International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 03 | Mar 2025 www.irjet.net p-ISSN: 2395-0072

Prediction and Detection of Black Hole Attack Using the COOJA Simulator

Dr. K. SOUMYA[1], BALUSU DEEPIKA[2], BOJJA AKHILA[3], BONTHALAKOTI REVATHI[4], CHALLA NAGA VINAYA[5], Dr. S. PALLAM SETTI[6]

[1]Assistant Professor, Department of Computer Science and Systems Engineering, Andhra University College of Engineering for Women, Visakhapatnam, Andhra Pradesh, India
[2-5]B. Tech Final Year, Computer Science and Systems Engineering, Andhra University College of Engineering for Women, Visakhapatnam, Andhra Pradesh, India
[6]Founder & CEO, Dr Pallam Setti Center for Research & Technology, A-hub, Andhra University, Visakhapatnam, Andhra Pradesh, India

---

Abstract - *Routing Protocol for Low-Power and Lossy Networks (RPL) is widely used in Wireless Sensor Networks (WSNs). This protocol is vulnerable to routing attacks. One such attack is the Black Hole attack. In this attack, a malicious node falsely advertises an optimal path and tries to attract traffic. This results in dropping of packets which severely degrades the network performance.*

In this work, we simulated Blackhole attack with and without a malicious node using Cooja simulator 3.0 and Contiki-Ng operating system.

From the results, it is found that in the absence of a malicious node, the network maintains a high Packet Delivery Ratio (PDR) of around 99%, with minimal packet loss and low delay, ensuring stable communication. However, in the presence of a malicious node, PDR drops drastically to around 0.15%, while packet loss increases significantly, along with higher delay and jitter, leading to severe network disruption. To mitigate this, anomaly detection techniques like Autoencoder and Isolation Forest (iForest) were implemented, reinforcing the need for improved RPL security strategies.

Key Words: Cooja simulator, rpl based attacks, WSN security, IoT security, Anomaly detection

I. INTRODUCTION

The growing adoption of Internet of Things (IoT) and Wireless Sensor Networks (WSNs) across industries has driven measurable progress, delivering both economic value and societal impact. Yet, these systems remain vulnerable to persistent security threats. One such attack is denial-of-service (DoS). This targets Routing Protocol for Low-Power and Lossy Networks (RPL). As such, blackhole attack compromises the routing integrity, there by escalates latency and drains energy reserves. This potentially causes cascading network failures. This work emphasizes the prediction and detection of RPL-centric attacks through simulations done in the Cooja environment which is a benchmark platform for IoT network modeling. By evaluating traffic anomalies, mapping attack signatures, and quantifying operational impacts, the study seeks to establish adaptive defense protocols for critical IoT infrastructures. This work offers practical solutions for three core challenges namely threat forecasting, anomaly recognition, and post-incident forensic analysis within resource-constrained WSN and IoT ecosystems.

II. REVIEW OF LITERATURE

WSNs operate in IoT applications as they provide real-time data collection and transfer capabilities. Since RPL operates in an accessible environment with constrained resources it faces severe security risks over its open sarchitecture from Routing Protocol for Low-Power and Lossy Networks attacks.[5] RPL protocol enables efficient WSN routing. There have been regular attacks targeting RPL using black hole methods which take advantage of its exposed vulnerabilities. [1]

Many studies have investigated how RPL attacks affect the operational stability and performance quality of WSNs [2]. The attacks have a significant impact on packet delivery ratio and latency degradation which presents major security issues for WSN networks.[6] Research on the black hole attack exists extensively because it leads to devastating effects on data delivery. A single black hole node according to Khan et al. (2021) [3] causes significant reduction in data packet delivery by simply consuming packets which never reach their destination nodes. An Intrusion Detection System designed by Singh and Sharma (2018) [4] detects black hole attacks by using traffic monitoring alongside anomaly detection methods which provides improved packet delivery rates. These systems bring excessive computational difficulties to WSN networks due to restrictions on resources.

The current defensive protocols for RPL focuses on implementing authentication features along with anomaly detection features to enhance its security. [7] Security and resource efficiency continue to be direct challenges for the implementation of RPL security enhancements using cryptographic techniques and lightweight ids as recommended by Raza et al (2019) [4]. The authors Gupta and Verma (2020) [4] developed trust-based routing approaches which evaluate node behaviors to determine trust values thus reducing RPL attack vulnerabilities. The defense methods exhibit potential yet their ability to counter black hole attacks. The current research fails to adequately explore the integrated effect that RPL attacks using Cooja exert on network performance according to existing academic literature.[9] Finne et al. present a Cooja extension named Multi Trace [10] that collects simulation logs at multiple levels at the same time. We use Cooja network simulator for Contiki OS to run our experiments and multi-trace to generate our dataset. It is widely used RPL network simulator. Using Cooja's Multi-Trace extension [8], we create our own IDS dataset. With this dataset, we test and evaluate our proposed ML models.

III. METHODOLOGY

The following steps are implemented in prediction, detection and mitigation of RPL-based attacks using Cooja simulator.

1. Network Setup in Cooja Simulator
A IoT network is configured in Cooja simulator under Contiki-NG OS using RPL protocols.[9] The sensor nodes are deployed alongside a sink node to create a Directed Acyclic Graph (DAG) topology. Operational roles are assigned to legitimate and malicious nodes to replicate standard and adversarial behaviors.

2. Simulation of RPL-Based Attacks
Black hole attack is simulated by configuring malicious nodes to broadcast false optimal routes, inducing packet loss through traffic redirection.

3. Data Collection & Feature Extraction
Network traffic logs are captured through Wireshark and archived for subsequent evaluation.
Key metrics like packet loss rate (PDR), hop count, variance, end-to-end latency, and routing update frequency are isolated for analysis.
Log normalization into CSV format is performed to enable machine processing.

4. Data Preprocessing & Visualization
Data cleansing removes artifacts and redundancies while preserving attack signatures.
MATLAB 4.2.3 is used to generate 3D visualizations, to map topological deviations caused by intrusion events.

5. Anomaly Detection Using Machine Learning
The Isolation Forest algorithm is used to identify behavioral outliers in network operations.
Autoencoders reconstruct baseline traffic patterns, enabling anomaly flagging through reconstruction error thresholds.

6. Performance Evaluation & Analysis
Detection accuracy metrics undergo rigorous assessment, including false positive rate, precision, recall, and F1-score calculations.
Comparative analysis evaluates network efficiency across pre-attack, attack-phase, and post-mitigation states.

7. Mitigation & Security Enhancement
Mitigation strategies are formulated based on detection outcomes and attack severity rankings.
Protocol enhancements are proposed for RPL routing mechanisms and security frameworks to deter similar exploits.

IV. Network Simulation

A Flowchart for RPL based Attacks is shown in figure1.

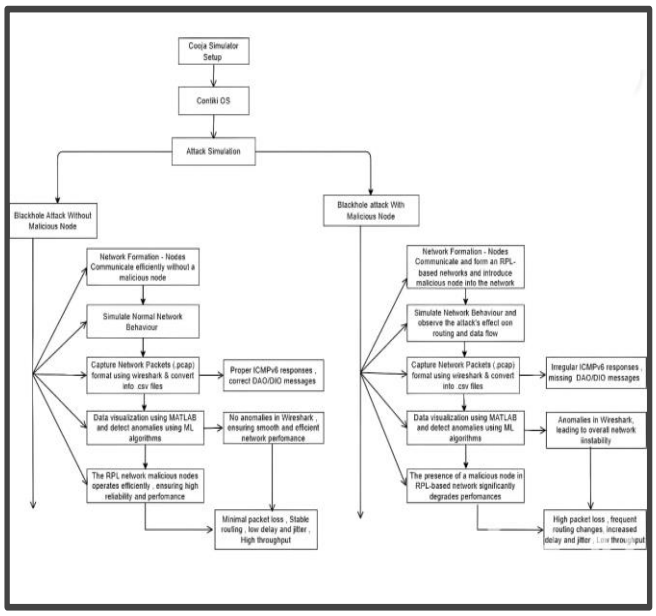

Fig 1. Flowchart for Rpl based Attacks and Performance Analysis Using Cooja and Contiki OS

Step 1: Data Collection & Preprocessing

(1) Simulating RPL Attacks in Cooja (Contiki-NG)
Cooja simulator creates a network topology with IoT sensor nodes running the RPL protocol.[9] A blackhole attack is injected into malicious nodes, that manipulate routing updates. This attacks network performance, such as increased packet loss, route instability, and energy consumption.

(2) Capturing Network Traffic Using Wireshark 4.2.3

Wireshark is used to analyze packet-level communication between nodes. It captures the network traffic in. pcap (packet capture) format to record routing changes, dropped packets and suspicious behaviors. It identifies the key indicators of attacks, such as abnormal rank changes or packet forwarding inconsistencies.

(3) Converting Logs to CSV for Analysis

Export the .pcap logs to a structured CSV file using Wireshark's export feature or Python scripting. This extracts essential packet details like source/destination IP, timestamp, sequence number, and hop count for anomaly detection.

(4) Feature Selection for Machine Learning

Identify the relevant features that indicate attack patterns:

- Packet Loss Rate – Higher losses suggest Black Hole attacks.
- Packet Forwarding Behavior – Nodes failing to forward packets may be malicious.

(5) Data Cleaning & Normalization

Remove duplicate or irrelevant entries to ensure dataset accuracy. Normalize feature values (e.g., scale rank and hop count) to standardize inputs for machine learning models.

Handle missing values and balance the dataset to prevent model bias.

Step 2: Anomaly Detection

(1) Model Selection for Anomaly Detection

Isolation Forest: Detects anomalies by isolating rare patterns in packet behavior.

Autoencoders: A neural network-based approach that reconstructs normal traffic and flags deviations as attacks.

(2) Training the Model

Use the preprocessed dataset containing both normal and attack scenarios.

Train models on selected features: packet loss, hop count, rank changes, forwarding behavior, etc.

Separate data into training (70%) and testing (30%) sets for evaluation.

Step 3: Visualization & Interpretation

(1) Tools for Visualization

- Python Libraries: Matplotlib, Seaborn, Plotly for interactive graphs
- MATLAB: Advanced 3D plotting for attack impact analysis

(2) Attack Trend Analysis:

- Line Plot: Tracks variations in key metrics (latency, PDR, throughput) over time to identify attack patterns.
- Scatter Plot: Displays anomalies by plotting packet behaviors (e.g., hop count vs. packet loss)
- Histogram: Shows the frequency distribution of delays, helping detect abnormal network behavior
- 3D Scatter Plot: Visualizes multi-dimensional attack trends by mapping packet loss, rank changes, and delay in a 3D space
- Bar Chart: Compares network performance metrics (before and after attack detection) to highlight improvements.

Step 4: Performance Evaluation of the Network

To assess the impact of RPL-based attacks and the effectiveness of the detection model, key network performance metrics are analyzed.

(1) Metrics for Evaluation [4]

- Latency: Measures the time taken for a packet to travel from source to destination. High latency indicates network congestion or attack impact.
- Jitter: Represents the variation in packet delay. Increased jitter can be a sign of routing instability caused by attacks.
- Packet Delivery Ratio (PDR): Ratio of successfully delivered packets to total sent packets. A lower PDR suggests packet drops due to attacks like Black Hole.
- Throughput: Amount of data successfully transmitted over a period. Reduced throughput signals network degradation.
- End-to-End Delay: Average time taken for a packet to traverse the network. Increased delay may indicate attack-induced retransmissions.

VI. RESULTS & ANALYSIS

The simulations demonstrated the impact of RPL-based attacks on network performance and reliability.

The Cooja simulator of this work is shown in figure2. The packets captured in Wireshark is shown in figure3. The visualization of blackhole attack detection in MATLAB with packet count analysis over time is presented in fugure4. The network performance metrics, including throughput, delay, packet delivery ratio (PDR), latency, jitter, and time is tabulated in table1. The Scatter plot illustrating anomaly detection in packet count over time is shown in figure5.

A graph comparing Packet Delivery Ratio (PDR) with and without a malicious node is shown in figure6.

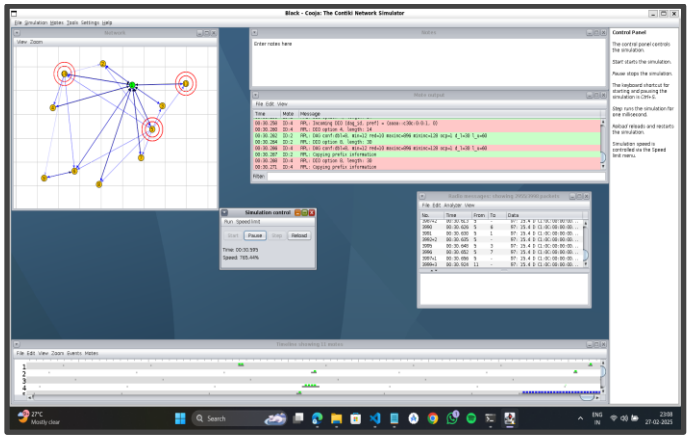

Fig2. Setting up Cooja simulation with network topology, packet logs, and node interactions

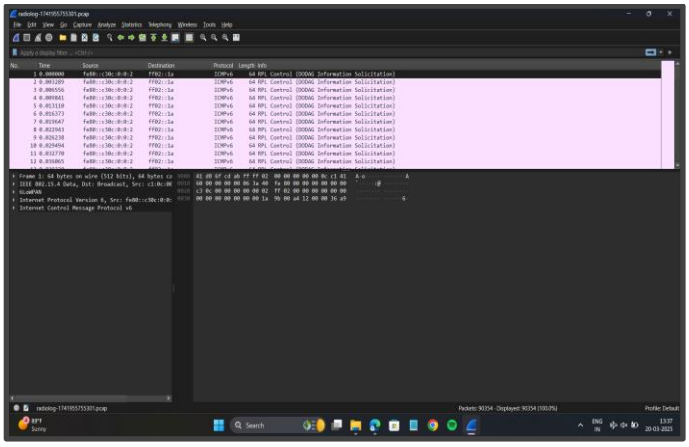

Fig3. Analyzing captured RPL control messages in Wireshark from Cooja simulation

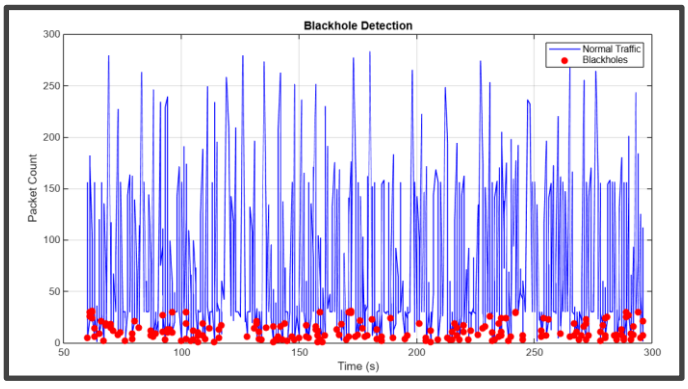

Fig4. Visualizing blackhole attack detection in MATLAB with packet count analysis over time

Throughput (KBps)	Delay (s)	PDR%	Latency	Jitter	second
13.69248458	0.037518	0.050073	1.012973	0	60
13.69248458	0.046044	0.0408	1.000697	0.012276	60
13.69248458	0.006493	0.289312	0.998131	0.002566	60
13.69248458	0.202595	0.009273	1.000845	0.002714	60
38.63322889	0.043509	0.042655	1.001495	0.00065	61
38.63322889	0.033357	0.055637	0.999021	0.002474	61
38.63322889	0.038488	0.048219	1.001123	0.002102	61
38.63322889	0.033357	0.055637	0.999021	0.002102	61
38.63322889	0.005498	0.337531	0.999878	0.000857	61
38.63322889	0.005818	0.318985	0.990599	0.009279	61

Table1. Table showing network performance metrics, including throughput, delay, packet delivery ratio (PDR), latency, jitter, and time.

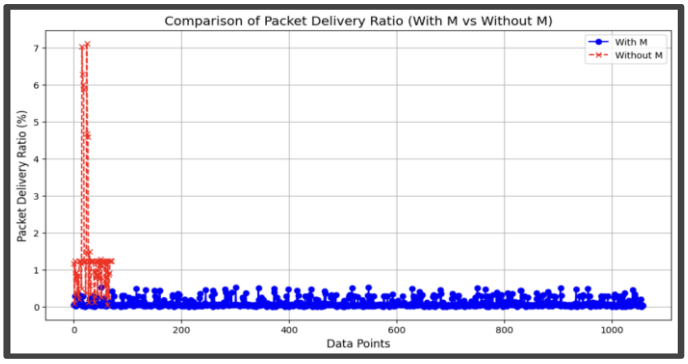

Fig5. Scatter plot illustrating anomaly detection in packet count over time

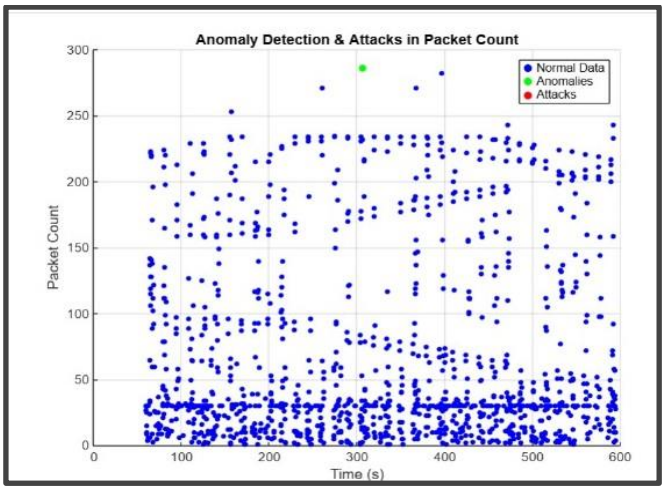

Fig6. Graph comparing Packet Delivery Ratio (PDR) with and without a malicious node

The results indicate a significant drop in PDR under attack scenarios, with Black Hole (0.15%) causing severe packet loss. Increased delay and fluctuating throughput further highlight network congestion, instability, and frequent topology changes due to malicious node behavior.

Anomaly detection findings reinforce this impact, with Autoencoder identifying up to 14,003 anomalies and Isolation Forest detecting 42,671. The high accuracy (92%) of AI-based models demonstrates their effectiveness in proactive RPL attack mitigation, reducing false positives and improving threat detection in real time.

These results validate the potential of ML-driven anomaly detection and forecasting to enhance the security of RPL-based networks, enabling adaptive defense mechanisms for IoT-based communication systems.[7]

VII. CONCLUSIONS & FUTURE SCOPE OF WORK

This work presents an efficient methodology for detecting and predicting RPL-based attacks (blackhole attack) using the Cooja simulator and Wireshark for network traffic analysis. Machine learning techniques like Isolation Forest and Autoencoders, effectively identified anomalies, distinguishing normal and malicious traffic patterns. MATLAB-based visualizations provided clear insights into attack behaviors, while evaluation metrics such as latency, delay, throughput, and Packet Delivery Ratio demonstrated the reliability of the approach. The research enhances RPL network security and contributes to cybersecurity anomaly detection by offering a scalable and adaptable solution for resource-limited IoT environments. Future work aims to protect attacks in WSN and IoT environments.

REFERENCES

1. Airehrour, David, Jairo Gutierrez, and Sayan Kumar Ray. "A trust-based defence scheme for mitigating blackhole and selective forwarding attacks in the RPL routing protocol". Australian Journal of Telecommunications and the Digital Economy 6.1 (2018):41.

2. Jiang, Jun, Yuhong Liu, and Behnam Dezfouli. "A Root-based Defense Mechanism Against RPLBlackholeAttacksinInternetofThingsNetworks ."2018 Asia-PacificSignalandInformation Processing Association Annual Summit and Conference (APSIPA ASC). IEEE,2018.

3. Mohammad Nikravan, Ali Movaghar and Mehdi Hosseinzadeh, "A Lightweight Defense Approach to Mitigate Version Number and Rank Attacks in Low-Power and Lossy Networks", Wireless Personal Communications, Volume 99, Issue 2, 2018, pp. 1035-1059.

4. Hkiri, A., et al., RPL-Based IoT Networks under Decreased Rank Attack: Performance Analysis in Static and Mobile Environments. Computers, Materials & Continua, 2024. 78(1).

5. F. ″ Osterlind, "A Sensor Network Simulator for the Contiki OS," SICS Technical Report, Tech. Rep. T2006:5, May 2006. [19] "Contiki: The Open Source OS for the Internet of Things," http://www. contiki-os.org/, 2015, [Online; accessed 13-September-2015].

6. Chen, Binbin, Yuan Li, and Daisuke Mashima. "Analysis and enhancement of RPL under packet drop attacks."201810thInternationalConferenceonCommunicationSystems&Networks (COMSNETS). IEEE, 2018.

7. T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, and M. Richardson, "A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)," RFC 7416 (Informational), Internet Engineering Task Force, Jan. 2015. [Online]. Available: http://www.ietf.org/rfc/rfc7416.txt

8. "Contiki: The Open Source OS for the Internet of Things," http://www. contiki-os.org/, 2015, [Online; accessed 13-September-2015].

9. F. ″ Osterlind, "A Sensor Network Simulator for the Contiki OS," SICS Technical Report, Tech. Rep. T2006:5, May 2006.

10. N. Finne, J. Eriksson, T. Voigt, G. Suciu, M.-A. Sachian, J. Ko, and H. Keipour, "Multi-Trace: Multi-level Data Trace Generation with the Cooja Simulator," in 2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS), 2021, pp. 390–395

BIOGRAPHIES

BALUSU DEEPIKA
Student
Andhra University College of Engineering for Women

BOJJA AKHILA
Student
Andhra University College of Engineering for Women

BONTHALAKOTI REVATHI
Student
Andhra University College of Engineering for Women

CHALLA NAGA VINAYA
Student
Andhra University College of Engineering for Women