

## A trust based secure access control using authentication mechanism for interoperability in internet of things

Shashikala Narayanappa<sup>1</sup>, Tulavanur Narayanareddy Anitha<sup>2</sup>, Priti Mishra<sup>3</sup>, Renuka Patil Herakal<sup>4</sup>, Jayasudha Kolor<sup>5</sup>

<sup>1</sup>Department of Computer Science and Engineering, REVA University and Research Scholar, Affiliated to Visvesvaraya Technological University, Belagavi, India

<sup>2</sup>Department of Computer Science and Engineering, Sir M. Visvesvaraya Institute of Technology, Bengaluru, India

<sup>3</sup>Department of Information Science and Engineering, Atria Institute of Technology, Bengaluru, India

<sup>4</sup>Department of Computer Science and Engineering, GITAM (deemed to be) University, Bengaluru, India

<sup>5</sup>Department of Artificial Intelligence and Machine Learning, Sri Krishna Institute of Technology, Bengaluru, India

### Article Info

#### Article history:

Received Jul 8, 2023

Revised Sep 30, 2023

Accepted Oct 20, 2023

#### Keywords:

Contiki/cool simulator

Internet of things

Interoperability

Routing protocol for low-power and lossy networks

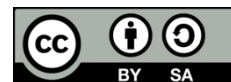
Trust based mechanism

Wireless sensor networks

### ABSTRACT

The internet of things (IoT) is a revolutionary innovation in many aspects of our society including interactions, financial activity, and global security such as the military and battlefield internet. Due to the limited energy and processing capacity of network devices, security, energy consumption, compatibility, and device heterogeneity are the long-term IoT problems. As a result, energy and security are critical for data transmission across edge and IoT networks. Existing IoT interoperability techniques need more computation time, have unreliable authentication mechanisms that break easily, lose data easily, and have low confidentiality. In this paper, a key agreement protocol-based authentication mechanism for IoT devices is offered as a solution to this issue. This system makes use of information exchange, which must be secured to prevent access by unauthorized users. Using a compact contiki/cool simulator, the performance and design of the suggested framework are validated. The simulation findings are evaluated based on detection of malicious nodes after 60 minutes of simulation. The suggested trust method, which is based on privacy access control, reduced packet loss ratio to 0.32%, consumed 0.39% power, and had the greatest average residual energy of 0.99 mJoules at 10 nodes.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



### Corresponding Author:

Shashikala Narayanappa

Department of Computer Science and Engineering, REVA University and Research Scholar, Affiliated to Visvesvaraya Technological University

Belagavi, Karnataka, India

Email: Shashikalan2006@gmail.com

## 1. INTRODUCTION

The interrelated physical devices in a network interact with one another to facilitate smart decision-making by keeping track of analyzing their environment. Organizations focus drastically on the internet for regular communication within the organization as well as long-distance company conferences. Networks or devices in a smart city, industrial automation, and households are now linked to the internet, allowing for faster and more efficient communication [1], [2]. The internet of things (IoT) is used as an information network in most real-world applications. It links multiple devices and system components via enhanced information and communication technology (ICT) and improved embedded devices such as digitalized sensors, meters, and controllers [3]. Wireless sensor networks (WSNs) have greatly enhanced the technology utilization of IoT, which primarily includes gathering and sending information over wireless channels.

IoT based protocols for authentication are suggested to offer user anonymity against malicious users and inactive adversaries to satisfy the security characteristics of the session key, forward secrecy, mutual authentication, and IoT security [4], [5].

The challenge of security 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 like industrial and healthcare domains [6]–[8]. In the real world, safe and secure connections are primary challenges due to the heterogeneity of IoT tools, and the shortage of resources, while some of the resources connected to the internet protocol (IP) hosts are powerful. Furthermore, IoT-connected devices must be secure with authentications like end-to-end (E2E) connections [9]–[11]. 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. The frequent occurrence of IoT attacks results in financial loss or worse. Attestation is a low-cost method of identifying malicious devices. However, providing authentication between device-to-device approaches costs more in terms of authentication time, communication overhead, as well as scalability issues. Therefore, new attestation technologies which are dependable and scalable need to be protected for network operations involving IoT devices [12]–[15]. To normalize and stabilize the security needs of IoT's physical, network, and application layers, energy consumption must be reduced [16]. 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 [17]. Most conventional security methods are not up to snuff to protect the industrial strategies of most firms and business sectors. The root exploit, botnets, spyware, worm, and Trojan are some of the critical IoT security issues to be dealt with [18]. Different IoT devices has different security requirements such as security built into the device, security of information communications, information storage inside frameworks, and its application [19], [20]. Poor security measures lead to the cause of various attacks in the network which prevents packets from being received at the border route. The packet distribution in the network is mostly influenced by the black hole attacks and sinkhole attacks [21]. The black hole attacks happen when an attacker node acts as a single node. The sinkhole attacks occur when the intruder attempts to attract possible paths allowing him to control the circulation of data in the network. Due to these attacks, the energy efficiency of the nodes will be reduced which results in the less data packets delivery [22]. The objective of these attacks is to tamper the neighbourhood which affects the routing operations, getting more resources, and exploitation. Hence to overcome these attacks, a secure routing protocols must be developed to avoid attacks and eliminate malicious nodes from the network. The improvement of quality of service (QoS) parameters such as latency, delivery of packets, resource utilization and so on, can also enhance the networks routing [23], [24].

Some of the existing researches based on IoT interoperability are described as: Anuradha *et al.* [25] 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, this approach was not suitable to detect all types of cancer-related to blood, skin, breast, and lungs. Abbasi *et al.* [26] 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 is high with this service-oriented framework. However, this framework did not help operate communications between dependent services and applications. For further investigation, artificial intelligence (AI) techniques can improve the overall procedure of trust measurements.

Gali and Nidumolu [27] presented a chaotic bumble bees mating optimization (CBBMO) for secure data transmission with trust sensing model (CBBMOR-TSM) to design trust model with secure routing. The bumble bees mating optimization (BBMO) is stimulated by the mating nature of a swarm of bumble bees. To improve the convergence rate of the BBMO technique, the CBBMO model is defined by the integration of chaotic concept into the classical BBMO technique. This method has achieved better results in detecting malicious nodes and also in developing secure routing path with trust parameters. However, due to limited IoT resources in this method, there is drawback in performing data aggregation. Dhurandher *et al.* [28] presented a cooperative and feedback-based trustable energy-efficient routing protocol (CFTEERP) to overcome the issues in generic data communications due to complex security algorithms. This protocol calculates local trust value (LTV) and global trust value (GTV) of each node using node attributes and K-means-based feedback evaluation procedures. With the proposed protocol, the method has achieved better

results in building energy and trust routing path but efficient trust validations are not carried out which is a major drawback. Zhang *et al.* [29] presented an energy-efficient multilevel secure routing (EEMSR) protocol to consider clustering for reasonable solution of conserving energy. A cluster-based multihop routing protocol was utilized to reduce the high communication overhead due to the scalability of IoT networks. This approach has achieved better results in achieving an energy-efficient and secure routing but there is a high latency requirement in IoT applications, which is a major drawback.

Djedjig *et al.* [30] metric-based routing protocol for low-power and lossy networks (RPL) trustworthiness scheme (MRTS) to address the issues of security concerns in RPL by evaluating trust parameters and developing a secure routing network. According to simulations, the proposed approach was effective by means of throughput, energy usage, rank changes of nodes, and packet delivery ratio. Additionally, a mathematical modeling analysis demonstrates that trust based routing has the isotonicity and monotonicity qualities necessary for routing and that MRTS satisfies the consistency, optimality, and loop-freeness requirements. It is claimed that MRTS can be used as a technique for the repeated dilemma of prisoner's and that this will show its cooperative enforcement characteristic. MRTS needs to meet further requirements, like movement, and have its services tested towards different trust thresholds. The RPL protocol has been protected from insider attacks, according to Hassan *et al.* [31], who provided a variety of trust-based techniques. As a result, a hierarchical trust-based technique called CTrust-RPL was recommended for evaluating node trust based on their forwarding actions. 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.

Boualam *et al.* [32] suggested an efficient and secure RPL with an improved Diffie-Hellman algorithm to provide authentication and integrity of RPL data. The developed approach employed an objective function to decide the optimal paths precisely. The developed optimal path has achieved better results in transferring packets with required security measures. The security properties of the protocols were specified by using the automatic validation of internet security protocols and applications. The high security level was provided for the secret key exchange among IoT nodes. However, this approach consumed more energy and most of the trust parameters were neglected, which is a limitation of this work. Oukessou *et al.* [33] have introduced an improved uplink throughput and energy efficiency long-range wide area network (LoRAWAN) using 2 hop low energy adaptive clustering hierarchical routing protocol (LEACH). The long range (LoRA) utilize chirp spread spectrum (CSS) technique that utilize wideband linear frequency of chirp pulses to modulate the information of the signal. Moreover, a spreading factor was used to parameterize the values which ranges from 7 to 12. The suggested approach minimizes the energy consumption of nodes by uniformly distributing energy to each node. But, the gateway present in the LoRAWAN cannot respond for both the slots. Hassani *et al.* [34] have introduced multi-constraints-based objective function with adaptive stability (MCAS-OF) to indicate the radio strength, node energy consumption with parent selection approach. The suggested approach considers the stability of the network by utilizing an adaptive threshold by considering multi-constraint metrics. The suggested approach balances the workload among the nodes with minimal latency during packet transmission. However, MCAS-OF does not achieve better result when it was tested on real sky mote platform.

The major contributions to this work are listed: i) A key agreement-based mechanism with authentication provides 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; ii) Secure data access is achieved between 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; iii) To achieve secure information exchange and low computational complexity, a secure access control with the key agreement is introduced into the network. Due to this, only authorized users can access the information. The present manuscript is organized as follows: section 2 describes the proposed methodology of this work. Section 3 illustrates results along with a comparative analysis of performance metrics. Section 4 provides a conclusion of the work.

## 2. METHOD

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 Figure 1. Each layer in the framework is linked with 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 measurements like true value and trust degree. 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 are various important and dependent conditions in which interactions between two or more IoT must be verified.

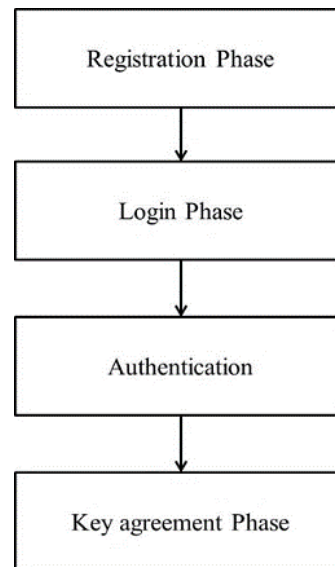


Figure 1. Flow chart of the proposed method

## 2.1. IoT devices

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. Figure 1 represents the scenario of available physical devices in several application domains, where the service domain refers to the geographic area with a different type 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 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.

## 2.2. Registration phase

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 IDs in storage, and preserves all other pertinent data. IoT interactions should therefore be categorized and managed following the registration layer namely service classification, privacy and access control, trust management, and blockchain.

### 2.2.1. Login phase

This module focuses on another major concern among IoT devices i.e., privacy. Since IoT is integrated with human daily life, appropriate preservations of privacy 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. Overall, acquisition issues are resolved. 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.

## 2.3. Authentication phase

The context-aware secure services to requesters in the IoT context and 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. The proposed authentication mechanism enables users for secure communication through IoT devices by

initializing trust parameters in the network. 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. 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. It is more specifically the relationship between the quality 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. By the involvement of a belief theory among the key elements of the node the trust model computes the uncertainty. The proposed model can work efficiently with the binary logic, where the node's energy does not strain in IoT devices. And by utilizing the calculations which are complex over the control layer the adaptive trust parameters, can be determined by terms of packet loss ratio (PLR) and forwarding delay (FD) parameters as input and detects the malicious nodes and remove them from the network by initiating certain parameters as per trust calculation on each node of the network. The PLR and FD are the QoS parameters used for trust calculation as shown in (1) and (2):

- Packet loss rate ( $P_{LR}$ ): it is a ratio of packets dropped ( $P_d$ ) by the receiver nodes to the total packets ( $P_t$ ) from the sender node, which is calculated using (1):

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

- Forwarding delay ( $F_D$ ): the  $F_D$  is the time interval between receiving a packet from the sender and then forwarding it to the next node as shown in (2):

$$F_D = P_R - P_F \quad (2)$$

where,  $P_R$  is the packet received time, and  $P_F$  is packet forwarding time.

The nodes are classified as trusted or untrusted by providing 0.5 threshold value, where trusted nodes used for secure routing and communication. The node trust is updated using a time-based update technique, which can detect rogue nodes in real time while simultaneously addressing high computational challenges and low memory resources. Malicious nodes are removed from the network, and sensor nodes are placed in the test region. The node trust is measured in terms of the success rate of the node as shown in (3) and (4).

$$T_{SR} = \frac{P_F}{P_R} \quad (3)$$

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

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.

#### 2.4. Key agreement phase

After completing the procedure of registration and trust calculation, an IoT intends to request and access a huge range of services accessible on neighboring IoT. This layer serves as the basis for the service management process. This layer stores all data that is relevant to the availability of services in the region. Thus, service handling is inextricably linked with context management to dynamically embrace new availability matrices in response to variations in sharing context-based updates accordingly. The logic used to measure the terms b, u and d is based on the linear relationship between time and the parameters of trust. 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.

### 3. RESULTS

The effectiveness of the proposed trust based framework is evaluated using simulations. In this paper, a contiki/cooja simulator is used for validation. Contiki can be used for high-performance and secure communication between low-powered radio frequency identification (RFID) chips in wireless networks. The proposed model uses attack detection, attack detection time, packet loss ratio, power consumption, and

residual energy parameters to validate our mechanism. The following simulation setup has been used for the evaluation of the proposed model topology as in Table 1.

Table 1. Simulation results of contiki/cooja simulator

Parameter	Value
Area	70×70 m
No. of nodes	30
Tx ratio	%
Rx ratio	30% to 100%
Malicious nodes	28, 29 and 30
Transmission range	50 m
Simulation time	60 minutes

Contiki/cooja simulator is used for the evaluation of the proposed network model, which is an open source and light weight operating system. A total of 30 nodes are considered for evaluating the nodes trust and to detect malicious nodes within the simulation time of 60 minutes. Results show that the proposed mechanism detected three nodes 28, 29, and 30 as a malicious nodes out of 30 nodes. The results are measured in terms of the packet loss ratio, attack detection and its time, power consumption, and residual energy.

### 3.1. Quantitative evaluation

In this section, we compared the existing metric based RPL trustworthiness scheme (MRTS) [26] and C Trust-RPL [27] with the proposed privacy access control-based trust mechanism. These methods are compared 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 proposed firefly optimization technique, the network achieved better results compared to the existing methods.

#### 3.1.1. Attack detection

An exact and accurate detection of a black hole attack at any given time in the network is known as attack detection. The comparison of black hole detection is represented in Figure 2 with the existing methods MRTS and C Trust-RPL. Both methods detected many malicious nodes in the initial stage since there were more malicious entities as shown in Figure 2. 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 C Trust-RPL are given in Table 2.

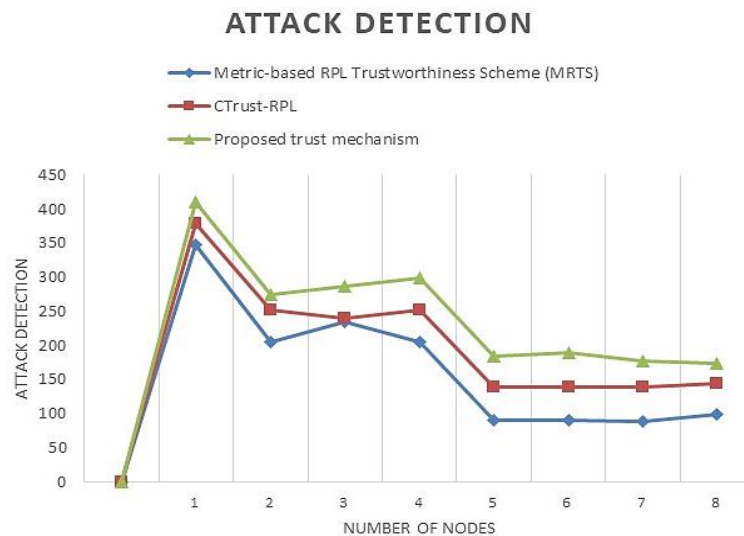


Figure 2. Attack detection

Table 2. Comparison of trust-based RPL mechanism for attack detection of malicious nodes

Malicious nodes	Attack detection		
	MRTS [26]	C Trust-RPL[27]	Proposed trust mechanism
1	348	380	410
2	205	252	275
3	235	240	287
4	205	252	300
5	90	140	185
6	90	140	190
7	89	140	178
8	99	145	175
9	85	130	155
10	90	140	184

**3.1.2. Attack detection time**

The efficiency of the proposed model in detecting attacks in less time is compared with the existing methods of MRTS and C Trust-RPL. Figure 3 shows the graphical representation of attack detection time compared to the proposed modified firefly algorithm. Initially, for one malicious node, the attack detection time is shown and then increased one by one in order. In Figure 3, 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. Table 3 shows a comparison of trust-based RPL mechanisms for attack detection time.

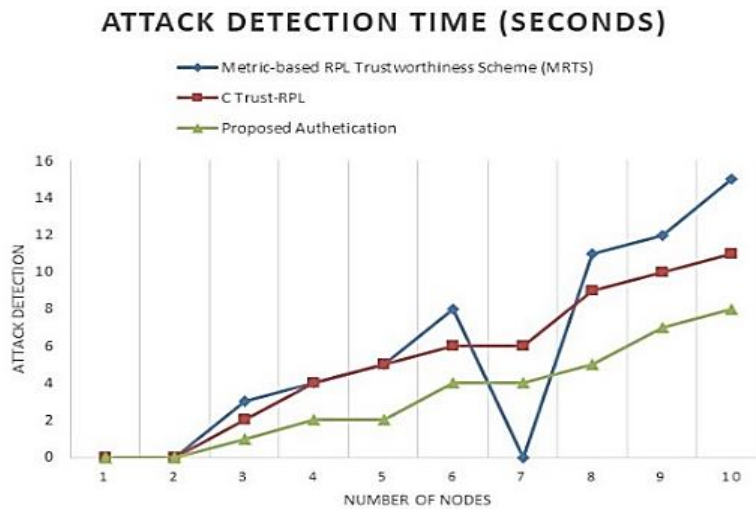


Figure 3. Attack detection time

Table 3. Comparison of trust based RPL mechanism for attack detection time

Number of Attacks	Attack detection time (seconds)		
	MRTS [26]	C Trust-RPL [27]	Proposed trust mechanism
1	0	0	0
2	3	2	1
3	4	4	2
4	5	5	2
5	8	6	4
6	0	6	4
7	11	9	5
8	12	10	7
9	15	11	8
10	18	14	8

**3.1.3. 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 Figure 4. Figure 4 shows the comparison of existing methods'

packet loss ratio to the proposed method. The existing methods MRTS and C Trust-RPL are compared with the proposed trust based privacy access control mechanism. The packet loss ratio of 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 10 is 0.32, 0.49 for MRTS [26], and 0.39 for C Trust RPL [27]. Thus, the proposed framework has given a better defense mechanism against black hole attacks with less packet loss ratio. Table 4 shows the comparison of trust based RPL mechanism for packet loss ratio.

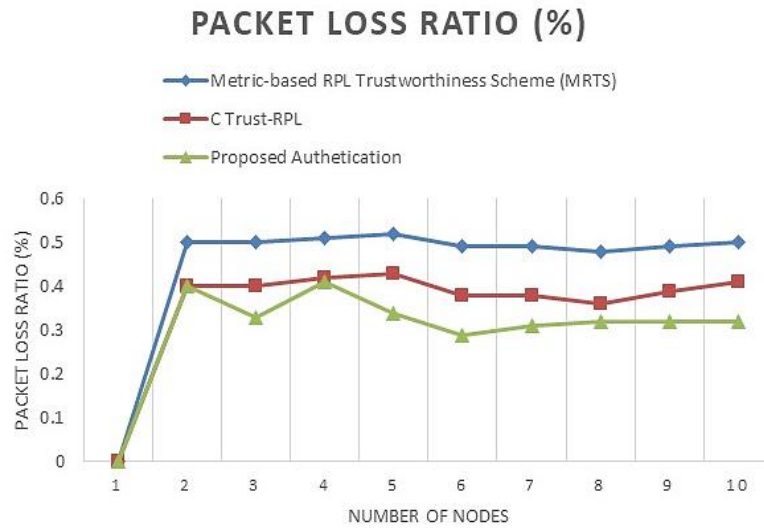


Figure 4. Packet loss ratio

Table 4. Comparison of trust based RPL mechanism for packet loss ratio

Number of Nodes	Packet loss ratio (%)		
	MRTS [26]	C Trust-RPL [27]	Proposed trust mechanism
1	0.50	0.40	0.40
2	0.50	0.40	0.33
3	0.51	0.42	0.31
4	0.52	0.43	0.34
5	0.49	0.38	0.29
6	0.49	0.38	0.31
7	0.48	0.36	0.32
8	0.49	0.39	0.32
9	0.50	0.41	0.32
10	0.49	0.39	0.32

**3.1.4. Power consumption**

The proposed trust based mechanism achieved less power consumption compared to the existing methods MRTS and C Trust-RPL. The power 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 an attached mitigation mechanism, the power consumption is less. Figure 5 shows the graphical representation of the power consumption of the proposed method in comparison to the existing methods. Table 5 represents power consumption values for the 10 nodes in the network.

**3.1.5. 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 C Trust-RPL. The average residual energy of the proposed method is 0.87 mJoules and the existing methods MRTS and C Trust-RPL are 0.3 and 0.7 mJ. Table 6 shows the average residual energy values and its graphical representation is shown in Figure 6.



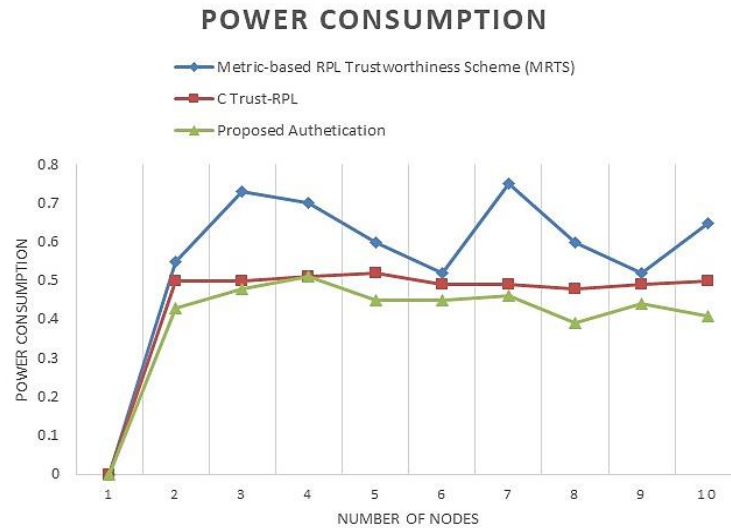


Figure 5. Power consumption

Table 5. Comparison of trust based RPL mechanism for power consumption

Number of Nodes	Power consumption		
	MRTS [26]	C Trust-RPL [27]	Proposed trust mechanism
1	0.55	0.5	0.43
2	0.73	0.5	0.48
3	0.7	0.51	0.51
4	0.6	0.52	0.45
5	0.52	0.49	0.45
6	0.75	0.49	0.46
7	0.6	0.48	0.39
8	0.52	0.49	0.44
9	0.65	0.5	0.41
10	0.75	0.49	0.39

Table 6. Comparison of trust based RPL mechanism for Average residual energy

Time (minutes)	Average residual energy (mJoules)		
	MRTS [26]	C Trust-RPL [27]	Proposed trust mechanism
1	1	1	1
2	0.99	0.99	1
3	0.94	0.98	0.99
4	0.91	0.97	0.99
5	0.88	0.96	0.97
6	0.85	0.95	0.97
7	0.82	0.94	1.02
8	0.8	0.93	0.93
9	0.72	0.92	0.98
10	0.77	0.91	0.99

### 3.2. Discussion

From the results, it is analysed that the proposed method has the capability of providing authentication in IoT devices by using key agreement protocol. Trust evaluation, privacy preserving and energy consumption of nodes are problem in existing secure RPL protocols. Proposed method has the authentication mechanism for trust evaluation, key based agreement for privacy preserving and due to reduced redundancy energy consumption also reduced further. From the comparison with the existing methods, MRTS [26] has limitations such as movement, and have its services tested towards different trust thresholds. The C Trust-RPL [27] has a limitation of low scalability-based approach in terms of trust parameters. These limitations are overcome by adding more scalable trust parameters in the network of IoT devices. Even though, the proposed approach has contributed to develop the energy efficient and secure routing in IoT devices, it still has ramifications such as prevention of black holes and data loss. The future work focuses of preventing and mitigating black hole attacks and data loss before occurring in the network.

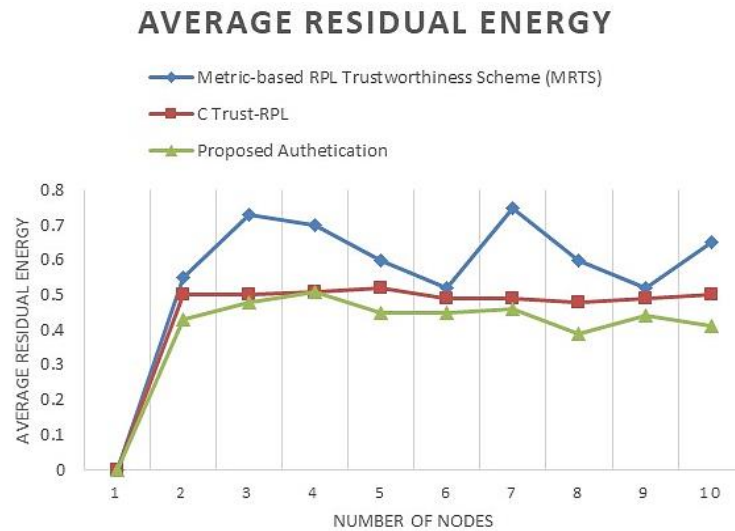


Figure 6. Average residual energy

#### 4. CONCLUSION

An energy-efficient, trust based interoperability framework for identifying and isolating black hole attacks is included in the proposed RPL routing protocol. To preserve the limited IoT devices' energy, a control layer computed the trust values. Using the privacy access control to observe the exchange of packets between the nodes, it was 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 C Trust-RPL in terms of attack detection time, power consumption, and average residual energy. The proposed mechanism used 35% less energy and had a lower average packet loss ratio difference. However, the proposed mechanism supports a huge number of devices such as RPL which are interconnected. In the future, research will concentrate on improving more scalable and distributed trust-based mechanisms to satisfy the increasing demands of distributive IoT deployments, as well as addressing other attacks in RPL networks, such as selective forwarding attacks, rank, and black holes. Future research focuses on developing a lightweight communication to secure data against disruptions in data transmission.





#### REFERENCES

- [1] C. K. Rath, A. K. Mandal, and A. Sarkar, "Microservice based scalable IoT architecture for device interoperability," *Computer Standards and Interfaces*, vol. 84, Mar. 2023, doi: 10.1016/j.csi.2022.103697.
- [2] E. E. K. Senoo, E. Akansah, I. Mendonça, and M. Aritsugi, "Monitoring and control framework for IoT, implemented for smart agriculture," *Sensors*, vol. 23, no. 5, Mar. 2023, doi: 10.3390/s23052714.
- [3] M. Zaminkar, F. Sarkohaki, and R. Fotuhi, "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, Nov. 2021, doi: 10.1002/dac.4693.
- [4] S. M. Muzammal, R. K. Murugesan, N. Z. Jhanjhi, M. S. Hossain, and A. Yassine, "Trust and mobility-based protocol for secure routing in internet of things," *Sensors*, vol. 22, no. 16, Aug. 2022, doi: 10.3390/s22166215.
- [5] S. Sharma and V. K. Verma, "Security explorations for routing attacks in low power networks on internet of things," *Journal of Supercomputing*, vol. 77, no. 5, pp. 4778–4812, Oct. 2021, doi: 10.1007/s11227-020-03471-z.
- [6] M. Alotaibi, "Improved blowfish algorithm-based secure routing technique in IoT-based WSN," *IEEE Access*, vol. 9, pp. 159187–159197, 2021, doi: 10.1109/ACCESS.2021.3130005.
- [7] S. Awan, N. Javaid, S. Ullah, A. U. Khan, A. M. Qamar, and J. G. Choi, "Blockchain based secure routing and trust management in wireless sensor networks," *Sensors*, vol. 22, no. 2, Jan. 2022, doi: 10.3390/s22020411.
- [8] K. Haseeb, A. Rehman, T. Saba, S. A. Bahaj, and J. Lloret, "Device-to-device (D2D) multi-criteria learning algorithm using secured sensors," *Sensors*, vol. 22, no. 6, Mar. 2022, doi: 10.3390/s22062115.
- [9] I. Haque and D. Saha, "SoftIoT: A resource-aware SDN/NFV-based IoT network," *Journal of Network and Computer Applications*, vol. 193, Nov. 2021, doi: 10.1016/j.jnca.2021.103208.
- [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, Mar. 2021, doi: 10.1109/JIOT.2020.3027427.
- [11] A. Kore and S. Patil, "Reliable and secure data transmission in smart healthcare application of internet of things," *2021 IEEE Bombay Section Signature Conference, IBSSC 2021*, Nov. 2021, doi: 10.1109/IBSSC53889.2021.9673462.
- [12] G. K. Ragesh and A. Kumar, "Trust-based secure routing and message delivery protocol for signal processing attacks in IoT applications," *Journal of Supercomputing*, vol. 79, no. 3, pp. 2882–2909, Aug. 2023, doi: 10.1007/s11227-022-04766-z.
- [13] M. Šarac, N. Pavlović, N. Bacanin, F. Al-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, Nov. 2021, doi: 10.1016/j.egy.2021.07.078.




- [14] S. Hameed *et al.*, “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, Mar. 2021, doi: 10.1109/JSEN.2021.3052009.
- [15] 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, Sep. 2022, doi: 10.3390/s22187052.
- [16] P. Singh, M. Khari, and S. Vimal, “EESMT: An energy efficient hybrid scheme for securing mobile ad hoc networks using IoT,” *Wireless Personal Communications*, vol. 126, no. 3, pp. 2149–2173, Aug. 2022, doi: 10.1007/s11277-021-08764-x.
- [17] K. S. Alshudukhi, M. A. Khemakhem, F. E. Eassa, and K. M. Jambi, “An interoperable blockchain security frameworks based on microservices and smart contract in IoT environment,” *Electronics (Switzerland)*, vol. 12, no. 3, Feb. 2023, doi: 10.3390/electronics12030776.
- [18] A. Kumar *et al.*, “Revolutionary strategies analysis and proposed system for future infrastructure in internet of things,” *Sustainability (Switzerland)*, vol. 14, no. 1, Dec. 2022, doi: 10.3390/su14010071.
- [19] N. Shashikala and M. R. Mundada, “Internet of things (IoT) for secure data and M2M communications—a study,” in *Lecture Notes on Data Engineering and Communications Technologies*, vol. 139, Springer Nature Singapore, 2023, pp. 13–28.
- [20] N. Shashikala and M. R. Mundada, “Secured communication strategies for internet of things sensors,” *3rd IEEE International Virtual Conference on Innovations in Power and Advanced Computing Technologies, i-PACT 2021*, Nov. 2021, doi: 10.1109/i-PACT52855.2021.9696487.
- [21] N. H. Kamis, W. Yassin, M. F. Abdollah, S. F. A. Razak, and S. Yogarayan, “Blackhole attacks in internet of things networks: a review,” *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 30, no. 2, pp. 1080–1090, May 2023, doi: 10.11591/ijeecs.v30.i2.pp1080-1090.
- [22] S. W. Nourillean, M. D. Hassib, and Y. A. Mohammed, “Internet of things based wireless sensor network: a review,” *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 27, no. 1, pp. 246–261, Jul. 2022, doi: 10.11591/ijeecs.v27.i1.pp246-261.
- [23] H. F. Jassim, M. A. Tawfeeq, and S. M. Mahmoud, “Overlapped hierarchical clusters routing protocol for improving quality of service,” *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 19, no. 3, pp. 705–715, Jun. 2021, doi: 10.12928/TELKOMNIKA.v19i3.18354.
- [24] B. H. Patel and P. Shah, “RPL routing protocol performance under sinkhole and selective forwarding attack: Experimental and simulated evaluation,” *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 18, no. 4, pp. 1849–1856, Aug. 2020, doi: 10.12928/TELKOMNIKA.V18I4.15768.
- [25] M. Anuradha *et al.*, “IoT enabled cancer prediction system to enhance the authentication and security using cloud computing,” *Microprocessors and Microsystems*, vol. 80, Feb. 2021, doi: 10.1016/j.micpro.2020.103301.
- [26] M. A. Abbasi, Z. A. Memon, N. M. Durrani, W. Haider, K. Lacey, 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, Feb. 2021, doi: 10.1007/s10586-021-03243-1.
- [27] S. Gali and V. Nidumolu, “An intelligent trust sensing scheme with metaheuristic based secure routing protocol for Internet of Things,” *Cluster Computing*, vol. 25, no. 3, pp. 1779–1789, Nov. 2022, doi: 10.1007/s10586-021-03473-3.
- [28] S. K. Dhurandher, J. Singh, P. Nicopolitidis, R. Kumar, and G. Gupta, “A blockchain-based secure routing protocol for opportunistic networks,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 4, pp. 2191–2203, Mar. 2022, doi: 10.1007/s12652-021-02981-9.
- [29] Y. Zhang, Q. Ren, K. Song, Y. Liu, T. Zhang, and Y. Qian, “An energy-efficient multilevel secure routing protocol in IoT networks,” *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 10539–10553, Jul. 2022, doi: 10.1109/IIOT.2021.3121529.
- [30] 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, Jun. 2020, doi: 10.1016/j.jisa.2020.102467.
- [31] 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,” *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 3, Jan. 2021, doi: 10.1002/ett.4224.
- [32] S. R. Boualam, M. Ouaisa, M. Ouaisa, and A. Ezzouhairi, “Secure and efficient routing protocol for low-power and lossy networks for IoT networks,” *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 27, no. 1, pp. 478–487, Jul. 2022, doi: 10.11591/ijeecs.v27.i1.pp478-487.
- [33] Y. Oukessou, M. Baslam, and M. Oukessou, “Improved uplink throughput and energy efficiency of LoRaWAN using 2-hop LEACH protocol,” *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 24, no. 3, pp. 1557–1563, Dec. 2021, doi: 10.11591/ijeecs.v24.i3.pp1557-1563.
- [34] A. E. Hassani, A. Sahel, A. Badri, and E. M. Ilham, “Multi-Constraints based RPL objective function with adaptive stability for high traffic IoT applications,” *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 22, no. 1, pp. 407–418, Apr. 2021, doi: 10.11591/ijeecs.v22.i1.pp407-418.

## BIOGRAPHIES OF AUTHORS






**Shashikala Narayanappa**     received M. Tech degree in computer science and engineering from VTU, Belagavi, India in 2013. I am currently pursuing Ph.D. degree in VTU, Belagavi, India. My research interest includes internet of things, wireless sensor networks, and security. Her membership in professional bodies is: life time membership in MIE, IEEE, CSI, CRSI. She can be contacted at email: Shashikalan2006@gmail.com.






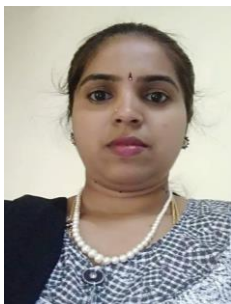
**Tulavanur Narayanareddy Anitha**    has 24 years teaching and research experience in the field of computer science and engineering and served in different colleges since 1997. Currently She is serving as Professor and HOD in the Department of Computer Science and Engineering, Sir M. Visvesvaraya Institute of Technology, Bangalore, Karnataka. She was awarded Ph.D. degree in “an efficient and scalable dynamic load balancing using multi parameters on load aware distributed multi cluster servers” by Visveswaraiiah Technological University, Belagavi in 2016. She is appointed as Referee for Ph.D. examination at the Visveswaraiiah Technological University and Reva University, Bangalore March 2017. She has received recognition as GUIDE for Ph.D. program under computer science and engineering from VTU, in January. 2017. She has published 40 research papers in reputed international and Indian research journals in UGC Care Group – I and Group –II lists under SCOPUS and other Journals, Google Scholar and has been a part of various workshops and seminars conducted all over Karnataka. She has a life membership on CSI, ISTE, FIE and IFERP. She is a member of board of examiner in Visveswaraiiah Technological University. She has been invited as speaker/resource person/subject expert at Faculty/Session Chair for international conference at various Engineering Colleges in Karnataka. She is been invited as External Examiner for Theory & Practical Examinations at various Engineering Colleges in Karnataka associated with various universities such as Reva University, Visveswaraiiah Technological University, Autonomous University. She is an active member of advisory board, editorial board member of international research journals of India, Springer and IJCS. She has supervised many graduates, post-graduate students and research scholars for the research and projects fulfilment of their degree program. She has published book chapters in national/international books. Dr. T N Anitha has received Best Researcher awards from I2OR and Green ThinkerZ. She can be contacted at email: Anithareddytn72@gmail.com.






**Priti Mishra**    earned a bachelor's degree in information science and engineering from SRSIT College of Engineering in Bangalore, which is affiliated with VTU. MVJ College of Engineering, affiliated to VTU, Bangalore, and Maharaj Vinayak Global University, Jaipur, respectively, with a PG in computer science & engineering and a Ph. D in computer science, with a focus on network security. She's been a teacher for the past 18 years. She has authored several books and published paper in national and international journals and has presented papers in international and national conferences. There are 2 scholars who have been awarded under her guidance. She is currently employed in East West College of Engineering, Bangalore, as a professor and HOD in the Department of Computer Science and Engineering. She can be contacted at email: mpriits@redifmail.com.



**Renuka Patil Herakal**    is working as an Asst. Professor in Department of Computer Science and Engineering at GITAM (Deemed to be) University, Bangalore, Karnataka, INDIA. She has completed M. Tech (CSE) under VTU in the year 2013 and Ph. D. under VTU in the field of WSN and AI & ML. She has an experience of 13 years in teaching. She has published 13 papers in international journals and 4 papers in international conference. Her areas of interest are wireless sensor networks, artificial intelligence, machine learning, cloud computing and natural language processing. She can be contacted at email: rherakal@gitam.edu.



**Jayasudha Kolor**    has 20 years teaching experience in various colleges since 1998. Currently She is serving as “Associate Professor” in Atria Institute of Technology, Bangalore, and Karnataka. She was awarded Ph.D. degree in “Development of Multilayer Soft Tissue Model for Applications in Virtual Surgery” by Visvesvaraya Technological University, Belagavi in 2021. She has published various research papers in reputed international research journals, also in UGC Care Group – I and Group-II lists under Scopus journals, Google Scholar and has been a part of various workshops, seminars and Faculty Development Programs attended and conducted. She has published book and book chapters in national/international books. She has one patent filed and published. Her membership in professional bodies is: life time membership in ISTE, CSI, CRSI and professional membership in IFERP (Institute for Engineering Research and Publication). She can be contacted at email: jayasudhakaiml@skit.org.in.