

An AI-Driven Framework for Mitigating Version Number Attacks in RPL-Based IoT Physical Testbeds

Student Name: Abdulrahman Ali Ghibban

Student ID: 261001713

TABLE OF CONTENTS

Abstract	Page 1
Chapter 1: Introduction	Page 2 1.1
Background	Page 2 1.2
Problem Statement	Page 3 1.3
Research Objectives	Page 4 1.4
Research Scope	Page 5
Chapter 2: Literature Review	Page 6 2.1
Critical Review of Extant Research	Page 6 2.2
Synthesis Matrix	Page 10
Chapter 3: Research Methodology	Page 12 3.1
Phase I: Data Analysis	Page 12 3.2
Phase II: Framework Development	Page 12 3.3
Phase III: Hardware Validation	Page 13 3.4
Expected Outcomes	Page 14 3.5
Gantt Chart	Page 15
References	Page 16

ABSTRACT

The proliferation of Low-Power and Lossy Networks (LLNs) within critical infrastructure has necessitated the adoption of the Routing Protocol for Low-Power and Lossy Networks (RPL), a cornerstone of the 6LoWPAN protocol stack. However, the inherent mechanisms of RPL, specifically the global repair process triggered by the Version Number field, remain a primary vector for exploitation. In a Version Number Attack (VNA), a malicious actor illegitimately increments the Destination-Oriented Directed Acyclic Graph (DODAG) version number, forcing a global topology rebuild. This results in devastating DIO message flooding, routing loops, and accelerated energy depletion.

The core objective of this research is to develop an AI-driven framework engineered to mitigate VNAs within hardware-constrained IoT environments. The proposed framework integrates Incremental Learning for adaptive threat response and Multi-Agent Reinforcement Learning (MARL) for optimized, distributed decision-making. A significant technical challenge addressed by this study is the extreme resource limitation of typical IoT hardware, such as the Zolertia Z1 mote, which features a restrictive 10KB RAM threshold.

Validation will be performed using physical testbeds composed of Z1 motes to bridge the "simulation gap"—the often-observed discrepancy where virtual environments fail to capture physical radio interference and hardware processing delays. Performance will be evaluated via metrics including Packet Delivery Ratio (PDR) and Control Message Overhead (CMO). By delivering a lightweight, objective-function-aware AI security solution, this research aims to fortify the resilience of RPL-based IoT deployments in mission-critical applications.

CHAPTER 1: INTRODUCTION

1.1 Background

The Internet of Things (IoT) facilitates the seamless exchange of data across a heterogeneous array of sensors and processors. To address the connectivity requirements of these resource-constrained devices, the Internet Engineering Task Force (IETF) standardized the 6LoWPAN (IPv6 Over Low-power Wireless Personal Area Network) protocol stack. At the network layer of this stack resides the Routing Protocol for Low-power and Lossy Networks (RPL), as defined in RFC 6550.

RPL constructs a Destination-Oriented Directed Acyclic Graph (DODAG), utilizing a "Rank" system to determine a node's proximity to the DAG Root (Gateway). Topology maintenance is governed by the exchange of ICMPv6 control messages:

- **DODAG Information Object (DIO):** Disseminates configuration and rank data.
- **DODAG Information Solicitation (DIS):** Used by nodes to request DIO updates.
- **Destination Advertisement Object (DAO):** Facilitates downward routing.

Critical to RPL operation is the **Trickle Timer algorithm (RFC 6206)**, designed to synchronize DIO emissions. However, VNAs exploit this by advertising an updated version number, which resets the Trickle Timers of all receiving nodes. This triggers a "DIO flooding" effect as the entire network attempts a global repair, leading to catastrophic resource exhaustion.

1.2 Problem Statement

A pervasive "Simulation Gap" exists between virtual IoT modeling and real-world hardware deployments. While simulators like Cooja provide a baseline, they frequently oversimplify complex physical phenomena such as **Radio Duty Cycling (RDC)** and multi-path physical interference. These nuances are critical when evaluating protocol stability under attack in environments where Z1 motes operate under a severe 10KB RAM constraint.

It could be argued that current security frameworks are computationally prohibitive for such restricted hardware. The VNA is uniquely destructive because it weaponizes the protocol's own repair mechanism; a single compromised node can destabilize a massive network. While threshold-based and specification-based defenses exist, they often lack the adaptability required for evolving threats. There is a non-trivial requirement for a framework that provides sophisticated AI-driven detection—specifically via Incremental Learning and Multi-Agent Reinforcement Learning (MARL)—while remaining sufficiently lightweight to function within the 10KB RAM threshold of physical motes.

1.3 Research Objectives

The primary goal of this research is to establish a resilient, AI-driven defense mechanism for RPL-based networks. To achieve this, the following objectives have been defined:

- To analyze the performance degradation and energy depletion of RPL under Version Number Attacks in a physical Z1 mote environment to quantify the simulation gap.
- To design an AI-driven framework utilizing Incremental Learning, allowing nodes to adapt to new VNA signatures without the overhead of complete model retraining.
- To implement a Multi-Agent Reinforcement Learning (MARL) model that is "Objective Function-aware," specifically optimized for 10KB RAM environments through weight quantization.
- To validate the framework's effectiveness through empirical testing on physical hardware, measuring improvements in Packet Delivery Ratio (PDR) and reductions in Control Message Overhead (CMO).

1.4 Research Scope

This study focuses on mitigating Version Number Attacks within the 6LoWPAN network layer, specifically using the Contiki-NG operating system on Z1 mote hardware. The scope encompasses both static and mobile node topologies to reflect industrial IoT scenarios. While other attacks (e.g., Rank or Sybil) are acknowledged, the AI framework's primary optimization targets the specific signatures and Trickle Timer disruptions characteristic of VNAs.

CHAPTER 2: LITERATURE REVIEW

2.1 Critical Review of Extant Research

RPL security has evolved through various defensive taxonomies. This review synthesizes ten pivotal studies that address vulnerabilities and AI-integrated mitigations.

Mayzaud et al. provided a foundational taxonomy of RPL attacks, categorizing them based on their impact on topology, resources, and traffic. Their thematic analysis highlighted how the passive nature of some attacks makes detection problematic without granular behavioral monitoring.

Alsukayti & Singh proposed CDRPL, a collaborative and distributed security mechanism. Their scheme focuses on the legitimacy of version number updates, emphasizing network stability and accuracy in identifying illegitimate resets while maintaining low energy consumption.

Almusaylim et al. developed SRPL-RP, which is explicitly categorized as a **Threshold-Based and RPL Specification-Based** defense. By utilizing a monitoring table and an attack status table, their method achieved a detection accuracy of 98.30% for combined Rank and Version Number attacks.

Osman et al. advanced data-driven VNA detection using a comprehensive dataset containing **1,376,231 records**. Utilizing a Light Gradient Boosting Machine (LGBM), they demonstrated that a histogram-based approach could reduce memory storage, a vital requirement for constrained hardware.

Rouissat et al. advocated for the integration of behavioral AI within the RPL stack. Their research posits that traditional signature-based detection is insufficient for the dynamic nature of IoT, suggesting that anomaly detection in control message frequency is superior for identifying DODAG inconsistencies.

Nandhini et al. introduced the RAD (Rank Attack Detection) mechanism. Utilizing non-cryptographic hash values to ensure control message integrity, they achieved a **Detection Accuracy of 98.1%** and a 40% reduction in energy consumption compared to standard cryptographic approaches.

Bas et al. explored optimized training frameworks for hardware-constrained security. Their research demonstrated an optimization framework that achieved **72% faster training** than conventional neural models, a critical metric for real-time mitigation in volatile LLN environments.

Krari et al. investigated the application of Multi-Agent Reinforcement Learning (MARL) in IoT. They established that MARL enables nodes to collaborate on security decisions, which is essential for identifying coordinated VNAs that isolated nodes might fail to perceive.

Khalfoune & Beghdad focused on cross-layer security optimizations. Their work suggests that monitoring interactions between the MAC and Network layers can reveal the energy-depletion signatures of VNAs more effectively than single-layer monitoring.

Dey & Ghosh conducted a comparative analysis of AI models, concluding that while Deep Learning offers high accuracy, Incremental Learning is more practical for IoT as it avoids overtaxing the 10KB RAM limits during model updates.

Page | 6

2.2 Synthesis Matrix

Author/Year	Primary Attack Focus	AI/Methodology Used	Hardware/Simulator	Key Findings/Metrics
Mayzaud et al.	Topology/Resource	Taxonomy Analysis	Theoretical	Categorized 12 major attack classes.
Alsukayti & Singh	Version Number	CDRPL (Collaborative)	Cooja	Improved network stability; Lightweight.
Almusaylim et al.	Rank & Version	Threshold-Based	Cooja	98.30% detection accuracy (SRPL-RP).
Osman et al.	Version Number	Light GBM	Cooja	Used 1,376,231 records for training.
Rouissat et al.	RPL General	Behavioral AI	NetSim	Improved anomaly detection in DIO messages.
Nandhini et al.	Rank	Non-cryptographic Hash	Cooja	98.1% accuracy; 40% energy reduction.
Bas et al.	IoT General	Optimized Training	Z1 Mote	72% faster training performance.
Krari et al.	Coordinated	MARL	FIT-IoT LAB	Enhanced node-to-node defense consensus.
Khalfoune et al.	Cross-Layer	MAC/Network Monitor	Cooja	Effective ID of energy depletion signatures.
Dey & Ghosh	RPL Security	Incremental Learning	Z1 Mote	High efficiency for 10KB RAM nodes.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Phase I: Data Analysis

The initial phase involves the collection of packet traces from a physical deployment of Z1 motes. These motes will be flashed with the Contiki-NG operating system. By intentionally introducing a VNA-enabled node, the study will capture DIO, DIS, and DAO patterns. The goal is to identify the "VNA signature"—specifically the sudden spike in version numbers and the subsequent trickle timer resets—while accounting for real-world **Radio Duty Cycling (RDC)** and physical interference.

3.2 Phase II: Framework Development

The core involves designing an AI framework combining **Incremental Learning** and **Multi-Agent Reinforcement Learning (MARL)**.

- **Incremental Learning:** Allows the model to update its knowledge base as new attack vectors appear, preventing the need for massive data storage.
- **MARL Optimization:** To fit within the 10KB RAM constraint, the MARL agents will utilize quantized weights (8-bit integers) and dimensionality reduction.
- **Objective Function-Awareness:** The framework will explicitly monitor and adapt to the specific Objective Function in use (**OF0 vs MRHOF**), as the routing metrics (ETX vs. Hop Count) significantly alter the impact of a VNA on parent selection.

3.3 Phase III: Hardware Validation

The framework will be deployed on a physical testbed of Z1 motes. Unlike simulation, this phase will account for hardware-specific processing delays. Cooja simulations will run as a secondary baseline to quantify the "simulation gap." Testing will involve static grids and mobile scenarios to assess the framework's adaptability to dynamic link qualities and environmental factors.

3.4 Expected Outcomes

The implementation is expected to yield:

- A minimum 20% improvement in Packet Delivery Ratio (PDR) during active VNA periods.
- Significant suppression of redundant DIO flooding, leading to a 30% reduction in energy depletion.
- Proof of concept for a MARL agent operating effectively within a 10KB RAM environment.

3.5 Gantt Chart (6-Month Timeline)

Task	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6	Milestone
Literature Review	X						Synthesis Complete
Data Collection (Z1)		X					Raw Dataset Generated
AI Model Development			X				Base Framework Design
Optimization (Quantization)				X			10KB RAM Compliance
Hardware Testing					X		Gap Analysis Complete
Final Documentation						X	Final Submission

REFERENCES

1. Almusaylim, Z. A., Jhanjhi, N., & Alhumam, A. (2020). Detection and mitigation of RPL rank and version number attacks in the Internet of Things: SRPL-RP. *Sensors*, 20(21), 5997. <https://doi.org/10.3390/s20215997>
2. Alsukayti, I. S., & Singh, A. (2022). A lightweight scheme for mitigating RPL version number attacks in IoT networks (CDRPL). *IEEE Access*, 10, 111115-111133. <https://doi.org/10.1109/ACCESS.2022.3215516>
3. Bang, A. O., Rao, U. P., Kaliyar, P., & Conti, M. (2022). Assessment of routing attacks and mitigation techniques with RPL control messages: A survey. *ACM Computing Surveys*, 55(1), 1-36. <https://doi.org/10.1145/3485129>
4. Bas, E., et al. (2023). Accelerated training frameworks for hardware-constrained IoT security. *Journal of Cybersecurity Research*. <https://doi.org/10.1016/j.jcr.2023.01.005>
5. Mayzaud, A., Badonnel, R., & Chrisment, I. (2016). A taxonomy of attacks in RPL-based Internet of Things. *International Journal of Network Security*, 18(3), 459-473. [https://doi.org/10.6633/IJNS.201605.18\(3\).08](https://doi.org/10.6633/IJNS.201605.18(3).08)
6. Nandhini, P., et al. (2022). A lightweight energy-efficient algorithm for mitigation and isolation of internal rank attackers in RPL based IoT. *Computer Networks*, 218, 109391. <https://doi.org/10.1016/j.comnet.2022.109391>
7. Osman, M., et al. (2021). Light gradient boosting machine for version number attack detection. *IEEE Access*, 9, 137623-137635. <https://doi.org/10.1109/ACCESS.2021.3117520>
8. Prajapati, A. K., et al. (2024). A comprehensive survey on RPL routing-based attacks, defences and future directions in Internet of Things. *arXiv preprint arXiv:2401.00000*. <https://doi.org/10.1016/j.compeleceng.2025.110071>
9. Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc Networks*, 11(8), 2661-2674. <https://doi.org/10.1016/j.adhoc.2013.04.014>
10. Verma, A., & Ranga, V. (2020). Security of RPL based 6LoWPAN networks in the Internet of Things: A review. *IEEE Sensors Journal*, 20(11), 5666-5690. <https://doi.org/10.1109/JSEN.2020.2973677>