Received: April 5, 2023. Revised: May 25, 2023.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

An Efficient Internet of Things Interoperability Model Using Secure Access Control Mechanism

G. S. Sapna[1]* Shashikumar Dandinashivara Revanna[1]

[1]*Department of Information Science and Engineering, Cambridge Institute of Technology, Bengaluru, India*
* Corresponding author's Email: sap.katapady@gmail.com

Abstract: Internet of Things (IoT) is a revolutionary innovation in many aspects of our society like financial activities, communication activities, and global security such as the military and battlefields' internet. Security and energy play a crucial role in data transmission across IoT and edge networks. In this research, a trust mechanism based on privacy access control is proposed for IoT devices' interoperability. Most of the existing researches on achieving interoperability for IoT devices has drawbacks such as overlapping of systems, uneven distribution of data, lack of data security, high power consumption, and low optimization of resources. The main objective of this research is to focus and overcome these challenges by introducing a privacy access control mechanism that includes trust parameters of IoT device interoperability. A routing protocol for low-power and lossy networks (RPL) mode of operation is set in the direction of multipoint-to-point traffic flow, except in the downward flow direction. Sensor nodes send data packets to the sink node, which transmits the information to the server to determine the trust values in this mode. To validate the performance, a widely used lightweight low-power wireless simulator Contiki/cooja simulator is implemented. The simulation results of the proposed model have shown a transmission ratio of 100%, a receiver ratio of 30 to 100%, and the detection of malicious nodes in a simulation time of 60 minutes. With the use of the proposed trust mechanism based on privacy access control, a less packet loss ratio of 0.43% is achieved along with less power consumption of 0.4%, and the highest average residual energy of 0.87mJoules at node 30.

Keywords: Contiki/Cooja simulator, Interoperability, IoT devices, Routing protocol, Trust based mechanism, Wireless sensor networks.

1. Introduction

The internet of things (IoT) has evolved as an extremely important in our daily lives which is evolving as a technological developing era by integrating virtual-based systems and machine ecosystems through the internet to produce adequacy and convenience in academic research, industries, and human lives [1]. Many applications, such as the healthcare industry, cities, and monitoring surroundings, etc., run through IoT networks and Software-Defined networking (SDN) controllers. Most IoT devices are composed of resource-constrained, low-power sensors (energy, memory, processing). Additionally, these sensors connect wirelessly, establishing a multi-hop wireless network that is susceptible to interference [2]. Wireless sensor networks, a type of low-power and lossy network known as LLN, are now a critical enabling technology for the IoT, bringing a wide range of network applications integrated into the established infrastructure of the internet [3]. The information exchange between two or more systems is known as interoperability and the Internet of IoT enables secure data transmission between devices by enabling interoperability. The challenge of interoperability in information technology has existed for a long time and has been focused on multiple levels, such as networking, syntactic, and semantic levels, as well as numerous domains, such as the industrial and healthcare domain [4]. Safe and secure connections are a primary challenge in real world applications due to the heterogenetic nature of IoT tools, and the shortage of resources. due to this, only a few resources get to connect to IP (Internet Protocol)

hosts which are safe and secure. Furthermore, IoT-connected devices must be secure with authentications like end to end (E2E) connections [5]. Like other networks, IoT security is dependent on confidentiality and trust. As a result, attack detection systems are one of the primary defence methods against IoT attacks. The frequent occurrence of IoT attacks results in financial loss or worse. Attestation is a low-cost method of identifying malicious devices. However, naive device-to-device remote authentication has a high cost in terms of authentication time and communication overhead, as well as scalability issues [6]. 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 for the physical layer, network, layer, and application layer of IoT [7, 8] 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 [9]. Most conventional security methods are not up to snuff to protect the industrial strategies of most firms and business sectors. The root exploits, botnets, spyware, worm, and Trojans are some of the critical IoT security issues to be dealt with [10]. The major contributions to this work are listed below:

- A trust-based mechanism with privacy access control provides interoperability in IoT devices by assessing the behavior of node trust in the RPL networks. This method also achieved less computational storage and bandwidth, efficient energy, and the highest throughput at the node level.

- Interoperability is achieved by avoiding malicious nodes in the network using secure and trust based RPL networks and the trust parameters of the network are validated using the Contiki/cooja simulator.
- Less computational complexity can be obtained with the proposed trust based mechanism. High interoperability is achieved by mitigating malicious attacks in the network.

The present manuscript is organized as follows: Section 2 includes related work on IoT Interoperability. Section 3 describes the proposed methodology of this work. Section 4 illustrates results along with a comparative analysis of performance metrics. Section 5 provides a conclusion of the work.

2. Literature review

The RPL protocol has been protected from insider attacks, according to T Hassen [8], who provided a variety of trust-based techniques. As a result, a hierarchical trust-based technique called CTrust-RPL is recommended for evaluating node trust based on their forwarding actions. In order to conserve computing, storage, and energy resources at the node level, this study sends difficult trust-related computations to the controller, a higher layer. To address the expanding demands of distributed IoT deployments and counter additional potential assaults, the C-trust model must create a distributed and more scalable trust-based approach. Anuradha [11] developed a system to predict cancer using the Internet of Things to test whether blood results were normal or abnormal by improving security enhancement and authentication in the cloud area. The processing and enhancement of healthcare computations through encryption and decryption with the advanced encryption standard (AES) algorithm was the primary intention of this work. Encryption was performed on the reports of cancer patients and saved in the cloud database for quick analysis through the Internet by healthcare nurses or doctors to manage the patient data confidential. This proposed approach has achieved the highest efficiency, system performance and throughput compared to the existing encryption systems. However, the major issue with AES is that the entity with whom the data is shared must be able to receive the key, which is a drawback. Mohammad Asad Abbasi [12] proposed a multi-layer framework to address the interoperability issues in heterogeneous IoTs, and design an interoperability framework with trust-based parameters. Various interaction services with different time intervals have been tested with this approach along with the analysis of the decay rate. The overall performance in terms of reliability and availability was high with this service-oriented framework. However, this framework did not help operate communications between dependent services and applications. For further investigation, AI techniques can improve the overall procedure of trust measurements. Kalyani [13] proposed an approach to enhance security measurements of sensitive data in IoT using the cryptographic-based optimal homomorphic encryption (OHE) method. Initially, the sensitive data of IoT was categorized using deep learning neural network structure (DNN) followed by encryption and decryption using the OHE method. Later an encrypted key was generated which was further authenticated using the step size firefly

optimization algorithm which built privacy preserving of data in IoT. This proposed approach achieved high accuracy, sensitivity, specificity, and less computational time with the highest key breaking time and security.

Abbas Yazdinejad [14] proposed a block chain based architecture to provide secure P2P communication among SDN controllers and IoT devices. An optimum authentication key was used to provide secure communications among IoT devices. This energy-efficient based routing protocol provided efficient authentication and also a secure mechanism to transfer files in the SDN region. The performance of the architecture achieved greater results with the highest throughput, less energy consumption, and low delay compared to the existing EESCFD, SMSN, AODV, and DSDV routing protocols. The method does not take the energy resources and comparability of IoT devices into account, which was a limitation of this work. Saravana Balaji [15] developed a network infrastructure to create a balanced harmonious environment where the block chain was controlled and managed with the resources present in it. A novel architecture was introduced to enhance privacy and secure authentication and handle the inconspicuousness in IoT devices with the use of a simple size of the extensible block chain. Two novel algorithms namely: shared time-dependent (STD) and shared throughput administrative (STA) algorithms were implemented. STD reduces irregularity in latency and extraction operations whereas, STA helps in maintain the better performance of block chain and is accountable for the network's transmission load. The proposed approach created a poor communication channel for the block chain which was a limitation of this work. The obtained experimental results have shown that the proposed method reduces the irregularity of data, latency and maximizes the block chain's extensibility. Ali Hassan Sodhro [16] developed a framework for IoT based decentralized applications to enable block chain-based security techniques. A random and master key generation mechanism was also introduced for the processing and transmission of encrypted data. A decision was made based on the process of analytic hierarchy for secure interoperability, convergence, and reliability for block chain driven IoT systems and achieved the same. However, this method was not suitable in the health industry for secure data transmission, which was a limitation of this work. Manikannan [17] proposed an energy-efficient and mobility optimization-based RPL framework to achieve a stable and reliable protocol. An mRPL-based firefly optimization algorithm was introduced to improve the performance of end-to-end delay, Packet delivery ratio (PDR), and power consumption. Low energy, and limited resources were the limitations of this work which needs attention while building mobility management networks. For further research, the number of mobile nodes for real-time applications used in 6LoWPAN with network security can be increased. N Djedjiga [21] Metric-based RPL Trustworthiness Scheme (MRTS) that includes trust evaluation for secure routing topology creation addresses the lack of reliable security measures in RPL. Many simulations demonstrate that MRTS is effective in terms of throughput, energy usage, nodes' rank changes, and packet delivery ratio. Additionally, a mathematical modelling analysis demonstrates that the trust-based routing metric possesses the isotonicity and monotonicity qualities necessary for a routing protocol and that MRTS satisfies the consistency, optimality, and loop-freeness requirements. It is claimed that MRTS can be used as a strategy for the repeated Prisoner's Dilemma and that this will show its cooperative enforcement characteristic. MRTS needs to meet further requirements, like mobility, and have its functionalities tested against various trust thresholds.

The trust model proposed by Mustafa Ghaleb [22] collects suggestions from other nodes in the IoT ecosystem using subjective logic as the default artificial reasoning over ambiguous propositions. Additionally, it oversees and preserves the trust connections made through direct contact. It also defends against dishonest nodes that give false ratings for nefarious purposes. Because it uses a Fog-based hierarchy design, which enables IoT nodes to report or request the trust values of other nodes, the trust model is scalable in contrast to previous trust models. Further findings show that our proposed trust model isolates untrustworthy conduct inside the network and prevents untrustworthy nodes from damaging the reputations of trustworthy nodes. The untrustworthy behavior pattern cannot be properly separated from the network nodes using Mustafa's trust model. To optimize the communication network in both a static and mobile setting, Niharika Panda [23] proposed modified smart home optimization path (MSHOP). In order to achieve the goal, a method that enhances path selection by changing the current objective functions of RPL was developed. On the basis of many factors, including the packet reception ratio, network overhead, throughput, average latency, and overall energy consumption, the proposed smart home architectures are assessed and contrasted. To prevent the loss of crucial messages, MSHOP must further increase the message transmission rate on time.

According to Ahmed Motmi [24], a trust management technique is suggested for protecting IoT, and the conversion of industrial applications to IoT and the internet of things causes multiple changes in the communication processes. Wireless sensor networks with unmanaged wireless topologies that were compromised as a result of the design of their resource-constrained nodes were the ones who first noticed this transition. The security protocol makes advantage of the secure constrained application protocol-mandated datagram transport layer security (DTLS) to safeguard sensitive information being sent (CoAP). DTLS required robust support for industrial applications connected through high-bandwidth networks because it was made for powerful devices. Other IoT-related trust-based attacks in industrial environments, such as ballot-stuffing attacks, opportunistic service assaults, bad-mouthing attacks, and self-promotion attacks, are not detected by trust management techniques.

The limitations found from the literature survey are poor communication between dependant services, lack of energy resources and comparability, lack of security in data transmission, limited resources. These limitations can be overcome by the proposed method as discussed in the section 4.2.

3. Methodology:

The main aim of this work is to design an interoperability framework for privacy and security enhancement through services provided by IoT. The proposed framework is divided into the things layer, registration layer, and service handling layer as shown in Fig. 1. Each layer in the framework is linked to the next layer. For initial trust calculations, a dynamic parameter selection and weight assignment are used. The proposed framework's design includes a focus on trust measurement and detecting malicious nodes as shown in Fig. 2. Following that, some of the parameters which are important for services are calculated and for trust calculation, parameters like trust value and trust degree are considered. Following the estimation of the aggregated trust value, the controller will keep updating the interaction table and the trustworthiness of IoT, and finally, the trust degree will be defined. Following that, for each interaction, the value of trust is computed and shared within the interacted services by utilizing the trust factor. Nonetheless, there a various important and dependent conditions in which interactions between two or more IoT must be verified.

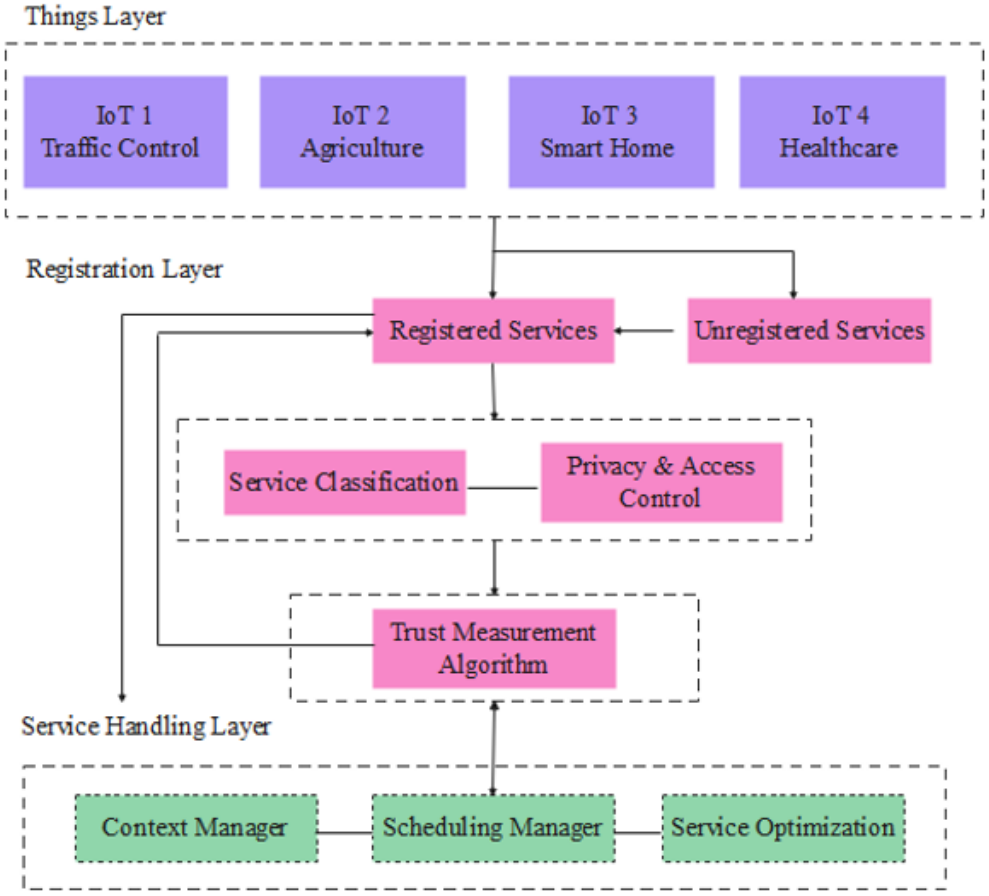

Figure. 1 Flow chart of the proposed method

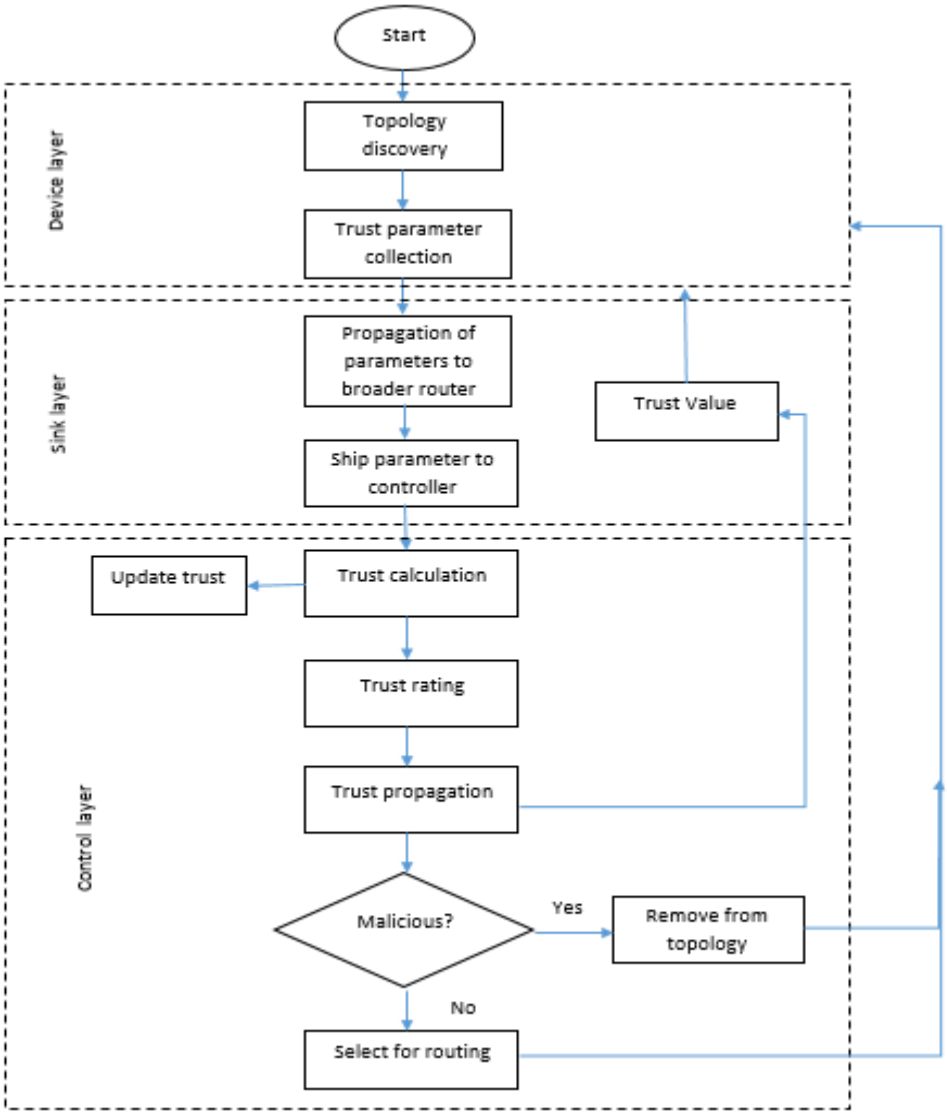

Figure. 2 Flow chart for detecting malicious nodes with trust measurement

3.1 Things layer

The things Layer is the framework's topmost layer. Future IoT service usage optimization necessitates the creation of new services from existing ones, which can be accomplished by analyzing the combined relationships, context, and availability of services. Fig. 1. Represents the scenario of available physical devices in several application domains, where the service domain refers to the geographic area with different types of heterogeneous and homogeneous services. This location could be a house, a park, a street, a building, a hospital, a bank, or anything else. The things layer works as a pass-through layer that takes information or request of service from various sources and routes them to the layers below it for processing and completion. The most crucial gadgets connected to this layer include sensors, smart gadgets, wearables, security cameras, and smart cars. The data request and service requests for the next layer are carried out by this layer.

3.2 Registration layer

This layer utilizes features like device id, computing power, and memory to register devices and their respective services. For the devices, all of this information is stored in the registration layer. It registers the services, keeps their ID’s in storage, and preserves all other pertinent data. IoT interactions should therefore be categorized and managed by the registration layer namely service classification, privacy and access control, trust management, and blockchain.

3.2.1. Service classification

In this layer different classes are made for manageability and comfort from offered services. Services are divided into groups based on how critical they are. The five service categories are as follows:

1. Elementary services
2. Order support services
3. Utility services
4. Healthcare services
5. Traffic and transportation services

The level of criticality of these interactions can be determined based on these categories, and it is possible to decide which interactions require verification and which do not depend on these levels.

3.2.2. Privacy and access control

This module focuses on another major concern of IoT devices i.e., privacy. Since, IoT is becoming more prevalent in people's daily life, appropriate preservations of privacy for end users must be implemented. must be implemented for end users. The emphasis of this module is on implementing various rules for restricting access to services and sharing of resources. Data security, secure data exchange, distributed access of data and its access permissions are the main responsibilities. The definition of user and application privacy policies is another goal of this module. Additionally, it will safeguard users' privacy.

3.2.3. Trust measurement

The context-aware secure services to requesters in the IoT context become a key component of trust measurement, and it has evolved into a driving force to meet future IoT privacy and security requirements. The main objective of this module is to offer dependable access to the IoT services that are currently offered. In this sense, an IoT's trust $\overline{T}_{(q)}$ can be described as its actions while using an IoT protocol during a given period "t". It is more specifically the relationship between the quality (q) of service provided by two or more IoTs that exchange services. As a result, an IoT's activity is both a measure and a function of trust. This section discusses the proposed Trust based RPL mechanism, which supports analyzing IoT node trust behavior and correcting behaviors of network management by finding and blocking malicious nodes if suspicious signs are detected. A Contiki/cooja simulator is used for the simulation of trust parameters. Fig. 3 represents the topology of sensor nodes in the Contiki simulator. From Fig. 3, sink nodes are 31 and 32,

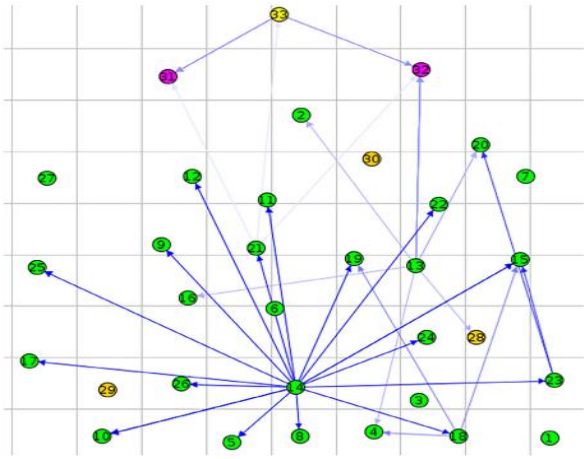

Figure. 3 Topology of Contiki simulator

malicious nodes are 28 to 30 and the remaining are the normal nodes.

The proposed method establishes the trust among uncertainty between the nodes based upon the computation of the trustworthiness of nodes and their uncertainty in trust value. By the involvement of a belief theory among the key elements of the node, the trust model computes the uncertainty. The model can be energy efficient because of the probability and binary logic, and nodes do not strain for IoT devices. Additionally, the adaptive trust parameters will be established using the packet loss ratio (PLR) and FD (false detection) as input by using complex calculations over the control layer. As per trust calculation, certain parameters on each node of the network are initiated to detect malicious nodes and remove them from the network. The node trust in the service network is eliminated when the trust value is less. This scenario arises when the IoT doesn't provide services with better accuracy, security measures, privacy control, reliability and other parameters than other IoT. The trust measurement lifecycle consists of 5 stages highly trustable (direct trust), partially trustable (only for a particular application), neutral (uncertain), partially distrust-able (only for a particular application), and highly distrust-able. By this trust measurement lifecycle, the controller examines the service permissions which are represented by an access permission table, when a controller gets a service request. Few services cannot get permitted without previous history and a trust level greater than the threshold value. The direct trust is determined by the success rate of the node as represented by Eq. (1) and Eq. (2)

$$T_{SR} = {}^{P_F}/_{P_R} \tag{1}$$

$$P_F = P_R - P_D \tag{2}$$

Where, T_{SR} is the total success rate of the node, SR is the ratio of number of packets forwarded (P_F), P_R is the number of packets received, and P_D is number of packets dropped.

The ratio of packets dropped (Pd) by the receiving node to all packets delivered from the sender node (Pt) is known as the "Packet Loss Rate" (PLR), which is given by Eq. (3). The period of time between receiving a packet from the sender and sending it to the following node is known as the "Forwarding Delay" (FD) is given by Eq. (4).

$$PLR = \frac{P_d}{P_t} \tag{3}$$

$$FD = PR_t - FR_t \tag{4}$$

Based on these PLR and FD parameters, positive (p) and negative (n) interactions are computed as shown in Eqs. (5–7). Let W = (b, d, u) represent node A's assessment of node B's reliability. Where, respectively, b, d, and u stand for belief, disbelief, and uncertainty. All three of these factors added together always equal 1.

$$b_{ij} = \frac{p}{p+n+k} \tag{5}$$

$$d_{ij} = \frac{n}{p+n+k} \tag{6}$$

$$u_{ij} = \frac{k}{p+n+k} \tag{7}$$

Where, b_{ij}, d_{ij}, and u_{ij} represents the degree of belief of node i have on node j by taking the ration of positive parameter with the sum of all the three parameters p, n, and constant (k).

The energy level of the node is determined by the ratio of remaining energy and maximum energy of the node as given in Eq. (8). The maximum energy level is 1 for a node with full battery.

$$T_{EL} = {}^{E_R}/_{E_M} \tag{8}$$

Where, T_{EL} is the energy level of the node, E_R is the remaining energy and E_M is the maximum energy.

3.3 Service handling layer

After completing the procedure of registration and trust calculation, an IoT intends to request and access a huge range of services accessible on neighbouring IoT. This layer is the foundation of the service management process, storing all relevant data to the availability of services in the region. As a result, service handling is inextricably linked with context management to dynamically embrace new availability matrices in response to changes in sharing context-based updates.

The trustworthiness of nodes is calculated as illustrated in algorithm below. The input parameters are represented by PLR and FD. The output is the malicious node and its removal from the topology. The trust parameters are computed for each node in the network, after initiation of specific thresholds.

Algorithm:

Input: PLR, FD

Output: Detection of Malicious Nodes

Declare $t_1, t_2, n = 0, p = 0$ and $k = 2$

Declare PLR and FD thresholds based on $t_1, and\ t_2$

PLR=PD/PT

FD= PR_t-PF_t

For nodes in nodes

if PLR$< t_1$ and FD$< t_2$

$P = p + 1$

Else

$N = n + 1$

End for

Compute $u = \frac{k}{(p+n+k)}, d = \frac{n}{(p+n+k)}, b = \frac{p}{(p+n+k)}$

if $d > 0.5$ then

N_ status≤ Not trusted

Else if b > 0.5 then

N_ status≤ trusted

Else

N_ status≤ not verified

End if

If N_ status = trusted, then

Select routing

Else

Remove the node from the network

End if

3.3.1. Algorithm explanation

Initially, the topology is initialized with threshold values with $t_1, t_2, n = 0, p = 0$ and $k = 2$. The values of PLR and FD are measured based on t_1 and t_2 values. The PLR and FD of each node is calculated and the values of each node are compared based on these calculations. The nodes within the threshold values are said to be positive nodes, otherwise known as negative nodes. Based on these, the computations of b, u, and d are measured. The logic used to measure the terms b, u, and d is based on the linear relationship between time and the parameters of trust.

Table 1. Simulation results of the Contiki/cooja simulator

Parameter	Value
Area	$70m \times 70m$
No. of nodes	30
Tx ratio	100%
Rx ratio	30 to 100 %
Malicious nodes	28,29 and 30
Transmission range	50 m
Simulation Time	60 inutes

Table 2. Comparison of RPL for attack detection of malicious nodes in terms of PLR and FD

Malicious nodes	Attack detection time(seconds)			
	RPL	PLR-RPL	FD-RPL	PLR+FD – RPL (proposed)
10	14	12	11	8
20	31	28	25	20
30	43	40	38	35
40	56	54	52	49
50	64	62	60	58

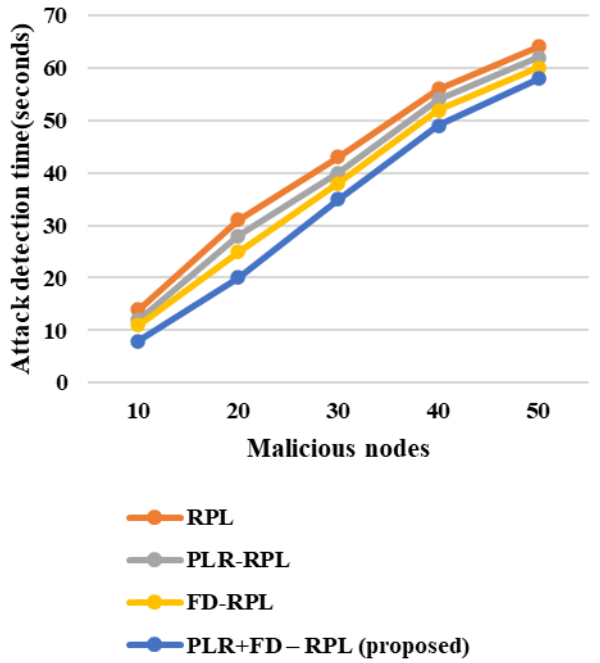

Figure. 4 Attack detection time in RPL based on PLR and FD

Table 3. Comparison of RPL for power consumption of malicious nodes in terms of PLR and FD

Malicious nodes	Power consumption (mJoules)			
	RPL	PLR-RPL	FD-RPL	PLR+FD – RPL (proposed)
10	0.40	0.43	0.42	0.39
20	0.52	0.49	0.47	0.45
30	0.51	0.49	0.46	0.45
40	0.54	0.52	0.50	0.48
50	0.57	0.55	0.54	0.52

The calculation is performed for each node, and the trust rating threshold is established. It is determined to be a legitimate node of the network and can be included in routing after the rating of propagation of trust is completed and it has the value of b always to be greater than a threshold; otherwise, it will be removed. The proposed algorithm's complexity is reduced by the message overhead, and it is O(n) in algorithmic form.

4. Results

The effectiveness of the proposed trust-based framework is evaluated using simulations. For modelling the proposed trust based RPL environment, we employ Cooja 2.7 on a Linux platform with an Intel(R) 2.54 GHz CPU and 1 GB RAM, the simulation is run. Our system relies on multipoint-to-multipoint traffic flow, and RPL's operation mode is No Downward. In this mode, packets are forwarded from the sensor nodes to the sink node, which then forwarded the data to the server to determine the trust values. Contiki can be used for high-performance and secure communication between low-powered RFID chips in wireless networks.

The proposed model measures parameters such as attack detection, attack detection time, packet loss ratio, power consumption, and residual energy to validate the mechanism. The following simulation setup has been used for the evaluation of the proposed model topology as shown in Table 1.

4.1 Quantitative evaluation

The proposed trust mechanism is evaluated on the basis of PLR and FD of nodes in the network. In this section, the proposed method is compared with the RPL, PLR-RPL, and FD-RPL in terms of attack detection time and power consumption as shown in Table 2 and Table 3.

From Table 2, it is observed that the proposed trust mechanism with combined PLR and FD achieved less attack detection time when compared to RPL, PLR-RPL, FD-RPL. The graphical representation of the quantitative analysis of Table 2 is represented in Fig. 4.

From Table 3, it is observed that the proposed trust mechanism with combined PLR and FD achieved less power consumption when compared to RPL, PLR-RPL, FD-RPL. The graphical representation of the quantitative analysis of Table 3 is represented in Fig. 5.

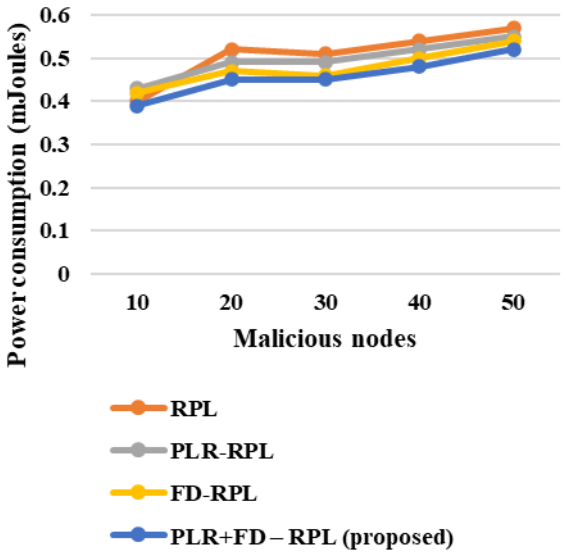

Figure. 5 Power consumption of RPL based on PLR and FD

4.2 Comparative evaluation

In this section, the existing Metric based RPL Trustworthiness Scheme (MRTS) [21], Modified Smart Home Optimization Path (MSHOP) [23] and CTrust-RPL [8] are compared with the proposed privacy access control-based trust mechanism in terms of performance metrics such as attack detection, attack detection time, packet loss ratio, power consumption and average residual energy of RPL networks in IoT devices. With the utilization of the proposed trust-based mechanism, the network achieved better results compared to the existing methods.

- **Comparative discussion**

According to the literature survey of existing techniques such as [8, 21, 23], there are some limitations in achieving IoT interoperability. Some of those limitations includes poor communication channel, less trust based measures, data disclosure, and less energy resources. To overcome this drawback, a privacy access control based trust mechanism is developed to achieve interoperability in IoT devices by introducing trust parameters within the network. Similarly, in reference [14], the energy resources and IoT device compatibility are not considered which causes higher power consumption to the overall network. To overcome this, our proposed method has included attack mitigation mechanism for low power consumption. In reference [17], low energy and limited resources were the limitations, which needs attention while building mobility management networks. To overcome this our proposed method manages the resources with stable energy and requirements to maintain the mobility architecture.

4.2.1. Attack detection

The exact and accurate detection of black hole attacks at any given time in the network is known as attack detection. The comparison of attack detection for various nodes is represented in Fig. 6 with the existing methods MRTS and Ctrust RPL. Both methods detected many malicious nodes in the initial stage since there were more malicious entities as shown in Fig. 6. The no. of malicious nodes gradually becomes low once the node trust was fully achieved. It is because of the proactive nature of RPL networks, adversary nodes were eliminated from the network topology and alternative routes were discovered before the network gets completely drained. The representation of attack detection in two existing methods MRTS and Ctrust-RPL are given in Table 4.

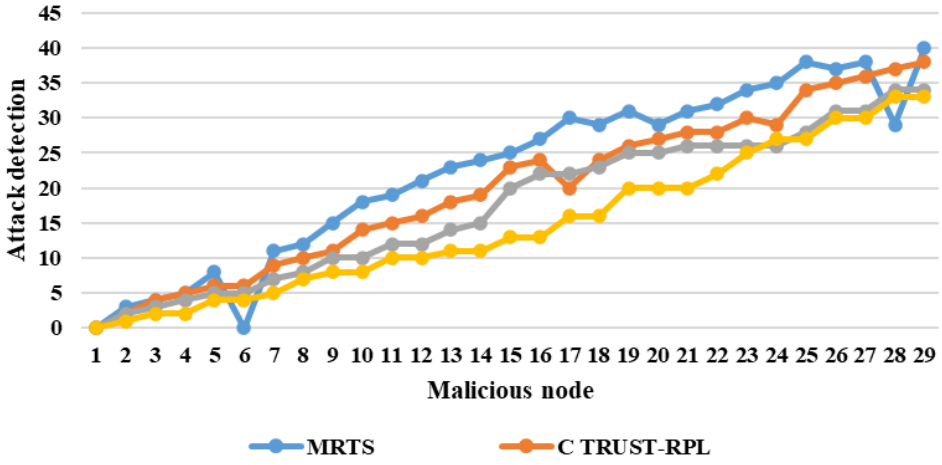

Figure. 6 Attack detection

Table 4. Comparison of trust based RPL mechanism for attack detection of malicious nodes

Malicious nodes	Attack detection			
	Metric-based RPL Trustworthiness Scheme (MRTS)[21]	CTrust-RPL[8]	MSHOP [23]	Proposed trust mechanism
1	348	380	390	410
2	205	252	260	275
3	235	240	247	287
4	205	252	262	300
5	90	140	150	185
6	90	140	147	190
7	89	140	150	178
8	99	145	152	175
9	85	130	139	155
10	90	140	149	184
11	90	140	150	176
12	95	142	150	169
13	95	130	139	157
14	85	145	154	177
15	95	140	146	190
16	95	140	148	182
17	55	100	107	132
18	60	95	100	116
19	52	60	68	100
20	30	55	63	103
21	50	60	68	108
22	45	55	64	82
23	40	52	57	101
24	70	95	101	127
25	75	100	105	127
26	50	60	70	108
27	45	55	63	98
28	50	85	93	117
29	45	52	59	79

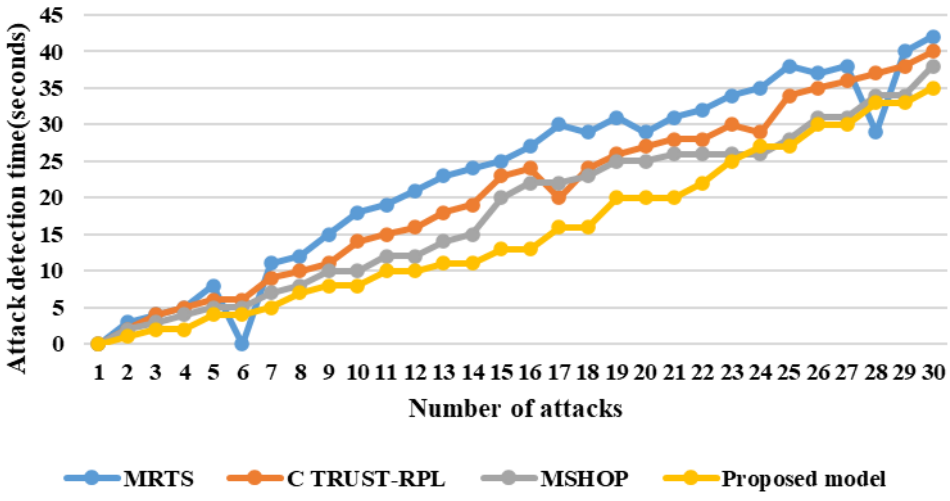

Figure. 7 Attack detection time

4.2.2. Attack detection time:

The efficiency of the proposed model in detecting attacks in less time is compared with the existing methods of MRTS, MSHOP and CTrust-RPL. Fig. 7 shows the graphical representation of attack detection time compared to the proposed trust based mechanism. The attack detection time for one malicious node is shown first, then increased in one

Table 5. Comparison of trust based RPL mechanism for attack detection time

Number of Attacks	Attack detection time(seconds)			
	Metric-based RPL Trustworthiness Scheme (MRTS) [21]	C Trust-RPL[8]	MSHOP [23]	Proposed trust mechanism
1	0	0	0	0
2	3	2	2	1
3	4	4	3	2
4	5	5	4	2
5	8	6	5	4
6	0	6	5	4
7	11	9	7	5
8	12	10	8	7
9	15	11	10	8
10	18	14	10	8
11	19	15	12	10
12	21	16	12	10
13	23	18	14	11
14	24	19	15	11
15	25	23	20	13
16	27	24	22	13
17	30	20	22	16
18	29	24	23	16
19	31	26	25	20
20	29	27	25	20
21	31	28	26	20
22	32	28	26	22
23	34	30	26	25
24	35	29	26	27
25	38	34	28	27
26	37	35	31	30
27	38	36	31	30
28	29	37	34	33
29	40	38	34	33
30	42	40	38	35

by one order. In Fig. 7 the second node detection keeps increasing in proportion to the increase in the number of attacks. However, the proposed optimization technique shows less time in attack detection compared to the existing methods. The representation of attack detection time in two existing methods MRTS and Ctrust-RPL are given in Table 5.

4.2.3. Packet loss ratio:

The ratio which depicts the lost packet to the total number of sent packets is known as the packet loss ratio and it is graphically represented in Fig. 8. Fig. 8 shows the comparison of existing methods' packet loss ratio to the proposed method. The existing methods MRTS and CTrust-RPL are compared with the proposed trust based privacy access control mechanism as shown in Table 6. The packet loss ratio pf the proposed framework is less compared to the existing methods even under the same network parameters. Due to the similar parameters, some of the patterns look natural for both frameworks. On average the packet loss ratio for the proposed framework at node 15 is 0.32 for node 15, 0.5 for reference [21], and 0.4 for reference [8]. Thus, the proposed framework has given a better defence mechanism against black hole attacks with a less packet loss ratio.

The mathematical expression for calculating PLR is given by Eq. (9).

$$PLR = \frac{N^{tx} - N^{rx}}{N^{tx}} \times 100 \quad (9)$$

Where, N^{tx} is the total number of packets transmitted and N^{rx} is the number of packets received.

4.2.4. Power consumption:

The proposed trust based mechanism achieved less power consumption compared to the existing methods MRTS and CTrust-RPL. The power

Table 6. Comparison of trust based RPL mechanism for packet loss ratio

Number of Nodes	Packet loss ratio(%)			
	Metric-based RPL Trustworthiness Scheme (MRTS) [21]	C Trust-RPL[8]	MSHOP [23]	Proposed trust mechanism
1	0.5	0.4	0.39	0.4
2	0.5	0.4	0.38	0.33
3	0.51	0.42	0.40	0.41
4	0.52	0.43	0.42	0.34
5	0.49	0.38	0.37	0.29
6	0.49	0.38	0.37	0.31
7	0.48	0.36	0.34	0.32
8	0.49	0.39	0.37	0.32
9	0.5	0.41	0.40	0.32
10	0.49	0.39	0.38	0.32
11	0.5	0.4	0.38	0.35
12	0.49	0.39	0.38	0.31
13	0.5	0.4	0.39	0.36
14	0.5	0.4	0.38	0.35
15	0.5	0.4	0.38	0.35
16	0.5	0.4	0.38	0.33
17	0.49	0.39	0.38	0.35
18	0.5	0.4	0.39	0.31
19	0.49	0.39	0.37	0.32
20	0.49	0.39	0.37	0.32
21	0.51	0.4	0.39	0.32
22	0.49	0.41	0.39	0.34
23	0.52	0.43	0.42	0.34
24	0.53	0.4	0.38	0.35
25	0.5	0.4	0.38	0.36
26	0.5	0.39	0.37	0.32
27	0.49	0.39	0.37	0.33
28	0.5	0.4	0.38	0.34
29	0.5	0.4	0.39	0.34
30	0.48	0.37	0.36	0.33

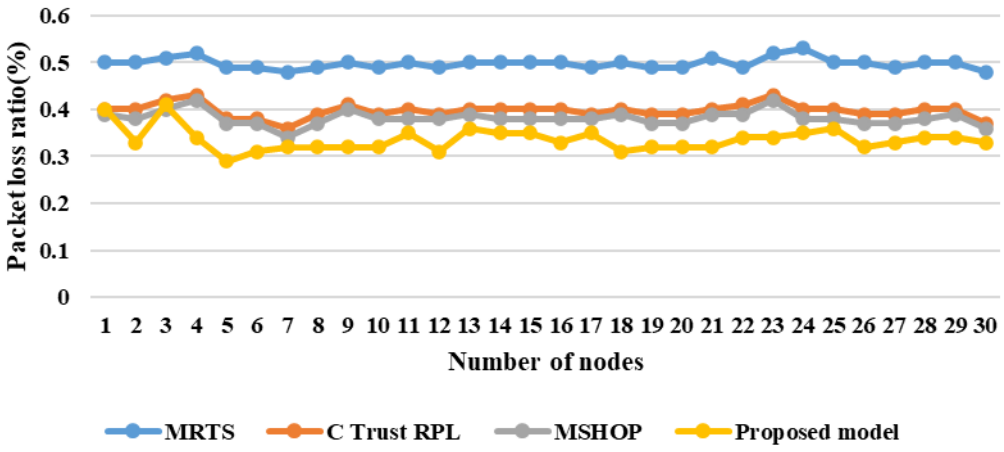

Figure. 8 Packet loss ratio

consumption for the existing methods is very high when compared to the proposed optimization method as the existing methods do not have a mechanism for attack mitigation to deal with the packet drops caused by malicious nodes in the network. As the proposed method have the attached mitigation mechanism, the power consumption is less. Fig. 9 shows the graphical representation of the power consumption of the proposed method in comparison to the existing methods. Table 7 represents power consumption

Table 7. Comparison of trust-based RPL mechanism for power consumption

Number of Nodes	Power consumption			
	Metric-based RPL Trustworthiness Scheme (MRTS) [21]	C Trust-RPL[8]	MSHOP [23]	Proposed trust mechanism
1	0.55	0.5	0.49	0.43
2	0.73	0.5	0.48	0.48
3	0.7	0.51	0.49	0.51
4	0.6	0.52	0.51	0.45
5	0.52	0.49	0.47	0.45
6	0.75	0.49	0.48	0.46
7	0.6	0.48	0.47	0.39
8	0.52	0.49	0.48	0.44
9	0.65	0.5	0.49	0.41
10	0.75	0.49	0.48	0.39
11	0.69	0.5	0.48	0.49
12	0.6	0.49	0.47	0.44
13	0.52	0.5	0.49	0.45
14	0.64	0.5	0.49	0.44
15	0.52	0.5	0.49	0.43
16	0.62	0.5	0.49	0.49
17	0.51	0.49	0.47	0.41
18	0.69	0.5	0.49	0.44
19	0.67	0.49	0.48	0.41
20	0.59	0.49	0.48	0.45
21	0.69	0.51	0.49	0.46
22	0.6	0.49	0.48	0.49
23	0.82	0.52	0.50	0.49
24	0.79	0.53	0.52	0.45
25	0.59	0.5	0.48	0.4
26	0.65	0.5	0.49	0.41
27	0.6	0.49	0.47	0.39
28	0.55	0.5	0.48	0.41
29	0.61	0.5	0.48	0.41
30	0.65	0.48	0.46	0.45

values for the 30 nodes in the network. The amount power consumed in a node is given by Eq. (10).

$$PC = \frac{E_{total}}{t_{cpu}+t_{lpm}} \quad (10)$$

Where, E_{total} is the total energy, t_{cpu} is the CPU's spent time, and t_{lpm} is the time spent by low power modes.

4.2.5. Average residual energy

The node's average residual energy in the network is saved with the proposed mechanism during the simulation. With the proposed trust mechanism with privacy access control, the RPL network achieved high residual energy compared to the existing methods MRTS and CTrust-RPL. The average residual energy of the proposed method is 0.87mJoules and the existing methods MRTS and CTrust-RPL are 0.3mJ and 0.7mJ. At 29th minute, a huge variation in energy depletion can be viewed as shown in Fig. 9. Table 8 shows the average residual energy values and its graphical representation is shown in Fig. 10. The total residual energy is calculated as shown in Eq. (11).

$$E_{total-curr(i)} = E_{res}(i) + E_{harvest}(i) \quad (11)$$

Where, the total current energy of node i is given by $E_{total-curr(i)}$, the residual energy of node i is given by $E_{res}(i)$, and the total harvested energy of node i is given by $E_{harvest}(i)$.

5. Conclusion

An energy-efficient, trust-based interoperability framework for identifying and isolating black hole attacks is included in the proposed RPL routing protocol. A control layer in the network computes the trust values to conserve the limited energy of IoT devices. Using the privacy access control to observe the exchange of packets between the nodes, it was

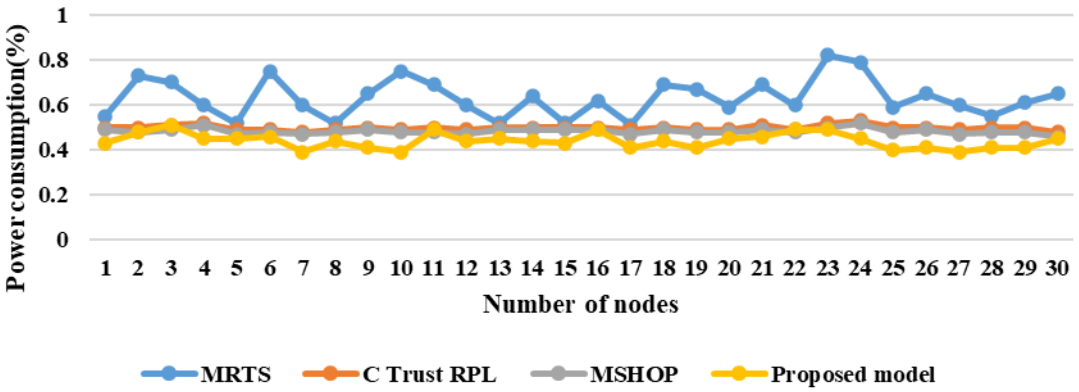

Figure. 9 Power consumption

Table 8. Comparison of trust based RPL mechanism for average residual energy

Time (minutes)	Average residual energy(mJoules)			
	Metric-based RPL Trustworthiness Scheme (MRTS) [21]	C Trust-RPL[8]	MSHOP [23]	Proposed trust mechanism
1	1	1	1	1
2	0.99	0.99	1	1
3	0.94	0.98	0.99	0.99
4	0.91	0.97	0.99	0.99
5	0.88	0.96	0.97	0.97
6	0.85	0.95	0.97	0.97
7	0.82	0.94	0.95	1.02
8	0.8	0.93	0.95	0.93
9	0.72	0.92	0.93	0.98
10	0.77	0.91	0.93	0.99
11	0.78	0.9	0.91	0.98
12	0.7	0.89	0.91	0.92
13	0.66	0.88	0.90	0.95
14	0.67	0.87	0.88	0.94
15	0.68	0.86	0.88	0.95
16	0.6	0.85	0.87	0.92
17	0.52	0.84	0.85	0.85
18	0.56	0.83	0.85	0.86
19	0.58	0.82	0.83	0.91
20	0.5	0.81	0.83	0.82
21	0.42	0.8	0.81	0.85
22	0.46	0.78	0.79	0.85
23	0.48	0.77	0.78	0.84
24	0.4	0.76	0.77	0.8
25	0.4	0.75	0.76	0.78
26	0.39	0.74	0.76	0.76
27	0.35	0.73	0.75	0.83
28	0.34	0.72	0.74	0.79
29	0.33	0.71	0.72	0.79
30	0.3	0.7	0.72	0.75

possible to identify and remove nodes that are malicious in the network. According to the results obtained after simulation, the proposed method performs better than MRTS and CTrust-RPL in terms of attack detection time, power consumption, and average residual energy. The proposed mechanism used 35% less energy and has a lower average packet loss ratio difference. However, the proposed mechanism supports a huge number of interconnected RPL devices. In the future, research will concentrate on improving scalable and distributed trust-based mechanisms to satisfy the

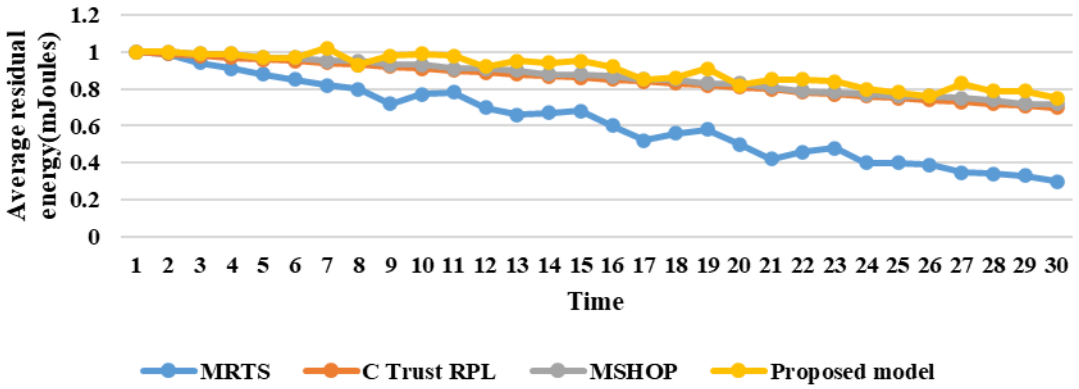

Figure. 10 Average residual energy

increasing demands of distributive IoT deployments, as well as addressing other attacks in RPL networks, such as selective forwarding attacks, rank, and selective forwarding attacks. Additional research would look into the trust model's vulnerabilities by implementing a modified packet format of firefly (FF) optimization algorithm.

Nomenclature

Terms	Representation
T_{SR}	Total success rate of the node
T_{EL}	Energy level of the node
PLR	Packet Loss Ratio
FD	False Detection
P_F	Packets forwarded
P_R	Packets received
E_R	Remaining energy
E_M	Maximum energy
u	belief
b	disbelief
u	uncertainty

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

For this research work all authors' have equally contributed in Conceptualization, methodology, validation, resources, writing—original draft preparation, writing—review and editing.

References

[1] A. Jaleel, T. Mahmood, M. A. Hassan, G. Bano, and S. K. Khurshid, "Towards Medical Data Interoperability Through Collaboration of Healthcare Devices", *IEEE Access*, Vol. 8, pp. 132302-132319, 2020.

[2] M. Zaminkar and R. Fotohi, "SoS-RPL: securing internet of things against sinkhole attack using RPL protocol-based node rating and ranking mechanism", *Wireless Personal Communications*, Vol. 114, No. 2, pp. 1287-1312, 2020.

[3] M. Zaminkar, F. Sarkohaki, and R. Fotohi, "A method based on encryption and node rating for securing the RPL protocol communications in the IoT ecosystem", *International Journal of Communication Systems*, Vol. 34, No. 3, p. e4693, 2020.

[4] M. Conti, P. Kaliyar, M. M. Rabbani, and S. Ranise, "Attestation-enabled secure and scalable routing protocol for IoT networks", *Ad Hoc Networks*, Vol. 98, p. 102054, 2020.

[5] S. Sharma and V. K. Verma, "Security explorations for routing attacks in low power networks on internet of things", *The Journal of Supercomputing*, Vol. 77, No. 5, pp. 4778-4812, 2021.

[6] K. M. Tsiouris, D. Gatsios, V. Tsakanikas, A. A. Pardalis, I. Kouris, T. Androutsou, M. Tarousi, N. V. Sedlar, I. Somarakis, F. Mostajeran, N. Filipovic, H. Akker, D. D. Koutsouris, and D. I. Fotiadis, "Designing interoperable telehealth platforms: bridging IoT devices with cloud infrastructures", *Enterprise Information Systems*, Vol. 14, No. 8, pp. 1194-1218, 2020.

[7] R. K. Das, N. Ahmed, F. H. Pohrmen, A. K. Maji, and G. Saha, "6LE-SDN: An Edge-Based Software-Defined Network for Internet of Things", *IEEE Internet of Things Journal*, Vol. 7, No. 8, pp. 7725-7733, 2020.

[8] T. U. 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",

Transactions on Emerging Telecommunications Technologies, Vol. 32, No. 3, p. e4224, 2021.

[9] I. Haque and D. Saha, "SoftIoT: A resource-aware SDN/NFV-based IoT network", *Journal of Network and Computer Applications*, Vol. 193, p.103208, 2021.

[10] T. Theodorou and L. Mamatas, "SD-MIoT: A Software-Defined Networking Solution for Mobile Internet of Things", *IEEE Internet of Things Journal*, Vol. 8, No. 6, pp. 4604-4617, 2021.

[11] M. Anuradha, T. Jayasankar, N. B. Prakash, M. Y. Sikkandar, G. R. Hemalakshmi, C. Bharatiraja, and A. S. F. Britto, "IoT enabled cancer prediction system to enhance the authentication and security using cloud computing", *Microprocessors and Microsystems*, Vol. 80, p. 103301, 2021.

[12] 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 Computing*, Vol. 24, No. 3, pp. 2133-2160, 2021.

[13] G. Kalyani and S. Chaudhari, "An efficient approach for enhancing security in Internet of Things using the optimum authentication key", *International Journal of Computers and Applications*, Vol. 42, No. 3, pp. 306-314, 2020.

[14] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K. K. R. Choo, "An Energy-Efficient SDN Controller Architecture for IoT Networks With Blockchain-Based Security", *IEEE Transactions on Services Computing*, Vol. 13, No. 4, pp. 625-638, 2020.

[15] B. S. Balaji, P. V. Raja, A. Nayyar, P. Sanjeevikumar, and S. Pandiyan, "Enhancement of Security and Handling the Inconspicuousness in IoT Using a Simple Size Extensible Blockchain", *Energies*, Vol. 13, No. 7, p. 1795, 2020.

[16] A. H. Sodhro, S. Pirbhulal, M. Muzammal, and L. Zongwei, "Towards blockchain-enabled security technique for industrial internet of things based decentralized applications", *Journal of Grid Computing*, Vol. 18, No. 4, pp. 615-628, 2020.

[17] K. Manikannan and V. Nagarajan, "Optimized mobility management for RPL/6LoWPAN based IoT network architecture using the firefly algorithm", *Microprocessors and Microsystems*, Vol. 77, p. 103193, 2020.

[18] M. Šarac, N. Pavlović, N. Bacanin, F. A. Turjman, and S. Adamović, "Increasing privacy and security by integrating a Blockchain Secure Interface into an IoT Device Security Gateway Architecture", *Energy Reports*, Vol. 7, pp. 8075-8082, 2021.

[19] S. Hameed, S. A. Shah, Q. S. Saeed, S. Siddiqui, I. Ali, A. Vedeshin, and D. Draheim, "A scalable key and trust management solution for IoT sensors using SDN and blockchain technology", *IEEE Sensors Journal*, Vol. 21, No. 6, pp. 8716-8733, 2021.

[20] E. M. A. Nassar, A. M. Iliyasu, P. M. E. Kafrawy, O. Y. Song, A. K. Bashir, and A. A. A. E. Latif, "DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems", *IEEE Access*, Vol. 8, pp. 111223-111238, 2020.

[21] 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.

[22] M. Ghaleb, and F. Azzedin, "Trust-Aware Fog-Based IoT Environments: Artificial Reasoning Approach", *Applied Sciences*, Vol. 13, No. 6, p. 3665, 2023.

[23] N. Panda and M. Supriya, "Efficient data transmission using trusted third party in smart home environments", *EURASIP Journal on Wireless Communications and Networking*, Vol. 1, p. 118, 2022.

[24] A. Motmi, S. Alhazmi, A. A. Khadrah, A. A. Mousa, and F. Alhosban, "Trust Management in Industrial Internet of Things using a Trusted E-Lithe Protocol", *International Journal of Advanced Computer Science and Applications*, Vol. 13, No. 2, pp. 334-345, 2022.