International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7
DOI: https://doi.org/10.17762/ijritcc.v11i7.7788
***Article Received**: 16 April 2023* ***Revised**: 10 June 2023* ***Accepted**: 28 June 2023*

Securing IoT Attacks: A Machine Learning Approach for Developing Lightweight Trust-Based Intrusion Detection System

Anup W. Burange[1], Dr. Vaishali M. Deshmukh[2]
[1]Department of CSE
Prof. Ram Meghe Institute of Technology &Research
Badnera, Maharashtra, India
E-mail: awburange@mitra.ac.in
[2]Associate Professor, Department of CSE,
Prof. Ram Meghe Institute of Technology &Research
Badnera, Maharashtra, India
E-mail: vmdeshmukh@mitra.ac.in

Abstract—The routing process in the Internet of Things (IoT) presents challenges in industrial applications due to its complexity, involving multiple devices, critical decision-making, and accurate data transmission. The complexity further increases with dynamic IoT devices, which creates opportunities for potential intruders to disrupt routing. Traditional security measures are inadequate for IoT devices with limited battery capabilities. Although RPL (Routing Protocol for Low Energy and Lossy Networks) is commonly used for IoT routing, it remains vulnerable to security threats. This study aims to detect and isolate three routing attacks on RPL: Rank, Sybil, and Wormhole. To achieve this, a lightweight trust-based secured routing system is proposed, utilizing machine learning techniques to derive values for devices in new networks, where initial trust values are unavailable. The system demonstrates successful detection and isolation of attacks, achieving an accuracy of 98.59%, precision of 98%, recall of 99%, and f-score of 98%, thereby reinforcing its effectiveness. Attacker nodes are identified and promptly disabled, ensuring a secure routing environment. Validation on a generated dataset further confirms the reliability of the system.

Keywords- Secured Routing, Lightweight IDS, Trust Based System, IoT Routing Security.

I. INTRODUCTION

Technological advancements in social network technologies are paving the way for revolutionary services like the Internet of Things (IoT), which have become ubiquitous and deeply integrated into every aspect of our daily lives [1]. The future holds a vast number of devices connecting to the internet, making the security of 6LoWPAN essential. However, keeping pace with rapid technological developments in constrained devices is challenging. Secured routing, especially in multi-hop communication structures, emerges as a crucial research area [2]. Conventional intrusion detection systems are impractical in resource-limited environments.

A lightweight method for detecting anomalies in 6LoWPAN networks must be developed to address various routing disruptions, including subtle attacks. Furthermore, with mobility becoming a key parameter for limited devices, it is essential to devise attack detection strategies for mobile environments. Trust management has shown promise in routing decisions and security [3], yet more precise and interpretable trust-based intrusion detection systems need to be established. Trust management also plays a vital role in ensuring long-term success by granting decision-making autonomy among

6LoWPAN devices. In the current IoT landscape, security remains a major concern [5]. Modern security methods can defend against specific IoT attacks, but there is still vulnerability to malicious behavior that can disrupt routing, potentially compromising user security and privacy. As trust is a critical factor in interpersonal relationships, it also defines node behavior in a network [4]. To ensure a secure and robust IoT environment, addressing security flaws and countering various attacks is of utmost importance [6].

1. We propose securing the RPL routing protocol through the development and examination of trust metrics based on nodes' behavior, attributes, and mobility.
2. Our focus is on designing and implementing an algorithm for trust calculation and detecting specific attacks (Rank, Wormhole, and Sybil).
3. We simulate the modified RPL protocol with integrated trust computation to generate a dataset of trust values.

4. Applying machine learning techniques, to establish trust values for users who lack initial ratings, by analyzing their historical behaviors and transaction patterns.
5. To evaluate the proposed model's performance in comparison to existing approaches, we will conduct simulations, considering factors such as packet delivery ratio, packet loss rate, and average power consumption.

The study's structure is as follows:

Chapter II delves into the background of previous research in the field, encompassing related studies conducted in the past. In Chapter III, we present the research methods employed. Chapter IV contains the pseudo code for attack detection, Chapter V entails the key research findings and outcomes. Finally, Chapter VI concludes the paper with references.

II. RELATED WORK

The Intrusion Detection Systems, which examine network activity and spot malicious node behavior, are also used to defend against network attacks [7]. Due to typical IDS systems' high resource consumption and inadequacy, lightweight intrusion detection systems are crucial for networks when devices have limited resources, since they are better able to analyze and identify malicious activities [8].

For the purpose of spotting on-off attacks, a protocol based on fuzzy logic was developed [9] , attacks based on contradictory behavior, and other malicious nodes. Through the use of this protocol, nodes could safely move between clusters. Additionally, a messaging system resembling serial transmission was used for safe message encryption. Fuzzy logic was also used in the protocol to identify bad nodes and restrict their un-trusted role in generating incorrect suggestions about other nodes in the network.

In a subsequent study, [10] created an IoT service trust propagation model. By relying on social contact, friend compatibility ratings, and interest ties while employing the community as the filter, the method used decentralized collaborative filtering to compile the responses.

Incorporating a model based on machine learning, Upul Jaysinghe et al. [11] calculated the trustworthiness of individual nodes to use in the routing process. They conduct a trust evaluation on various aspects of a genuine dataset. Their approach is general enough to be used in a broad range of fields, such as smart parking systems, smart homes, and more. Their concept is built on trust in the user's expertise, track record, and overall reputation. Techniques such as feature extraction, clustering, labeling, and classification were employed. Using unsupervised learning, labels of trustworthiness are applied to the data. An SVM-based trust prediction model is then used to generate the final trust value.

In their study, Ali Hamid Farea et al.[12] proposed a methodology to detect Internet of Things (IoT) attacks using machine learning (ML) techniques. They curated a new dataset comprising IoT assaults, analyzing three common attack types: denial-of-service, brute-force, and other-oriented attacks. The ML-based approach employs decision trees for decision-making. The researchers found that a multiclass random decision forest ML-based model outperformed choice tree jungle regression, decision forest tree regression, and enhanced decision tree regression in effectively identifying IoT risks.

A study by [13] developed a new security framework. SRF-IoT was created to identify rank-and-file threats. In order to obtain intelligence and select the optimal path for network packets, the suggested method employs an external SRF-IDS, making it a trust-based system. The suggested method makes it easier to avoid hostile attackers. It also cuts down on the number of parent switches and speeds up the network.

Consider the evidence presented in [14]. By identifying Learning-based IoT attack models, they try to prove that the IoT is secure. This allows for the integration of diverse devices into networks, which in turn allows for the provision of high-quality, intelligent services without compromising users' personal information. Security measures for the Internet of Things include authentication, access control, virus detection, and safe offloading, among others.

The Friedman test has been adopted as a means of comparing different types of attacks. The authors [15] provided a summary of the RPL protocol and proposed a taxonomy of all current additions to the Rank attack, including the many strategies for mitigating or detecting it.

Authors in Using the Contiki Operating System and the Cooja Simulator, they [16] built a wormhole intrusion detection system considering RSSI. After deploying IDS against wormhole attacks, it was found that the crafted IDS successfully uncovered the threat 90% of the time [17].

The authors [18] introduced three decentralized-centralized approaches that employ the trust management approach to identify malicious nodes. As soon as a threat is identified, it must be eliminated from the system. In particular, the system is designed to tackle three well-known attacks against RPL protocol: selective forwarding, sinkholes, and version numbers. The system can be adapted to a wide variety of attacks.

The key concept of the novel hybrid trust-based IDS for WSNs [19] is that every sensor node in the network assigns a functional reputation value to each of its neighbors based on the data it collects about the latter's actions. By fusing functional reputation values and misuse detection criteria, Base Station (BS) can identify malevolent nodes. The misuse detection technique and functional reputation-based trust evaluation are used in the suggested system. The simulation findings demonstrate that the control packets don't significantly increase the workload, making the deployment of the method possible.

In the study [20], In order to better identify intrusions, a convolutional neural network (CNN) with BiLSTM-based attention and a knowledge graph were developed. By combining knowledge-based graph-based feature extraction with statistical analysis-based feature extraction, the IDS enhances its ability to capture contextual semantic relationships and crucial aspects of IoT network traffic. The proposed technique effectively extracts significant features from both normal and malicious requests, encompassing DoS, probing, R2L, and U2R attacks.

Defenses against rank and black hole attacks are the primary focus of this research [21]. Incorporating RPL with a lightweight trust model in their opinion, the proposed SMTrust model is superior to the alternatives. Combining rank and blackhole attack defense with other network performance metrics, such as topology robustness, throughput, packet loss rate, and energy use.

In several layers, wireless sensor networks are attacked. One method for maintaining the security of data transmission in wireless sensor networks is cryptography. In consideration of the limitations of WSNs, a proposed method [26] is presented. The time complexity is the greatest for the given approach. The method's specifics and core notions are described in such a way that the algorithm may be implemented operationally.

DDoS attacks try to prevent authorized users from accessing network resources. This research recommends an evidence-theory-based security strategy for defending software-defined wireless sensor networks from distributed denial-of-service attacks [27]. The software-defined wireless sensor network's control plane contains the security model as a security unit, which is used to detect suspicious traffic. In the initial stages of detection, DDoS attacks may be countered with the use of a software-defined network's central controller and the entropy approach.

III. PROPOSED METHODOLOGY

In this study, the system model is divided into attack simulation-detection phase, dataset collection and preparation, Pre-procesing of data, model training and result.

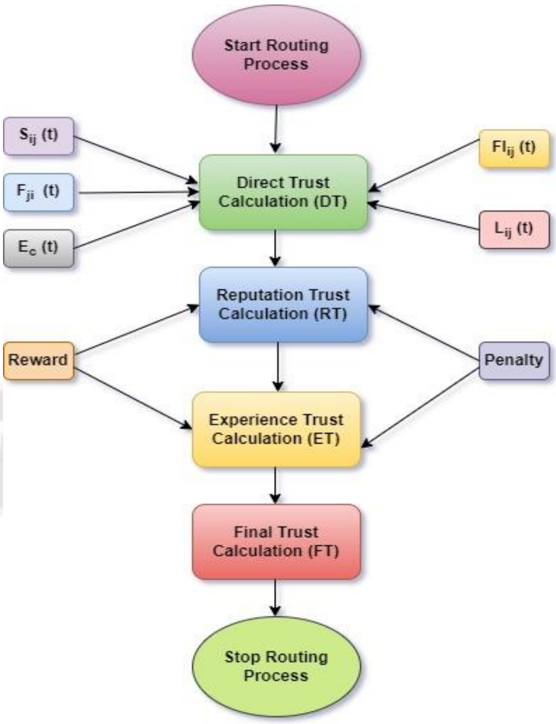
Start Routing Process
S_{ij} (t)
F_{ji} (t)
E_c (t)
Direct Trust Calculation (DT)
FI_{ij} (t)
L_{ij} (t)
Reputation Trust Calculation (RT)
Reward
Penalty
Experience Trust Calculation (ET)
Final Trust Calculation (FT)
Stop Routing Process

Figure 1. Architecture of the proposed model

A. *Trust Calculation Algorithm*

Trust Evaluation Algorithm for Dynamic Networks

1. Network Partitioning:
Divide the dynamic network into subnets, assigning each node to a specific subnet.
2. Direct Trust Calculation:
For each node, determine the following key factors:
- Sij(t): Total packets transmitted by node i to node j (as a trustor and trustee).
- Fji(t): Total packets forwarded by node j on behalf of node i.
- FIij(t): Frequency of interactions between nodes i and j.
- Lij(t): Duration of interactions between nodes i and j.
- E: Energy expenditure by a node due to mobility.

Calculate Direct Trust (DT) using the following formula:

$$DT(i,j)(t) = \frac{\text{Fji}(t)}{(Sij(t) + k[Sij(t) - Fji(t)])} \qquad Eq.(1)$$

where,

$$K = 0.02 + \left(0.005\ for\ FIij(t)\right) + \left(0.005\ for\ Lij(t)\right) + (0.005\ for\ Ec) \qquad Eq.(2)$$

3. Reputation Trust Estimation:
Reputation Trust (RT) relies on the sink node's input. Upon receiving a packet, the sink node acknowledges the sender, and the receiver node acknowledges the sink node. In-path nodes are rewarded if both acknowledgments are received; otherwise, they face penalties.
Reputation Trust (RT) using the following formula:

***Article Received**: 16 April 2023 **Revised**: 10 June 2023 **Accepted**: 28 June 2023*

Compute

$$RT(i,m) = DT\,for\ node\ 'm' + K(reward\ or\ penalty) \qquad Eq.(3)$$

4. Experience Trust Computation:
'Border Router' (BR) maintains the experience value for each subnet. At 20-second intervals, 'BR' requests trust values from the sink node by sending a "Request packet." The sink node responds with a "trust packet" containing the trust values of all nodes in its subnet.
Calculate Experience Trust (ET) using the following formula:

$$ET = \frac{(RT + n)}{Total\ no.of\ nodes\ in\ subnet} \qquad Eq.(4)$$

5. Final Network Trust Determination:
The final trust in a subnet is the sum of three factors:
- Average DT of all nodes.
- Average RT of all nodes.
- Average ET of all subnets.

Compute Final Trust using the following formula:

$$Final\ Trust = Avg.DT + Avg.RT + Avg.ET \qquad Eq(5)$$

Note: The specific values for Threshold_DT and K can be adjusted to optimize the algorithm's performance for different network scenarios. The trust management algorithm is designed to calculate trust values for each individual node in the network. If a node's trust level falls below the threshold, it is compared with attributes of known attacks to determine its maliciousness. This algorithm is well-suited for evaluating trust in dynamic networks and can be adapted to various applications requiring trustworthy node behavior.

B. RPL Simulation

The Internet of Things (IoT) is simulated using the Cooja Contiki Simulator 3.0, with "Tmote Sky" IoT devices utilized as low-power wireless modules commonly employed in sensor networks [22]. The sink node acts as the central access point for all other nodes to connect to the internet, gathering data from different sources to construct the DODAG (Destination Oriented Directed Acyclic Graph). Each attack type is simulated for a duration of 5 minutes (300 seconds) to evaluate its effects.

TABLE I. SIMULATION PARAMETERS

Simulator	Cooja
Physical Layer	IEEE 802.15.4
Network layer	RPL
Number of Nodes	15, 30
Number of Attacker Nodes	20 % of attacker nodes (Rank attack, Wormhole Attack, Sybil Attack)
Mote type	Sky
Radio Model	Unit Disk Graph Medium (UDGM)
Transmission Range	50m
Area	100m * 100m
Objective function	MRHOF
Positioning	Random Positioning
Simulation Time	300 sec
Mobility model	Random Way-point model

C. Attack Detection

It assembles information from several sources in order to facilitate the development of DODAG. Simulations run for 5 minutes (300 sec) for each attack type. Three attacks are launched during this phase: Rank, Sybil, and Wormhole. Each node's position inside a DAG in relation to the root node is represented by the rank value. In order to locate a new parent node, the nodes raise their rank values. Rank plays a vital role in parent node selection; therefore, an attack on the Rank value can cause serious damage to the routing behavior of a network. The malicious node in a Sybil attack uses the identities of numerous nodes on the same physical node. It asserts several false identities. The security of the network, the integrity of the data, and the consumption of resources are all compromised by this type of attack. In our system, if a node changes its identity, it will be quickly recorded by BR because it has a broad view of all subnets. Each node's identification in a certain subnet is maintained by BR.

One of the most challenging attacks to stop or identify is the wormhole attack. During this attack, a fast wormhole tunnel is built between two remotely hacked routers. In this attack, a wormhole tunnel is built between two remotely hacked routers. By routing the majority of the traffic through the tunnel, this tunnel is then utilized to alter the network's routing behaviour. This creates a shift in routing operations. Wormhole detection in our system is based on rank check and RSSI. Additionally, if the attacking node is a member of a different subnet, BR will send an "Alert" message to the sink, which can then add the node to its routing table as a suspicious entry and broadcast the message to all nodes.

IV. PSEUDO CODE FOR ATTACK DETECTION

➢ Rank Attack Detection

1. Network Initialization:
   - Start the routing process using RPL and begin the trust calculation process.
2. Preferred Parent Verification:
   - Verify the preferred_parent list managed by the "BR" (Base Rank) node.
3. Node Rank Check:
   - If the rank of any node, except for the preferred_parent list node, is equal to 1, proceed to the next step; otherwise, terminate the algorithm.
4. Trust Score Evaluation:
   - Calculate the trust score of the node with a rank equal to 1, considering its interactions, packet forwarding, and behavior history.
5. Rank Attack Identification:
   - Compare the trust score against a predefined threshold score.
   - If the trust score falls below the threshold score, classify the node as a potential Rank attack initiator.

➢ Sybil Attack Detection

1. Network Initialization:
   - Start the routing process using RPL (Routing Protocol for Low-power and Lossy Networks).
   - Begin the trust calculation process.
2. Neighbor Cache and IP Cache:
   - Nodes receive DIO (DODAG Information Object) messages from neighboring nodes and store them in their neighbor cache.
   - Record the IP addresses of neighboring nodes in each node's IP cache.
3. Duplicate IP Address Check:
   - After a 60-second interval, the sink node analyzes the IP cache of each node to identify any duplicate IP address entries.
4. Location and RSSI Verification:
   - For nodes with duplicate IP address entries, verify their physical location and Received Signal Strength Indicator (RSSI).
5. Trust Score Evaluation:
   - Calculate the trust score of the node with the duplicate entry based on location, RSSI, and historical behavior.
   - Compare the trust score against a predefined threshold score.
6. Sybil Attack Identification:
   - If the trust score is below the threshold score, classify the node as a potential Sybil attacker.

➢ Wormhole Attack Detection

1. Network Initialization:
   - Start the routing process using RPL (Routing Protocol for Low-power and Lossy Networks).
   - Initiate trust calculation to establish a trustworthy network.
2. Neighbor Cache and DIO Reception:
   - Nodes receive DIO (DODAG Information Object) messages from neighboring nodes and store them in their neighbor cache.
3. Location and RSSI Calculation:
   - When an incoming DIO message is received from another node, extract the location information and Received Signal Strength Indicator (RSSI) value from the packet.
4. Distance Computation:
   - Calculate the distance between the current node and the source node of the received packet using the extracted location information.
5. Distance Verification:
   - Verify the distance calculated based on both the location and RSSI values.
   - If a significant mismatch in distance is detected (indicating potential wormhole presence), proceed to the next step.
6. Trust Score Evaluation:
   - Check the trust score of the node associated with the potential wormhole.
   - Compare the trust score against a predefined threshold trust level.
7. Wormhole Attack Identification:
   - If the trust score is below the threshold trust level, classify the node as a potential attacker node involved in the wormhole attack.

A. Data Collection

This stage collects the data, which is generated through the simulation model, consisting of 15 to 30 nodes with some attacker nodes, and also the method of intrusion detection based on trust to spot these attacks on the basis of their behavioral characteristics. Based on the parameters mentioned above, the DT, RT, and ET will be calculated for each node by this system,

DOI: https://doi.org/10.17762/ijritcc.v11i7.7788
***Article Received**: 16 April 2023 **Revised**: 10 June 2023 **Accepted**: 28 June 2023*

between the range 0 and 1. The lowest trust value is zero, and the highest trust value is one. Based on the values generated for each node, it can be categorized as follows:

TABLE II. NODE'S CATEGORY

Node id	Trust Value	Status
-	0.75 – 1	**Good**
-	0.50 -0.75	**Average**
-	0.25-0.50	**Below Avg.** (Will be checked for attack patterns)
-	0-0.25	**Poor** (Removed from the network if it maintains this value for 60 sec.)

B. Data Pre-Processing

The system is prepared so that when the packets are transferred between the nodes, the related attributes, using which the trust values are generated, are displayed in the mote output of the COOJA simulation. From mote output, the values are converted to.csv format. Trust values of individual nodes for 1, 2, and 5-minutes are generated in.csv format.

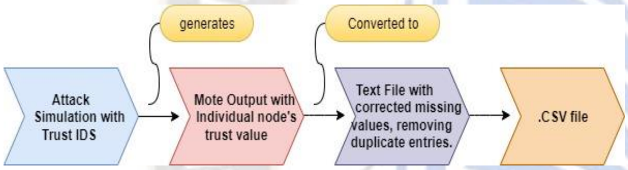
generates
Converted to
Attack Simulation with Trust IDS
Mote Output with Individual node's trust value
Text File with corrected missing values, removing duplicate entries.
.CSV file

Figure 2. Data Pre-processing steps

V. RESULT AND FINDINGS

Extensive analysis was conducted using Python in this study to develop a proposed model for identifying RPL-based IoT network threats, including Rank, Sybil, and Wormhole. The model was trained using 70% of the dataset, and subsequently, its performance was evaluated under test conditions using the remaining 30%.

A. Binary Classification

In binary classification, the primary goal is to predict the category to which a specific entity belongs, often involving two distinct groups [23]. In this study, we employed supervised learning with binary classification to determine whether a given node is an attacker or benign. To achieve this, generalized machine learning algorithms, specifically the support vector machine (SVM) and the K-nearest neighbor (KNN) algorithm, were utilized. KNN is a non-parametric approach that identifies the k-nearest data points to a given input, while SVM is a parametric method that seeks the optimal separating hyperplane for data classification. Although other classification methods could be applied, we opted for KNN and SVM due to their exceptional performance and versatility in handling the specific type of data employed in this study. The SVM model achieved a training accuracy of 98.44% and a testing accuracy of 94.54%. On the other hand, the KNN model demonstrated a training accuracy of 99.37% and a testing accuracy of 97.24%, as depicted in the figure below.

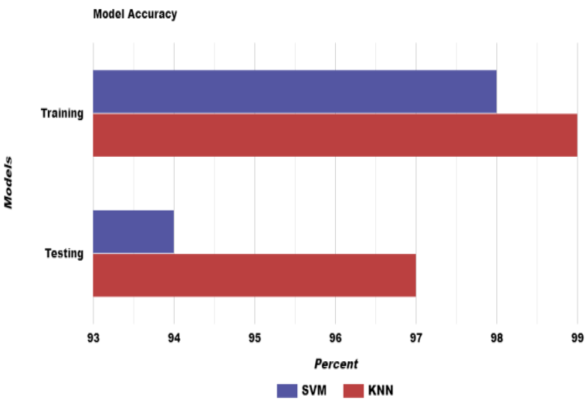

Figure 3. Model Accuracy

Performance analysis using two algorithms namely SVM & KNN are shown in below tables.

TABLE III. USING SVM

Using SVM		
Evaluation Metric	**Train/Test**	**Result**
Accuracy	Tr	98.44
	Ts	94.54
Precision	Tr	0.95
	Ts	0.96
Recall	Tr	0.94
	Ts	0.96
f-1 score	Tr	0.95
	Ts	0.96

TABLE IV. USING KNN

Using KNN		
Evaluation Metric	**Train/Test**	**Result**
Accuracy	Tr	99.78
	Ts	98.59
Precision	Tr	0.99
	Ts	0.98
Recall	Tr	0.99
	Ts	0.99
f-1 score	Tr	0.98
	Ts	0.98

Following is the scatterplot showing classification of attacker and benign nodes based on their final trust values.

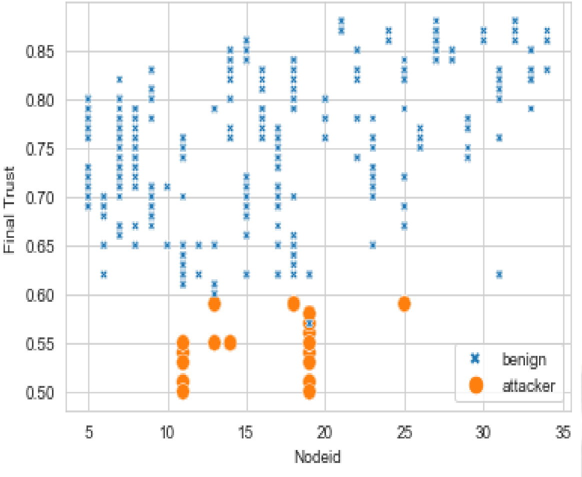

Figure 4: Classification of Attacker and Benign nodes

Following figure shows the true positivity rate of proposed model with existing models.

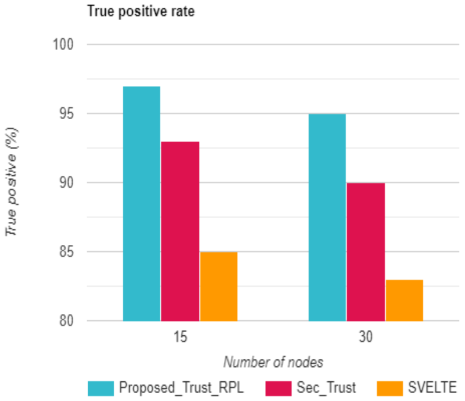

Figure 5: True Positivity Rate

B. Multi-class Classification

Multiclass classification categorizes entities into three distinct attack groups based on their attributes or features. The pie chart below illustrates the detection and classification of various attacks, each falling into specific attack categories determined by their attributes. The chart clearly indicates that the percentage of Sybil attacks is considerably lower than that of Rank attacks, while the percentage of normal nodes is significantly higher in comparison to the attacks.

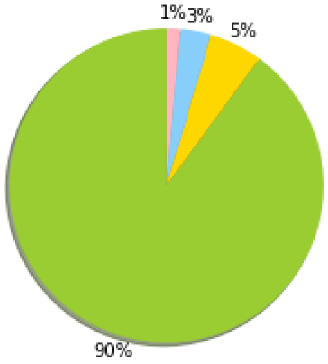

Figure 6: Multiclass Classification of Attacks

Comparison of results with similar RPL attacks related studies

TABLE V. COMPARISON STUDY

Study(Attack)	**PDR**	**Packet Drops**	**No. of nodes and Attackers**
Sec-Trust (Rank, Sybil) [24]	80	22-23%	30
SVELTE [13]	92.8	8.2%	28+4 (Attackers)
Our proposed (Trust-RPL)	92	15%	36+ 4 (Rank Attacker) 36+2 (Sybil Attacker) 36+2 (Wormhole Attacker)

The comparison metrics in the table include packet delivery ratio (PDR), packet drops (%), and the number of nodes engaged in the routing process. Notably, the SRF-IoT exhibits a high PDR of 92.8% and the lowest packet drops (%) at 8.2%. In contrast, our proposed system shows a slightly lower PDR compared to SVELTE [13], with higher packet drops (%) attributed to the involvement of numerous dynamic nodes. The study considered two scenarios: static with 15 and 30 nodes, and dynamic with 15 and 30 nodes. The presence of dynamic nodes results in increased overhead for control messages and packet losses.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7
DOI: https://doi.org/10.17762/ijritcc.v11i7.7788
***Article Received**: 16 April 2023 **Revised**: 10 June 2023 **Accepted**: 28 June 2023*

C. Lightweight

The IoT nodes utilizing RPL for routing operate on limited battery power, making battery drainage a significant concern [25]. When designing Intrusion Detection Systems (IDS) for such devices, prioritizing performance parameters like energy consumption and packet overhead becomes crucial. In this study, we aimed to reduce the additional burden of implementing a trust-based system by assigning more responsibility to sink nodes and base stations (BR). To measure the average power consumption of nodes in the COOJA simulator, we utilized the inbuilt "power tracker" plug-in. The comparison of average power consumption per node was conducted to assess the system's overhead, as depicted in the figure below.

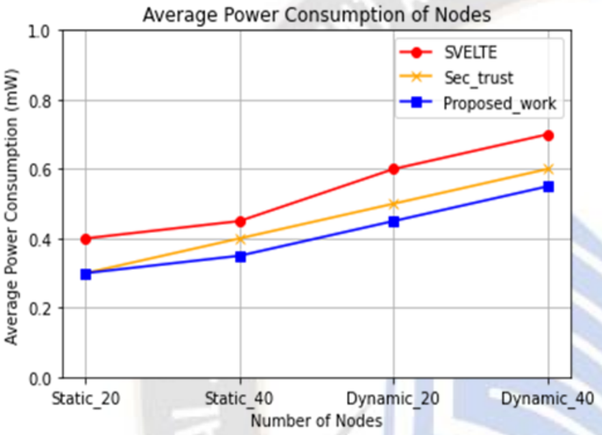

Figure 7: Average power consumption

VI. CONCLUSION

This study introduces an innovative trust-based security system designed to detect routing attacks on RPL within Contiki's Cooja simulator. The system relies on hybrid trust, distributing the responsibility of evaluating trust values among individual nodes, sink nodes, and BR. It combines direct trust (DT), reputation trust (RT), and experience trust (ET) to evaluate the final trust of the network. Using the COOJA 3.0 simulator, a dataset containing trust values for all participating nodes in the routing process is generated. This dataset serves as the foundation for machine learning predictions. Binary classification identifies attacker or benign nodes, while multiclass prediction detects specific attack types. Our system's performance is compared to previous studies in terms of accuracy, PDR, packet loss, power consumption, and computation consumption, showcasing promising results. The hybrid trust evaluation renders this system lightweight and adaptable, effectively detecting Rank, Wormhole, and Sybil attacks for secure routing between nodes. In the future, this approach can extend to detect additional attacks by studying their behaviours and incorporating social attributes as trust metrics.

ACKNOWLEDGMENT

The research was not funded by any specific grants from public, commercial, or not-for-profit sectors. The authors express their gratitude to Prof. Ram Meghe Institute of Technology and Research for their support and provision of all the necessary lab facilities to conduct this research.

REFERENCES

[1] M. AL-Hawawreh, N. Moustafa, and E. Sitnikova, “Identification of malicious activities in industrial internet of things based on deep learning models,” Journal of Information Security Application, vol. 41, pp. 1–11, 2018.

[2] Deshmukh, Amruta & Pund, Mahendra. “Optimizing Routing Performance in P2P Networks Using Machine Learning.” Advanced Informatics for Computing Research, 10.1007/978-981-15-0111-1_20., 2019

[3] E. Canbalaban and S. Sen, “A Cross-Layer Intrusion Detection System for RPL-Based Internet of Things,” in Ad-Hoc, Mobile, and Wireless Networks, pp. 214–227, 2020.

[4] R. Mehta and M. M. Parmar, “Trust based mechanism for Securing IoT Routing Protocol RPL against Wormhole & Grayhole Attacks,” In: 3rd International Conference for Convergence in Technology (I2CT), 2018.

[5] S. Raza, L. Wallgren, and T. Voigt, “SVELTE: Real-time intrusion detection in the Internet of Things,” Ad Hoc Networks, vol. 11, no. 8, pp. 2661–2674, 2013.

[6] J. Pacheco and S. Hariri, “IoT Security Framework for Smart Cyber Infrastructures,” In: IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W),2016.

[7] Garg, P. ., Sharma, N. ., Sonal, & Shukla, B. . (2023). Predicting the Risk of Cardiovascular Diseases using Machine Learning Techniques. International Journal of Intelligent Systems and Applications in Engineering, 11(2s), 165 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2520

[8] D. Arshad, M. Asim, N. Tariq, T. Baker, H. Tawfik, and D. Al-Jumeily OBE, “THC-RPL: A lightweight Trust-enabled routing in RPL-based IoT networks against Sybil attack,” PLoS One, vol. 17, no. 7, p. e0271277, 2022.

[9] G. Thamilarasu and S. Chawla, “Towards deep-learning-driven intrusion detection for the Internet of Things,” Sensors (Basel), vol. 19, no. 9, p. 1977, 2019.

[10] M. D. Alshehri and F. K. Hussain, “A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT),” Computing, vol. 101, no. 7, pp. 791–818, 2019.

[11] I.-R. Chen and J. Guo, “Hierarchical trust management of community of interest groups in mobile ad hoc networks,” Ad Hoc Networks, vol. 33, pp. 154–167, 2015.

[12] U. Jayasinghe, G. M. Lee, T.-W. Um, and Q. Shi, “Machine learning based trust computational model for IoT services,” IEEE Transactions on Sustainable Computing., vol. 4, no. 1, pp. 39–52, 2019.

[13] A. H. Farea and K. Küçük, “EAI Endorsed Transactions Detections of IoT Attacks via Machine Learning Based Approaches with Cooja,” in EAI, vol. 7, pp. 1–12, 2022.

[14] Raza, S., Wallgren, L., & Voigt, T. "SVELTE: Real-time intrusion detection in the Internet of Things". Ad Hoc Networks, 11(8), 2661–2674. https://doi.org/10.1016/j.adhoc.2013.04.014, 2013.

[15] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?," IEEE Signal Processing Magazine, vol. 35, no. 5, pp. 41–49, 2018.

[16] Prof. Bhushan Thakre, Dr. R.M Thakre. (2017). Analysis of Modified Current Controller and its Implementation in Automotive LED. International Journal of New Practices in Management and Engineering, 6(04), 01 - 06. https://doi.org/10.17762/ijnpme.v6i04.60

[17] M. A. Boudouaia, A. Ali-Pacha, A. Abouaissa, and P. Lorenz, "Security against rank attack in RPL protocol," IEEE Network., vol. 34, no. 4, pp. 133–139, 2020.

[18] S. Deshmukh-Bhosale and S. S. Sonavane, "A real-time intrusion detection system for wormhole attack in the RPL based internet of things," Procedia Manufacturing., vol. 32, pp. 840–847, 2019.

[19] F. Medjek, D. Tandjaoui, I. Romdhani, and N. Djedjig, "A trust-based intrusion detection system for mobile RPL based networks," In: IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017

[20] Z. A. Khan and P. Herrmann, "A trust based distributed intrusion detection mechanism for internet of things," In: IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), 2017.

[21] M. M. Ozcelik, E. Irmak, and S. Ozdemir, "A hybrid trust based intrusion detection system for wireless sensor networks," In: International Symposium on Networks, Computers and Communications (ISNCC), 2017.

[22] X. Yang, G. Peng, D. Zhang, and Y. Lv, "An enhanced intrusion detection system for IoT networks based on deep learning and knowledge graph," Secure Communication Network, vol. 2022, pp. 1–21, 2022.

[23] 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 (Basel), vol. 22, no. 18, 2022.

[24] S. B. Thigale, R. K. Pandey, P. R. Gadekar, V. A. Dhotre, and A. A. Junnarkar, "Lightweight novel trust based framework for IoT enabled wireless network communications," Periodicals of Engineering and Natural Sciences (PEN), vol. 7, no. 3, p. 1126, 2019.

[25] J. Canedo and A. Skjellum, "Using machine learning to secure IoT systems," In: 14th Annual Conference on Privacy, Security and Trust (PST), 2016.

[26] Jang Bahadur Saini, D. . (2022). Pre-Processing Based Wavelets Neural Network for Removing Artifacts in EEG Data. Research Journal of Computer Systems and Engineering, 3(1), 43–47. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/40

[27] D. Airehrour, J. A. Gutierrez, and S. K. Ray, "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things," Future Generation Computer Systems, vol. 93, pp. 860–876, 2019.

[28] E. Kfoury, J. Saab, P. Younes, and R. Achkar, "A self organizing map intrusion detection system for RPL protocol attacks," International Journal of Interdisciplinary Telecommunication Networks, vol. 11, no. 1, pp. 30–43, 2019.

[29] Omid Mahdi Ebadati E, Farshad Eshghi, Amin Zamani, "Security Enhancement of Wireless Sensor Networks: A Hybrid Efficient Encryption Algorithm Approach." Journal of Information System and Telecommunication, vol. 6, no. 23, pp. 180–192, 2018.

[30] García, A., Petrović, M., Ivanov, G., Smith, J., & Cohen, D. Enhancing Medical Diagnosis with Machine Learning and Image Processing. Kuwait Journal of Machine Learning, 1(4). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/143

[31] N. Farzaneh and R. Hoseini, "Confronting DDoS attacks in software-defined wireless sensor networks based on evidence theory," Journal of Information Systems and Telecommunication, vol. 9, no. 33, pp. 25–36, 2021.