RESEARCH ARTICLE

An Interoperability Framework for Enhanced Security of Handheld Devices Using IoT-Based Secure Energy Efficient Firefly Optimization Algorithm

G.S. Sapna
Department of Information Science and Engineering, Cambridge Institute of Technology, Bengaluru, India.
sap.katapady@outlook.com

Shashikumar Dandinashivara Revanna
Department of Computer Science and Engineering, Cambridge Institute of Technology, Bengaluru, India.
shashikumardr@gmail.com

Received: 18 July 2023 / Revised: 03 October 2023 / Accepted: 08 October 2023 / Published: 30 October 2023

Abstract – Security is a major challenge in the Internet of Things (IoT) domain as it plays a crucial role in a safe and uninterrupted data transmission, across various hand-held devices connected to the network. Establishing a secure Routing Protocol for Low power and lossy networks (RPL) is necessary and crucial, as it is the standard RPL network in IoT that helps to remove malicious nodes from the network. The existing researches focused on developing energy-saving techniques, malicious node detection techniques, as well as security-enhancing techniques, but neglected energy efficiency, and other trust-related considerations. This resulted in reduced confidentiality and unauthorized access to user data. To overcome these limitations, a Secure Energy Efficient Firefly Optimization Algorithm in RPL (SEEFOA-RPL) is proposed in this research for establishing a reliable and energy-efficient routing path by using Destination-Oriented Directed Acyclic Graph (DODAG) architecture. The proposed algorithm improves security measures in handheld devices such as smartphones, wearable watches, digital cameras, portable media players, and tablets. Initially, a trust model for the RPL network is established to calculate the trust parameters that help in building a secure routing in the network. The SEEFOA is capable of solving complex optimization problems, and finds the best optimum solution for a secure-energy efficient routing path. The proposed SEEFOA-RPL delivers a high-level performance in terms of Detection Rate (DR), False Negative Rate (FNR), and False Positive Rate (FPR), respectively measured at 99%, 12%, and 17% in an attack interval 4, and Packet Drop Ratio (PDR) measured at 82% in an attack interval of 1.5.

Index Terms – Destination-Oriented Directed Acyclic Graph, Energy Efficiency, Internet of Things, Malicious Nodes Detection, Routing Protocol for Low Power and Lossy Networks, Secure Energy Efficient Firefly Optimization Algorithm.

1. INTRODUCTION

IoT refers to a topology of interconnected smart devices that communicate over a wireless internet medium. These devices exchange information and process data, allowing them to function in the global environment. [1]. A trust mechanism should be added to improve routing security in protocols, particularly in Low Power and Lossy Networks (LLNs) which are often used by IoT devices. The trust mechanism usually operates at the energy and control layer and effectively detects and isolates blackhole attacks. These trust values are calculated based on packet exchange observations among nodes, aiming at conservation of energy in IoT devices [2, 3]. For secure routing in Mobile Ad hoc Networks (MANETs) with IoT devices, introducing a real-time secure routing method is the need of the hour. This method not only focuses on discovering intermediate route nodes, but also takes into account the presence and trustworthiness of IoT devices by improving Quality of Service (QoS) parameters [4, 5]. A blockchain-based system is advantageous for easily identifying damaged sensor nodes, engaged in LLN configuration. This type of framework establishes a secure data link in IoT-LLN with an attack detection mechanism, by enhancing the performance of the routing attack detection algorithms [6, 7].

Ensuring security in RPL for end-to-end communication is a primary design challenge. To solve the lack of robust security mechanisms in RPL, a trustworthy scheme must be developed. The RPL establishes one or more routes to send a message to sink by creating DODAG. A metric-based trust scheme achieves low energy consumption and a high packet delivery ratio by detecting and isolating attacks, and employing an energy-balanced topology mechanism [8, 9]. Furthermore, IoT-connected devices must be secure with authentications like end-to-end (E2E) connections. Like other networks, IoT security is dependent on confidentiality and trust. As a result, attack detection systems are one of the primary defense methods against IoT attacks [10]. Attestation is a low-cost method of identifying malicious devices. However, remote authentication in device-to-device has a high cost in terms of authentication, scalability, and communication overhead [11].

Therefore, new attestation technologies that are dependable and scalable, are needed to protect network operations involving IoT devices. The energy consumption is lowered during normalization and stabilization of the physical layer, network layer, and application layer of IoT [12, 13]. Cloud computing technology provides the base foundation and storage for data processes in IoT, and methodologies based on cloud cryptography are presented as a standout compared to other approaches to ensure data security in many IoT applications [14]. Most conventional security methods are not robust enough to protect the industrial strategic data of most firms and business sectors. Root exploits, botnets, spyware, worm, and trojans are some of the critical IoT security issues to be dealt with [15]. Though the existing researches concentrated on creating methods for detecting malicious nodes, boosting security without sacrificing energy efficiency, and other trust-related factors, user data was still subject to unauthorised access leading to reduced confidentiality.

The main objective of this research focuses on developing a Secure Energy Efficient Firefly Optimisation Algorithm in RPL (SEEFOA-RPL) for creating dependable and energy-efficient routing pathways using the Destination-Oriented Directed Acyclic Graph (DODAG) architecture. The objectives/contributions of this work are:

- To propose the SEEFOA-RPL approach for establishing optimum routing in RPL networks of IoT-based handheld devices with security and energy efficiency.
- To introduce trust parameters in the proposed routing algorithm for scaling up its security and also to increase packet throughput and decrease the delay.
- To find the best optimal solution through the SEEFOA algorithm by avoiding networks' malicious nodes using secure and trust-based RPL networks and the trust parameters of the network.

The organization of the manuscript is arranged as follows: Section 2 is the overview of existing methods and section 3 briefs the proposed methodology. Section 4 gives the simulations of the proposed method, and section 5 provides the conclusion for the proposed research.

2. RELATED WORK

Hosseinzadeh et al. [16] implemented a secure routing based on a cluster tree with a dragonfly algorithm for IoT to ensure communication security. Trust-based clustering was introduced to select cluster head nodes and the proposed framework established a routing tree based on the Dragonfly Algorithm (DA-Tree). The DA-Tree evaluated the routing tree quality and also balanced the energy consumption along with the boosting of network lifetime. However, this implemented approach had less PDR.

Muzammal et al. [17] presented a Security, Mobility, and Trust based model (SMTrust) to address the blackhole attacks in RPL from static and mobile nodes. The presented approach outperformed existing methods due to the advantage of lightweight structure, easy implementation and integration, as well as enhanced network performance. The performance was evaluated using the cooja simulator, in which the results depicted the developed secure routing. However, the E2E delay and power consumption had be improved since it contributes in developing a secure routing path.

Agiollo et al. [18] developed an approach to detect 14 routing attacks in RPL-Based IoT. Based on the simulations of various attacks, the network logs were collected and a new dataset was built using NetSim software. The proposed approach was implemented based on this dataset and achieved better results in identifying the attacks. The proposed method did not require heavy computation, which was an advantage of this work. However, NetSim failed to implement certain RPL flags to simulate DODAG inconsistency and strong mode attacks.

Khadidos et al. [19] presented data security with IoT sensors based on the mechanism of Random Hashing for medical applications of IoT cloud environment. For enhanced security of healthcare data, Probabilistic Super Learning and Random Hashing were implemented in AI-based intelligent feature learning mechanism. The developed security mechanism had low computational complexity, optimal performance outcome, high processing speed, and accurate attack detection. However, this approach was not suitable for real time applications, which resulted in increased frequency of various security attacks.

Abbasi et al. [20] developed a trust-based middleware framework with multi-layers to focus on interoperability-related issues. The trust parameters were selected based on their weight ranges, for various service interactions, by using a trust base algorithm. The system performance was measured in terms of decay factor and decay time interval. It achieved better results with the use of trust algorithm. However, the ability to decide which factors to be considered in trust calculation, was not provided by the algorithm.

Gupta et al. [21] suggested a healthcare cyber-physical framework for the diagnosis of encephalitis. This method was based on software techniques and information fusion. For the in-depth analysis of the data in electronic medical records, IoT-based sensors and user devices were utilized. The performance of this method was evaluated based on the assessment results of fog and cloud layers. However, there were not enough security aspects considered in this approach which might result in the insider attacks due to malicious nodes.

Muzammal et al. [22] developed a trust and mobility based framework with a secure routing protocol. This method analysed the trust parameters which included mobile-based metrics, to provide security against normal and black hole attacks in IoT. The output results demonstrated that, the method achieved better performance with the enhanced network capacity of stabilizing the topology. However, the enhancement of power consumption was poor and the results must be evaluated with the more number of network nodes with the test bed experiments.

Medjek et al. [23] implemented a method to mitigate the DODAG Information Solicitation attack in RPL networks. The suggested mechanism was designed to improve the efficiency of the RPL-Maximum Response Code framework, power consumption, and also to control the data packet overhead. However, validation of the developed solution's efficiency was required in real testbeds, under the dynamic nature of the network.

Zaminkar et al. [24] presented a SoS RPL known as Securing IoT against Sinkhole Attack to address the issue of sinkhole detection method in IoT. A sinkhole detection mechanism was also suggested in this approach to overcome the networks' routing attacks. The fake DIO (DODAG Information Object) messages, generated by the malicious nodes, were also detected and added to the blacklist, with this presented approach. SoS RPL achieved high-level performance, however, a slight degradation was observed in the PDR of SoS-RPL due to random factors in the simulation.

Nandhini et al. [25] developed Enhanced Rank Attack Detection Algorithm (E-RAD) to detect the rank attackers and establish secure routing in IoT networks. The goal of E-RAD was to control DIO packet creation and use DIS (DODAG Information Solicitation) message solicitation, to eliminate rank attackers. If an attacker went unnoticed, they were located using the consistency check of the hash value in the DAO (Destination Advertisement Object) message. However, the occurrence of malicious nodes were not prevented in the early stages, due to the failed recognition of nodes mobility.

The common limitations found from the existing methods of IoT-based RPL are low-security routing path, less energy efficiency, high network complexity, high power consumption, and less consideration of trust parameters. These limitations are overcome with the proposed SEEFOA-RPL method by considering trust parameters, energy efficiency, and security measures as the primary concerns.

2.1. Problem Statement

There are significant flaws in the current researches of IoT-based RPL, which are of serious concern.

- IoT networks are exposed to a variety of malicious attacks and data breaches due to the relevant issue of low security inside the specified routing paths.
- Second, these systems' energy efficiency is far from ideal, resulting in inefficient resource use and perhaps shorter device lifespans.
- Additionally, the increased network complexity linked to existing approaches, makes deployment and maintenance more difficult, necessitating the use of simpler and more efficient alternatives.
- In addition to operating expenses, the significant power consumption seen in these configurations, raises environmental concerns about the network's sustainability.
- The routing algorithms' inadequate inclusion of trust parameters, prevents further resolving of security and reliability difficulties.

Due to the growing concerns of these limitations, there is an immediate need for the creation and application of improved solutions, to guarantee an effective and secure routing for portable device networks based on the IoT, thereby supporting the streamlined and reliable functioning of these systems.

3. METHODOLOGY

The objective of the proposed method is to discover a secure routing with a firefly optimization algorithm, by using a trust mechanism in the RPL network of IoT-based handheld devices. Initially, the topology is discovered in the device layer and then the trust parameters are calculated in the control layer. A secure routing is established with the calculated trust parameters, using the FOA algorithm. The proposed work flow is depicted by Figure 1.

3.1. Device Layer

The responsibilities of actuators and sensor nodes are: sensing, gathering information, processing data that is collected from surroundings, and transferring this data to the root nodes which are deployed in the LLNs. These devices depend on RPL routing protocol to connect to the border router. To perform routing and communication of the gathered data, each node is connected to its neighboring node by systematic links. This layer is primarily concerned with network discovery and establishment, since it senses data from its surroundings, as well as from neighboring nodes, by observing their activity and behaviour. Hence, according to their forwarding behavior, the nodes mark the neighboring nodes as positive or negative.

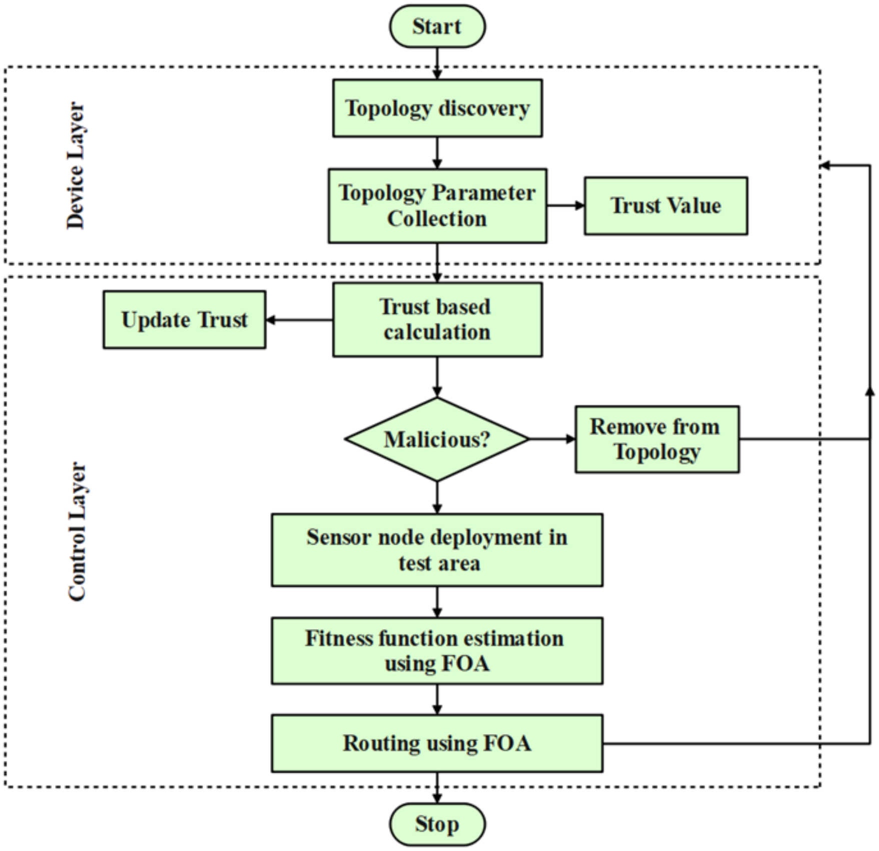

Figure 1 Flowchart of the Proposed SEEFOA Model

3.2. Control Layer

The control layer supports the device layer to perform its corresponding operations safely, and also to enhance its communication ability. In the control layer, the complete trust model is implemented, which includes trust calculation, trust updating, detecting malicious nodes, removing them from topology, node deployment, and estimation of fitness function as well as routing using FFA. The primary purpose of this layer is to calculate trust values and to handle complex computations that are related to the trust values. This implemented trust model in this layer results in low energy consumption and less memory overhead.

3.2.1. Trust Model Development

The developed trust model builds the trust level among the entities while assuring the uncertainty level. An energy-efficient trust model, which does not strain IoT devices, is established in the control layer by shipping all complex calculations. The adaptive trust parameters like Packet Loss Rate (P_{LR}) and Forwarding Delay (F_D) are input parameters. Detection and removal of malicious nodes from the topology are the output parameters to calculate the trustworthiness of nodes. These trust parameters are calculated for each network node after initializing certain thresholds. However, the trust level calculation depends on the chosen trust parameters as some parameters make the initiated mechanism more complex. Therefore to avoid this, only QoS parameters like P_{LR} and F_D are used for trust calculation.

- Packet Loss Rate (P_{LR}): The P_{LR} is measured as shown in Eq. (1) which is a ratio of packets dropped (P_d) by the receiver nodes to the total packets (P_t) from the sender node.

$$P_{LR} = \frac{P_d}{P_t} \qquad (1)$$

- Forwarding Delay (F_D): The time involved in obtaining a packet from the sender and delivering it to the following node is known as F_D which is measured as shown in Eq. (2)

$$F_D = PR_t - PF_t \qquad (2)$$

Where, PR_t is the packet received time, and PF_t is packet forwarding time.

The trust values of nodes are measured and rated based on the belief, disbelief, and uncertainty parameters with a threshold value of 0.5. The nodes are rated as trusted and non-trusted nodes, in which the trusted nodes are employed for secure routing and communication. The trust parameter values are measured in the control layer and transferred to all the sensor nodes through a central node. Due to the presence of trust values in the control layer, the framework depends on centralized trust propagation. The node trust is updated using a time-based update method which can detect malicious nodes on time, and also solve high computational issues with limited memory resources. The detected malicious nodes are eliminated and the sensor nodes are deployed in the test area of network. The node trust is measured in terms of nodes' success rate as represented by Eq. (3) and Eq. (4)

$$T_{SR} = {}^{P_F}/_{P_R} \qquad (3)$$

$$P_F = P_R - P_D \qquad (4)$$

Where, T_{SR} is the total nodes' success rate, SR is the ratio of the number of packets forwarded (P_F), P_R is received number of packets, and P_D is dropped number of packets. The computed values of P_F, P_R, T_{SR} are given as input to the FOA to calculate the fitness of each network node. Based on the evaluation, a secure routing path is devised as discussed in the consecutive section.

3.3. Secure Energy Efficient Firefly Optimization Algorithm (SEEFOA)-RPL

The algorithm of firefly optimization is a more generalized form of Particle Swarm Optimization (PSO). When compared to Ant Colony Optimization and PSO, the Firefly algorithm generates more effective and consistent results. This paper identifies a simple implementation of the Firefly algorithm for the best interoperability in the IoT environment. The mobile uses the FOA to choose the lowest ranked access point when it comes to data transfer in the form of packets. The data packets aim for the root through this node and move through fewer hops. The mobile node should have data regarding the destination path and the nearby related access points, in case the information is shared between the router and leaf nodes. In RPL routing, the packet is typically routed towards a single router (root). But when these nodes are non-root nodes, it is easy for two random routers to communicate. This technique is commonly known as peer-to-peer communication, and it facilitates routers to recognize and create paths to other routers based on a reactive mechanism for successful interoperability among IoT devices such as smartphones, digital watches, and other such handheld devices. The SEEFOA-RPL can be implemented for real time applications of IoT-based hand-held devices such as smartphones, wearable watches, digital cameras, portable media players, and tablet computers to enhance security in RPL networks, and to send data packets from sender to receiver through an optimal routing.

In this algorithm, the fireflies are artificially created in the problem space and deployed randomly. The FFA has the ability to solve complex optimization problems. The randomly deployed fireflies emit their light intensity as a signal to other fireflies and move towards flies with high intensity light. The information exchange will take place in the form of light between the fireflies and the brightest firefly moves around the problem space for an optimal solution. Following the brightest firefly, all fireflies try to move in its direction. The light absorption of the fireflies and the distance between each firefly is calculated using Eq. (5) and (6)

$$\beta(dis) = \beta_0 \times e^{-\gamma dis^2} \qquad (5)$$

Where, the light absorption is denoted by β, the distance between the fireflies is given by dis, and light absorption coefficient is given by γ.

$$dis = \sqrt{\sum_{k=1}^{d}\left(y_{ik} - y_{jk}\right)} \qquad (6)$$

Where, dis gives the distance between fireflies y_i and y_j. The movement of i^{th} firefly depends on the attraction of j^{th} firefly which is calculated using Eq. (7).

$$y_i = y_i + \beta_0 \times e^{-\gamma dis^2}\left(y_{ik} - y_{jk}\right) + \alpha\left(rand - \frac{1}{2}\right) \qquad (7)$$

Where, y_i denotes the current position of firefly, $\beta_0 \times e^{-\gamma dis^2}\left(y_{ik} - y_{jk}\right)$ denotes the attraction of firefly, and $\left(rand - \frac{1}{2}\right)$ denotes the random function within the range of 0,1.

Although FOA algorithm was used for routing in RPL networks of existing methods, only the residual energy (RE) was considered as a fitness function, due to which the expected security level could not be achieved. To overcome this, an energy efficient secure routing is proposed in this research, where, security, energy, link cost, path cost, and delay are calculated. The RE present in "x" node of RPL is calculated as shown in Eq. (8)

$$RE(x) = \frac{E_{current}}{E_{total}} \qquad (8)$$

Where the current energy in the network is given by the $E_{current}$ and total energy in the network node is given by the E_{total}. The link between each node is measured based on the data delay between each node from node x to y as given in Eq. (9)

$$delay(x, y) = \frac{1}{FDD \times RDD} \qquad (9)$$

Where the forward data delivery is given by FDD and reverse data delivery is given by the RDD. The quality of nodes is measured based on the rank parameter as shown in Eq. (10).

$$Rank(x) = Rank\ (parent\ node(x)) + R_i \qquad (10)$$

Where, rank of node x is measured using R_i which is the increased rank value, and $parent\ node(x)$ is the parent rank of node x. The rank shows the distance from the participant's node to the DODAG root as shown in Figure 2.

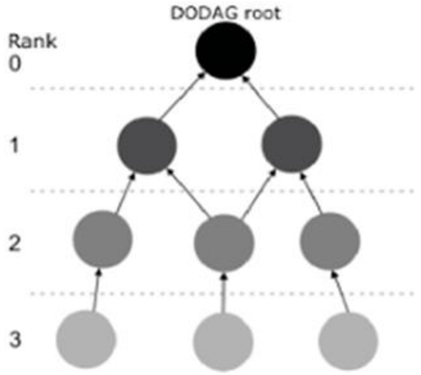

Figure 2 Illustration of Nodes in DODAG Root

3.3.1. Pseudocode

```
Begin
While Launch Cooja
    Initialize Motes
    Generate Mote Compilation for RPL Router
    Initialize DODAG network
    $I \leftarrow I_{min}$
    $counter \leftarrow I$
    $state \leftarrow I$
    Define Path directories
    Initialize the firefly agents for all paths $X_i$ where $i = 1,2,3, \dots n$
    Define best path $T$
    While ($k < maximum\ iterations$):
        Normalize the distance between Firefly
        Compute fitness of all paths by search agent
        Update position of search agent
        Bring search agent return if it goes beyond boundary
    end while
    Update $T$ if better value found
    At beginning of each interval
        $c \leftarrow 0$
        $b \leftarrow random(l/2, l)$
    Received Consistent Transmission
        $c \leftarrow c + I$
    Random timer expires
        if ($c < k$) then
            Transmit Scheduled DIO
        else
            Suppress Scheduled DIO
        End if
    Whenever the interval $I$ expires
        if ($counter < state$) then
            $I \leftarrow I_{min}$
            $counter + +$
        else
            $I \leftarrow I \times 2$ and $resp \leftarrow I$
        End if
        If ($I > I_{max}$) then
            $I \leftarrow I_{max}$
        End if
    Repeat the process for each packet
end while
End
```

Pseudocode 1 Secure Energy Efficient Firefly Optimization Algorithm (SEEFOA)-RPL

The provided pseudocode 1 outlines a theoretical framework for managing a network of IoT devices, specifically focusing on aspects like simulation, routing protocol, and optimization. The pseudocode 1 begins by launching a Cooja simulation environment, which is often used for simulating IoT networks. It initializes network nodes or "motes" and configures them to work as RPL routers. DODAG network structure is established, which is commonly used in low-power IoT networks for efficient routing. Path directories are defined, suggesting the existence of multiple communication paths within the network. Firefly agents are initialized for these paths, which play the role of intelligent agents responsible for optimizing these paths. A variable "T" is defined to represent the best path, which implies an ongoing optimization process. Within a loop with a maximum iteration count, the pseudocode 1 normalizes the distance between firefly agents, computes the fitness of paths using a search agent, and updates the position of these agents. If a search agent goes beyond boundaries, it is brought back. The pseudocode 1 updates the best path "T" if a better value is found. This is the main goal of optimization algorithm to find the most efficient communication path within the network. At the beginning of each interval, the code handles the reception of consistent transmissions, random timer expirations, and potentially, the decision to transmit or suppress DIOs based on certain conditions. The pseudocode 1 comprises handling of intervals, conditions, and packet processing, implying that these actions are performed iteratively for different network packets. This pseudocode 1 represents a network management and optimization process in an IoT environment, encompassing aspects like routing (RPL) control, path optimization using intelligent agents (firefly agents), and periodic communication management.

3.3.2. Fitness Function

The process of finding an optimal parent for secure data transfer, gives the fitness function of the proposed method. It is obtained from the RE, delay, and trust mechanism with a weighted value from 0 to 0.5. The final optimal solution is obtained at the weighted value 0.5. The fitness function is measured as shown in Eq. (11)

$$fit = w_1 \times RE(y_i) + w_2 \times delay(y_i) + w_3 \times T_{SR}(y_i) \quad (11)$$

Where, w_1, w_2, w_3 are the weighted values, y_i denotes the current position of the firefly, RE is the residual energy, and T_{SR} is the node trust determined by the trust rate.

If $(y_i) \geq fit$, then the RPL rank for the optimal parent is calculated, else the node movement will be updated to select the optimal parent in DODAG to transfer the data. The ideal path for sending packets from the source node is determined as output for the proposed FFA algorithm. The output for the FFA algorithm is decided based on the computation of fitness for all paths and its cost metric for each node with 100 iterations.

4. EXPERIMENTAL RESULTS

To evaluate the performance of the proposed SEEFOA, an open source and light weight operating system known as Contiki/cooja simulator is used. All the simulations of the proposed work are performed in this simulator. A 50-node network topology is created and nodes are distributed using a random topology. Contiki is used for high-performance and secure communication between low-powered RFID chips in wireless networks. The RPL protocol uses routing metrics such as received packets per node, average routing metric (average routing cost), network hops, instantaneous and average power consumption. Each of these metrics is calculated for 50 nodes and each node is monitored in terms of received packets or duplicates per node.

4.1. Received Packets Per Node

The amount of received packets per node is said to be the number of packets a node or a device receives in a network. Each network node receives and processes the packets according to the routing instructions of the network. The data packets are sent from source to destination node through intermediate nodes. The measure of received packets per node is graphically represented in Figure 3.

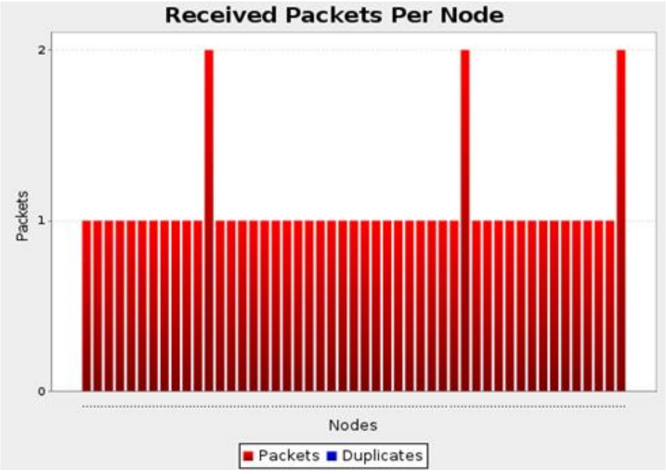

Figure 3 Illustration of Number of Packets Received Per Node

From Figure 3, the maximum of 2 received packets are analyzed for 50 nodes, in which some of the nodes have received 1 packet and some of the nodes have received 2 packets. The duplicate packets will be detected if there is any packet duplicated or received twice at the receiver host.

4.2. Average Routing Metric (ARM)

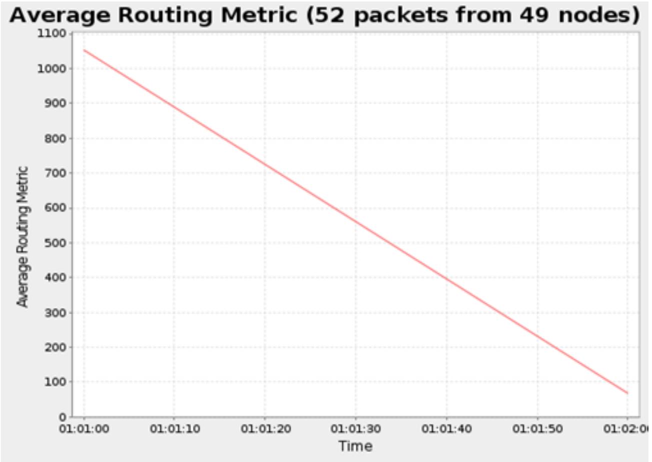

Figure 4 Illustration of Average Routing Metric

The average routing metric is a unit to calculate the optimal routing path and also to reject unsuitable paths. This can be measured based on the hop count, path reliability, bandwidth, latency, and load. The ARM for 49 nodes is calculated in this experiment and graphically represented in Figure 4.

From Figure 4, the average routing metric/average routing cost is calculated. 52 packets are received from 49 nodes in the time period of 1 minute. The suitable path to transfer the 52 packets is measured by considering network hops as well.

4.3. Network Hops

The number of network devices through which the data passes from source to destination is known as network hops. A hop occurs when a packet is passed from one device to the next. Every hop introduces latency due to the high processing time taken by the packets. The graphical representation of network hops is given in Figure 5.

From Figure 5, the maximum of 3 network hops is considered for 50 nodes. Out of which, the last hop and average hop is calculated for each node. Here, a minimum of 1 hop and a maximum of 3 hops are considered for each node.

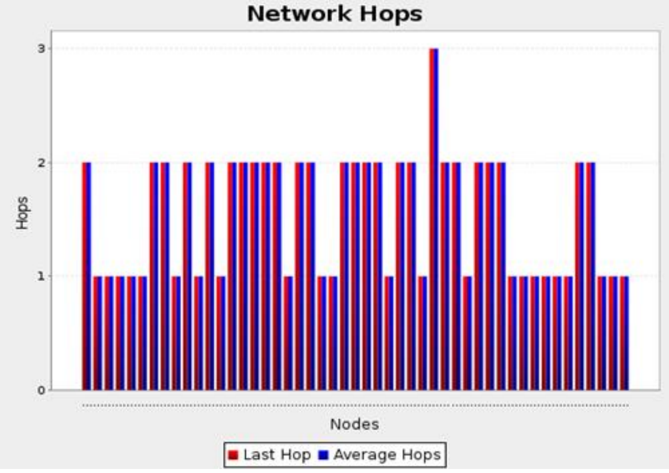

Figure 5 Illustration of Network Hops

4.4. Instantaneous and Average Power Consumption

The instantaneous and average power consumption for each node is measured in terms of Low Power Mode (LPM), CPU, Radio listening, and Radio transmission. The LPM is the power consumed by a node in sleeping mode, the CPU is the power consumed by a node in activation mode, and Radio listen and Radio transmit is the node power in its received state and transmission state.

From Figure 6 and Figure 7, it is observed that the LPM obtained for all nodes is constant. The variation in CPU power, Radio listen and Radio transmit can be observed for each node which is measured in mV.

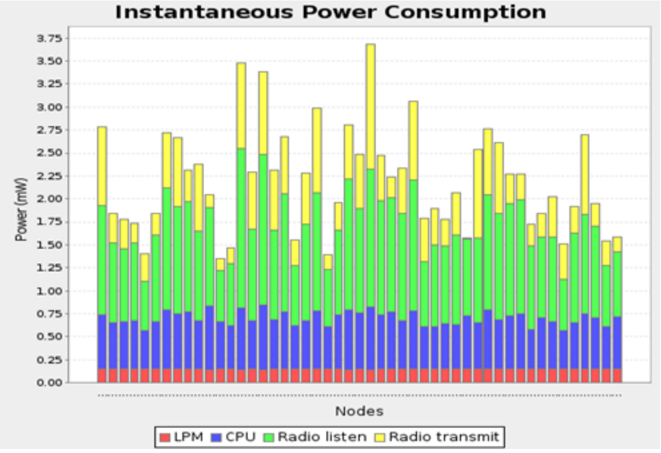

Figure 6 Illustration of Instantaneous Power Consumption

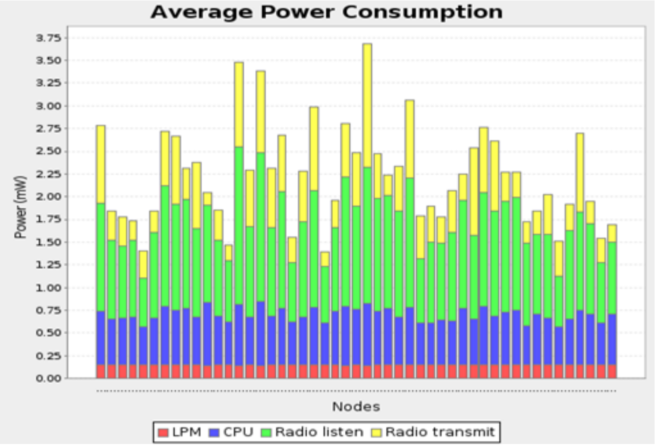

Figure 7 Illustration of Average Power Consumption

4.5. Quantitative Analysis

The proposed model is evaluated with conventional techniques such as Routing Protocol for Low power and lossy networks (RPL), Secure Trust based RPL (RPL-SecTrust), Securing the IoT Against Sinkhole Attack using RPL (RPL-SoS), Packet Loss Ratio and False Detection based RPL (PLR+FDRPL). The evaluation is performed in terms of Detection Rate (DR), False Negative Rate (FNR), False Positive Rate (FPR), and Packet Delivery Ratio (PDR) as shown in Tables (1- 3).

From Table 1, it is observed that the detection rate of attacks in different forms of RPL network nodes is analyzed in an attack interval of [0.5 – 4]. Compared to the conventional techniques the proposed method has shown exceptional results in attack detection. The attacks are detected if majority of the nodes are malicious in the network. If there is malicious behavior among nodes, the target object is recognized. If the malicious node is left undetected, it creates its replications in the network which leads to a large class of insidious attacks.

Table 1 Analysis of Detection Rate for 50 Nodes and 100 Nodes

PD	DR%									
	50 Nodes					100 Nodes				
	RPL	RPL-SecTrust	RPL-SoS	PLR+FDRPL	SEEFOA-RPL	RPL	RPL-SecTrust	RPL-SoS	PLR+FDRPL	SEEFOA-RPL
0.5	69	75	77	77	90	69	73	77	74	90
1	69	75	78	78	91	67	74	76	75	91
1.5	70	76	78	80	93	68	75	77	79	90
2	71	78	79	81	95	68	75	76	80	93
2.5	73	80	80	83	97	70	79	77	81	96
3	74	81	81	87	97	72	81	79	84	94
3.5	75	82	82	88	98	74	79	80	86	98
4	76	83	83	90	99	75	82	80	88	99

Table 2 Analysis of Packet Delivery Ratio for 50 Nodes and 100 Nodes

Attack interval	PDR%									
	50 Nodes					100 Nodes				
	RPL	RPL-SecTrust	RPL-SoS	PLR+FDRPL	SEEFOA-RPL	RPL	RPL-SecTrust	RPL-SoS	PLR+FDRPL	SEEFOA-RPL
0.5	60	75	76	77	80	58	72	75	76	80
1	63	73	73	74	81	61	72	73	71	80
1.5	66	71	70	70	82	65	71	69	69	79

Table 3 Analysis of FNR and FPR for 50 Nodes and 100 Nodes

Attack Interval	50 Nodes						100 Nodes				
	Performance metrics	RPL	RPL-SecTrust	RPL-SoS	PLR+FD RPL	SEEF OA-RPL	RPL	RPL-SecTrust	RPL-SoS	PLR+ FDRPL	SEEFOA -RPL
0.5	FNR%	19.78	16.78	16.23	16	17.99	19.78	18.78	16.23	18	18.99
1		18.56	15.28	15.02	15	16.67	18.56	15.28	16.02	15	17.67
1.5		18.55	13.67	13.34	14.01	16	21.55	16.67	13.34	15.01	17
2		17.6	13.06	13	14	15.89	18.6	14.06	14	14	16.89
2.5		16.44	14.09	14	13.45	14.73	19.44	15.09	16	15.45	17.73
3		16.77	13.43	13.06	13	14.04	16.77	16.43	13.06	15	16.04
3.5		16.3	12.78	12.04	12.1	13	19.3	14.78	14.04	15.1	13
4		15.5	11.8	11	11.1	12	17.5	12.8	11	14.1	15
0.5	FPR%	28.2	24.1	23	20	22.1	30.2	25.1	26	22	23.1
1		27.6	23.5	22.1	19.9	21.7	28.6	25.5	24.1	21.9	22.7

1.5		26	23.1	20.5	19.3	21	28	25.1	22.5	20.3	23
2		25.1	21.1	19.5	18.7	20	26.1	22.1	19.5	21.7	22
2.5		24.4	20.7	19.1	18.3	20.4	25.4	21.7	20.1	21.3	21.4
3		23.1	19.6	18.5	17.8	19	24.1	19.6	21.5	17.8	19
3.5		22.6	19.1	18.1	17.2	18.2	23.6	19.1	18.1	18.2	19.2
4		22	18	17	16	17	25	21	19	17	19

Table 4 Performance Analysis of the Proposed Method with Existing Methods

Attack Interval	Performance Metrics	RPL-SoS [24]	SMTrust [17]	SEEFOA-RPL
0.5	DR%	89	75	90
1		91	77	91
1.5		93	79	93
2		94	81	95
2.5		95	83	97
3		97	85	97
3.5		97	87	98
4		98	89	99
0.5	PDR%	80	76	80
1		82	78	81
1.5		86	81	82
0.5	FNR%	12.98	15	17.99
1		12.8	14	16.67
1.5		11.8	12.5	16
2		11.5	12	15.89
2.5		10.5	11	14.73
0.5	DR%	89	75	90
1		91	77	91
1.5		93	79	93
2		94	81	95
2.5		95	83	97
3		97	85	97
3.5		97	87	98
4		98	89	99
3		9.8	10.5	14.04
3.5		9.65	10.1	13

4		9.2	10	12
0.5	FPR%	15.6	19.5	22.1
1		14.6	19.1	21.7
1.5		14.2	18	21
2		13.7	17	20
2.5		13.4	16	20.4
3		13.8	15.8	19
3.5		13.3	15.4	18.2
4		12.4	15	17

From Table 2, it is observed that the analysis of PDR for different forms of RPL network nodes is performed in an attack interval of [0.5 – 1.5]. Compared to conventional techniques the proposed method has shown exceptional results in identifying whether all the data packets reach the sink from the sensor node. The proposed method has gained above 80% PDR compared to the other forms of RPL.

From Table 3, it is observed that the analysis of FNR and FPR for different forms of RPL network nodes is performed in an attack interval of [0.5 – 4]. With reference to conventional techniques, the proposed method has shown exceptional results of FPR and FNR which show the incorrect decisions of malicious node detection. The FPR and FNR are comparatively less for the proposed method which describes that there are less number of incorrect decisions on identifying malicious nodes.

4.6. Comparative Analysis

The proposed SEEFOA-RPL is compared to the conventional techniques such as SoS-RPL known as Securing Internet of Things against Sinkhole Attack using RPL [24] and SecTrust-RPL known as Security Trust Mobility based RPL (SMTrust) [17] as shown in table 4. The graphical representations of these comparative results are provided by Figure 8 and Figure 9.

Table 4 clarifies that, the proposed method accomplishes high-level outcomes compared to traditional RPL networks in terms of DR, PDR, FNR, and FPR. The SEEFOA has the advantage of greater efficiency and easier implementation. Even though the proposed approach attained better results, it also has limitations of high computational complexity and low convergence speed.

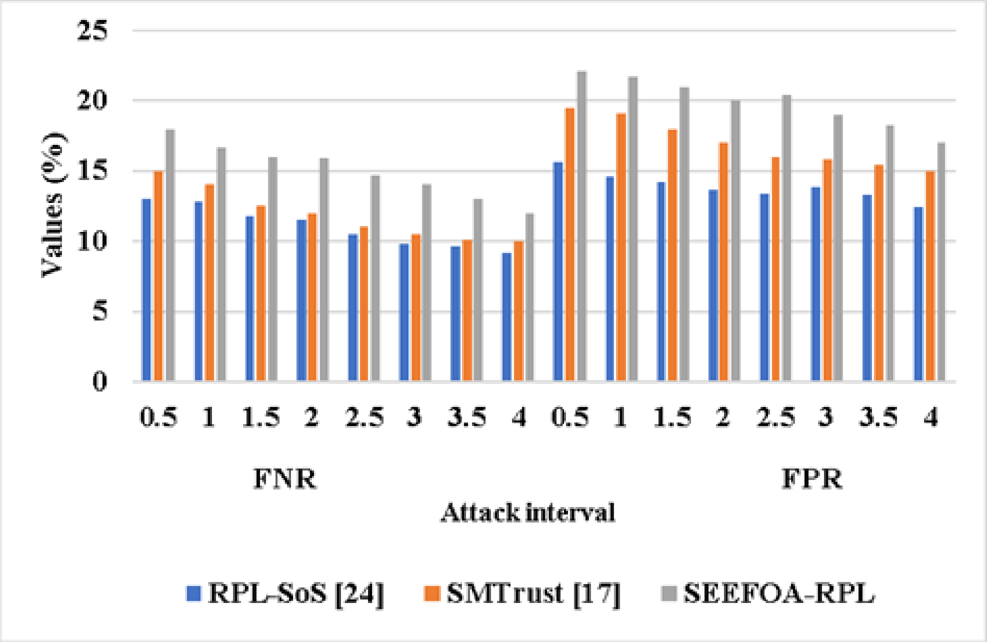

Figure 8 Graphical Analysis of FNR and FPR of SEEFOA-RPL with Conventional Methods

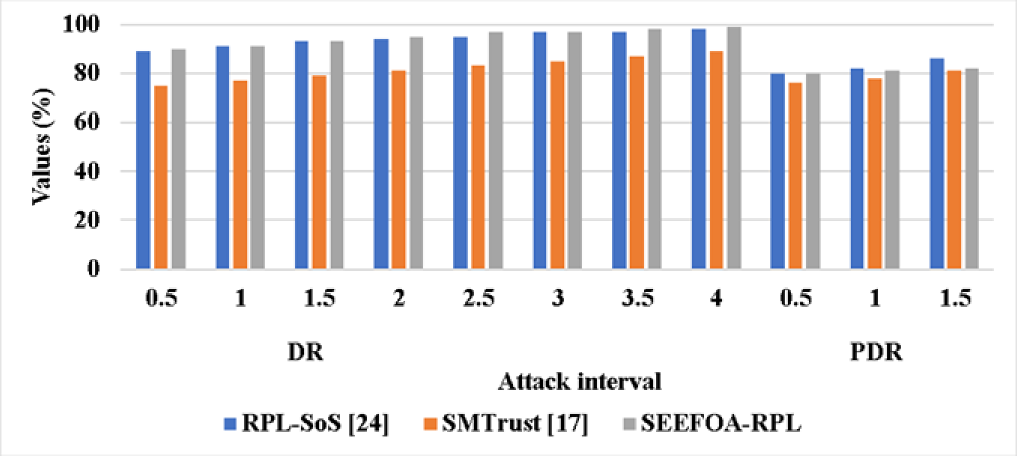

Figure 9 Graphical Analysis of DR and PDR of SEEFOA-RPL with Conventional Methods

4.7. Discussion

The proposed SEEFOA-RPL's performance is evaluated quantitatively and comparatively in terms of DR, PDR, FNR, and FPR with the conventional methods of RPL, RPL-SecTrust, RPL-SoS, and PLR+FDRPL. RPL allows flexibility in route creation. It is frequently used when dependability and energy efficiency are crucial. Even though RPL has certain security features, it might not be appropriate for highly secure IoT applications.

RPL-SecTrust is appropriate for IoT applications that demand robust security since it places a high emphasis on maintaining trustworthiness and security in LLNs. Features that RPL lacks, such as digital signatures, safe authentication, and secure data transmission, is present in RPL-SecTrust. RPL-SoS specifically addresses the threat of sinkhole attacks in LLNs that involve malicious nodes diverting traffic, monitoring route metrics and taking corrective actions. Its primary focus is on security against sinkhole attacks, which makes it valuable for applications with this specific security concern.

PLR+FDRPL addresses packet loss and false detection issues within the RPL protocol. While it does not primarily focus on security, it indirectly contributes to reliability and possibly security by reducing the impact of packet loss and false detections. These routing protocols cater to different aspects of LLNs and IoT applications. RPL is a foundational protocol for efficient routing in constrained networks. RPL-SecTrust enhances RPL with robust security features. RPL-SoS specializes in mitigating sinkhole attacks.

PLR+FDRPL mitigate packet loss and false detection issues, which impact both reliability and security indirectly. To overcome all the limitations in the existing mechanisms of RPL, the SEEFOA- RPL is proposed. By calculating the trust parameters and energy of the nodes, the secure routing path is established which achieved the DR of 99%, PDR of 82%, FNR of 12%, and FPR of 17%.

5. CONCLUSION

To overcome the issues of less confidentiality in user access data of IoT-based handheld devices, a secure and energy-efficient routing is established by performing an optimal routing mechanism. This mechanism is implemented with a novel SEEFOA- RPL method which uses the FOA algorithm to identify an optimal routing path in the networks of handheld devices. The data packets are securely transmitted to the sink by eliminating malicious nodes. The secure transmission of data packets in handheld devices is achieved because of the high consideration of trust parameters, security measures, and energy efficiency protocols. The obtained results that have shown the greater efficacy of SEEFOA-RPL, are measured as follows: DR is 99%, PDR is 82%, FNR is 12%, and FPR is 17%. However, the proposed approach has certain limitations of high computational complexity and low convergence speed. The future work may be more focused on the avoidance of intrusion attacks and black hole attacks in IoT-based handheld devices.

REFERENCES

[1] Y. Xu, J. Liu, Y. Shen, J. Liu, X. Jiang, and T. Taleb, "Incentive Jamming-Based Secure Routing in Decentralized Internet of Things," IEEE Internet Things J., vol. 8, no. 4, pp. 3000–3013, 2021

[2] T. Ul Hassan, M. Asim, T. Baker, J. Hassan, and N. Tariq, "CTrust-RPL : A control layer-based trust mechanism for supporting secure routing in routing protocol for low power and lossy networks-based Internet of Things applications," Trans Emerging Tel Tech, vol. 32, no. 3, 2021.

[3] P. Sathyaraj and D. Rukmani Devi, "Designing the routing protocol with secured IoT devices and QoS over Manet using trust-based performance evaluation method," J Ambient Intell Human Comput, vol. 12, no. 7, pp. 6987–6995, Jul. 2021.

[4] R. Sahay, G. Geethakumari, and B. Mitra, "A novel blockchain based framework to secure IoT-LLNs against routing attacks," Computing, vol. 102, no. 11, pp. 2445–2470, 2020.

[5] R. Nagaraju et al., "Secure Routing-Based Energy Optimization for IoT Application with Heterogeneous Wireless Sensor Networks," Energies, vol. 15, no. 13, p. 4777, 2022.

[6] S. Sharma and V. K. Verma, "Security explorations for routing attacks in low power networks on internet of things," J Supercomput, vol. 77, no. 5, pp. 4778–4812, 2021.

[7] S. Md. Mujeeb, R. Praveen Sam, and K. Madhavi, "Adaptive EHTARA: An Energy-Efficient and Trust Aware Secure Routing Algorithm for Big Data Classification in IoT Network," Wireless Pers Commun, vol. 121, no. 1, pp. 621–646, 2021.

[8] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, "Trust-aware and cooperative routing protocol for IoT security," Journal of Information Security and Applications, vol. 52, p. 102467, 2020.

[9] Y. Shibasaki, K. Iwamura, and K. Sato, "A Communication-Efficient Secure Routing Protocol for IoT Networks," Sensors, vol. 22, no. 19, p. 7503, 2022.

[10] A. Pliatsios, K. Kotis, and C. Goumopoulos, "A systematic review on semantic interoperability in the IoE-enabled smart cities," Internet of Things, vol. 22, p. 100754, 2023.

[11] Z. A. Almusaylim, N. Jhanjhi, and A. Alhumam, "Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP," Sensors, vol. 20, no. 21, p. 5997, 2020.

[12] A. Sharma and N. Kumar, "Third Eye: An Intelligent and Secure Route Planning Scheme for Critical Services Provisions in Internet of Vehicles Environment," IEEE Systems Journal, vol. 16, no. 1, pp. 1217–1227, 2022.

[13] E. O'Connell, W. O'Brien, M. Bhattacharya, D. Moore, and M. Penica, "Digital Twins: Enabling Interoperability in Smart Manufacturing Networks," Telecom, vol. 4, no. 2, pp. 265–278, May 2023.

[14] G. Pradeep Reddy and Y. V. Pavan Kumar, "Internet of Things Based Communication Architecture for Switchport Security and Energy Management in Interoperable Smart Microgrids," Arab J Sci Eng, vol. 48, no. 5, pp. 5809–5827, May 2023.

[15] I. Roussaki et al., "Building an interoperable space for smart agriculture," Digital Communications and Networks, vol. 9, no. 1, pp. 183–193, Feb. 2023.

[16] M. Hosseinzadeh et al., "A Cluster-Tree-Based Secure Routing Protocol Using Dragonfly Algorithm (DA) in the Internet of Things (IoT) for Smart Agriculture," Mathematics, vol. 11, no. 1, p. 80, 2022.

[17] S. M. Muzammal, R. K. Murugesan, N. Z. Jhanjhi, M. Humayun, A. O. Ibrahim, and A. Abdelmaboud, "A Trust-Based Model for Secure Routing against RPL Attacks in Internet of Things," Sensors, vol. 22, no. 18, p. 7052, 2022.

[18] A. Agiollo, M. Conti, P. Kaliyar, T.-N. Lin, and L. Pajola, "DETONAR: Detection of Routing Attacks in RPL-Based IoT," IEEE Trans. Netw. Serv. Manage., vol. 18, no. 2, pp. 1178–1190, 2021.

[19] A. O. Khadidos, S. Shitharth, A. O. Khadidos, K. Sangeetha, and K. H. Alyoubi, "Healthcare Data Security Using IoT Sensors Based on Random Hashing Mechanism," Journal of Sensors, vol. 2022, pp. 1–17, 2022.

[20] M. A. Abbasi, Z. A. Memon, N. M. Durrani, W. Haider, K. Laeeq, and G. A. Mallah, "A multi-layer trust-based middleware framework for handling interoperability issues in heterogeneous IOTs," Cluster Comput, vol. 24, no. 3, pp. 2133–2160, 2021.

[21] A. Gupta and A. Singh, "An Intelligent Healthcare Cyber Physical Framework for Encephalitis Diagnosis Based on Information Fusion and Soft-Computing Techniques," New Gener. Comput., vol. 40, no. 4, pp. 1093–1123, Dec. 2022.

[22] S. M. Muzammal, R. K. Murugesan, N. Jhanjhi, M. S. Hossain, and A. Yassine, "Trust and Mobility-Based Protocol for Secure Routing in Internet of Things," Sensors, vol. 22, no. 16, p. 6215, 2022.

[23] F. Medjek, D. Tandjaoui, N. Djedjig, and I. Romdhani, "Multicast DIS attack mitigation in RPL-based IoT-LLNs," Journal of Information Security and Applications, vol. 61, p. 102939, Sep. 2021.

[24] M. Zaminkar and R. Fotohi, "SoS-RPL: Securing Internet of Things Against Sinkhole Attack Using RPL Protocol-Based Node Rating and Ranking Mechanism," Wireless Pers Commun, vol. 114, no. 2, pp. 1287–1312, Sep. 2020.

[25] P.S. Nandhini, S. Kuppuswami, S. Malliga, and R. DeviPriya, "nhanced Rank Attack Detection Algorithm (E-RAD) for securing RPL-based IoT networks by early detection and isolation of rank attackers," The Journal of Supercomputing, vol. 79, no. 6, pp.6825-6848, 2023.

Authors

G.S. Sapna obtained her B.E degree in Computer Science and Engineering from Visvesvaraya Technological University (VTU). She was awarded Master's degree in Computer Networks and Engineering from Visvesvaraya Technological University (VTU). She is pursuing Ph.D degree from Visvesvaraya Technological University (VTU). Currently, she is an Assistant professor in the Department of Information Science and Engineering, Cambridge Institute of Technology, Visvesvaraya Technological University (VTU). Her specializations include Computer Networks and security, Machine Learning. Her current research interests are Security in Internet of Things.

Shashikumar Dandinashivara Revanna received BE degree from Mysore University and ME degree from Bangalore University, Bangalore and Ph.D in Information and Communication Technology at Fakir Mohan University, Balasore, Orissa. He is currently working as Professor and HoD, Dept. of Computer Science, Cambridge Institute of Technology, Visvesvaraya Technological University (VTU). His research interests include Microprocessors, Pattern Recognition, and Biometrics, Computer Networks, Data mining and Data Warehouse He has published 20 research publications in referred National and International Journals. He is the reviewer for some of the International journals.

How to cite this article:

G.S. Sapna, Shashikumar Dandinashivara Revanna, "An Interoperability Framework for Enhanced Security of Handheld Devices Using IoT-Based Secure Energy Efficient Firefly Optimization Algorithm", International Journal of Computer Networks and Applications (IJCNA), 10(5), PP: 763-775, 2023, DOI: 10.22247/ijcna/2023/223422.