

MID OCEAN UNIVERSITY

**Research Methodology in Computer Science
(AI800)**

Assignment 2

**Machine Learning-Based Detection of Version Number Attacks in RPL-Based Internet of
Things Networks**

Student: Fatemah Waleed

Lecturer: Dr. Mohammed Anbar

Abstract

The Routing Protocol for Low-Power and Lossy Networks (RPL) is widely used in Internet of Things (IoT) environments. However, it is vulnerable to Version Number Attacks (VNAs), which can significantly affect routing performance and network stability. This report reviews existing literature and identifies research gaps related to attack detection. The study proposes a research direction focused on machine learning techniques capable of providing accurate, lightweight, and scalable attack detection suitable for real-world IoT environments.

Introduction

The rapid expansion of IoT technologies has increased the need for secure communication protocols. RPL is a commonly used routing protocol for resource-constrained devices. Despite its advantages, attackers can exploit routing vulnerabilities through Version Number Attacks, leading to increased overhead, reduced packet delivery rates, and network instability. Therefore, developing effective detection mechanisms is essential for maintaining IoT security.

Literature Review

Mayzaud et al. (2017) introduced a distributed monitoring approach for detecting Version Number Attacks with acceptable overhead. Almusaylim et al. (2020) proposed a security framework that improved network stability and packet delivery. Osman et al. (2021) demonstrated that machine learning models can achieve detection accuracy exceeding 99%. Verma and Ranga (2020) compared several machine learning algorithms and identified Random Forest and Gradient Boosting as effective solutions. Sharma et al. (2023) employed deep learning techniques to improve intrusion detection performance. Although these studies achieved promising results, challenges related to computational complexity, scalability, and real-world deployment remain unresolved.

Problem Statement

Version Number Attacks remain one of the most serious security threats in RPL-based IoT networks. Existing detection methods often suffer from limitations such as high computational requirements, dependency on large training datasets, limited scalability, or evaluation only within simulation environments. As IoT applications continue to expand into critical domains such as healthcare, smart cities, and industrial automation, there is an urgent need for a lightweight and accurate machine learning-based detection mechanism. Therefore, further research is required to develop a solution that effectively detects Version Number Attacks while maintaining scalability, energy efficiency, and suitability for practical deployment.

Research Goal

To develop an effective and lightweight machine learning-based model for detecting Version Number Attacks in RPL-based Internet of Things networks.

Research Objectives

1. To analyze the impact of Version Number Attacks on the security and performance of RPL-based IoT networks.
2. To review and evaluate existing detection and mitigation approaches proposed in the literature.
3. To design a machine learning-based model capable of detecting malicious routing behavior.
4. To evaluate the proposed model using performance metrics such as accuracy, precision, recall, and resource utilization.
5. To compare the proposed model with existing approaches in terms of detection capability, efficiency, and scalability.

Conclusion

The reviewed literature confirms that Version Number Attacks pose a significant threat to RPL-based IoT networks. While machine learning and deep learning approaches have demonstrated excellent detection performance, several challenges remain, including computational cost and deployment feasibility. This research aims to address these challenges through the development of a lightweight and practical machine learning-based detection model.

References

- Mayzaud, A., Badonnel, R., & Chrisment, I. (2017). A Distributed Monitoring Strategy for Detecting Version Number Attacks in RPL-Based Networks.
- Almusaylim, Z. A., et al. (2020). Detection and Mitigation of RPL Rank and Version Number Attacks in Smart IoT Networks.
- Alsukayti, I. S., & Singh, A. (2022). A Lightweight Scheme for Mitigating RPL Version Number Attacks in IoT Networks.
- Osman, M., et al. (2021). ML-LGBM: A Machine Learning Model Based on Light Gradient Boosting Machine for Detection of Version Number Attacks.
- Verma, A., & Ranga, V. (2020). Machine Learning Techniques for Security in RPL-Based IoT Networks.
- Sharma, P., et al. (2023). Deep Learning-Based Intrusion Detection for IoT Networks.