International Journal of Applied Mathematics
Volume 38 No. 5 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

EFFICIENT DETECTION AND MITIGATION OF SYBIL AND CLONE ID ATTACKS IN IOT USING PARTICLE SWARM OPTIMIZED DECISION TREE

Brindhadevi J [a, *], **Dr. Devarajan K** [b]

[a] Research scholar, Department of Electronics and Communication Engineering, Annamalai University, India.

[b] Assistant Professor, Department of Electronics and Communication Engineering, Annamalai University, India.

E-mail: j.jothini@gmail.com [a], devarajan_lecturer@yahoo.com[b]

Abstract

The Internet of Things (IoT) has revolutionized modern communications by enabling seamless connectivity among resource-constrained devices. Routing Protocol for Low Power and Lossy Networks (RPL) serves as the backbone for routing in IoT, ensuring energy efficiency and reliable data transmission. However, RPL is vulnerable to severe routing threats such as Sybil and Clone ID attacks, which compromise network performance and data integrity. This study introduces a novel machine learning framework that employs two models: a Decision Tree-based Attack Detection Model (DT-ADM) and an optimized version (ODT-ADM), which leverages Particle Swarm Optimization (PSO) for feature selection to enhance detection accuracy. The models are evaluated under two scenarios: detection of individual attacks (Sybil or Clone ID) and detection of combined attacks. Results demonstrate that the optimized model significantly improves Packet delivery ratio, reduces overhead, enhances energy efficiency, and lowers latency. This study highlights the potential of machine learning in strengthening IoT security against complex routing attacks, ensuring a more robust and reliable IoT ecosystem.

Keywords: Clone ID Attack, Decision Tree, IoT, Machine Learning, Particle Swarm Optimization, Routing Attacks, RPL, Security, Sybil Attack.

Introduction

To facilitate smooth automation and improve user experiences, a wide network of linked devices, sensors, and systems is referred to as the Internet of Things (IoT). These devices frequently use lightweight communication protocols and function in contexts with limited resources. A popular routing protocol in the Internet of Things, the Routing Protocol for Low-Power and Lossy Networks (RPL) was created to provide dependable and energy-efficient data transfer in these networks. However, IoT is susceptible to several security risks, such as routing attacks, due to its dispersed and resource-constrained nature. Strong detection and mitigation measures are necessary because routing attacks, such as Sybil attacks and Clone ID attacks, take advantage of RPL's flaws to interfere with network operations, reduce performance, and endanger data security.

Received: August 04 ,2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

1.1 Sybil Attack

A Sybil attack is a threat to network security in which a malicious node creates several false identities or nodes to gain an excessive amount of authority. By posing as trustworthy nodes, altering routing tables, and depleting resources, this attack can interfere with regular network operations in the context of RPL (Routing Protocol for Low-Power and Lossy Networks). Sybil attacks are characterized by lower packet delivery ratio (PDR), resource depletion, disruption of the Destination Oriented Directed Acyclic Graph (DODAG) structure, and fake node IDs.

1.2 Clone ID Attack

A Clone ID assault, often referred to as a node replication attack, happens when a malicious actor creates duplicate nodes at various network locations while mimicking the identity of a genuine node. Network security may be endangered, performance may suffer, and routing loops may result from this attack. Clone ID attacks are characterized by their ability to replicate authentic IDs, produce irregularities in routing tables, compel nodes to engage in duplicate communication, and result in higher routing overhead, weakened trust, and accelerated battery consumption.

Despite significant progress in securing RPL networks, most existing detection mechanisms are designed to handle either Sybil or Clone ID attacks individually. Additionally, the majority of machine learning-based methods utilize all available input features, which increases computational overhead and energy consumption are important concerns in constrained IoT devices. Notably, very few studies have addressed the combined detection of both attacks or applied feature optimization techniques to improve model efficiency. To bridge this gap, this study proposes a lightweight, scalable machine learning framework using Decision Trees (DT) for classification, enhanced by Particle Swarm Optimization (PSO) for intelligent feature selection. The proposed approach effectively detects Sybil and Clone ID attacks individually and in combination, while reducing resource usage, making it well-suited for real-world IoT deployments.

2. Related Works

Several studies have utilized ML and DL techniques for detecting Sybil and Clone ID attacks in RPL networks. Table 1 summarizes existing works and their respective methodologies. While some focus on trust models or deep learning classifiers, few address network QoS or multi-attack scenarios.

Table 1. Machine Learning Role in Sybil and Clone ID Attack Detection in RPL-based IoT Networks

S.No	Author(s) & Year	Type of Attack	Technique / Model	Evaluation Metrics	Observations
1	Pu (2020)	Sybil	Gini Index	Accuracy, Isolation	Achieves a high detection rate and lower energy use

Received: August 04 ,2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

				Latency, Energy Consumption	
2	Arshad et al. (2022)	Sybil	Hybrid Trust & Cooperative Routing Protocol	Detection Time, Communication Cost, Energy Consumption	Reduces communication cost; trust threshold enhances accuracy
3	Khan et al. (2023)	Sybil	Collaborative with Random Password Generation	Throughput, Average Delay, Detection Rate	Higher latency due to collaborative overhead
4	Hassan et al. (2023)	Sybil	Gini-based Trust Model	Isolation Latency, Delay, Energy Consumption	Reduces delay and energy consumption through a trust model
5	Burange & Deshmukh (2022)	Sybil	Trust-Based Detection	Throughput, Packet Overhead, Delay	Effective in static networks
6	Chulerttiyawong & Jamalipour (2023)	Sybil	Tree-based ML Models (Weka)	Detection Accuracy	Risk of overfitting due to limited features
7	Ul Haq & Saqlain (2023)	Sybil	Ensemble (Naïve Bayes + Boosting)	Detection Accuracy	Tested on NSL-KDD; lacks QoS analysis
8	Cakir et al. (2020)	Sybil	GRU (Deep Learning)	PDR, Energy, Model Accuracy	Performs well on small networks
9	Hussain et al. (2024)	Sybil	Game Theory-Based Trust Model	Throughput, Delay, Energy Consumption	Effective in smaller networks with trust thresholds
10	Morales-Molina et al. (2021)	Clone ID	Dense Neural Network	Accuracy, Precision, Recall	Focuses on model metrics, not network behavior

Received: August 04 ,2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

11	Mirshahjafari & Ghahfarokhi (2019)	Clone ID + Sinkhole	Trust Model	Power Consumption, True Positive Rate	Uses energy-based node trust for detection
12	Raoof et al. (2018)	Clone ID	ML + Rank & Trust	Qualitative	General review of RPL attacks and detection mechanisms
13	Agiollo et al. (2021)	Clone ID	DETONAR	Detection Rate, Time	Uses packet analysis; lacks full QoS analysis
14	Verma & Ranga (2020)	Clone ID	CoSec-RPL (Outlier Detection)	Delay, PDR, Accuracy	Best suited for small networks
15	Adarbah et al. (2022)	Clone ID	Fuzzy Logic Protocol	PDR, Delay, F1-Score	Needs real-time mobile network validation
16	Al-Amiedy et al. (2022)	Clone ID	Literature Review (Various ML/DL Methods)	Model & Network Measures	Summarized available ML/DL techniques
17	Shahid et al. (2024)	Clone ID	Feedforward NN, CNN, LSTM	Accuracy, Precision, Recall, F1-Score	LSTM shows best performance among all evaluated models
18	Sharma et al. (2023)	Clone ID	Q-learning	PDR, Delay, Power Consumption	Scalable but needs tuning for dynamic networks
19	Golla & Pallamsetty (2022)	Sybil + Others	ECC + Q-learning	Network QoS	Achieves higher QoS in small networks
20	Kiraz & Yilmaz (2021)	RPL Attacks	Fuzzy + Tree-Based ML	Detection Accuracy, Network Metrics	Tree-based models outperform other ML techniques

Received: August 04 ,2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

From the analysis of existing works, it is evident that while several machine learning models and trust-based systems have been applied for Sybil and Clone ID attack detection, none have incorporated optimization techniques for feature selection in this context. Most models use all available parameters, increasing overhead and complexity. Furthermore, limited studies address the detection of both attacks simultaneously. To fill this gap, our proposed method introduces feature optimization using PSO to intelligently reduce the feature space, improve detection accuracy, and enhance the system's efficiency, especially in resource-constrained IoT networks.

3. Contribution of the Paper

This paper contributes to enhancing the security and reliability of RPL-based IoT networks through the following key innovations:

- This work proposes a machine learning-based model to detect both Sybil and Clone ID attacks. It supports detection in both individual and combined attack scenarios in RPL-based IoT networks.
- Particle Swarm Optimization is applied to select the most relevant input features. This reduces computational complexity and improves detection accuracy.
- Two models, a standard Decision Tree and a PSO, are developed and compared across multiple metrics. PSO-DT consistently outperforms DT in both detection and network performance.
- Both model-level and network-level metrics are analyzed for performance evaluation. These include accuracy, precision, recall, PDR, delay, energy consumption, and overhead.

4. Proposed Methodology

This paper addresses machine learning (ML)- based Routing attack detection, such as clone ID attacks and Sybil attacks, in the RPL network. To detect these attacks, the network is designed using the parameters in Table 2. ML techniques identify the pattern in the dataset through their input feature for attack detection, while in the trust-based calculation, the detection is based on the trust threshold set for detection. Due to this automated detection nature, this paper utilized ML-based attack detection for the RPL network. Here, two types of ML models were proposed for attack detection. Those models are as follows:

- Decision tree (DT) based Attack detection (DT-ADM)
- Optimized Decision tree-based attack detection. (ODT-ADM)

4.1 Decision Tree (DT)

In Machine Learning (ML), the Decision Tree is one of the algorithms that can perform both classification and regression operations. It provides results by splitting the dataset into a tree-like structure using criteria like Gini Index, Information gain, or variance reduction. Here, the topmost node of the tree will be the root node, and the final prediction will be taken from the leaf nodes. DT attracts many users due to its advantages, such as an easier way of representation, the ability to handle non-linear data relationships, and the optimization of

Received: August 04 ,2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

feature sets. Sometimes, DT may also lead to overfitting and non-smooth boundaries between its variables. The steps in DT are as follows:

- Selects the best attribute and metric for splitting the dataset.
- Start splitting till it reaches the stop condition.
- At the end of the stopping condition, assign labels to leaf nodes through voting or their average values.

Figure 2 shows the sample output of the DT operation, which splits the data into normal, Sybil, and clone ID attacks using the Gini Index as the condition metric for classification.

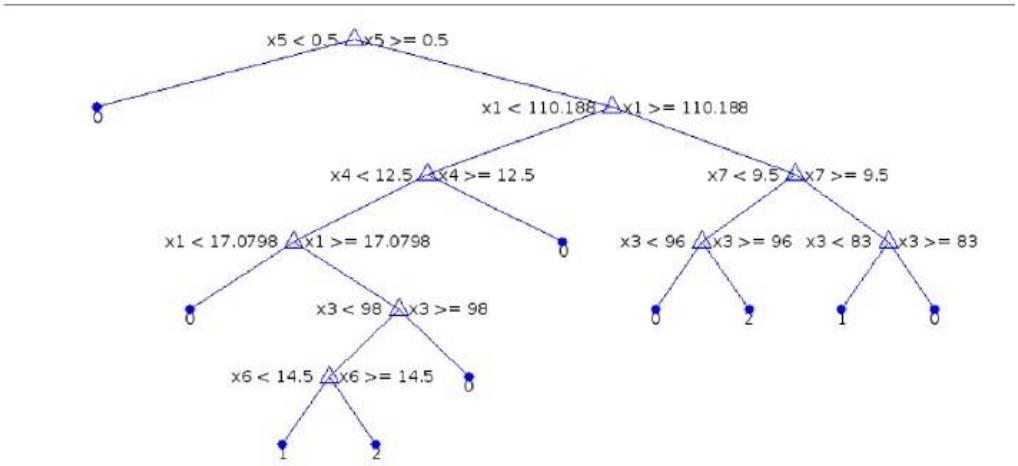


Figure 2. Performance of DT on combined attacks

To enhance the model's performance, the input attributes were optimized using particle swarm optimization, and the corresponding steps are given in the following section.

In this work, Decision Tree (DT) is used as the existing model for attack detection in RPL-based IoT networks. It is chosen due to its simplicity, interpretability, and low computational overhead, making it highly suitable for resource-constrained IoT devices. Unlike many existing works that rely on complex models such as neural networks or ensemble classifiers, DT provides fast classification, requires minimal tuning, and is effective even with limited datasets.

4.2 Decision Tree -Attack Detection

In DT-ADM, the attacks were detected by utilizing all the input features of the dataset, such as node position, energy, Packet sent, packet received, neighbors, and repeated ID. This makes it an ideal benchmark to evaluate the performance improvements introduced by the proposed optimized model using PSO.

Received: August 04 ,2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

4.3 Particle Swarm Optimization-based Decision Tree

Decision Trees (DTs) are widely utilized for detecting network attacks such as Sybil and Clone ID attacks in RPL networks due to their simplicity and interpretability. Sybil attacks involve a single malicious node forging multiple identities, while Clone ID attacks involve duplicating legitimate node IDs to compromise the network. By leveraging key features such as node position, energy, neighbors, packets sent and received, and repeated IDs, DTs can classify nodes effectively into normal or malicious categories. When both Sybil and Clone ID attacks are present, a combined detection approach is employed, analyzing multiple attack patterns simultaneously. The optimized DT model, using techniques like Particle Swarm Optimization (PSO), enhances the detection accuracy by selecting the most critical features, reducing computational overhead, and improving performance metrics such as Packet Delivery Ratio (PDR), delay, energy consumption, and overhead. Thus, DT and optimized DT approaches are powerful tools for addressing single and combined attack scenarios in RPL networks.

4.4 ODT-ADM: Optimized Attack Detection

While in ODT-ADM, the Particle Swarm optimization is used to find the two optimal parameters among packet send, packet receive, neighbors, energy, and repeated ID. The PSO is used here because it is lightweight, converges quickly, and requires minimal tuning, and reduce energy consumption which making it ideal for constrained IoT networks. These two optimal parameters will be combined with the node position for the final decision tree-based attack detection. Both these models were tested under two scenarios as follows:

4.4.1 Scenario 1

In scenario 1, either the clone ID or the Sybil attack alone is injected into the network. This scenario helps to analyze the proposed model's performance on individual attack detection.

4.4.2 Scenario 2

In scenario 2, both attacks were injected into the network. This scenario analysis helps to analyze the dynamic nature of ML model detection in multiple attack detection at a time. It analyzes the automated ML detection in finding both types of attacks.

4.5 Proposed Work Architecture

Figure 1 illustrates the architecture of the proposed method, which constitutes a PSO-optimized Decision Tree framework designed to detect Sybil and Clone ID attacks within IoT RPL networks. This framework collects data from IoT nodes to construct features and subsequently applies these features to both models to accurately classify the attacks. Then, the performance metrics were evaluated for enhanced results.

Received: August 04 ,2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

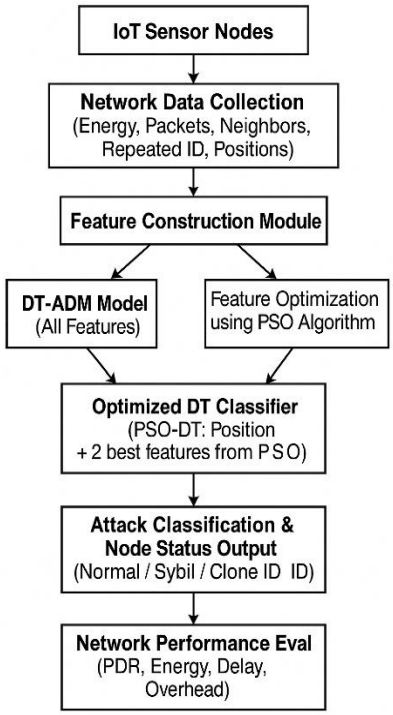


Figure 1. Block diagram of the proposed PSO-optimized DT attack detection system in RPL-based IoT networks.

4.6 Particle Swarm Optimization-based Feature Selection

In this, the particle swarm optimization is used to select the two optimal features among packet send, packet received, neighbors, energy, and repeated ID. Because collecting all information from nodes will result in higher computational time and complexity. Hence, in this case, the two optimal attributes, along with position, will be used for training the model. The steps for feature selection using PSO are as follows:

Step 1: Begin

Step 2: Initialise PSO parameters for both the algorithm and the position update process as given in Tables 2 and 3. Table 2 parameters are used for the algorithm operation. Table 3parameters are used for the position update process

Table 2: PSO Algorithm Parameters (AP) & notations

AP	**Range**
LB (Lower bound)	[1 1]
UB (Upper Bound)	[5 5]
Iteration Count (IC)	50
Swarm Count (SC)	25
Output dimension	2

Received: August 04 ,2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

	Any number between 0 and 1
Current Iteration	C_i
Next Iteration	N_i

Table 3: Position Update Parameters

	Range
Learning Coefficient	0.7
Social Coefficient (sc)	1.3
Weight Inertia (WI)	0.7

Step 3. PSO begins its operation using the parameters in Tables 2 and 3. The PSO optimizes its position by evaluating its fitness function through equation 1.

Objective function = minimize [DTE]	(1)

Step 4: At the end of each iteration, the two best solutions will be calculated. One is Global (G), which represents the overall best solutions for all completed iterations, and local (L), which represents the best solution of the current completed iteration.

Step 5: Like solutions, the positions were also updated for each iteration using equations 2 and 3.

$\mathrm{P}(N_i) = \mathrm{P}(C_i) + \mathrm{V}(N_i)$	(2)

Here, P and V represent the position and velocity of swarms. Like position, the velocity also gets updated for each iteration using equation 3.

$V(N_i) = W_i * V(C_i) + L_C * R_1 * L + S_C * R_2 * G)$	(3)

Step 6: Steps 3 to 5 repeat until the iteration count is reached. Once the iteration count is reached, the optimal attributes for classification will be obtained.

5. Simulations

The proposed work utilized the Table 4 parameters for realizing the network simulation in a Python 3.9 software in Spyder environment. The methodology is based on a custom-generated dataset named rpl_attack_dataset_sybil_clone_full.csv, which simulates the behavior of IoT nodes in an RPL network environment under two distinct scenarios. The training and

Received: August 04 ,2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

implementation of the proposed system were executed in the same environment by using the Matplotlib library, which is used for data management, visualisation, and model creation. The robust model evaluation was ensured by dividing the dataset into 80% training and 20% testing sets. The baseline model was a typical Decision Tree Classifier with entropy-based splitting. A Particle Swarm Optimisation (PSO) technique was used to improve detection performance. It used 30 particles and 100 iterations to choose the most significant feature subset before training. The stability and scalability of the model were evaluated by simulating increasing node densities, from 10 to 100 IoT nodes, by implanting malicious nodes in the ratio of 1:10 in the network. Table 4 parameters are common for both the DT model and the Optimized DT model.

Table 4: RPL network parameters

Parameters	**Values**
RPL Network Definition	
Total Number of Nodes	10 to 100
Area	300* 300 m^2
Communication range	50m
Topology	Random
Mote Type	Zolertia Zl
RPL objective function	MRHOF
RPL routing mode	Storing Mode
Radio Medium Model	UDGM
Random Generation Parameters	
Energy range	[50 100]
Average Traffic Rate	10 packets/second
Packets Sent	5-15
Packets Received	3-12
Labels	0- Normal 1- Sybil 2- Clone ID

Received: August 04 ,2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

With the Table 4 parameters, the node distribution of normal, clone, and Sybil in the RPL network is presented in Figure 3. The corresponding data transmission information was saved as a CSV file for attack detection.

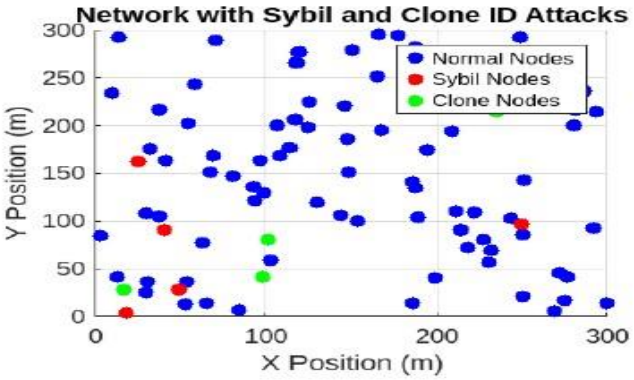


Figure 3. Node distributions

With the attack information, the DT and Optimized DT performed their classification process, and their results were analyzed in terms of both model metrics and network metrics for both scenarios. In model metrics, accuracy, precision, and recall were used for analysis. While network metrics, the PDR, Delay, Energy consumption, and total overhead were used for analysis.

6. Results and Discussion

6.1 Scenario 1 Analysis

In scenario 1, the individual attack detection analysis was performed for both the decision tree and the optimized decision tree. The corresponding performance was analysed using network and model metrics and is presented in a graph representation in figures and tabular format in Table 5.

I. Network Metric analysis

In this, the network QoS was analyzed using the proposed DT and PSO-DT for clone ID and Sybil attacks individually, and their results were presented in Figures 4 to 11.

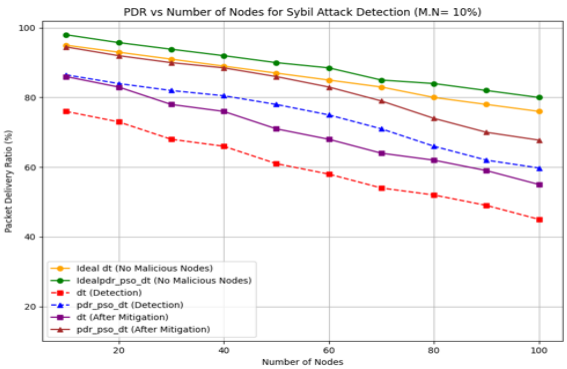


Figure 4: Packet Delivery Ratio

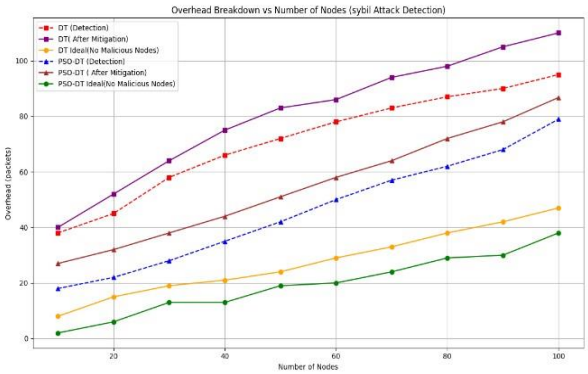


Figure 5: Total Overhead

Received: August 04 ,2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

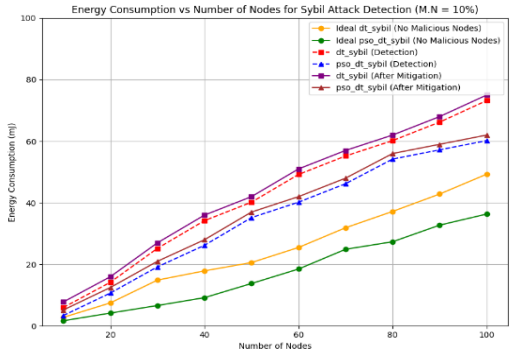


Figure 6: Energy Consumption

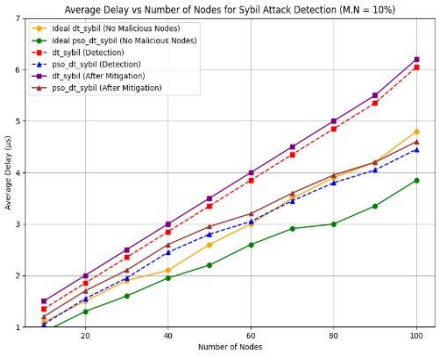


Figure 7: Average Delay

The study demonstrates that PSO-based optimization outperforms Decision Tree (DT) in all metrics for sybil attack, including Packet Delivery Ratio (PDR), Total Overhead, Energy Consumption, and Average Delay. In each graphical representation, we illustrate the comparative analysis of the ideal range (when no malicious activity is detected within the nodes), detection range, and mitigation range values distinctly for both the proposed PSO-DT methodology and the existing DT framework. The PDR decreases with an increase in network density, while the PSO-DT consistently has a higher PDR, as shown in Figure 4. In Figure 5, the total overhead increases with network size, while the PSO-DT reduces the unnecessary message transmission by starting at 25 packets and reaching 85 packets. Energy consumption increases with network size and activity, but the optimized model consistently shows lower consumption, demonstrating better energy efficiency in Figure 6. Average delay also decreases in network transmission, from 1.2 µs to 4.6 µs, indicating growing congestion and processing times. The PSO-DT model reduces delays, improving network responsiveness shown in Figure 7. In conclusion, PSO-DT outperforms standard DT in all metrics, including higher PDR, lower Total Overhead, reduced energy consumption, and shorter Average Delay. These improvements make PSO-DT a superior approach for attack detection in IoT-based RPL networks, especially in scenarios with increasing network size and complexity. The optimized model demonstrates better energy efficiency and reduces delays, making it a superior approach for IoT-based RPL network

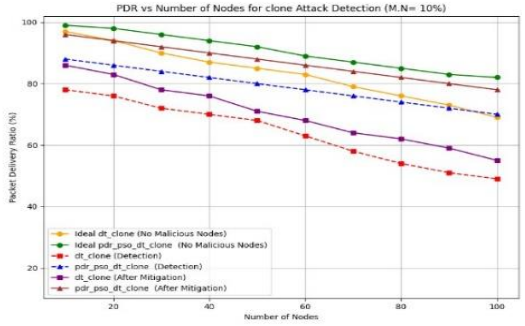


Figure 8: Packet Delivery Ratio

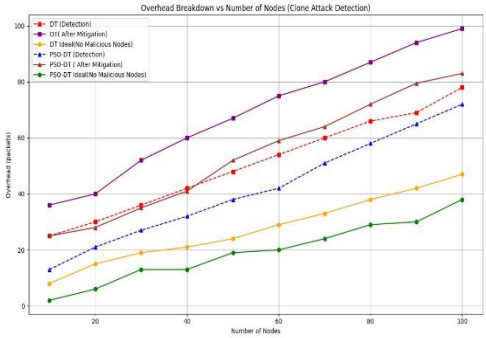


Figure 9: Total Overhead

Received: August 04 ,2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The study demonstrates that PSO-based optimization outperforms Decision Tree (DT) in all metrics for clone ID attack, including Packet Delivery Ratio (PDR), Total Overhead, Energy Consumption, and Average Delay, as shown in Figures 8 to 11. The PDR decreases with an increase in network density, while the PSO-DT consistently has a higher PDR. The total overhead increases with network size, while the PSO-DT reduces it by starting at 20 packets and reaching 80 packets. Energy consumption increases with network size and activity, but the optimized model consistently shows lower consumption, demonstrating better energy efficiency. Average delay also decreases with network size, from 0.8 µs to 3.5 µs, indicating growing congestion and processing times.

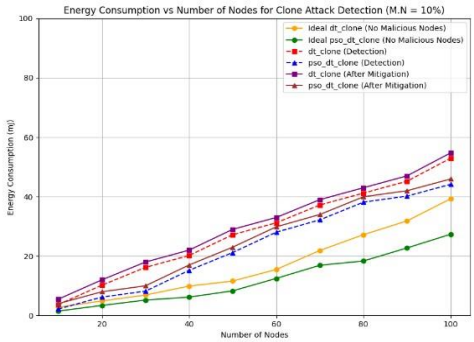


Figure 10: Energy Consumption

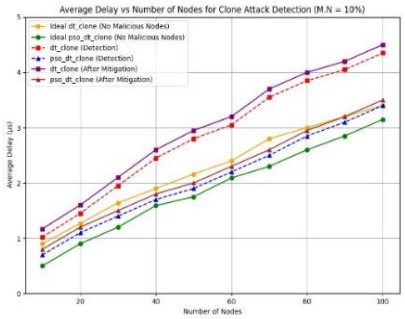


Figure 11: Average Delay

The PSO-DT model reduces delays, improving network responsiveness. In conclusion, PSO-DT outperforms standard DT in all metrics, including higher PDR, lower Total Overhead, reduced energy consumption, and shorter Average Delay. These improvements make PSO-DT a superior approach for attack detection in IoT-based RPL networks, especially in scenarios with increasing network size and complexity. The optimized model demonstrates better energy efficiency and reduces delays, making it a superior approach for IoT-based RPL networks.

II.Model metrics

In this, the model performance was analyzed in identifying individual attacks in the RPL network through Accuracy, precision, and recall, and its values are presented in Table 5.

Table 5. Scenario 1 Model analysis

Methods	Attacks	Accuracy (%)	Precision (%)	Recall (%)
DT	Clone	95.3	94.2	93.1
	Sybil	95.6	93.8	93.9
PSO-DT	Clone	98.85	95.2	94.1
	Sybil	97.6	94.8	94.9

Received: August 04 ,2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Particle Swarm Optimization (PSO-DT) outperforms DT in detecting Clone ID and Sybil attacks, demonstrating its effectiveness in improving classification models. This enhances precision, reduces false positives, and increases recall, ensuring reliable detection of malicious activities. PSO-DT is a robust solution for real-world IoT network security, as it optimizes input features, making it more efficient and reliable in mitigating routing attacks in IoT-based RPL networks.

5.2 Scenario 2

In scenario 2, both attacks will occur in the network at any time, and it is detected through both DT and PSO-DT. Like scenario 1, DT and PSO-DT performance in scenario 2 is analyzed using both model metrics and network metrics as shown in below figures and table. The Combined attack detection using PSO-DT is presented in the figure below.

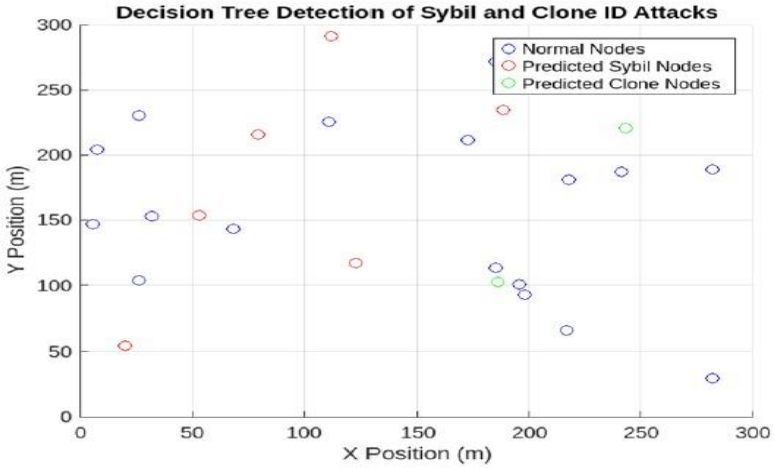
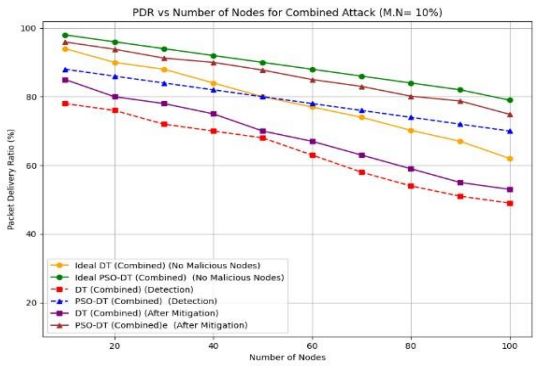


Figure 12. Node distributions

Figure 12 shows the node distribution, and the evaluation of combined attack detection using Decision Tree (DT) and optimized Decision Tree (PSO-DT) models reveals several key performance improvements.



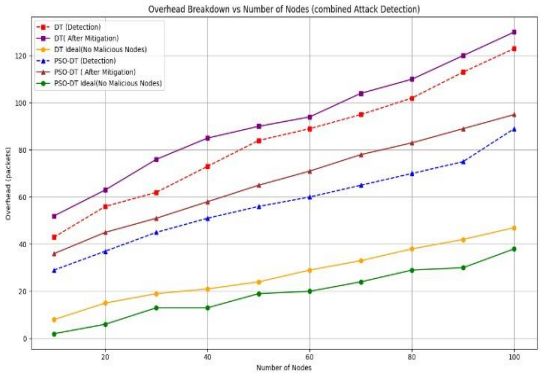


Figure 13: Packet Delivery Ratio **Figure 14: Total Overhead**

The PSO-DT model consistently has a higher Packet Delivery Ratio (PDR), reducing from 97% to 83%, demonstrating improved reliability in packet transmission as shown in Figure 13.

Received: August 04 ,2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

It also maintains lower total overhead, reducing redundant communication overhead and preserving network efficiency in Figure 14. The PSO-DT model also shows lower energy consumption across all node counts, optimizing energy utilization for resource-constrained IoT devices in Figure 15.

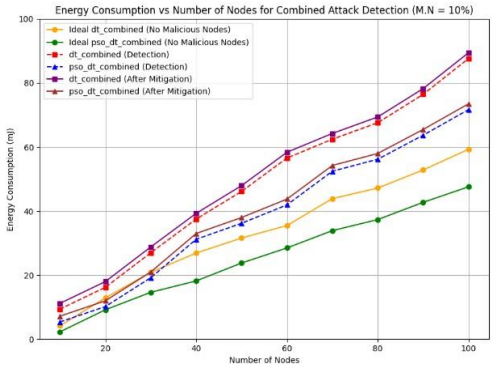


Figure 15: Energy Consumption

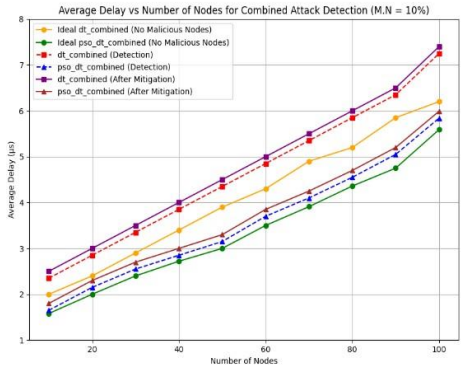


Figure 16: Average Delay

Additionally, Figure 16 shows that the PSO-DT model achieves consistently lower delay, ensuring faster data transmission and minimizing latency, crucial for real-time IoT applications. Overall, the PSO-DT model outperforms the standard DT in detecting combined attacks in RPL networks, demonstrating its suitability for dynamic and resource-constrained IoT environments.

III. Model metrics

In this, the model's performance was analyzed in identifying individual attacks in the RPL network. Accuracy, precision, and recall, along with their values, are presented in Table 6.

Table 6. Scenario 2 Model analysis

Methods	Attacks	Accuracy (%)	Precision (%)	Recall (%)
DT	Combined	94.3	93.2	92.1
PSO-DT	Combined	96.84	95.2	94.1

Particle Swarm Optimization (PSO-DT) outperforms DT in detecting combined attacks, demonstrating its effectiveness in improving classification models. This enhances precision, reduces false positives, and increases recall, ensuring reliable detection of malicious activities.

Table 7 presents a detailed comparison between the proposed PSO-DT model and existing state-of-the-art approaches, showcasing its superiority across critical performance metrics. The proposed PSO-DT achieves the maximum accuracy, improved packet delivery, shorter delay, and energy efficiency.

Received: August 04 ,2025

International Journal of Applied Mathematics
Volume 38 No. 5 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 7. Comparative Analysis of Proposed PSO-DT with Existing Models

Method	Detection Accuracy (%)	PDR (%)	Avg Delay (µs)	Energy (mJ)
Proposed PSO-DT	96.84	94.5	2.1	21.3
DT (Existing)	94.3	89.2	3.8	26.5
GRU [Cakir et al., 2020]	93.5	85.0	2.5	24.8
Trust-Model [Arshad et al.]	92.1	83.3	3.1	27.4

PSO-DT is a robust solution for multi-attack security for IoT environment, as it optimizes input features, making it more efficient and reliable in mitigating routing attacks in IoT-based RPL networks.

7. Conclusion

The study proposes a machine learning-based approach for detecting Sybil and Clone ID attacks in IoT networks using Decision Tree (DT) and an optimized PSO-DT model. Tested under individual and combined attack scenarios, PSO-DT achieved a superior accuracy of 97.6% for Sybil, 98.85% for Clone ID, and 96.84% for combined attacks. It outperformed DT by optimizing feature selection and tree parameters. The model demonstrated improvements in detection rate, energy efficiency, overhead reduction, and PDR recovery. Its adaptability to varying node densities and attack intensities makes it well-suited for large-scale, real-world IoT deployments.

8. Future Work

In the future, the proposed work can be further enhanced by analyzing all types of routing attacks and extending it to integrate blockchain-based consensus and real-time mitigation via smart contracts in the RPL-based IoT network.

9. Conflicts of Interest

The authors declare that they have no conflict of interest.

10. Acknowledgements

I would like to take this opportunity to acknowledge that there are no individuals or organizations that require recognition for their contributions to this work.

13. References

[1] Pu C. Sybil attack in RPL-based internet of things: analysis and defenses. *IEEE Internet Things J*. 2020;7(6):4937–4949.

Received: August 04 ,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[2] Arshad D, Asim M, Tariq N, Baker T, Tawfik H, Al-Jumeily D. THC-RPL: Trust-enabled routing in RPL-based IoT. *PLoS One*. 2022;17(7):e0271277.

[3] Khan MA, Hussain I, Bhatti A, Imran M. Collaborative detection of Sybil attacks in RPL. *Comput Mater Continua*. 2023;77(1):753–767.

[4] Hassan M, Rehman A, Faheem M. GITM: Gini index-based trust mechanism for Sybil attack mitigation in IoT. *IEEE Access*. 2023;11:62697–62720.

[5] Burange AW, Deshmukh VM. Detection of RPL attacks using trust mechanism. In: *Proc ACI@ISIC*; 2022. p. 152–162.

[6] Chulerttiyawong D, Jamalipour A. Sybil detection in the Internet of Farming Things using machine learning. *IEEE Internet Things J*. 2023;10(14):12854–12866.

[7] ul Haq HB, Saqlain M. Machine learning-based Sybil detection in RPL. *Theor Appl Comput Intell*. 2023;1(1):1–14.

[8] Cakir S, Sahingoz OK, Tomur E. GRU-based RPL attack detection model. *IEEE Access*. 2020;8:183678–183689.

[9] Hussain MZ, Rehman A, Abbas G, Faheem M. Trust-based lightweight system for Sybil mitigation in IoT. *PeerJ Comput Sci*. 2024;10:e2231.

[10] Morales-Molina CD, Santana M, Gonzalez J, Torres E. Neural network for Clone ID attack detection in WSNs. *Sensors*. 2021;21(9):3173.

[11] Mirshahjafari SMH, Ghahfarokhi BS. Hybrid CloneID and Sinkhole detection model for IoT networks. *Inf Secur J*. 2019;28(4–5):107–119.

[12] Raoof A, Matrawy A, Lung CH. Routing attacks and mitigation in RPL-based IoT: A survey. *IEEE Commun Surv Tutor*. 2018;21(2):1582–1606.

[13] Agiollo A, D'Orazio L, Di Pietro R. DETONAR: Lightweight RPL routing attack detection model. *IEEE Trans Netw Serv Manag*. 2021;18(2):1178–1190.

[14] Verma A, Ranga V. CoSec-RPL: Clone detection using outlier analysis in RPL-based IoT. *Telecommun Syst*. 2020;75(1):43–61.

[15] Adarbah HY, Abdulkader AM, Al-Otaibi SA, Mahgoub I. Secure authentication in RPL using ECDH. *IEEE Access*. 2022;11:11268–11280.

[16] Al-Amiedy TA, Al-Khafaji AJ, Jasim AT, Alrubaie A. A comprehensive review of ML/DL approaches in RPL security. *Sensors*. 2022;22(9):3400.

[17] Shahid U, Nazir B, Latif S, Kazmi K. Hybrid intrusion detection system for RPL using ML and DL. *IEEE Access*. 2024;12:45638–45653.

[18] Sharma G, Tripathi A, Rani S, Iqbal R. QSec-RPL: Q-learning-based secure routing protocol against RPL attacks. *Ad Hoc Netw*. 2023;142:103118.

Received: August 04 ,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[19] Golla K, Pallamsetty S. ECC-based ML-RPL protocol for secure communication. *Int J Netw Secur Appl*. 2022;14(2):15–29.

[20] Kiraz MU, Yilmaz A. Comparative evaluation of ML algorithms for RPL-based attack detection. In: *Int Conf Intell Fuzzy Syst*; 2021. p. 254–262.

BIBLOGRAPHY

J. Brindhadevi received her B.E. degree from St. Peter's College of Engineering and Technology from Avadi, Chennai, Tamil Nadu, India in 2016 and completed her M.E degree from Annamalai University, Chidambaram, Tamil Nadu, India in 2018. She is currently pursuing her PhD from Annamalai University, Chidambaram, Tamil Nadu. She also presented various academic research-based papers at several International Journals, and national and international conferences. Her research interest includes a wireless communication network, Internet of Things, and Network Security.

Dr. Devarajan. K received his B.E. degree from Krishnasamy College of Engineering and Technology, Cuddalore, Tamil Nadu, India in 2001 and M.E. degree from Annamalai University, Chidambaram, Tamil Nadu, India, in 2003. He also received his Doctorate degree from Annamalai University, Chidambaram, Tamil Nadu, India with the Department of Electrical and Electronics, in 2018. He is currently working as Asst. Professor with the department of Electronics and Communication Engineering, Annamalai University, Chidambaram, Tamil Nadu, India. He has published 15 national and international journals. His research area includes ad-hoc networks, Wireless Systems, Signal Processing and Communication Networks.

Received: August 04 ,2025