*energies*

MDPI

*Article*

# MHSEER: A Meta-Heuristic Secure and Energy-Efficient Routing Protocol for Wireless Sensor Network-Based Industrial IoT

**Anshika Sharma [1], Himanshi Babbar [1], Shalli Rani [1,*], Dipak Kumar Sah [2], Sountharrajan Sehar [3] and Gabriele Gianini [4,*]**

1 Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura 140401, Punjab, India; anshika.sharma@chitkara.edu.in (A.S.); himanshi.babbar@chitkara.edu.in (H.B.)
2 Department of Computer Engineering and Application, GLA University, Mathura 281406, Uttar Pradesh, India; dipak.sah@gla.ac.in
3 Department of Computer Science and Engineering, Amrita School of Computing, Chennai 601103, Amrita Vishwa Vidyapeetham, India; s_sountharrajan@ch.amrita.edu
4 Dipartimento di Informatica, Universita degli Studi di Milano, 20133 Milano, Italy
* Correspondence: shalli.rani@chitkara.edu.in (S.R.); gabriele.gianini@unimi.it (G.G.)

**Abstract:** Several industries use wireless sensor networks (WSN) for various tasks such as monitoring, data transmission, and data gathering. They find applications in the industrial internet of things (IIoT). WSNs are utilized to track and monitor changes in the environment. Since they include multiple small sensor nodes (SN), they are severely constrained, so resource management geared toward energy efficiency is crucial in this kind of network. Minimizing the power to interpret, transmit, and store data between various sensors poses important challenges. Experts have considered various ways to address these issues that unavoidably affect the network's performance: reducing energy usage while maintaining system throughput remains the primary research issue. Another important concern relates to network security. Specifically, intrusion detection and avoidance are major concerns. In this work, we introduce the meta-heuristic-based secure and energy-efficient routing (MHSEER) protocol for WSN-IIoT. The protocol learns the forwarding decisions using the number of hops, connection integrity characteristics, and accumulated remaining energy. To make the method more secure, the protocol also employs counter-encryption mode (CEM) to encrypt the data. A meta-heuristics study designed to achieve reliable learning is used in the suggested protocol. The protocol consists of two stages. The first stage uses a heuristics method to improve the option for dependable data routing. Security based on a computationally simple and random CEM is accomplished in the second stage. The proposed MHSEER protocol has been compared to the secure trust routing protocol for low power (Sectrust-RPL), heuristic-based energy-efficient routing (HBEER), secure and energy-aware heuristic-based routing (SEHR), and secure energy-aware meta-heuristic routing (SEAMHR) in terms of packet drop ratio, throughput, network delay, energy usage, and faulty pathways. The proposed protocol increases throughput to 95.81% and decreases the packet drop ratio, packet delay, energy consumption, and faulty pathways to 5.12%, 0.10 ms, 0.0102 mJ, and 6.51%, respectively.

**Keywords:** wireless sensor networks; industrial internet of things; sensor nodes; energy efficiency; meta-heuristic



**Citation:** Sharma, A.; Babbar, H.; Rani, S.; Sah, D.K.; Sehar, S.; Gianini, G. MHSEER: A Meta-Heuristic Secure and Energy-Efficient Routing Protocol for Wireless Sensor Network-Based Industrial IoT. *Energies* **2023**, *16*, 4198. https://doi.org10.3390/en16104198

Academic Editors: R. Maheswar, M. Kathirvelu and K. Mohanasundaram

Received: 22 April 2023
Revised: 14 May 2023
Accepted: 15 May 2023
Published: 19 May 2023



## 1. Introduction

The industrial internet of things (IIoT) paradigm relies heavily on wireless sensor networks (WSNs) [1], which are wireless networks without infrastructure facilities that are deployed using a wide variety of wireless sensors to assess operational, physical, or environmental conditions. In WSN, sensor nodes (SNs) with an inbuilt CPU manage the

system and are connected among them and to the base station (BS) [2] (which in turn can be linked to the internet). The nodes perform sensing, data processing, and transmission, whereas data collection, analysis, and delivery to the end user for decision-making are the BS's responsibilities [3]. Due to their versatility, WSNs have found application in several domains such as IoT, tracking and detection systems, conditions monitoring (relative humidity, temperature, and air density), patient evaluation, and agribusiness [4,5].

The key characteristic of WSN is that not only the storage capacity, memory, and CPU processor capabilities of the nodes are limited but their power consumption is considerably constrained [6,7]. Energy-efficient routing (EER) algorithms are therefore essential to reduce power consumption and extend the useful life of the network [8]. Furthermore, the network must be operated manually, which presents certain difficulties [9].

When designing protocols and hardware architectures, researchers should prioritize the effective utilization of the energy storage of SNs [10]. The approaches that have received the most attention include cluster formation and different data transmission communication methods. SNs are organized into a number of subsets, i.e., clusters, to reduce power usage for lengthy transmission [11]. Removing associated data that could reduce the total volume of data exchanged with the BS is the responsibility of a cluster head (CH) [2,12]. The CH transfers the combined information to the BS.

Since they are frequently placed in hazardous or distant locations and are therefore challenging to physically safeguard, sensor nodes are more susceptible to security attacks. They might also lack the ability to process information and the memory necessary to execute effective security regulations, which would make them more vulnerable to attacks. The probability of illegal access and compromised network security and integrity increases greatly as a result of such restrictions [13]. Most proposed solutions aim to increase resource efficiency and the timely distribution of data but neglect to address the reliability of sensor data, leaving a gap for hackers. For industrial operations, inaccurate or manipulated sensor data can have major repercussions, including malfunctioning equipment, delayed production, and safety risks. As a result, it is crucial to use secure protocols, encrypted data, and authentication methods to guarantee the integrity and validity of sensor data [14].

### 1.1. Objective

WSN-IIoT has the distinct benefit of enabling the continuous surveillance and oversight of industrial operations, which boosts productivity, safety, and effectiveness [15]. With the use of WSNs, preventative upkeep may be carried out on manufacturing equipment and processes, resulting in less downtime. WSNs can also aid in waste minimization and energy optimization, which can save money and assist the environment. WSN-IIoT may, in general, automate and revolutionize manufacturing operations by facilitating decision-making based on data. In order to balance the power usage and avoid unauthorized access, data manipulation, and exposure by malicious nodes on the network, an energy-efficient routing (EER) protocol solution should be created for IoT-based WSNs [16,17]. The purpose of this study is to propose a WSN routing technique that is secure and energy-efficient. The primary goals of the proposed MHSEER protocol are energy efficiency, stability, and reliability, in data transfer despite limited resources. To obtain the best possible data routing, some heuristics are utilized. To learn the routing decision, the MHSEER protocol uses integrated minimal resources, hop count, and connection integrity measures [18]. The suggested IIoT protocol has advantages such as improved security, decreased power consumption, and increased reliability. A secure routing protocol can shield critical data from cyberattacks and stop unauthorized users from connecting to the network. It helps IIoT devices use less energy, which extends their lifespans and minimizes their operating expenses, and by lowering the likelihood of network congestion and packet loss, the protocol can increase the reliability of IIoT systems. The MHSEER protocol is reliable thanks to encoding and the detection and segregation of hostile nodes; furthermore, it offers a method for dynamic routing [13]. The network monitoring between the BS and its surroundings and the energy-efficiency signals together provide effective load balancing

and lessen the issue of network segregation. We will show that, compared to existing state-of-the-art solutions, the MHSEER protocol improves the performance of low-power SNs in terms of different performance metrics [19]. The suggested Protocol in IIoT also has several drawbacks, such as complexity and compatibility. A safe routing protocol's implementation might be difficult and expensive because it calls for specialized knowledge and skills. Certain protocols might not work with some IIoT devices, which could restrict their operation or necessitate extra hardware modifications.

### *1.2. Contributions*

The paper's contributions are the following.

- An architecture of WSN-IIoT has been developed for the MHSEER protocol that helps minimize the delay and energy consumption of the network with maximum stability [14].
- To solve the above-mentioned issues, an MHSEER approach has been proposed, which enhances the choice for reliable data routing using a heuristic function and uses the encoding and decoding of data package based on counter encryption mode (CEM) [9].
- The proposed protocol compares the different parameters of a routing protocol such as throughput, network delay, packet drop rate, faulty pathways, and energy usage with the above-mentioned existing approaches. MHSEER increases the throughput and decreases metrics such as the packet drop rate and energy usage.

### *1.3. Structure*

The structure of this article is as follows: Section 2 outlines the state-of-the-art in energy-efficient routing protocols. Section 3 introduces the proposed architecture of WSN-IIoT for the secured and energy-efficiency protocol. A detailed discussion of the MHSEER protocol and the stages designed is presented in Section 4. Section 5 shows the experimental findings about MHSEER and compares them to the competing approaches. Finally, Section 6 summarizes the findings of the paper.

## 2. Related Work

Various works aim at providing routing protocols that are secure and energy-efficient. In 2019, Hamzah et al. [2] discussed a fuzzy approach for selecting cluster heads (CHs) based on five features: density, residual energy, suitability, and distance from the BS. Utilizing FL-EEC/D (fuzzy logic-based energy-efficient clustering) depending on minimal segregation among CHs, WSNs are created. SNs are evaluated for energy efficiency using the Gini index; clustering techniques normalize resource allocations between WSNs. The results show that the energy usage of the SN stabilized and the energy efficiency with respect to the lifetime of a network improved. In regard to the first cluster dead and half clusters dead, the outcomes demonstrate an average growth.

In 2019, Liu et al. [10] suggest a revised routing protocol to increase WSN resource efficiency. Residual network energy and network average energy are taken into account by the IEE-LEACH protocol in this study. In order to further increase the network's energy consumption, the proposed protocol also adopts a threshold for choosing CHs amongst some of the SNs and makes use of single-hop, multi-hop, and composite connections. The simulation findings demonstrate that this method greatly decreases WSN power use if compared with a number of current routing strategies.

In 2020, Hayajneh et al. [5] communicated with the OSI layers (physical, data link, network, topology, and application) to examine cyber threats in WSNs. The number of significant attacks is calculated, and security precautions are set up to detect attacks. A security technique is created to fix the flaws and identify other problems that require more investigation. This method was only used with a small number of SNs, which negatively impacted the performance performance of the network and did not increase network safety when there were many SNs present. However, the complexity, consumption, and transmit time would all significantly increase, making this potentially inappropriate for WSNs.

In 2020, Binu et al. [14] created an innovative African Buffalo-based two-tier data dissemination technique (AB-TTDD) to check the energy-drained unit early, before information transfer. A brand new temporary energy mapping algorithm (TEMA) was also created to sustain the pathway by producing the reference node rather than the energy-drained component. This innovative method has significantly decreased both power usage and the packet flow ratio. The current study demonstrates that routing maintenance and optimization in WSN may decrease energy usage. However, the proposed methodology's processing takes longer.

In 2020, Haseeb et al. [6] suggested SEHR for WSNs to detect and prevent data manipulation while achieving greater performance. The method provided reliable and insightful learning through the use of heuristic evaluation, which was taken from artificial intelligence (AI). This technique uses a heuristic approach to spot and guard against data breaches. The current metaheuristic method provides less accurate data categorization. The key generation portion of this approach needs to be enhanced because the counter block allows the key value to be identified. By taking into account asynchronous operations among the sensor nodes, energy consumption and routing efficiency can be further enhanced.

In 2022, Gurram et al. [9] discussed a SEAMHR technique in order to choose the best route to the target while preserving data integrity. The learned path is used to identify the most ideal neighbourhood, which serves as a redirector to send the information to the intended receiver, and mutation elephant herding optimization (MEHO) is used to enhance the meta-heuristic function. The SEAMHR method uses the AEDL approach and CTR-AEDL mode encrypted using private keys to encrypt and decrypt data. The MATLAB tool is used to conduct the experiment.However, the suggested protocol will not be expanded to take into account mobility requirements and multi-hop network interactions.

In 2022, Seyfollahi et al. [16] provided a composite energy-aware strategy for data forwarding in IoT, considering the need to extend IoT technologies and the NP-hardness of power management in diverse and dispersed IoT networks. By integrating the support vector machine (SVM), a popular machine learning (ML) approach, and the meta-heuristic heat transfer optimizer (HTOA) approach, this paper tried to implement an optimal method for routing and transmitting data. The results demonstrate that merging ML and HTOA has produced the best possible energy-conscious routing for the IoT.However, it should be taken into account that HTOA, like another optimizer, could become trapped in local optima.

In 2022, Behera et al. [4] briefly discussed low-energy adaptive clustering hierarchy (LEACH)-based and bioinspired protocols, their advantages and disadvantages, their underlying presuppositions, and the selection criteria for the CH to comprehend routing protocols with various structures, innovative tactics, and improved efficiency in the WSN environment. The scalability, durability, and packet-delivery rates of different protocols are contrasted and considered as performance aspects. Additionally, the exploration of developing cryptographic techniques for verified encryption in WSNs that support privacy and network safety is an option.

In 2023, ref. [20] the WSN is responsible for gathering and arranging sensed data before sending it to the base station (BS). As the battery power of sensor nodes is limited, it is crucial to employ effective techniques for data collection and transmission to ensure the extended operation of the sensor network. In this study, the researchers utilized the particle swarm optimization (PSO) method to establish the cluster in WSN. Additionally, they proposed an energy-efficient routing protocol (E-FEERP) based on fuzzy logic. The E-FEERP algorithm considers various factors such as battery energy, the average distance between sensor nodes (SN) and the BS, node density, and communication quality to transmit data from the cluster head (CH) to the BS optimally.

Other works study the problem of clustering and energy efficiency from a game theory perspective [21,22]. Indeed, game theory is routinely used as a framework for the modeling and analysis of performance and security networked systems [23–29]. The work by Gemeda et al. [30] addresses the issue of energy efficiency by proposing a protocol, called GREET,

based on non-coalitional game theory: the protocol is not power-aware, but it improves over LEACH in terms of network lifetime.

The current research increases throughput rates and decreases the packet loss rates, energy usage, defective routes, and packet delay of the WSN as compared to the existing energy-efficient protocol (Table 1), as indicated in the prior research.

**Table 1.** Comparative analysis of existing literature.

| Ref. No. | Year/ Author Name | Objective | Software Used | Parameter | Future Scope |
|---|---|---|---|---|---|
| [1] | 2019/ Airehrour et al. | By integrating the SecTrust system into the RPL protocol, a simulated exercise was conducted to demonstrate the SecTrust system's effectiveness at fending off Rank and Sybil assaults. | PhD Research Lab of Auckland University of Technology. | Throughput, packet drop rate. | To increase the network's integration of trustworthy nodes that have repaid their battery life by extending the SecTrust-RPL. |
| [2] | 2019/ Hamzah et al. | Utilize the gain ratio to assess how effectively the clustering methods can balance the energy distribution among WSN sensor nodes. A fuzzy logic-based CH election method, a k-means-based clustering method, and LEACH are contrasted with the suggested technique FL-EEC/D. | .NET | SN's residual power, the distance to the BS, the density of the SN, the compacting of the SN, and location appropriateness. | The Gini index is a reasonable assessment tool for assessing the routing protocols' energy effectiveness in WSNs for the metric of energy distribution balance. |
| [6] | 2020/ Haseeb et al. | The method provided reliable and insightful learning through the use of heuristic evaluation, which was taken from AI. This technique uses a heuristic approach to spot and guard against data breaches | MATLAB | Throughput, the ratio of packet drops, significant delay, consumed energy, erroneous routes, overhead on networks, and computational cost. | To make the system smarter and fault-tolerant by employing certain lightweight machine learning-based approaches to enhance the SEHR technique. |
| [8] | 2019/ Kuhlani et al. | Developed an accessible virtual structure that serves as an intermediary architecture between the sink and the nodes while sharing metadata and query messages in order to lessen the mobile sink's frequently current location to all nodes. | MATLAB | Average rate of delivery, average energy utilization, the lifespan of a network, and absolute delay. | The suggested approach can be further explained to understand the flow better. |
| [31] | 2019/ Alami et al. | To reduce the energy consumption of WSNs, hierarchical techniques that utilize clustering hierarchy are proposed. Data collection and transmission to a base station could be carried out using the nodes with the highest residual energy. | MATLAB | Stable timeframe, HNA, the lifespan of a network, network traffic, and throughput . | The suggested technique can be expanded to manage a system of mobile sinks and will analyze the network lifespan optimization. |

## 3. Proposed Architecture of WSN-IIoT for Energy Routing Protocol

The clustering process divides the network into various clusters in the WSN environment. Each cluster contains a CH node that transmits data collected from its SN network to the BS, as shown in Figure 1. In hierarchical protocols, choosing the CH node is a crucial decision that adds to the system overhead. The network will experience significant overhead if the CH node fails. The objective is to suggest an energy efficiency technique that minimizes system overhead and maximizes stability. The proposed protocol allows all nodes in a cluster to be CH nodes; however, the clusters are not required to contain a CH node [10]. The CH node is elected using a learned machine. In fact, consuming less energy, which is currently being spent on frequent selections of CH nodes, will hopefully lengthen network longevity. The nodes cooperate to send data to the BS; as a result, the nodes closest to the BS will use more resources than most of the other nodes. As a result, it is likely that the clusters near the BS change to a non-connected condition. As a result, the detected data are not sent to the BS. The clusters next to the BS have smaller sizes to address this issue. Hence, energy for transmitted data will be saved [11].

The proposed approach does not require the SNs to recognize the CH node. An SN uses its cluster-ID and some basic details about its distant neighbors in one hop to deliver data to the BS. The routing protocol employs a distributed and localized strategy to use a learning system to identify the best CH nodes for each cluster. Each node in this scenario can choose the optimum path for data transfer or act as a CH node [2].

An energy-efficient routing protocol is created. An algorithm is initialized right away to preserve the route to identify erroneous data proclamation from the nearby nodes and predicts link failure using its fitness function, as shown in Figure 2. As a result, the algorithm helps extend the node lifetime by reconstructing the path and optimizing the data drop ratio. Hence, the information is securely transmitted without being interrupted.

So, an algorithm is implemented to track the announcement of misleading data. The inclusion of the proposed approach in the routing protocol helps to detect fraudulent data announcements. The protocol also foresees energy-drained nodes early on and raises an alarm as a result. This alarm helps to start the maintenance of the route of the protocol that is elaborated in Figure 2 [14]. Some SNs are included in the homogeneous structure of the energy-efficient routing protocol, and each node is aware of its own position. The fitness function evaluates the node's full energy; therefore, it has an early awareness of connection failure based on the energy of the node. As a result, the algorithm is initiated when the monitoring node issues an alarm in the event that a connection failure occurs within a few moments. An energy-efficient routing protocol is an effective, expandable, and adaptable routing protocol. In wireless architecture, the data can be transmitted to the source and destination nodes via a variety of routes. There are some basic functions such as route preservation, maximizing the lifespan of a network, and minimizing packet drops for secure data transmission [32].

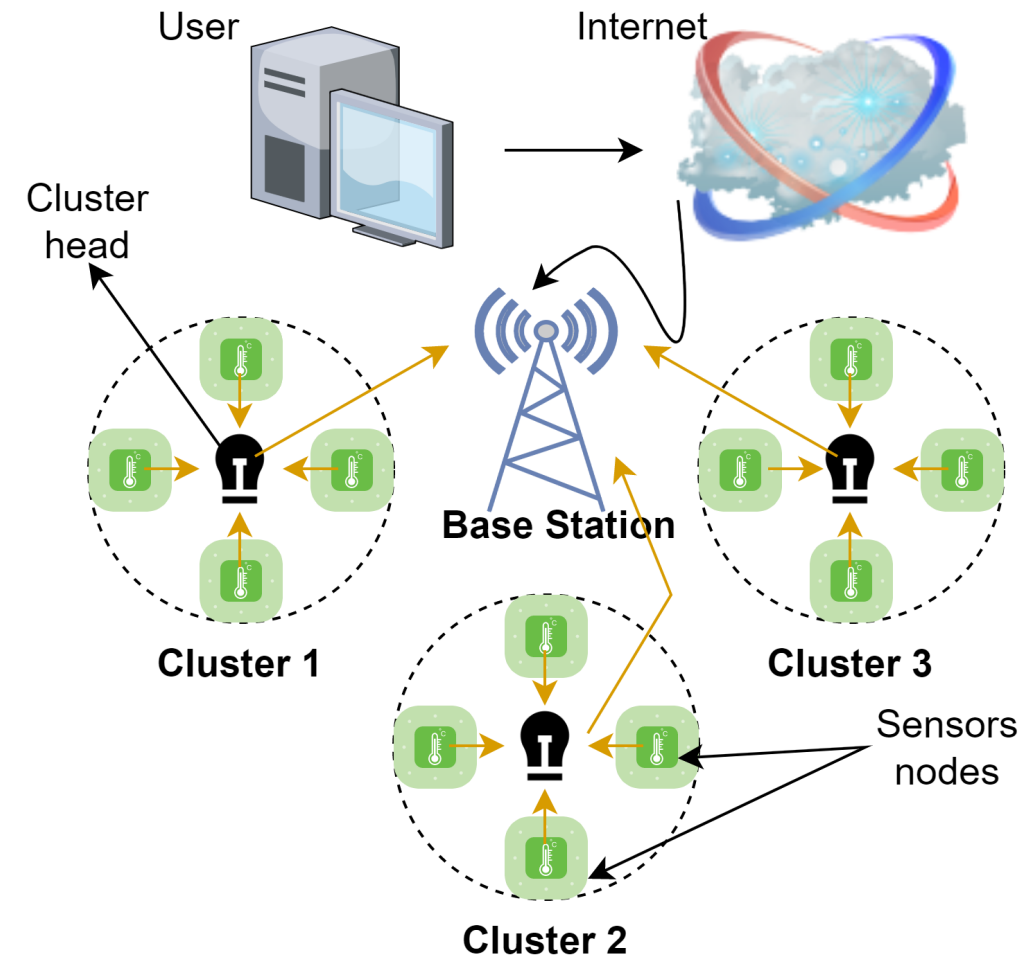


**Figure 1.** Framework of WSN in IIoT.

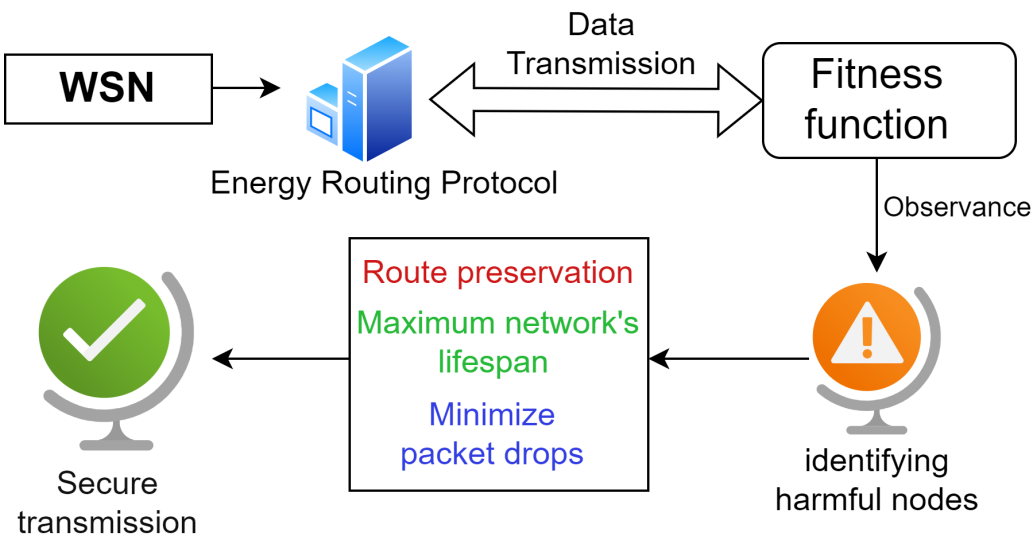


**Figure 2.** Architecture of WSN for energy-efficient routing protocol.

## 4. Methodology

This section describes the phases of the proposed MHSEER protocol in detail. The protocol uses link stability metrics, hop counts, and accumulated residual energies to make routing decisions. To begin with, the suggested MHSEER protocol uses a meta-heuristic

study built to produce reliable and wise learning [9]. The protocol is a metaheuristic technique that enhances reliable data routing. There are two primary stages to this project. The first stage of the proposed protocol enhances the choice for reliable data routing using a heuristic algorithm. The beam heuristic reduces the memory requirements of the nodes and provides efficient next-hop selection by utilizing a number of characteristics and link reliability [6]. In the second stage, a protocol that is secure, legitimate, and based on a computationally simple and random CEM is achieved [14]. The proposed protocol (Figure 3) simultaneously uses the encryption and decryption of data packets while utilizing less computational power from the nodes. Furthermore, alarm and traffic assessment techniques reduce the likelihood of link failure and uneven energy use in the network area [33].

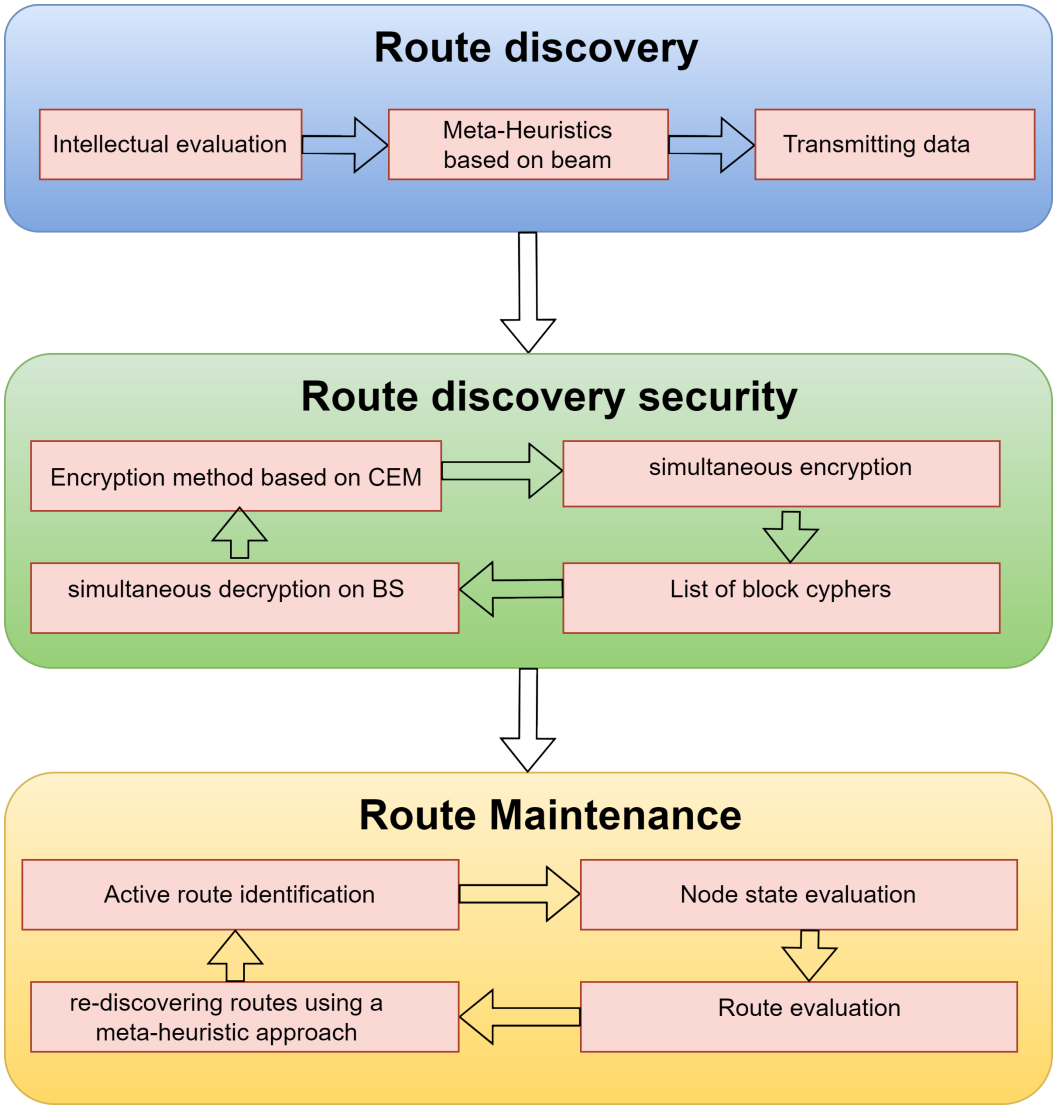


**Figure 3.** Design of the proposed method.

### *4.1. Route Discovery*

Suppose that the SNs are structured as graphs $G$, where $G(D, L)$ represents the graph, $L$ represents the optimal links between the two closely linked nodes $n_1$ and $n_2$, and $D$ is the density of the SNs. The MHSEER protocol uses the heuristic method in the first stage to estimate the relative weight for locating the best node as the next hop. The decision to route in the direction of the target node is guided by the heuristic function [34]. The source node validates its route entrance against the BS in a local database to start the discovery process. If it is discovered that the route meets the criteria for a number of hops to the BS

($h$), the degree of integrity of the link ($dl_i$), and the accumulated energy ($e_i$), the source node is selected as the next hop, and the packages are transferred directly to it [35]. Additionally, suppose that there is no viable route available that satisfies the routing criteria in the local database of the source node. In that case, each of the neighboring nodes must participate in the process of choosing the next hop. While accessing the affected links, the link integrity degree uses the hash function of cryptography to ascertain if the transmitted number of packets has been altered. Suppose node $i$ endangers a probe packet with p bits and sends it to node $j$ [36]. To identify its message code, $M_c$, node $i$ first delivers the probe packet $p_1$ to the hash function. Second, the received $M_c$ is added as $p_1 + M_c$ to the real probe packet and sent to node $j$. Node $j$ recalculates $M_c$ of the probe packet received by $p_1$ after receiving it along with $M_c$. One is used to denote the high threshold value, and zero is used to denote the low threshold value. The link's high threshold value indicates that it is very trustworthy and has a low fault rate. Residual energy aggregation $e_i$ is estimated in two stages [9]. The residual level $e_l$ is first continuously watched by each node, and then the residual energy's rate $e_r$ is calculated using Equation (1).

$$\sum me_n - ce_n \tag{1}$$

where $n$ is the neighbour, $me_n$ is the maximal energy, and $ce_n$ is the neighbour's energy consumption.

The node with the most accumulated residual energy is consequently assigned the highest precedence. Finally, the node examines the equivalent value that represents the hop count to the BS in its local table. The closer the node is to the BS, the less communication is required to transfer data, as indicated by a lower value. The heuristic function $h_f$ is then determined by adding all of the measured values of the accumulated residual energy, the integrity of the link, and the number of hops in a stack, as shown in the Equation (2).

$$h_f = a * (e_l + e_r) + b * \frac{1}{h} + c * dl_i \tag{2}$$

where $a$, $b$, and $c$ are the weighting coefficients and provide the heuristic function with a meaningful effect. Following the computation of $h_f$, every neighbor node communicates its knowledge to the SN to forecast the best course of action to take to reach the BS. The neighbor node with the highest $h_f$ indicates a superior rank for choosing the next hop. The proposed method uses the meta-heuristic protocol, which maximizes the suitable next-hop in a subset, to analyze the linked graph. In order to save memory and preserve the untrusted node while finding the next hop, the protocol creates node databases [37]. The beam meta-heuristics provide the method for choosing the best node as the next hop based on each node's greatest value. If we assume that, using beam heuristics, $h_{f0}, h_{f1}, \ldots, h_{fn}$, which have the highest weight value, then the weighted total $S(f_n)$ can be denoted as provided in the Equation (3)

$$S(f_n) = \sum h_{fi} \tag{3}$$

where $i$ = 0,1. . . ,$n$.

### *4.2. Route Discovery Security*

The proposed protocol concentrated on data protection for the selected beam based on heuristics routing in the second stage. To guarantee connectivity solutions with the least propagation delay, it also provides a route maintenance plan [6]. The proposed protocol uses a CEM that allows nodes to simultaneously encrypt data packets with randomization [38]. Three elements are required to start the CEM encoding method: a data package ($D_i$), a private key ($K$), and counter bits ($C$). To create the distinctive pattern of the counter block

$B_i$ shown in Equation (4), the node $N_i$ and counter bits are combined together and then sent through an encoding function $E_f$ using key $K$.

$$B_i = E_f(K(N_i + C)) \tag{4}$$

An encoder enables the encoding and decoding of the packet header, and a key generator is used to carry out the learning process. The network's parameters were optimized through a number of experiments, enabling the system to encode and decode data packets and $B_i$ very quickly. The activation function used in this experiment is given by Equation (5).

$$f(x) = \frac{1}{1 + e^{-x}} \tag{5}$$

where $f(x)$ is the sigmoid function. The originating nodes $n_i$ and $E_f$ are used to create the new counter block $B_{i+1}$ for the data packets $D_{i+1}$ after being concatenated with $N_i$ and $C$. The ciphertext sequences $c_i, \ldots, c_{n-1}, c_n$ nodes for $n_i, \ldots, n_{n-1}, n_n$ are consequently obtained in the BS, indicating that the decoding function $D_f$ with the same key is used to obtain authentic data packets $D_i$ where $i = 1, \ldots, n$ applying Equation (6).

$$D_i = [D_f(K(N_i + B_i))] \oplus c_i \tag{6}$$

### *4.3. Route Maintenance*

Some other routes are found with the help of route maintenance if the energy rates of the selected next-hop nodes drop to a particular threshold value [39]. As a result, data degradation and re-transmission are prevented. When an energy-inefficient node is found during the routing stage, it stops transmitting data and sends an error message to the origin node. The next subsequent hop is chosen to continue the data routing after the originating node uses the heuristic function to identify the node with the highest weight. The application of an energy threshold for the maintenance of the route significantly decreases the time of network and route intrusions [40]. Additionally, the quantity of packets received that the next-hops of the BS's neighbors broadcast to them determines the congestion ratio. The proposed method is used to determine the traffic rate ($Tf_r$) among the neighboring hops ($i$) or the BS given by Equation (7).

$$Tf_r = \frac{b_l - P_l}{B_m} \tag{7}$$

where $b_l$, $P_l$, and $B_m$ are the bandwidth of the link, the transmitted packets on the link, and the maximal bandwidth from $i$ to the BS, respectively.

## 5. Results and Discussion

This section describes the experimental findings and configuration of the proposed method over the Sectrust-RPL [1], SEHR [6], HBEER [6], and SEAMHR [9] approaches. The various network techniques are validated, tested, and verified using the MATLAB simulator tool to assess the results of the experiments. In terms of throughput, packet delay, defective routes, and energy consumption, the results are significantly better than the previous research's results. In addition, the performance of the linked methodologies and the proposed protocol is provided by taking into account variables such as end-to-end delay, fault pathways, throughput, packet drop ratio, and energy consumption. Table 2 displays the WSN parameter settings used in the simulation.

**Table 2.** Simulation parameters.

| Parameter | Value |
|---|---|
| Area of simulation | 300 ∗ 300 m |
| SNs | 250 |
| Infected nodes | 50 |
| Size of packets | 64 bits |
| Level of energy | 4 Joules |
| Position of BS | 200, 600 |
| Beamwidth | 4 |
| Control messages | 40 bits |
| Range of transmission | 40 m |
| Type of traffic | CBR |

Table 3 represents the comparative analysis of the proposed approach with the state of art approaches, and Figure 4 shows the graphical representation of the same.

**Table 3.** Comparative analysis of proposed approach with state-of-art approaches.

| Parameters | Sectrust-RPL | HBEER | SEHR | SEAMHR | Proposed |
|---|---|---|---|---|---|
| Throughput (%) | 74.94 | 79.75 | 86.16 | 94.64 | 95.81 |
| Packet drop ratio (%) | 25.66 | 19.71 | 13.32 | 7.34 | 5.12 |
| End-to-end delay (ms) | 0.178 | 0.162 | 0.136 | 0.114 | 0.10 |
| Energy consumption (mJ) | 0.0326 | 0.0252 | 0.0190 | 0.0154 | 0.0102 |
| Faulty routes (%) | 17.07 | 13.31 | 10.46 | 7.83 | 6.51 |

### *5.1. Throughput Analysis*

Table 4 depicts the analysis of the proposed throughput with the four existing methods. Figure 5 represents the throughput with respect to the different number of nodes. Additionally, by utilizing the CEM mechanism for information security, the proposed protocol lessens the possibility of rogue nodes impairing the operation of data transportation between the SNs and the BS. Furthermore, improving the delivery of packets and network access results from traffic monitoring between neighboring nodes and the BS, while the throughput is calculated by Equation (8).

$$Throughput = \frac{Recieved \quad packets}{Total \quad time} \tag{8}$$

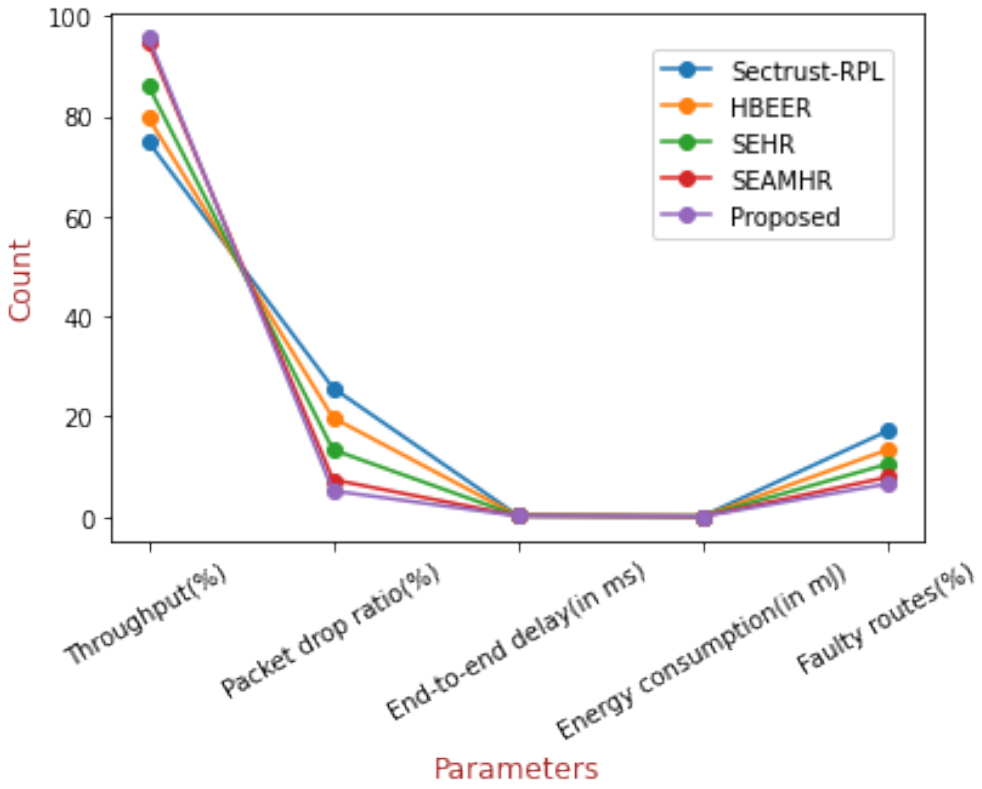


**Figure 4.** Comparative analysis of state-of-art approaches in terms of different parameters.

**Table 4.** Comparative analysis of proposed throughput (%) with state-of-art approaches.

| No. of Nodes | Sectrust-RPL | HBEER | SEHR | SEAMHR | Proposed |
|---|---|---|---|---|---|
| 50 | 78.8 | 85 | 89.8 | 95.2 | 95.8 |
| 100 | 77.4 | 84.4 | 89.2 | 94.9 | 96.2 |
| 150 | 76.2 | 82.3 | 86.3 | 94.76 | 95.9 |
| 200 | 74.94 | 79.75 | 86.16 | 94.64 | 95.12 |
| 250 | 70 | 76.2 | 85 | 92.8 | 93.25 |

Figure 5 shows the 250 nodes with respect to the throughput. In the case of 50 nodes, the proposed approach acquires the maximum throughput, i.e., 95.8%, as compared to the other existing approaches; in the case of 100 nodes, the proposed approach acquires 96.2% throughput in comparison to the existing approaches; in the case of 250 nodes, the proposed approach acquires 93.25% as compared to the existing approaches.

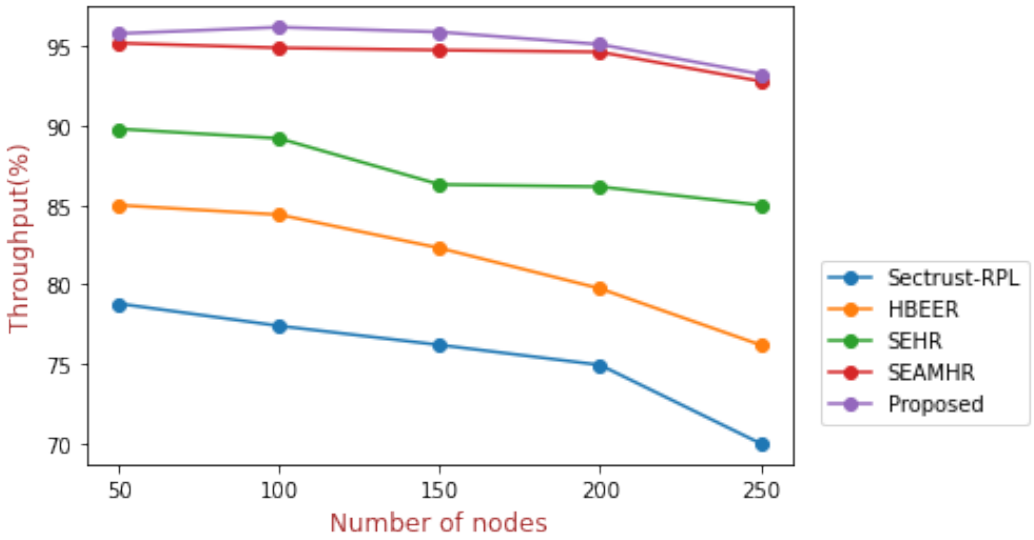


**Figure 5.** Throughput.

### *5.2. Packet Drop Ratio Analysis*

Table 5 shows the comparative analysis of the packet drop ratio of the four existing methods with the proposed approach. Figure 6 represents the packet drop rate with respect to the different numbers of nodes. In contrast to existing methods, the MHSEER protocol uses a beam heuristic approach to construct a residual energy-based weighted function, the number of hops to the BS, and the connection integrity criteria. Such an approach allows for the choice of the most reliable and energy-efficient nodes for packet transmission, and the packet drop ratio can be calculated by Equation (9).

$$Packet\ drop\ ratio = \frac{Received\ packets}{Total\ packets} \tag{9}$$

**Table 5.** Comparative analysis of proposed packet drop ratio (%) with state-of-art approaches.

| No. of Nodes | Sectrust-RPL | HBEER | SEHR | SEAMHR | Proposed |
|---|---|---|---|---|---|
| 50 | 22.51 | 16.22 | 10.11 | 5 | 4.8 |
| 100 | 23.63 | 16.32 | 12 | 6.21 | 5.10 |
| 150 | 24.94 | 17.41 | 13.24 | 7.12 | 6.56 |
| 200 | 25.66 | 19.71 | 13.32 | 7.34 | 6.85 |
| 250 | 30 | 21.27 | 15 | 9.54 | 8.24 |

Figure 6 depicts the minimum packet drop ratio in the proposed approach. As shown, if there are 50 nodes, it is 4.8% as compared to the existing approaches. If there are 250 nodes, it is 30% for Sectrust-RPL; 21.27% for HBEER; 15% for SEHR; 9.54% for SEAMHR; and 8.24% for the proposed approach, which is the minimum that is required.

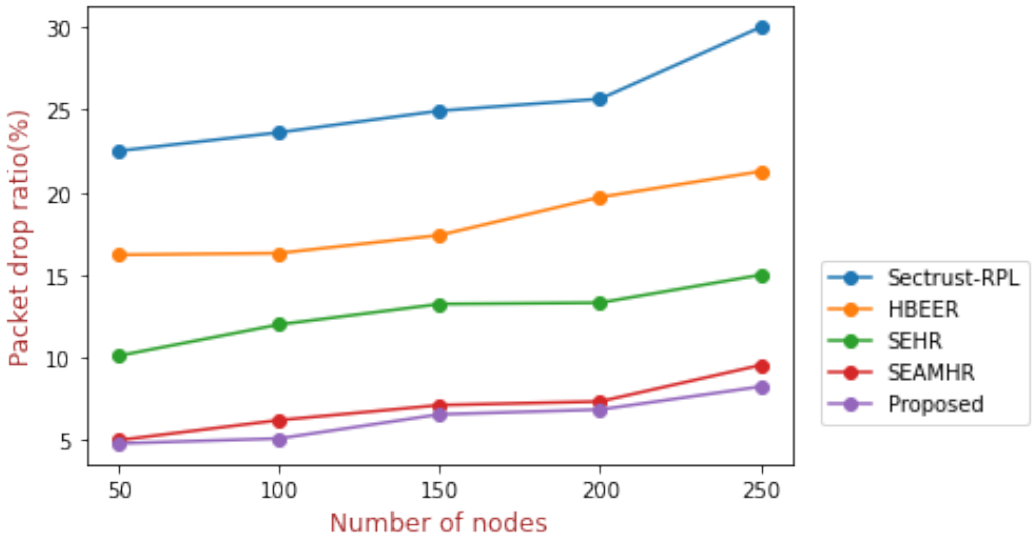


**Figure 6.** Packet drop ratio.

### *5.3. End-to-End Delay Analysis*

Table 6 depicts the comparative analysis of the packet delay of the four existing methods with the proposed approach. Figure 7 represents the end-to-end delay with respect to the different number of nodes. The proposed protocol reduces the likelihood of path re-finding with the lowest number of re-transference, in contrast to existing solutions, by selecting the security-aware and reliable path for the routing. Such a routing technique eventually reduces congestion issues and effectively utilizes the bandwidth of wireless channels to send data packets with the least amount of network delay.

**Table 6.** Comparative analysis of proposed end-to-end delay (ms) with state-of-art approaches.

| No. of Nodes | Sectrust-RPL | HBEER | SEHR | SEAMHR | Proposed |
|---|---|---|---|---|---|
| 50 | 0.152 | 0.141 | 0.120 | 0.0912 | 0.015 |
| 100 | 0.163 | 0.149 | 0.122 | 0.101 | 0.018 |
| 150 | 0.171 | 0.154 | 0.132 | 0.110 | 0.100 |
| 200 | 0.178 | 0.162 | 0.136 | 0.114 | 0.100 |
| 250 | 0.192 | 0.173 | 0.141 | 0.121 | 0.104 |

Figure 7 depicts the minimum end-to-end delay in the proposed approach. In case there are 100 nodes, the proposed approach acquires 0.015 ms, i.e., minimum delay, as compared to the existing approaches. In the case of 250 nodes, it acquires 0.192 ms for Sectrust-RPL, 0.173 ms for HBEER, 0.141 ms for SEHR, and 0.121 ms for SEAMHR; 0.104 ms has been acquired for the proposed approach.

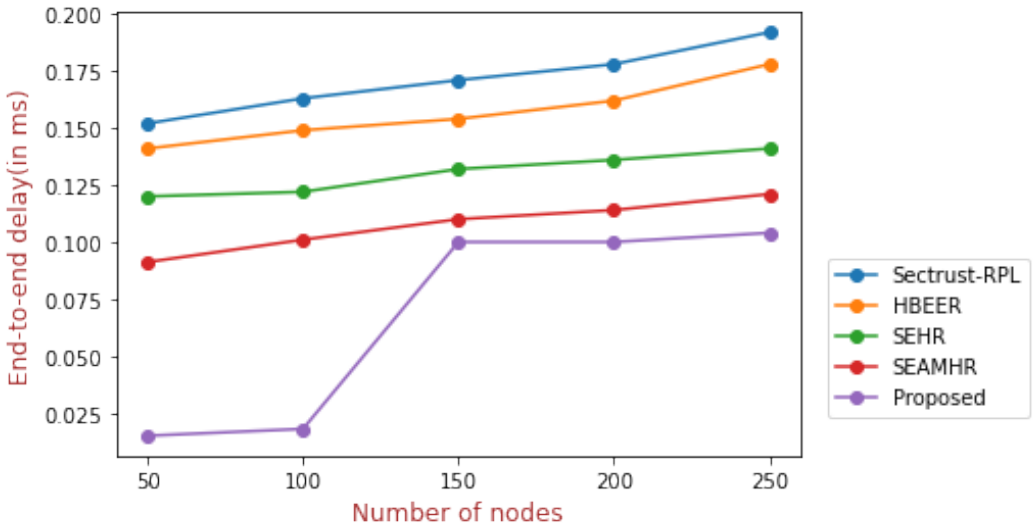


**Figure 7.** End-to-end delay.

### *5.4. Energy Consumption Analysis*

Table 7 compares the energy usage of the four existing methods with the proposed approach.

**Table 7.** Comparative analysis of proposed energy consumption (mJ) with state-of-art approaches.

| No. of Nodes | Sectrust-RPL | HBEER | SEHR | SEAMHR | Proposed |
|---|---|---|---|---|---|
| 50 | 0.0276 | 0.0211 | 0.013 | 0.0131 | 0.0122 |
| 100 | 0.0301 | 0.0212 | 0.0156 | 0.0143 | 0.0130 |
| 150 | 0.0313 | 0.0223 | 0.0179 | 0.0150 | 0.0141 |
| 200 | 0.0326 | 0.0252 | 0.0190 | 0.0154 | 0.0142 |
| 250 | 0.0355 | 0.0271 | 0.0223 | 0.0162 | 0.0155 |

Figure 8 represents the energy consumption with respect to the different numbers of nodes. The proposed method shows a minimal consumption of energy of 0.0102 mJ, while the existing Sectrust-RPL, HBEER, SEHR, and SEAMHR approaches show a consumption of 0.0326 mJ, 0.0252 mJ, 0.0190 mJ, and 0.0154 mJ, respectively. Because of the smart and risk-tolerant routing approach used by the proposed protocol, the routing pathways were stable for a considerable amount of time.

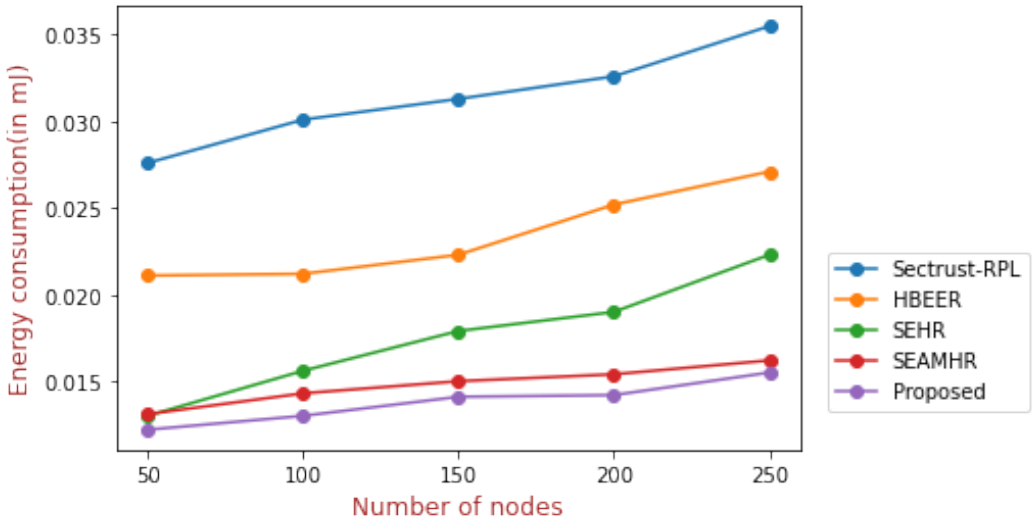


**Figure 8.** Energy consumption.

### *5.5. Faulty Routes Analysis*

Table 8 shows the comparative analysis of the faulty pathways of the four existing methods with the proposed approach.

**Table 8.** Comparative analysis of proposed faulty routes (%) with state-of-art approaches.

| No. of Nodes | Sectrust-RPL | HBEER | SEHR | SEAMHR | Proposed |
|---|---|---|---|---|---|
| 50 | 13.57 | 10.78 | 7.81 | 5.56 | 4.45 |
| 100 | 14.68 | 11.23 | 8.43 | 6.13 | 5.50 |
| 150 | 16.25 | 12.45 | 9.98 | 7.24 | 5.95 |
| 200 | 17.07 | 13.31 | 10.46 | 7.83 | 6.54 |
| 250 | 22.34 | 15.11 | 12.12 | 9.35 | 8.45 |

Figure 9 represents faulty pathways as a function of the number of nodes. The proposed approach shows a minimal faulty pathway of 6.51%, while the existing approaches Sectrust-RPL, HBEER, SEHR, and SEAMHR show 17.07%, 13.31%, 10.46%, and 7.83%, respectively. This is a result of the improvement of the decision to route the heuristic function pathway in the proposed protocol. Furthermore, the heuristic function generates smart conclusions that take into account a variety of factors, such as connection integrity, that promote the consistency of the data.

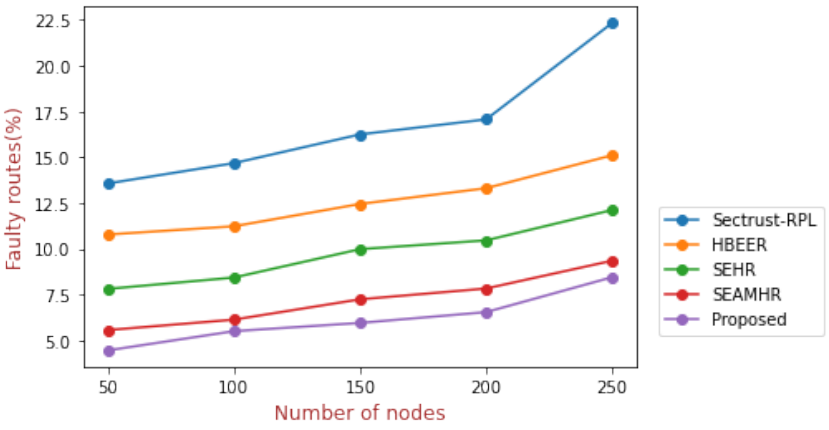


**Figure 9.** Faulty routes.

### *5.6. Findings and Implications for the Research*

The major objective of this study is to suggest a WSN routing technique that is secure and energy-efficient. The proposed MHSEER protocol's primary goals are energy efficiency, stability, and reliable data transfer capability because of its scarce resources. The finding of the paper demonstrates that the throughput rate of the protocol is 95.81%, and the packet drop ratio, packet delay, energy consumption, and faulty pathways are 5.12%, 0.10 ms, 0.0102 mJ, and 6.51%, respectively. As a result, the suggested method reduces energy consumption, erroneous routes, and latency while also greatly extending the network lifetime.

## 6. Conclusions

To optimize the routing strategy with wise judgments against malicious nodes, this paper provides a safe EER protocol for WSNs. To achieve dependable communication for WSN, the proposed protocol focuses on important elements, including energy usage, secure data transfer, packet delay, and route maintenance. Using all parameters that have an impact on the energy effectiveness of the WSN protocol is recommended to obtain the highest results from energy-efficient routing protocols. To achieve efficient next-hop decisions and decrease the use of node memory, the heuristic function uses a variety of factors and network integrities. Using different parameters, performance evaluations with existing approaches are shown. The approach offers improved network performance metrics such as throughput and reduced packet drop ratios, energy consumption, end-to-end delays, and defective routes. The proposed protocol increases throughput to 95.81% and decreases the packet drop ratio, packet delay, energy consumption, and faulty pathways to 5.12%, 0.10 ms, 0.0102 mJ, and 6.51%, respectively, in comparison to the existing energy-efficient routing protocol. However, if the proposed approach can be implemented using realistic datasets, it can produce far better outcomes. In future work, the proposed energy-efficient protocol will be implemented using real-world datasets for better results.

**Author Contributions:** Conceptualization, H.B. and A.S.; methodology, S.R. and A.S.; validation, A.S., D.K.S. and H.B.; formal analysis, S.S., S.R., and H.B.; investigation, S.R. and G.G.; resources, S.R.; data curation, G.G., and A.S.; and writing—original draft preparation, A.S. and H.B. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received external funding.

**Data Availability Statement:** Not applicable.

**Acknowledgments:** The work was partially supported by the MUSA (Multilayered Urban Sustainability Action) project, funded by the European Union—NextGenerationEU, under the National Recovery and Resilience Plan (NRRP) Mission 4 Component 2 Investment Line 1.5: strengthening of research structures and creation of R&D "innovation ecosystems", set up of "territorial leaders in R&D" (CUP G43C22001370007, Code ECS00000037). The work was also partially supported by the SERICS project (PE00000014) under the NRRP MUR program funded by the EU—NextGenerationEU.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Airehrour, D.; Gutierrez, J.A.; Ray, S.K. SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. *Future Gener. Comput. Syst.* **2019**, *93*, 860–876. [CrossRef]
2. Hamzah, A.; Shurman, M.; Al-Jarrah, O.; Taqieddin, E. Energy-efficient fuzzy-logic-based clustering technique for hierarchical routing protocols in wireless sensor networks. *Sensors* **2019**, *19*, 561. [CrossRef]
3. Sharma, S.; Kaur, A. Survey on wireless sensor network, Its Applications and Issues. In *Journal of Physics: Conference Series*; IOP Publishing: Bristol, UK, 2021; Volume 1969, p. 012042.
4. Behera, T.M.; Samal, U.C.; Mohapatra, S.K.; Khan, M.S.; Appasani, B.; Bizon, N.; Thounthong, P. Energy-Efficient Routing Protocols for Wireless Sensor Networks: Architectures, Strategies, and Performance. *Electronics* **2022**, *11*, 2282. [CrossRef]
5. Hayajneh, A.A.; Bhuiyan, M.Z.A.; McAndrew, I. A novel security protocol for wireless sensor networks with cooperative communication. *Computers* **2020**, *9*, 4. [CrossRef]

6. Haseeb, K.; Almustafa, K.M.; Jan, Z.; Saba, T.; Tariq, U. Secure and energy-aware heuristic routing protocol for wireless sensor network. *IEEE Access* **2020**, *8*, 163962–163974. [CrossRef]
7. Kumar, A.; Sharma, I. Enhancing Cybersecurity Policies with Blockchain Technology: A Survey. In Proceedings of the 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Greater Noida, India, 14–16 December 2022; pp. 1050–1054. [CrossRef]
8. Kuhlani, H.; Wang, X.; Hawbani, A.; Busaileh, O. Heuristic data dissemination for mobile sink networks. *Wirel. Netw.* **2020**, *26*, 479–493. [CrossRef]
9. Gurram, G.V.; Shariff, N.C.; Biradar, R.L. A Secure Energy Aware Meta-Heuristic Routing Protocol (SEAMHR) for sustainable IoT-Wireless Sensor Network (WSN). *Theor. Comput. Sci.* **2022**, *930*, 63–76. [CrossRef]
10. Liu, Y.; Wu, Q.; Zhao, T.; Tie, Y.; Bai, F.; Jin, M. An improved energy-efficient routing protocol for wireless sensor networks. *Sensors* **2019**, *19*, 4579. [CrossRef]
11. Qureshi, K.N.; Bashir, M.U.; Lloret, J.; Leon, A. Optimized cluster-based dynamic energy-aware routing protocol for wireless sensor networks in agriculture precision. *J. Sens.* **2020**, *2020*, 9040395. [CrossRef]
12. Sharma, S.; Guleria, K. Pneumonia Detection from Chest X-ray Images using Transfer Learning. In Proceedings of the 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 13–14 October 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–6.
13. Akin, E.; Korkmaz, T. Comparison of routing algorithms with static and dynamic link cost in software defined networking (SDN). *IEEE Access* **2019**, *7*, 148629–148644. [CrossRef]
14. Binu, G.; Shajimohan, B. A novel heuristic based energy efficient routing strategy in wireless sensor network. *Peer- Netw. Appl.* **2020**, *13*, 1853–1871. [CrossRef]
15. Gowri, S.; Pappa, C.K.; Tamilvizhi, T.; Nelson, L.; Surendran, R. Intelligent Analysis on Frameworks for Mobile App Development. In Proceedings of the 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 23–25 January 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1506–1512.
16. Seyfollahi, A.; Taami, T.; Ghaffari, A. Towards developing a machine learning-metaheuristic-enhanced energy-sensitive routing framework for the internet of things. *Microprocess. Microsyst.* **2023**, *96*, 104747. [CrossRef]
17. Yun, W.K.; Yoo, S.J. Q-learning-based data-aggregation-aware energy-efficient routing protocol for wireless sensor networks. *IEEE Access* **2021**, *9*, 10737–10750. [CrossRef]
18. Daanoune, I.; Baghdad, A.; Ballouk, A. An enhanced energy-efficient routing protocol for wireless sensor network. *Int. J. Electr. Comput. Eng. (2088–8708)* **2020**, *10*, 5462–5469. [CrossRef]
19. Liao, R.F.; Wen, H.; Wu, J.; Pan, F.; Xu, A.; Jiang, Y.; Xie, F.; Cao, M. Deep-learning-based physical layer authentication for industrial wireless sensor networks. *Sensors* **2019**, *19*, 2440. [CrossRef]
20. Narayan, V.; Daniel, A.; Chaturvedi, P. E-FEERP: Enhanced Fuzzy-based Energy Efficient Routing Protocol for Wireless Sensor Network. *Wirel. Pers. Commun.* **2023**, 1–28. [CrossRef]
21. Gemeda, K.A.; Gianini, G.; Libsie, M. The effect of node selfishness on the performance of WSN cluster-based routing algorithms. In Proceedings of the AFRICON 2015, Addis Ababa, Ethiopia, 14–17 September 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 1–5.
22. Gemeda, K.A.; Gianini, G.; Libsie, M. Collaborative packets forwarding to extend lifetime of multi-authority wireless sensor networks. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), Palladam, India, 10–11 February 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 513–519.
23. Manshaei, M.H.; Zhu, Q.; Alpcan, T.; Bacşar, T.; Hubaux, J.P. Game theory meets network security and privacy. *ACM Comput. Surv. (CSUR)* **2013**, *45*, 25. [CrossRef]
24. Gianini, G.; Damiani, E.; Mayer, T.R.; Coquil, D.; Kosch, H.; Brunie, L. Many-player inspection games in networked environments. In Proceedings of the 2013 7th IEEE International Conference on Digital Ecosystems and Technologies (DEST), Menlo Park, CA, USA, 24–26 July 2013; IEEE: Piscataway, NJ, USA, 2013; pp. 1–6.
25. Lena Cota, G.; Mokhtar, S.B.; Lawall, J.; Muller, G.; Gianini, G.; Damiani, E.; Brunie, L. A framework for the design configuration of accountable selfish-resilient Peer-to-Peer systems. In Proceedings of the 2015 IEEE 34th Symposium on Reliable Distributed Systems (SRDS), Montreal, QC, Canada, 28 September–1 October 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 276–285.
26. Lena Cota, G.; Mokhtar, S.B.; Gianini, G.; Damiani, E.; Lawall, J.; Muller, G.; Brunie, L. Analysing Selfishness Flooding with SEINE. In Proceedings of the 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Denver, CO, USA, 26–29 June 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 603–614.
27. Lena Cota, G.; Mokhtar, S.B.; Gianini, G.; Damiani, E.; Lawall, J.; Muller, G.; Brunie, L. RACOON++: A semi-automatic framework for the selfishness-aware design of cooperative systems. *IEEE Trans. Dependable Secur. Comput.* **2017**, *16*, 635–650. [CrossRef]
28. Gianini, G.; Mio, C.; Fossi, L.G.; Egyed-Zsigmon, E. A Watermark Inspection Game for IoT Settings. In Proceedings of the 2019 IEEE World Congress on Services (SERVICES), Milan, Italy, 8–13 July 2019; IEEE: Piscataway, NJ, USA, 2019; Volume 2642, pp. 29–34.
29. Gianini, G.; Viola, F.; Lena-Cota, G.; Lin, J. Hybrid Inspector-Inspectee-Agent Games in Mobile Cloud Computing. In Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks, Alicante, Spain, 16–20 November 2020; pp. 95–100.
30. Gemeda, K.A.; Gianini, G.; Libsie, M. An evolutionary cluster-game approach for Wireless Sensor Networks in non-collaborative settings. *Pervasive Mob. Comput.* **2017**, *42*, 209–225. [CrossRef]

31. El Alami, H.; Najid, A. ECH: An enhanced clustering hierarchy approach to maximize lifetime of wireless sensor networks. *IEEE Access* **2019**, *7*, 107142–107153. [CrossRef]
32. Yin, Y.; Li, Y.; Gao, H.; Liang, T.; Pan, Q. FGC: GCN based federated learning approach for trust industrial service recommendation. *IEEE Trans. Ind. Inform.* **2022**, *19*, 3240–3250. [CrossRef]
33. Gao, H.; Huang, W.; Liu, T.; Yin, Y.; Li, Y. Ppo2: Location privacy-oriented task offloading to edge computing using reinforcement learning for intelligent autonomous transport systems. *IEEE Trans. Intell. Transp. Syst.* **2022**. [CrossRef]
34. Babbar, H.; Rani, S. Software-defined networking framework securing internet of things. In *Integration of WSN and IoT for Smart Cities*; Springer: Cham, Switzerland, 2020; pp. 1–14.
35. Babbar, H.; Rani, S.; Islam, S.M.; Iyer, S. QoS based Security Architecture for Software-Defined Wireless Sensor Networking. In Proceedings of the 2021 6th International Conference on Innovative Technology in Intelligent System and Industrial Applications (CITISIA), Sydney, Australia, 24–26 November 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–5.
36. Khalaf, O.I.; Abdulsahib, G.M. Energy efficient routing and reliable data transmission protocol in WSN. *Int. J. Adv. Soft Comput. Appl.* **2020**, *12*, 45–53.
37. Lilhore, U.K.; Khalaf, O.I.; Simaiya, S.; Tavera Romero, C.A.; Abdulsahib, G.M.; Kumar, D. A depth-controlled and energy-efficient routing protocol for underwater wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **2022**, *18*, 15501329221117118. [CrossRef]
38. Elsmany, E.F.A.; Omar, M.A.; Wan, T.C.; Altahir, A.A. EESRA: Energy efficient scalable routing algorithm for wireless sensor networks. *IEEE Access* **2019**, *7*, 96974–96983. [CrossRef]
39. Maheshwari, P.; Sharma, A.K.; Verma, K. Energy efficient cluster based routing protocol for WSN using butterfly optimization algorithm and ant colony optimization. *Ad. Hoc. Netw.* **2021**, *110*, 102317. [CrossRef]
40. Xu, C.; Xiong, Z.; Zhao, G.; Yu, S. An energy-efficient region source routing protocol for lifetime maximization in WSN. *IEEE Access* **2019**, *7*, 135277–135289. [CrossRef]