

Research Methodology in Computer Science (AI800)

Assignment 1 – Literature Review

Research Title: Machine Learning-Based Detection of Version Number Attacks in RPL-Based Internet of Things Networks

Abstract

The Routing Protocol for Low-Power and Lossy Networks (RPL) is widely used in Internet of Things (IoT) environments. Despite its popularity, RPL remains vulnerable to several routing attacks, particularly Version Number Attacks (VNAs). This literature review examines six major studies that proposed different approaches for detecting and mitigating VNAs. The review compares traditional monitoring mechanisms, lightweight security frameworks, machine learning models, and deep learning approaches.

Introduction

The rapid growth of IoT technologies has increased the need for secure routing protocols. RPL is specifically designed for constrained IoT devices; however, attackers can exploit routing vulnerabilities through Version Number Attacks. Such attacks may increase control overhead, reduce packet delivery rates, and consume network resources. Researchers have proposed several countermeasures ranging from lightweight monitoring systems to advanced machine learning-based detection techniques.

Paper 1: Mayzaud et al. (2017)

Methodology: Distributed Monitoring

Objective: Detect VNA attacks using distributed monitoring.

Key Findings: Successful attack detection with acceptable overhead.

Strengths: Lightweight and practical.

Weaknesses: Scalability concerns.

Paper 2: Almusaylim et al. (2020)

Methodology: Security Framework

Objective: Mitigate Rank and Version Number Attacks.

Key Findings: Improved packet delivery and network stability.

Strengths: Addresses multiple attacks.

Weaknesses: Simulation-only evaluation.

Paper 3: Alsukayti & Singh (2022)

Methodology: Lightweight Scheme

Objective: Provide low-cost protection.

Key Findings: Reduced attack effectiveness while preserving energy.

Strengths: Suitable for constrained devices.

Weaknesses: Limited large-scale testing.

Paper 4: Osman et al. (2021)

Methodology: LGBM Model

Objective: Apply machine learning to detect attacks.

Key Findings: Accuracy exceeded 99%.

Strengths: High detection capability.

Weaknesses: Requires training datasets.

Paper 5: Verma & Ranga (2020)

Methodology: ML Comparison

Objective: Compare ML algorithms.

Key Findings: Random Forest and Gradient Boosting performed best.

Strengths: Comprehensive comparison.

Weaknesses: Computational complexity.

Paper 6: Sharma et al. (2023)

Methodology: Deep Learning IDS

Objective: Develop intelligent intrusion detection.

Key Findings: High accuracy against unknown attacks.

Strengths: Strong adaptability.

Weaknesses: Resource intensive.

Comparative Analysis

The reviewed studies demonstrate a transition from traditional monitoring mechanisms toward intelligent machine learning and deep learning approaches. Traditional methods provide lightweight deployment and lower resource consumption, while machine learning models offer significantly higher detection accuracy. However, advanced AI-based methods often require larger datasets, increased computational resources, and more complex implementation. Most studies were evaluated in simulation environments, indicating the need for further real-world validation.

Summary Table of Reviewed Papers

Authors	Year	Methodology	Key Findings	Limitations
Mayzaud et al.	2017	Monitoring	Effective detection	Overhead
Almusaylim et al.	2020	Framework	Improved stability	Simulation only
Alsukayti & Singh	2022	Lightweight Scheme	Energy efficient	Limited scalability
Osman et al.	2021	LGBM	99%+ accuracy	Training data needed
Verma & Ranga	2020	ML Comparison	Best ML models identified	Complexity
Sharma et al.	2023	Deep Learning	High detection rate	Resource intensive

Synthesis of Literature

The literature reveals a common agreement that Version Number Attacks represent a serious threat to RPL-based IoT networks. While traditional approaches focus on monitoring network behavior, recent studies increasingly rely on machine learning and deep learning to improve detection performance. The main research gap lies in balancing security effectiveness, computational efficiency, scalability, and explainability. Future research should focus on lightweight machine learning solutions capable of operating efficiently in real-world IoT environments.

Conclusion

This review analyzed six studies related to Version Number Attack detection in RPL-based IoT networks. The findings indicate that AI-based techniques provide superior detection accuracy compared with conventional approaches. Nevertheless, challenges related to scalability, energy consumption, and real-world deployment remain open research issues.

References (APA Style)

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.