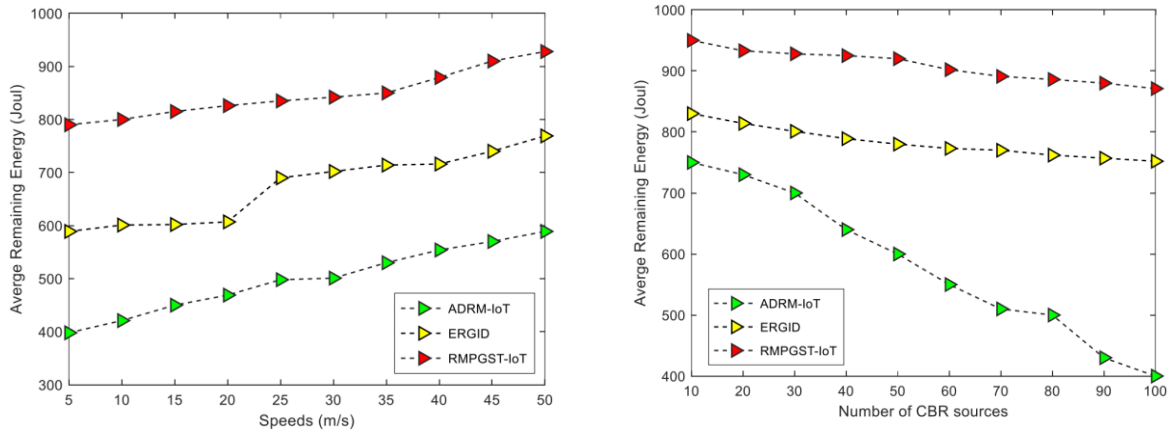
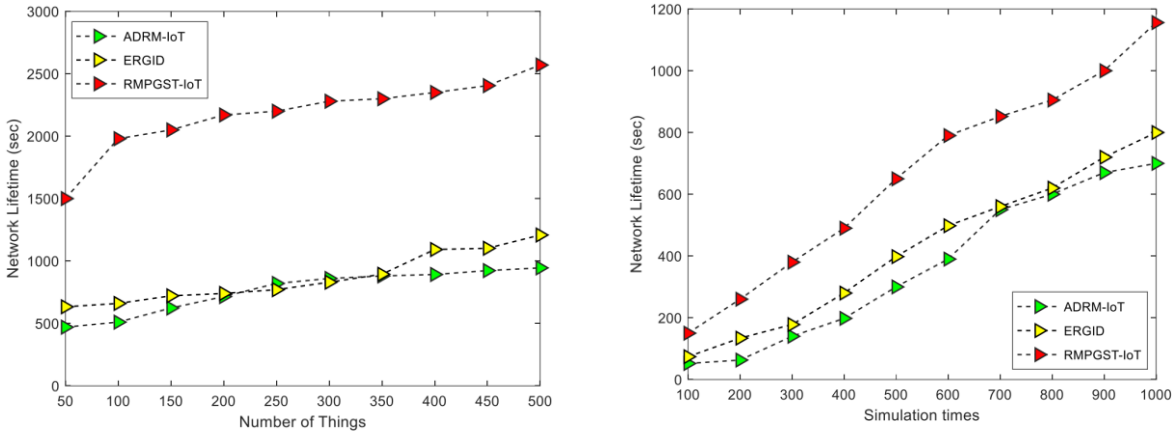



**Figure 3.** Comparison of the ELaM-IoT proposed scheme, ERGID and ADRM-IoT approaches in term of Average remaining energy. (a) Number of Things, (b) Simulation time, (c) Speeds, and (d) Number of CBR sources.

Comparison of network lifetime in shown in Figure 4. As proved by the graph, the proposed (ELaM-IoT) method shows a large network lifetime in comparison with other present methods. Increasing the number of CBR sources will reduce the network lifetime. In comparison to present approach, the proposed ELaM-IoT applies the large lifetime of network in 500 things 5200 rounds. The lifetime of network, in 100 nodes, for present approaches ERGID, and ADRM-IoT are 4800rounds, and 4100rounds respectively. In the ELaM-IoT method, by choosing high energy routes with fewer hops, premature deactivation of nodes in the network is prevented. Since the routes are selected for data transmission based on their remaining energy and fewer hops while also taking into consideration their noise rate and link expiration time, energy in the network nodes is depleted over a longer period of time and network lifetime is increase.

(a)

(b)




(c)

(d)

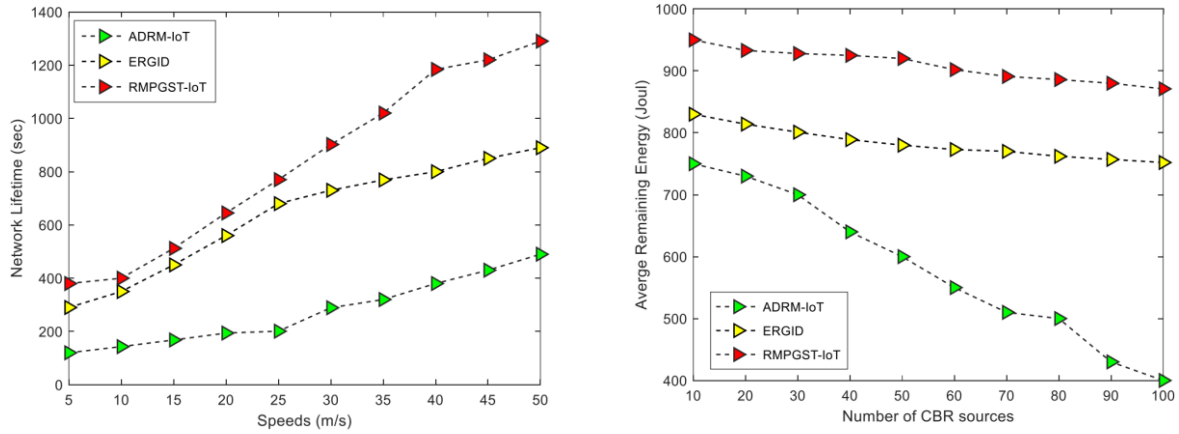



**Figure 4.** Comparing of the suggested scheme of ELaM-IoT, ERGID and ADRM-IoT approaches concerning to Lifetime. (a) The things number, (b) Simulation time, (c) Speeds, and (d) Number of CBR sources.

**Energy Balance:** The energy analysis is done by the 50 key nodes gathered from the other 500 nodes. The remaining energy and lifetime of 200, 400, 600, 800, 1000 s are used for analysis. Figure 5 indicates ELaM-IoT lifetime and remaining energy. The secondary energy amendment strategy provides a better energy balance impact.

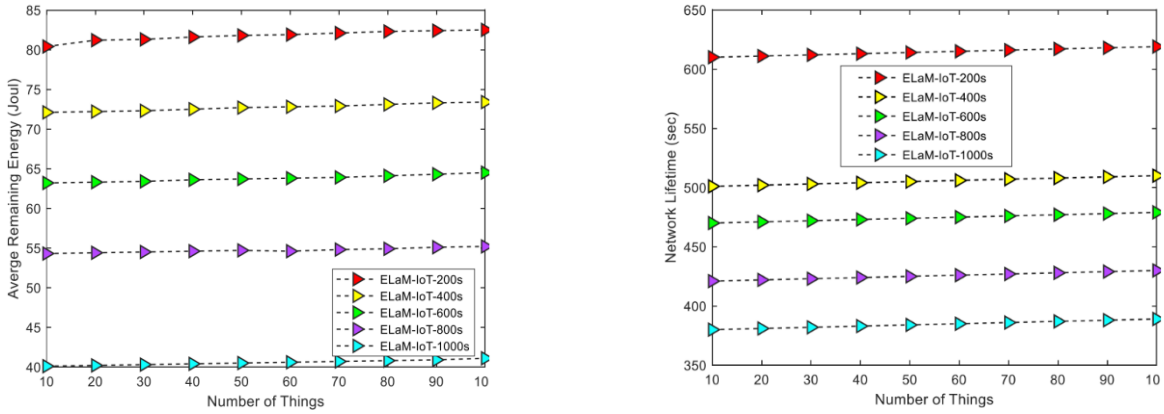



**Figure 5.** Comparison of the ELaM-IoT proposed scheme, in terms of energy distribution curve and lifetime at different times.

## 5. Conclusion

In this paper, this method is improved using composite metrics which choose the best paths used for separate routes to send packets. The protocol of Energy and Load aware RPL (ELaM-IoT) is proposed in this work which is an improved form for the protocol of RPL protocol. A composite metric is used by it, which is calculated based on hop count, remaining energy, Link Expiration Time (LET), load, and battery depletion index (BDI) for route selection. Applying the performance of NS-3, the ELaM-IoT scheme was investigated and displayed that it is a performance of a high level with a high network lifetime (above 89.73%) and a high mean remaining energy (above 74.23%) compared to the existing approaches.

In the future, we plan to explore the potential of utilizing a combination of blockchain and machine learning techniques to enhance the security aspects of the proposed ELaM-IoT routing protocol. One promising avenue for future research is to investigate the integration of blockchain technology and machine learning algorithms to bolster the security of IoT networks. Blockchain provides a decentralized and immutable ledger that can ensure the integrity and authenticity of IoT data and transactions. By incorporating blockchain into ELaM-IoT, we can establish a secure and trustworthy framework for routing decisions and data exchange among IoT devices. Furthermore, machine learning algorithms can be leveraged to analyze the data collected from IoT devices and identify potential security

threats or anomalies. By training machine learning models on historical data, we can develop predictive and adaptive security mechanisms that can detect and mitigate various types of attacks, such as unauthorized access, data tampering, or malicious behavior within the IoT network.

## Authors' Contributions

Authors equally contributed to this article.


## Acknowledgments

Authors thank all participants who participate in this study.


## Declaration of Interest

The authors report no conflict of interest.


## Funding

According to the authors, this article has no financial support.


## Ethical Considerations

All procedures performed in this study were under the ethical standards.

## References


[1] S. Sankar and P. Srinivasan, "Energy and load aware routing protocol for internet of things," *International Journal of Advances in Applied Sciences (IJAAS)*, vol. 7, no. 3, pp. 255-264, 2018. [Online]. Available: https://doi.org/10.11591/ijaas.v7.i3.pp255-264.

[2] I. S. Alsukayti, "The support of multipath routing in IPv6-based internet of things," *International Journal of Electrical & Computer Engineering*, vol. 10, no. 2, 2020. [Online]. Available: https://doi.org/10.11591/ijece.v10i2.pp2208-2220.

[3] C. H. Tseng, "Multipath load balancing routing for Internet of things," *Journal of Sensors*, vol. 2016, 2016.

[4] B. Ravaei, S. Ravaei, S. MoshrefZadeh, and O. Rahmani Seryasat, "An Efficient and Load Balanced Task Offloading in Vehicular Internet of things," *Transactions on Machine Intelligence*, vol. 5, no. 1, pp. 46-55, 2022, doi: 10.47176/TMI.2022.46.

[5] M. Moradi, "A Bayesian Model and Bayesian Classification on the Data Obtained from Children's Educational Activity in the IoT Environment," *Transactions on Machine Intelligence*, vol. 6, no. 3, pp. 126-136, 2023, doi: 10.47176/TMI.2023.126.

[6] M. Z. Hasan and F. Al-Turjman, "Optimizing multipath routing with guaranteed fault tolerance in Internet of Things," *IEEE Sensors Journal*, vol. 17, no. 19, pp. 6463-6473, 2017. [Online]. Available: https://doi.org/10.1109/JSEN.2017.2739188.

[7] F. Demicheli, "Design, implementation and evaluation of an energy efficient RPL routing metric," 2011.

[8] Q. Pan, J. Wu, A. K. Bashir, J. Li, and J. Wu, "Side-Channel Fuzzy Analysis-Based AI Model Extraction Attack with Information-Theoretic Perspective in Intelligent IoT," *IEEE Transactions on Fuzzy Systems*, vol. 30, pp. 4642-4656, 2022. [Online]. Available: https://doi.org/10.1109/TFUZZ.2022.3172991.

[9] Y. Xu *et al.*, "Intelligent IoT security monitoring based on fuzzy optimum-path forest classifier," *Soft Computing*, vol. 27, pp. 4279-4288, 2022. [Online]. Available: https://doi.org/10.1007/s00500-022-07350-y.

[10] A. Verma, G. Agarwal, A. K. Gupta, and M. Sain, "Novel Hybrid Intelligent Secure Cloud Internet of Things Based Disease Prediction and Diagnosis," *Electronics*, 2021. [Online]. Available: https://doi.org/10.3390/electronics10233013.

[11] C. Kharkongor, T. Chithralekha, and R. Varghese, "A SDN controller with energy efficient routing in the Internet of Things (IoT)," *Procedia Computer Science*, vol. 89, pp. 218-227, 2016. [Online]. Available: https://doi.org/10.1016/j.procs.2016.06.048.

[12] G. Hatzivasilis, I. Papaefstathiou, and C. Manifavas, "SCOTRES: secure routing for IoT and CPS," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2129-2141, 2017. [Online]. Available: https://doi.org/10.1109/JIOT.2017.2752801.

[13] T. Qiu, Y. Lv, F. Xia, N. Chen, J. Wan, and A. Tolba, "ERGID: An efficient routing protocol for emergency response Internet of Things," *Journal of Network and Computer Applications*, vol. 72, pp. 104-112, 2016. [Online]. Available: https://doi.org/10.1016/j.jnca.2016.06.009.

[14] Y. Tian and R. Hou, "An improved AOMDV routing protocol for internet of things," in *In 2010 International Conference on Computational Intelligence and Software Engineering (pp. 1-4). IEEE*, 2010. [Online]. Available: https://doi.org/10.1109/CISE.2010.5676940.

[15] J. Shen, A. Wang, C. Wang, P. C. Hung, and C. F. Lai, "An efficient centroid-based routing protocol for energy management in WSN-assisted IoT," *IEEE Access*, vol. 5, pp. 18469-18479, 2017. [Online]. Available: https://doi.org/10.1109/ACCESS.2017.2749606.

[16] A. A. AlZubi, M. Al-Maitah, and A. Alarifi, "A best-fit routing algorithm for non-redundant communication in large-scale IoT based network," *Computer Networks*, vol. 152, pp. 106-113, 2019. [Online]. Available: https://doi.org/10.1016/j.comnet.2019.01.030.

[17] F. Sarkohaki, R. Fotohi, and V. Ashrafian, "An efficient routing protocol in mobile ad-hoc networks by using artificial immune system," *International Journal of Advanced Computer Science and Applications (IJACSA), 8 (4)*, 2017.