
Assignment Report:

Literature Review Detection System for RPL Security

Student Name: Mohammed Yahya Alghazwani

Student ID: 261002006

Section: artificial intelligence

A Hybrid Lightweight and Machine Learning-Based Intrusion Detection System for Detecting Version Number Attacks in RPL-Based IoT Networks

1. Introduction

The Internet of Things (IoT) has transformed modern digital systems by enabling communication between billions of interconnected devices. These devices operate in constrained environments with limited processing power, memory, and energy resources. To support communication in such environments, the Routing Protocol for Low-Power and Lossy Networks (RPL) has been widely adopted.

Despite its efficiency, RPL is highly vulnerable to security threats due to its design limitations. One of the most critical threats is the Version Number Attack (VNA), which manipulates routing information to disrupt the network topology. This attack forces unnecessary global repairs, increases control message overhead, and drains energy resources, ultimately degrading network performance.

The need for effective intrusion detection systems (IDS) in IoT environments has become increasingly important. However, designing such systems is challenging due to resource constraints. This research explores hybrid approaches that combine lightweight techniques with machine learning to achieve both efficiency and high detection accuracy.

2. Literature Review

Several approaches have been proposed to detect version number attacks in RPL-based IoT networks. Distributed monitoring systems utilize dedicated nodes to observe network behavior and detect anomalies. These systems provide accurate detection but may introduce additional infrastructure requirements.

Lightweight approaches, such as parent supervision mechanisms, rely on monitoring relationships between nodes. These methods are efficient in terms of energy consumption but may fail in complex attack scenarios or large-scale networks.

Optimization-based intrusion detection systems, such as those using Grey Wolf Optimization, improve feature selection and classification performance. However, they may require parameter tuning and increased computational effort.

Machine learning approaches, including ensemble learning and Light Gradient Boosting Machine (LGBM), have demonstrated high detection accuracy. These models can process large datasets and identify complex patterns. However, they may not always be suitable for resource-constrained IoT devices.

Overall, the literature highlights a trade-off between efficiency and accuracy. Most existing solutions focus on either lightweight performance or high detection capability, but rarely both.

3. Problem Statement

The rapid expansion of IoT networks has increased their exposure to security threats, particularly routing attacks such as Version Number Attacks. These attacks significantly impact network performance by causing unnecessary topology changes and increasing energy consumption.

Existing detection mechanisms present several limitations. Lightweight methods often lack the ability to accurately detect complex attack patterns, while machine learning methods may require high computational resources that are not suitable for IoT devices.

Additionally, many studies rely on simulated environments and limited datasets, which raises concerns about their applicability in real-world scenarios. There is also a lack of solutions that can effectively handle multiple types of attacks.

Therefore, there is a critical need for a hybrid intrusion detection system that combines the advantages of lightweight and machine learning approaches while minimizing their limitations.

4. Research Objectives

Primary Objective:

To design and develop a hybrid intrusion detection system for detecting version number attacks in RPL-based IoT networks.

Specific Objectives:

- To analyze the characteristics and impact of version number attacks.
- To review and evaluate existing intrusion detection techniques.
- To design a lightweight detection mechanism suitable for IoT devices.
- To develop a machine learning-based detection model.
- To integrate both approaches into a hybrid system.
- To evaluate the system using performance metrics such as accuracy, energy efficiency, and scalability.

5. Methodology

The proposed research will follow a structured methodology. First, a detailed analysis of version number attacks will be conducted to understand their behavior and impact. Next, a dataset will be prepared using simulation tools such as Cooja.

A lightweight monitoring mechanism will be developed to detect abnormal behavior in the network. In parallel, a machine learning model will be trained using extracted features from network traffic.

The hybrid system will integrate both components to achieve improved detection performance. Finally, the system will be evaluated using various performance metrics.

6. Critical Analysis

The reviewed studies demonstrate that no single approach can effectively address all challenges in IoT security. Lightweight methods are efficient but limited in detection capability, while machine learning models are accurate but resource-intensive.

This highlights the importance of hybrid approaches that combine the strengths of both techniques. Such approaches can provide a balance between performance and efficiency.

7. Research Gap

The main research gap identified is the lack of integrated solutions that balance accuracy and efficiency. Existing studies either focus on lightweight methods or machine learning approaches, but few attempt to combine them effectively.

Additionally, real-world validation and scalability remain significant challenges.

8. Conclusion

This research proposes a hybrid intrusion detection system to address the limitations of existing methods. By combining lightweight monitoring with machine learning techniques, the proposed system aims to achieve high detection accuracy while maintaining low resource consumption.

This approach is expected to enhance the security of RPL-based IoT networks and provide a practical solution for real-world deployment.

References

A Distributed Monitoring Strategy for Detecting Version Number Attacks in RPL-Based Networks. [RPL security – Dropbox](#)

Intrusion Detection System Based on a Modified Binary Grey Wolf Optimisation. [RPL security – Dropbox](#)

Parent Supervision Lightweight Solution Against Version Number Attacks for IoT Networks. [RPL security – Dropbox](#)

ELNIDS: Ensemble Learning Based Network Intrusion Detection System for RPL Based Internet of Things. [RPL security – Dropbox](#)

Version Attack Detection Using Claim Algorithm in RPL Based IoT Networks. [RPL security – Dropbox](#)

ML-LGBM: A Machine Learning Model Based on Light Gradient Boosting Machine for the Detection of Version Number Attacks in RPL-Based Networks. [RPL security – Dropbox](#)