J. Integr. Sci. Technol. 2023, 11(1), 431 Article

Journal of Integrated
SCIENCE & TECHNOLOGY

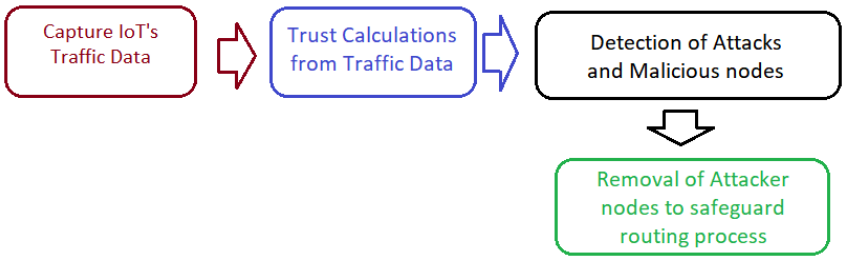
Trust based secured Routing system for low powered networks

Anup W. Burange, Vaishali M. Deshmukh*

Computer Science and Engineering Department, Prof. Ram Meghe Institute of Technology & Research, Badnera, Amravati, Maharashtra 444701. India

Received on: 10-Jul-2022, Accepted and Published on: 07-Oct-2022

ABSTRACT



The number of internet-connected IoT devices is increasing at a rapid speed. Because of this exponential growth, there are now some serious security concerns and challenges. As most of these devices are part of our daily activities, they contain personal private data which is getting transferred to some other location. When many IoT devices are in a network, they transfer the data on a hop-by-hop basis, which raises concerns about the routing security and trustworthiness of other IoT devices on which they are dependent for transferring their data. The goal of this study is to develop a safe environment for routing with the help of a trust analysis of each node participating in the network. Routing nodes are prone to some routing attacks like the Rank attack, wormhole attack, and Sybil attack. In this study, a lightweight trust-based system has been developed to detect and remove these attacks. The proposed model consists an accuracy of 98%. Moreover, proposed model is compared with earlier studies, proposed model's performance stands remarkable.

Keywords: Trust framework, Rank attack, Wormhole attack, Sybil Attack

INTRODUCTION

Considering Low Power Lossy Networks, one of the most important security requirements is a safe and reliable routing method due to the networks' inherent power and loss limitations.[1] For LLNs, the Routing Protocol for Low Power and Lossy Networks, i.e. (RPL), is one of the most suitable and most used routing protocols.[2] This protocol incorporates cryptography-based approaches for control messages' dependability and privacy against outside attackers. Attacks from malicious nodes represent a significant threat to the continued existence of IoT devices and the apps that depend on them.[3] The exponential rise in the number of Internet-enabled gadgets has opened the door to previously unexplored security holes. Use of IoT systems in every corner of the home raises the possibility that they will be subject to more severe attacks. Recent research has revealed that the existing RPL protocol is vulnerable to numerous routing attacks. These include the Rank attack, Sybil attack, Sinkhole attack, Blackhole attack, Version Number attack, and more. Also, research should be done to make sure that trust solutions for limited devices, like IoT, can be scaled up to work for billions of devices. Although many methods have been devised to address RPL security issues, they all have drawbacks that render them inadequate when used on resource-limited devices. Intrusion detection systems are also used to combat network attacks by monitoring network behaviour and flagging nodes that exhibit malicious activity.[4] It is crucial to design lightweight IDS for analysis and detection of harmful behaviour because studies reveal that typical IDS systems demand a great deal of resources, making them unsuitable for these types of networks where devices have restricted capabilities. Popular and tried-and-true security methods like encryption are hard to use because they require a lot of computing power and have few real-world uses.[5] More study is required to safeguard the routing process and routing judgments and to develop methods of protecting resource-limited devices from routing attacks. Due to the nature of RPL, research has thus far only focused on static systems, although mobility and detecting the energy level of nodes are two of the most challenging research motivations.[6,7] There is room for exciting discovery at the intersection between energy use at each node and the design of a novel mobility feature. Due to the growing number of devices and the wide range of devices being used, it is hard to ensure security

*Corresponding Author: Dr. V.M. Deshmukh
Email: awburange@mitra.ac.in (AWD), vmdeshmukh@mitra.ac.in (VMD)

Cite as: *J. Integr. Sci. Technol., 2023, 11(1), 431.*
URN:NBN:sciencein.jist.2023.v11.431

 ISSN: 2321-4635
http://pubs.thesciencein.org/jist

and secure routing in LLN.[8] The remaining chapters of the paper are organised as follows. Section on “Trust Management” describes work available related to it. Section on “Attacks in RPL Network” describes different attacks that are possible on the RPL network. Another section called “Related Work” elaborates the work done for making network routing secure. Section “Proposed Work” provides details on the proposed work. Section “Attack Detection and Isolation” algorithms are proposed for Rank, Wormhole and Sybil attacks. Experimental results, and Discussion on results are reported in next sections.

TRUST MANAGEMENT

Autonomous decision-making by devices is crucial to the future of 6LoWPAN networks, hence trust management is also important. In the same way that we use trust to characterise the nature of our interpersonal relationships, computer networks employ the term "trust" to describe the actions of one node toward another. In this regard, various researchers have proposed different models to establish trust between the nodes so as to develop trustworthy communication between them.[9,10]

A mathematical model was developed by Nabil Djedjig et al., which is named the Metric based RPL trustworthiness scheme (MRTS). It is described that the suggested technique is consistent, optimum, and does not create loops. With its cooperative trust mechanism, MRTS takes into account indirect recommendations as well as assessments of the behaviour of surrounding nodes. This protocol has some limitations, such as relying on node metric to determine the optimum way and not considering link metric, which in turn decreases the packet delivery ratio, an essential criterion for route reliability. Additionally, they added the Expected Transmissions per Exchange (ETX) extension to their protocol. They did not take into account the possibility of reintegrating previously recognised as untrusted nodes due to their lower energy into their network.[11]

The detection of malicious nodes and the potential for an On-Off attack, in which a node behaves both good and bad at different times, compromising the network, Carolina V.L. Mendoza et al. proposed a trust management model that makes use of direct trust gained through direct communication between nodes. The suggested system is decentralised, meaning decisions are made without reference to a single point of control. How many bad actors are in a network, where they are located, and how much traffic there is all play a role in spotting an attack. Cooja, a simulator built into Contiki OS, serves as the foundation for the system. Because they haven't considered recommendations from neighbours, they've judged trustworthiness only based on personal observation. Bad mouthing and selective forwarding attacks are two areas where the system might be improved.[12]

In order to determine which nodes to prioritise when determining the best possible route, Upul Jaysinghe et al. suggested a machine learning-based methodology to compute the trust value of nodes. They do a trust analysis on several properties of a real-world dataset. Their methodology is generic enough to be used in a wide variety of domains, including smart homes, smart parking systems, and more. They construct their model with the pillars of knowledge, expertise, and credibility as their foundation. They did tasks like feature extraction, grouping, labelling, and classification. Unsupervised learning is used to assign confidence labels to data. The trust thresholds are then used in an SVM-based trust prediction model to yield an overall trust score.[13]

Weizhi Meng elaborated on the role that traffic filtering and sampling play in determining an IoT device's reliability. Protecting IoT networks from a node that has authorised system access requires early trust map development. They have built a trust management strategy based on a Bayesian model that evaluates a packet’s state and traces a malicious node in terms of threshold. After realising that the aforementioned system would struggle under heavy traffic, they devised traffic filtration and traffic sampling to cut down on the number of packets. The Bayesian model is used for the trust assessment. They also noted some of the limitations of their model and potential workarounds.[14]

The study done by Seyyed Yasser Hashemi et al. proposes a thorough and flexible trust framework for the Internet of Things. The model takes into account service quality, contextual information, and peer-to-peer communication quality. However, they aren't the only dimensions the model can account for. Trust is determined by in-person interactions and word-of-mouth from the locals. The proposed method also makes use of separate and tacit processes to identify potentially harmful objects. To achieve a wide variety of objectives, the proposed model can be applied in a number of settings. As part of this work, they incorporated the trust model into RPL. They made use of the trust level in the RPL object function. The Cooja emulator running on Contiki 3.0 OS is used to test and evaluate the suggested method, and results are compared to those obtained utilising similar protocols. To a great extent, the suggested DCTM-RPL indicates the overall improvements in factors such as the number of parent changes, the packet loss percentage, the latency between send and receive, and the energy spent on average, compared to current protocols. It can also resist significant Sybil, Rank, and Blackhole attacks.[15]

ATTACKS ON RPL NETWORK

WORMHOLE ATTACK

This attack aims to cause chaos in the network's infrastructure and traffic patterns. It is possible to carry out this attack by establishing a tunnel between the two attackers and routing all traffic through it. A wormhole is an out-of-band link established between two nodes over an electrical or wireless medium. Packets can be forwarded much faster through wormholes than through traditional channels.[16,17] With the help of node locations and neighbor information, the unique intrusion detection system provided by Pavan Pongale et al. can identify wormhole attacks. This method uses the intensity of the received signal in order to identify a malicious or attacking node in a network. They proposed a hybrid architecture with certain modules centrally located on the 6BR and others dispersed among sensor nodes. Knowing your physical location can aid in spotting a Sybil attack. Only stationary nodes are taken into account. However, the system is said to be very efficient thanks to its low energy overhead and high true positive rates. The RPL network can be watched for attacks by adding more modules to this system.[18]

An intrusion detection system was created by Snehal Deshmukh Bhosale et al. to identify wormhole attacks and their perpetrators. In order to identify harmful nodes, they relied solely on the strength of the incoming signal. The deployed IDS is a hybrid one, meaning it combines central and decentralized components. Both a centralized and a distributed module can identify an assault on a network node. Using the Contiki operating system's cooja simulator, this method has a purported 90% success rate.[19] While sensor networks can take steps to ensure authenticity and confidentiality, they are nevertheless vulnerable to wormhole attacks. Due to their stealth capabilities, wormhole attacks pose a significant threat to WSNs and must be prevented. Due to the versatility of wormhole attacks, Rupinder Singh et al. offer a hybrid approach to detecting such attacks in wireless sensor networks (WSNs) called the wormhole resistant hybrid technique (WRHT). The suggested method incorporates aspects of both the watchdog and Delphi techniques. The proposed techniques draw upon the most useful aspects of both the Delphi and watchdog approaches. For the wormhole to be dealt with by the sensor network, WRHT employs a dual-detection strategy. Results from simulations show that the recommended approach is superior to the alternatives. The WRHT system can be added to existing sensor networks without any extra hardware or questionable network assumptions.[20]

Rank Attack

The Rank attack is a particular sort of traffic misappropriation attack. Malicious nodes will transmit DIO packets to their neighbors, claiming to be lower in rank than the other nodes. Rank 1 attackers can do significant damage to the network since DIO is the initial stage in DODAG production. The effect is that the neighbour nodes update their routing databases. As a result, the network suffers from the introduction of undesirable latency. Rank-based attacks hurt the performance of a network by making it take longer for packets to get from one end to the other, by reducing the number of packets that are delivered, and by increasing the amount of energy that network devices use by creating unoptimized pathways, loops, overhead, and more packet collisions.[21]-[22] Usman Shafique et al. propose a novel sink-based intrusion detection system that can accurately identify malicious nodes. Due to the central location of detection in this system, it requires less processing power to run. A thorough simulation study of SBIDS shows that it can be used to find rank attacks in RPL networks.[23] The Secure RPL Routing Protocol (SRPL-RP), proposed by Zahrah A. Almusaylim and others, reduces the vulnerability of RPL networks to rank and version number attacks. Simulation results from the study confirm that the proposed SRPL-RP enhances network safety, throughput, and accuracy. Extensive testing on many different network architectures showed that SRPL-RP consistently beats the best current countermeasures in terms of packet delivery ratio (PDR) and control message value. Also, this protocol has been shown to work well across a wide range of network architectures with an accuracy of more 95%.[24]

In the study led by Wijdan Choukri, a Deep Learning-based intrusion detection system (IDS) was introduced to monitor for rank attacks in the RPL protocol. This research is viewed as proof that the problem of intrusion detection on the Internet of Things can be resolved with artificial neural networks. The dataset was acquired using the Cooja simulator, and after development and evaluation, the ANN-based strategy showed excellent performance, with an accuracy of up to 96%, a 98% F1 score, and a 100% recall. The results demonstrate the potential of using an ANN method for identifying RPL protocol abuse.[25]

Sybil attack

The Sybil attack poses the greatest risk to mobile RPL because it can drastically limit performance by drastically increasing the amount of control overhead communication, which in turn drastically decreases the network's lifetime. A malicious attacker can simply impersonate a legitimate node by stealing its identity, and Then, they try to steal the BR's identity by interfering with the routing protocol, flooding the DODAG with fake control messages, and eventually taking over the network. Sybil attacks can be the cause of attacks like selective forwarding, denial of service, ranking, and version number attacks.[26]

For the purpose of preventing Sybil and Denial of Service (DoS) attacks on RPL networks in the IoT, Ashwini Nikam et al. offer an intrusion detection system that makes use of opinion metrics as an identifying technique. Based on its history of positive and negative interactions with data traffic transmission, the proposed mechanism assigns a value to each node's opinion metric. The node at the border router collects metrics and uses them to determine the location of the intrusion. Simulations and graphs of the results show that the method presented is a good way to protect against Sybil and DoS attacks.[27] Sybil attacks, which can lead to privacy leakage, identity theft, and wireless denial-of-service attacks, may be detected with the help of data from the physical layer's fine-grained channel state provided by Chundong Wang et al. In addition to showing the self-adaptive MUSIC algorithm, the CSI amplitude, and DBSCAN, the researchers explain in detail how to extract features from the system. The results of the testing demonstrate that the system is quite good at spotting both static and dynamic attacks. Researchers found that the static method's typical detection rate is 98.5% when no more than five clients are moving, while the detection rate for the dynamic technique is 99.5%.[28]

A cloud-based trust management technique (CbTMS) was put up by Shih-Hao Chang et al. to identify Sybil attacks in mobile crowd sensing (MCS) networks. Attacks named "Sybil" seek to breach systems by creating numerous "Sybil identities" for online users and using these identities to spread malicious information. The proposed CbTMS framework may manage trust and perform reputation checks to validate the MCS network nodes. To find suspicious Sybil nodes, it uses the Characteristics Checking Scheme (PCS) and the Trust Credit Assessment methodology (TCA). [29]

Related Work

The success of 6LoWPAN devices rests on their ability to make decisions on their own, free from human interference, and effective trust management is essential.[30] In the same way that trust is used to define relationships between people in our daily lives, trust in a network is defined as a node's conduct toward another node. [31]

A trustworthy and compact trust mechanism based on information fusion from several sources was proposed by Jie Yuan et al. for edge devices in the Internet of Things. Since our trust computing approach involves a multi-source feedback system to determine global trust, it is more secure against defamation attacks triggered by untrustworthy feedback providers. In IoT edge computing, they used a lightweight trust evaluation technique for collaborative network devices, which is perfect for IoT edge computing at scale.[32]

Using the long-short-term memory (LSTM) algorithm and a straightforward multi-attribute rating strategy, Yara Alghofaili et al. develop a paradigm for managing trust in Internet of Things (IoT) devices and services (SMART). They use long-term short-term memory (LSTM) to observe behavioural changes in response to the trust threshold, and the SMART to quantify that confidence shift. Measures such as recall, precision, accuracy, and the F-measure, researchers test the proposed model's performance on datasets of varied sizes. Deep learning and machine learning models that have already been made can be shown to work better with different iteration counts.[33]

Behshid Shayesteh, et al., propose A hybrid entity/data trust management technique was developed for an IoT-enabled service to track environmental health and accessibility. They propose an approach based on Bayesian learning that may accurately ascertain whether users are more likely to provide accurate or inaccurate observations. Each user's trustworthiness is calculated in this way. The results of these comparisons show that their trust management method is better in terms of both how well it estimates trust and how well it can handle a larger number of fake users.users.[34]

By using the energy and communication behaviors of IoT nodes as a major context, a new multi-context trust aware routing was built by Sowmya Gali et al. This process also attempted to find the shortest way, or minimal hop count path, in order to further guarantee a safe and less delayed path. The provision of a variety of factors in the route establishment has produced effective results using the proposed mechanism.[35]

Z.A. Khan et al propose a centralized system that uses the trust management technique to identify malicious nodes in the network has been proposed. Once an intrusion is discovered, it must be taken out of the network. The proposed mechanism is appropriate for three well-known assaults: sinkhole attacks, version number attacks, and selective forwarding attacks. The strategy is extremely adaptable and is simple to modify for different kinds of attacks. The trust metric computation only has to be updated for that.[36]

PROPOSED WORK

TRUST FRAMEWORK

The concept of trust management is applicable to making better routing decisions. [37] The trustworthiness of a node can be evaluated from the attributes of the routing behavior of that node.[38] Trust management in proposed work is based on three attributes, namely: knowledge, reputation, and experience.

TRUST CALCULATION ALGORITHM

Step 1: Subnet formation of all the nodes

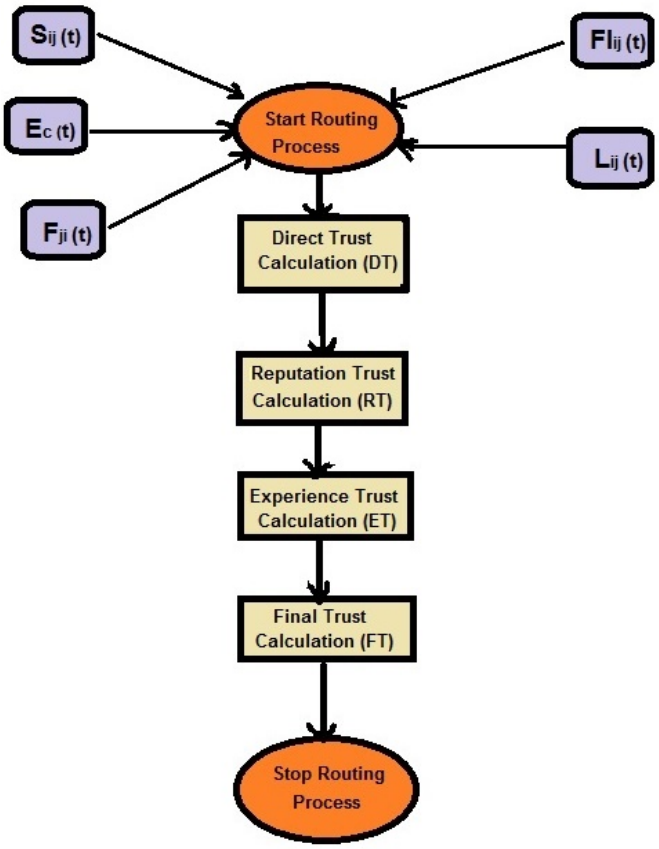


Figure 1. Trust Generation Framework

Step 2: Calculate the deciding factors for the computation of direct trust of all nodes participating in the routing process.

i) To identify the total number of packets sent by node "i" to node "j" (Trustor and trustee) i.e., $S_{ij}(t)$.

ii) To find the total number of packets forwarded by "j" on behalf of "i", i.e., $F_{ji}(t)$.

iii) to calculate the frequency of interaction, i.e., $FI_{ij}(t)$.

iv) Determine the length of the interaction e Lij (t).

v) Energy expended by a node as a result of mobility (as used in the mobility model) E

Step 3:-Compute Direct Trust by the following formula

Initially, k = 0.02 and indirect_penalty = 0.005.

$DT(i,j)(t) = F_{ji}(t) / (S_{ij}(t) + k[S_{ij}(t) - F_{ji}(t)])$

if DT < Threshold_DT

then

k =k +1 & indirect_penalty= 0.005+0.001.

Step 4: Determine Reputation Trust

Reputation Trust: The Sink node is crucial in determining Reputation Trust.

i) When a packet is received, the sink node sends an acknowledgement to the sender node.

ii) When a packet is received, the receiver node sends an acknowledgement to the sink node.

If the two conditions are met,

Then

Give rewards to in-path nodes.

else

Give penality to in-path nodes.

Calculate reputation trust by using the following formula:

RT(i,m) = DT(Direct trust) for node 'm' + K (Reward/penalty)

Step 5: Experience trust calculation.

Experience value will be maintained by 'BR' for each subnetwork.

if

'BR' requests for trust values to'sink' by sending a "Request packet" after each time interval of 20 sec.

Then

"Sink" sends the "trust packet" containing the trust values of all nodes in its respective subnet.

ET (i, m) (Experience trust) = [RT (Node m's reputation trust) + n/Total number of nodes in subnet].

Step 6: Determine your final level of trust.

The final trust in a subnet is the sum of three factors.

Final network trust = average DT (of all nodes) + average RT (of all nodes) + average ET (of all subnets)

ATTACK DETECTION AND ISOLATION

WORMHOLE ATTACK DETECTION ALGORITHM

Step 1: Begin the routing process by utilising RPL and the trust calculation process.

Step 2: Nodes begin to receive DIO messages from neighbouring nodes, which they then add to their neighbor's cache.

Step 3: When an incoming DIO message from another node is received, it calculates the received packet's location information and RSSI value.

Step 4: Compute the distance by accessing its own location and the location of the packet.

Step 5: Both distances, i.e., distance using location and RSSI, should be matched.

Step 6: If there is a mismatch in the distance and a high difference value is found, check the trust score of the node. If trust_score < threshold_trust, then it is termed an "attacker node."

SYBIL ATTACK DETECTION ALGORITHM

Step 1: Start the routing process using RPL and the trust calculation process

Step 2: Nodes start receiving DIO messages from their neighbors. After receiving them, they add them to their neighbor's cache.

Step 3: The IP addresses of the neighbouring nodes are saved in that node's IP_cache.

Step 4: The sink node will check the IP_cache of every node after 60 seconds. If you find duplicate IP address entries in IP_cache, check the location and RSSI.

Step 5: Check the trust score of that node that has a duplicate entry. If trust_score < threshold_score, then it is termed an attacker node.

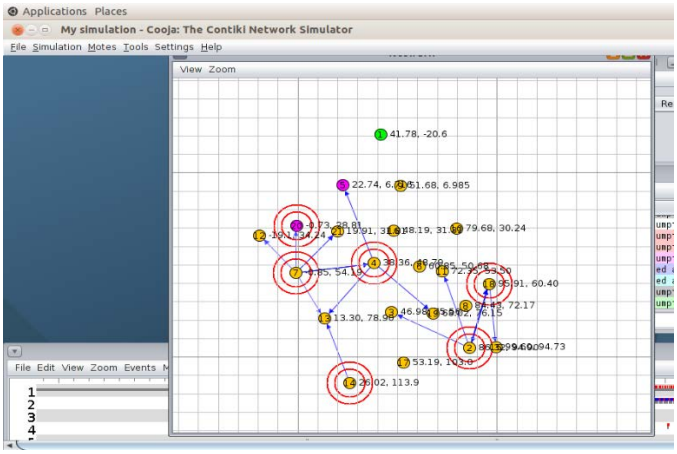


Figure 2. Wormhole Attack

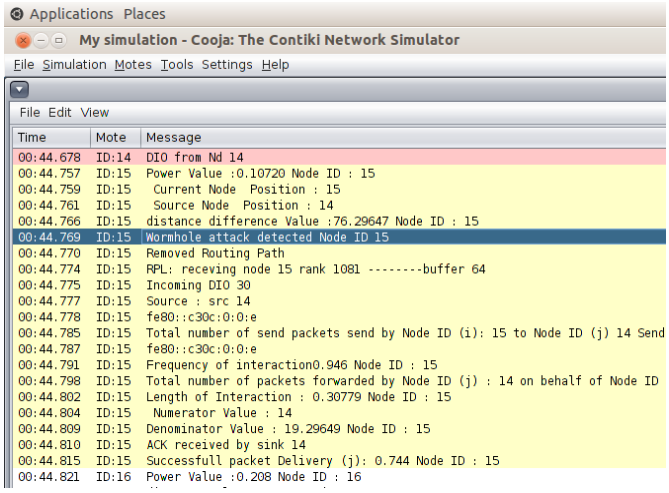


Figure 3. Wormhole attack detection

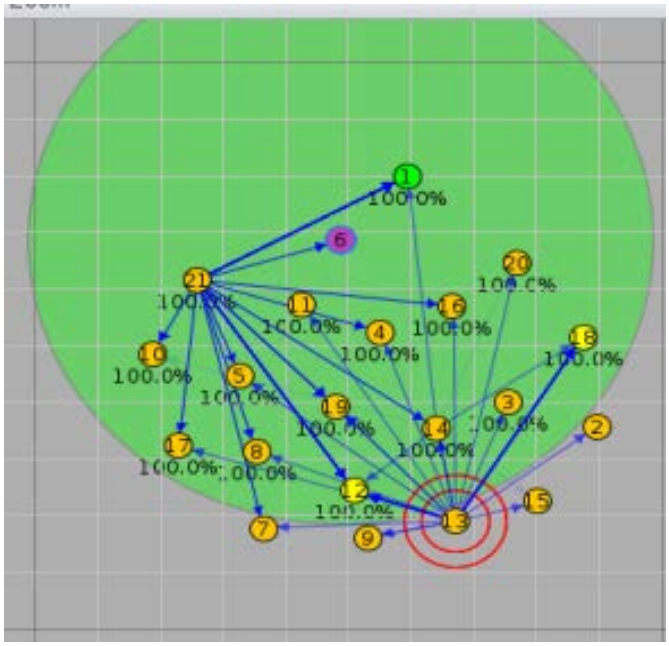


Figure 4. Sybil attack simulation

```
190 00:01.297      ID:20   fe80::212:7414:14:1414
191 00:01.302      ID:20   Created a connection with the server :: local/remote port 8765/5678
192 00:01.341      ID:13   DIS from nd 13
193 00:01.344      ID:2    DIS from nd 2
194 00:01.404      ID:17   DIS from nd 17
195 00:01.439      ID:21   DIS from nd 21
196 00:01.485      ID:9    DIS from nd 9
197 00:01.720      ID:5    DIS from nd 5
198 00:01.847      ID:6    DIS from nd 6
199 00:01.901      ID:16   DIS from nd 16
200 00:02.272      ID:20   DIS from nd 20
201 00:04.314      ID:10   DIS from nd 10
202 00:04.851      ID:1    DIO from Nd 1
203 00:04.894      ID:12   Incoming DIO 6
204 00:04.895      ID:12   Source : src 6
205 00:04.898      ID:12   fe80::212:7401:1:106
206 00:04.900      ID:12   Sybil attacker node Detected 6
207 00:04.906      ID:18   Incoming DIO 6
208 00:04.907      ID:3    Incoming DIO 30
209 00:04.907      ID:18   Source : src 6
210 00:04.908      ID:3    Source : src 1
211 00:04.910      ID:18   fe80::212:7401:1:106
212 00:04.911      ID:3    fe80::212:7401:1:101
213 00:04.912      ID:18   Sybil attacker node Detected 6
214 00:04.947      ID:21   Incoming DIO 30
215 00:04.948      ID:21   Source : src 1
216 00:04.951      ID:21   fe80::212:7401:1:101
217 00:04.975      ID:6    Incoming DIO 30
218 00:04.976      ID:6    Source : src 1
219 00:04.979      ID:6    fe80::212:7401:1:101
220 00:04.987      ID:15   Incoming DIO 30
221 00:04.987      ID:8    Incoming DIO 30
222 00:04.988      ID:15   Source : src 1
223 00:04.988      ID:8    Source : src 1
```

Figure 5. Sybil attack detection

RANK ATTACK DETECTION ALGORITHM

Step 1: Begin the routing process with RPL and trust calculation.

Step 2: Check the preferred_parent list maintained by "BR".

Step 3: If the rank of any other node (other than the preferred_parent list node) equals 1.

Step 4: Examine the trust score of the node with rank equal to 1. If trust_score < threshold_score, then it is termed an attacker node.

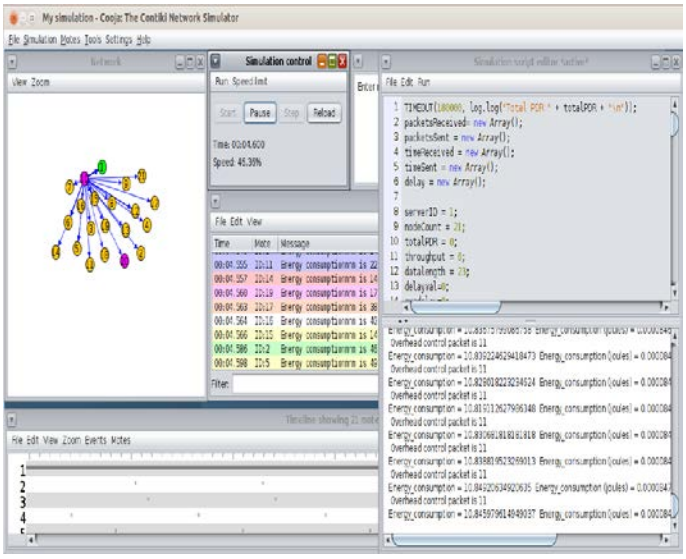


Figure 6. Rank attack simulation

```
10868 00:52.510      ID:6    Energy consumptionnnn is 7718 nd 6
10869 00:52.511      ID:19   Energy consumptionnnn is 8111 nd 19
10870 00:52.512      ID:13   Energy consumptionnnn is 8176 nd 13
10871 00:52.523      ID:7    Energy consumptionnnn is 7974 nd 7
10872 00:52.523      ID:16   Energy consumptionnnn is 8609 nd 16
10873 00:52.531      ID:17   Energy consumptionnnn is 7987 nd 17
10874 00:52.535      ID:12   Energy consumptionnnn is 7517 nd 12
10875 00:52.539      ID:8    Energy consumptionnnn is 7428 nd 8
10876 00:52.539      ID:5    Energy consumptionnnn is 8728 nd 5
10877 00:52.541      ID:20   Energy consumptionnnn is 8520 nd 20
10878 00:52.545      ID:9    Energy consumptionnnn is 7409 nd 9
10879 00:52.549      ID:4    Energy consumptionnnn is 7429 nd 4
10880 00:52.571      ID:18   Energy consumptionnnn is 7673 nd 18
10881 00:52.572      ID:10   Energy consumptionnnn is 8561 nd 10
10882 00:52.575      ID:11   Energy consumptionnnn is 8059 nd 11
10883 00:52.575      ID:10
10884 00:52.577      ID:10   Rank Attack detected node ID 10
10885 00:52.578      ID:6    DAO from nd 6
10886 00:52.578      ID:15   Energy consumptionnnn is 7885 nd 15
10887 00:52.579      ID:10   DIO from nd 10
10888 00:52.581      ID:3    Energy consumptionnnn is 7458 nd 3
10889 00:52.587      ID:6    Energy consumptionnnn is 7728 nd 6
10890 00:52.588      ID:10   Energy consumptionnnn is 8571 nd 10
10891 00:52.588      ID:1    Energy consumptionnnn is 227823 nd 1
10892 00:52.594      ID:2    Energy consumptionnnn is 7335 nd 2
10893 00:52.597      ID:21   Energy consumptionnnn is 8059 nd 21
10894 00:52.602      ID:14   Energy consumptionnnn is 6053 nd 14
10895 00:52.605      ID:19   Energy consumptionnnn is 8123 nd 19
10896 00:52.606      ID:13   Energy consumptionnnn is 8187 nd 13
10897 00:52.616      ID:6    Energy consumptionnnn is 7806 nd 6
10898 00:52.617      ID:7    Energy consumptionnnn is 7986 nd 7
10899 00:52.617      ID:16   Energy consumptionnnn is 8621 nd 16
10900 00:52.626      ID:17   Energy consumptionnnn is 7999 nd 17
10901 00:52.628      ID:12   Energy consumptionnnn is 7528 nd 12
```

Figure 7. Rank attack detection

RESULTS

We compared our results with MRHOF-RPL which is the default objective function used in traditional RPL protocol. We perform and compared the attack detection and isolation using above mentioned protocol with our system i.e Trust_RPL. Further we evaluated our system based on the attributes like Throughput, Packet Delivery Ratio, Delay, Energy Consumption, Overhead, etc. We performed simulation using the Contiki OS's Cooja Simulator. We divide the results into two scenarios, namely static and dynamic, in dynamic the nodes are constantly moving in predefined pattern. We considered the number of nodes as 15 and 30 for both static and dynamic scenarios. From the results, it is identified that our trust-based system outperformed the MRHOF-RPL in all performance parameters along with detection of three attacks namely Wormhole, Rank and Sybil.

DISCUSSION

One of the important parameters for trust computation is packet loss. For better performance and to achieve trustworthiness, packet loss should be kept to a minimum. The packet loss of individual nodes during system operation is shown in figure 8. In Figure 9, packet loss in two scenarios, static and dynamic, are shown for 15 and 30 nodes, respectively. From the graphs, it is clear that our system has minimum packet loss while detecting attacks. Not only is the attack detected in our system, but the attacker node is isolated from the routing process once it is detected. In figure 10, detection and isolation of the mentioned attacks are shown. On the metrics listed below, the system's performance is assessed. The ratio of total packets received to total packets sent is known as the packet delivery ratio. The comparison of this metric with MRHOF_RPL is shown in figure 11. Another metric called throughput which is the rate of successful data delivery of data packets is shown in figure 12. Overhead in RPL network is defined as the amount of control packets required for network path initialization. Comparison of this metric with MRHOF_RPL is shown in figure 13. Another metric called delay is the ratio of total received time to total sent time of packets. Comparison is shown in figure 14. Last metric for evaluation is energy consumption as most of the nodes or sensors used in RPL network are of limited battery therefore this metric is considered for evaluation and focus was to make the system

lightweight so that it would not cause any burden on nodes in network. Comparison graph is shown in figure 15.

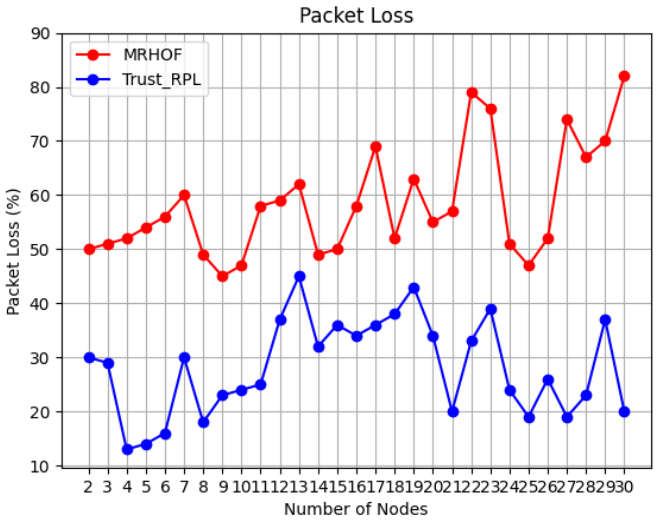


Figure 8. Packet Loss Comparison node wise

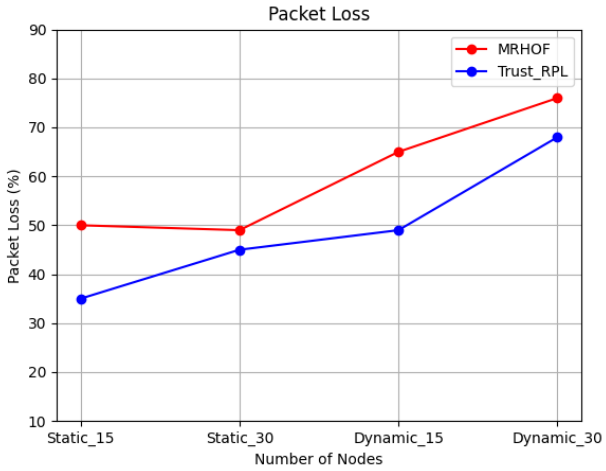


Figure 9. Packet Loss Comparison in Static & Dynamic

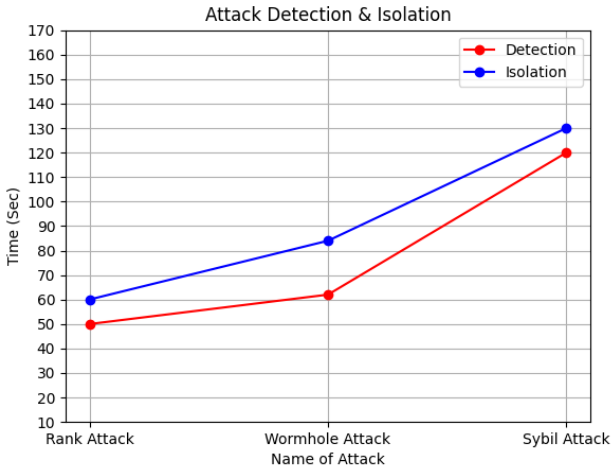


Figure 10. Attacks Detection & Isolation

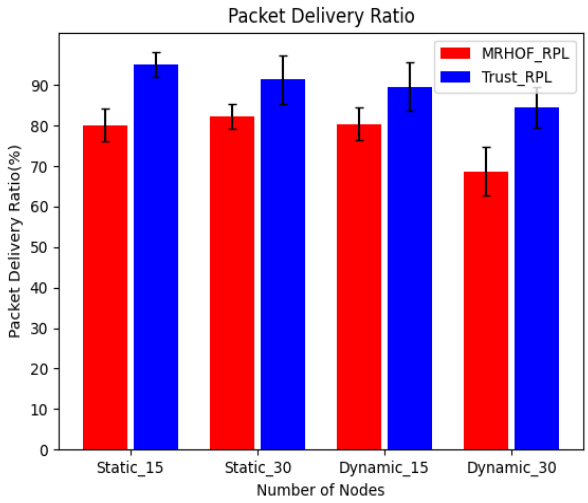


Figure 11. Packet Delivery Ratio Comparison

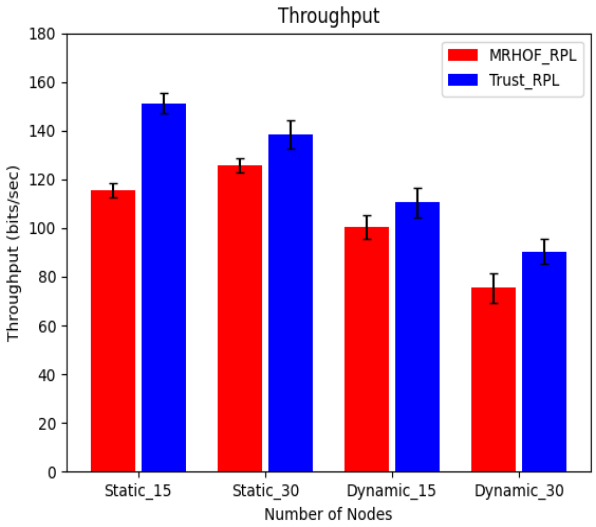


Figure 12. Throughput Comparison

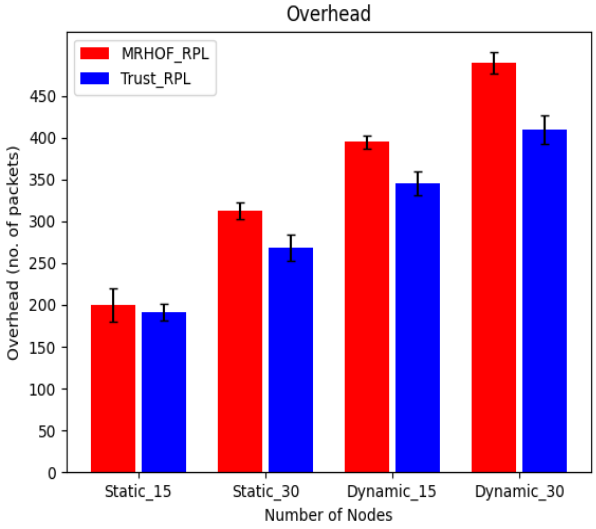


Figure 13. Packet Overhead Comparison

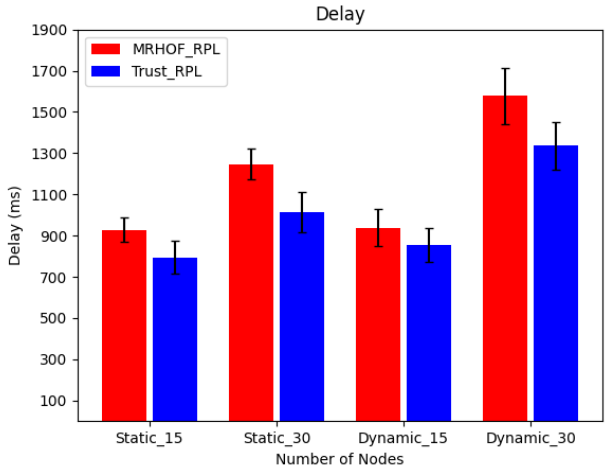


Figure 14. Comparison of Delay incurred in system

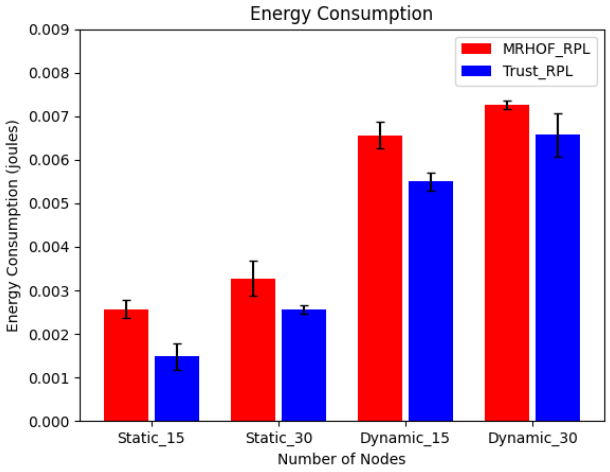


Figure 15. Energy Consumption Comparison

Conclusion & Future Scope

Malicious routing operations and attacks can easily compromise RPL routing networks.These malicious actions pose a threat to network resources and performance, as well as the ability to interfere with normal routing. The main issue in the detection and prevention of these attacks is resource consumption because these devices have limited power and computing capabilities. Proposed A trust-based system determines each node's trust value depending on how it forwards packets and the quality of those packets. An algorithm is used to find the routing attacks based on the attack pattern and the trust level of each node. The addition of sink nodes, combined trust, a distributed architecture, and minimal node overhead will make the system lighter and seem to be promising for making a reliable 6LoWPAN routing solution. In the future, machine learning can be applied to the trust dataset to get the accuracy of the model as well as to classify the trustworthy and untrustworthy behavior of a node.

Conflict of Interest

The authors state that there are no conflicts of interest in this work.

Acknowledgement

The authors are thankful to Department of CSE, Prof. Ram Meghe Institute of Technology & Research, Badnera for providing research facilities.

References

1. K. Phani Rama Krishna, R. Thirumuru. Optimized energy-efficient multi-hop routing algorithm for better coverage in mobile wireless sensor networks. *J. Integr. Sci. Technol.* **2022**, 10 (2), 100–109.
2. O. Gaddour, A. Koubâa. RPL in a nutshell: A survey. *Computer Networks* **2012**, 56 (14), 3163–3178.
3. P. Suganya, C.H. Pradeep Reddy. A survey and analysis on various objective functions defined for RPL in 6LOWPAN. *Int. J. Recent Technol. Engineering* **2019**, 7 (6), 403–411.
4. M. AL-Hawawreh, N. Moustafa, E. Sitnikova. Identification of malicious activities in industrial internet of things based on deep learning models. *J. Information Security Appl.* **2018**, 41, 1–11.
5. J. Pacheco, S. Hariri. IoT security framework for smart cyber infrastructures. *Proceedings - IEEE 1st International Workshops on Foundations and Applications of Self-Systems, FAS-W 2016* **2016**, 242–247.
6. A. Raoof, A. Matrawy, C.H. Lung. Routing Attacks and Mitigation Methods for RPL-Based Internet of Things. *IEEE Communications Surveys and Tutorials* **2019**, 21 (2), 1582–1606.
7. S.M.H. Mirshahjafari, B.S. Ghahfarokhi. Sinkhole+CloneID: A hybrid attack on RPL performance and detection method. *Information Security Journal* **2019**, 28 (4–5), 107–119.
8. K. Guo, Y. Lu, H. Gao, R. Cao. Artificial intelligence-based semantic internet of things in a user-centric smart city. *Sensors* **2018**, 18 (5).
9. R. Mehta, M.M. Parmar. Trust based mechanism for Securing IoT Routing Protocol RPL against Wormhole Grayhole Attacks. *2018 3rd International Conference for Convergence in Technology, I2CT 2018* **2018**, 1–6.
10. I.R. Chen, J. Guo. Hierarchical trust management of community of interest groups in mobile ad hoc networks. *Ad Hoc Networks* **2015**, 33, 154–167.
11. N. Djedjig, D. Tandjaoui, F. Medjek, I. Romdhani. Trust-aware and cooperative routing protocol for IoT security. *J. Information Security Appl.* **2020**, 52.
12. C.V.L. Mendoza, J.H. Kleinschmidt. Mitigating on-off attacks in the internet of things using a distributed trust management scheme. *Int. J. Distributed Sensor Networks* **2015**, 2015.
13. U. Jayasinghe, G.M. Lee, T.W. Um, Q. Shi. Machine Learning Based Trust Computational Model for IoT Services. *IEEE Transactions on Sustainable Computing* **2019**, 4 (1), 39–52.
14. W. Meng. Intrusion Detection in the Era of IoT: Building Trust via Traffic Filtering and Sampling. *Computer* **2018**, 51 (7), 36–43.
15. S.Y. Hashemi, F. Shams Aliee. Dynamic and comprehensive trust model for IoT and its integration into RPL. *J. Supercomputing* **2019**, 75 (7), 3555–3584.
16. M. Goyal, M. Dutta. Intrusion Detection of Wormhole Attack in IoT: A Review. *2018 International Conference on Circuits and Systems in Digital Enterprise Technology, ICCSDET 2018* **2018**, 1–5.
17. J. Arshad, M.A. Azad, R. Amad, et al. A Review of Performance, Energy and Privacy of Intrusion Detection Systems for IoT. *Electronics* **2020**, 9 (4), 1–24.
18. P. Pongle, G. Chavan. Real Time Intrusion and Wormhole Attack Detection in Internet of Things. *Int. J. Computer Appl.* **2015**, 121 (9), 1–9.
19. S. Deshmukh-Bhosale, S.S. Sonavane. A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things. *Procedia Manufacturing* **2019**, 32, 840–847.
20. R. Singh, J. Singh, R. Singh. WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks. *Mobile Information Systems* **2016**, 2016.
21. M.D. Alshehri, F.K. Hussain, O.K. Hussain. Clustering-Driven Intelligent Trust Management Methodology for the Internet of Things (CITM-IoT). *Mobile Networks and Applications* **2018**, 23 (3), 419–431.

22. A. Verma, V. Ranga. Evaluation of Network Intrusion Detection Systems for RPL Based 6LoWPAN Networks in IoT. *Wireless Personal Communications* **2019**, 108 (3), 1571–1594.
23. U. Shafique, A. Khan, A. Rehman, F. Bashir, M. Alam. Detection of rank attack in routing protocol for Low Power and Lossy Networks. *Annales des Telecommunications/Annals of Telecommunications* **2018**, 73 (7–8), 429–438.
24. Z.A. Almusaylim, N.Z. Jhanjhi, A. Alhumam. Detection and mitigation of RPL rank and version number attacks in the internet of things: SRPL-RP. *Sensors (Switzerland)* **2020**, 20 (21), 1–25.
25. W. Choukri, H. Lamaazi, N. Benamar. RPL rank attack detection using Deep Learning. *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies, 3ICT 2020* **2020**, 5–10.
26. S. Raza, L. Wallgren, T. Voigt. SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc Networks* **2013**, 11 (8), 2661–2674.
27. A. Nikam, D. Ambawade. Opinion Metric Based Intrusion Detection Mechanism for RPL Protocol in IoT. *2018 3rd International Conference for Convergence in Technology, I2CT 2018* **2018**, 1–6.
28. C. Wang, L. Zhu, L. Gong, et al. Accurate sybil attack detection based on fine-grained physical channel information. *Sensors* **2018**, 18 (3), 1–23.
29. S.H. Chang, Z.R. Chen. Protecting Mobile Crowd Sensing against Sybil Attacks Using Cloud Based Trust Management System. *Mobile Information Systems* **2016**, 2016.
30. S.K. Apat, J. Mishra, K.S. Raju, N. Padhy. The robust and efficient Machine learning model for smart farming decisions and allied intelligent agriculture decisions. *J. Integr. Sci. Technol.* **2022**, 10 (2), 139–155.
31. L. Wallgren, S. Raza, T. Voigt. Routing attacks and countermeasures in the RPL-based internet of things. *Int. J. Distributed Sensor Networks* **2013**, 2013.
32. J. Yuan, X. Li. A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information Fusion. *IEEE Access* **2018**, 6 (c), 23626–23638.
33. L.S.M. Technique. A Trust Management Model for IoT Devices and Services Based. **2022**.
34. B. Shayesteh, V. Hakami, A. Akbari. A trust management scheme for IoT-enabled environmental health/accessibility monitoring services. *International Journal of Information Security* **2020**, 19 (1), 93–110.
35. S. Gali, V. Nidumolu. Multi-context trust aware routing for internet of things. *Int. J. Intelligent Engin. Systems* **2019**, 12 (1), 189–200.
36. Z.A. Khan, P. Herrmann. A trust based distributed intrusion detection mechanism for internet of things. *Proceedings - International Conference on Advanced Information Networking and Applications, AINA* **2017**, 1169–1176.
37. H. Maddar, W. Kammoun, H. Youssef. Effective distributed trust management model for Internet of Things. *Procedia Computer Science* **2018**, 126, 321–334.
38. W. Alnumay, U. Ghosh, P. Chatterjee. A trust-based predictive model for mobile Ad Hoc network in internet of things. *Sensors* **2019**, 19 (6), 1–14.