

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

- **Name:** Abdulrahman Ali Ghibban
- **Student ID:** 261001713
- **Course:** Research Methodology in Computer Science (AI800)
- **Lecturer:** Dr. Mohammed Anbar

1. Problem Statement

The Internet of Things (IoT) landscape is fundamentally underpinned by the Routing Protocol for Low-Power and Lossy Networks (RPL), which organizes resource-constrained devices into a Destination-Oriented Directed Acyclic Graph (DODAG). However, the protocol's deterministic nature stands in stark contrast to the adversarial environments in which it is deployed, leaving it vulnerable to the Version Number Attack (VNA). In this exploit, a malicious actor illegitimately increments the DODAG version number, compelling the entire network to initiate an exhaustive global repair. As noted by Mayzaud et al. (2017), such frequent and unnecessary topology reformations disrupt network stability and place an unsustainable burden on battery-powered motes, leading to rapid energy depletion and shortened network longevity.

The significance of this threat has prompted several defensive responses. Algorithmic approaches like CDRPL (Alsukayti & Singh, 2022) focus on in-protocol collaborative detection, while advanced data-driven paradigms, such as the LightGBM model proposed by Osman et al. (2021), have achieved detection accuracies exceeding 99% in virtualized settings. Nevertheless, a palpable tension exists between these high-performing AI models and the physical reality of IoT hardware. For instance, while the LightGBM model reports a memory footprint of 347,530 bytes, typical MSP430-based Z1 motes possess only 8KB to 10KB of usable RAM. This massive discrepancy suggests that contemporary AI solutions may be computationally prohibitive for actual hardware deployment.

Furthermore, a critical "Simulation Gap" persists in the literature. Recent studies by Rouissat et al. (2023) and Nandhini et al. (2021) rely almost exclusively on the Cooja simulator for validation. These virtual environments are inherently sanitized; they fail to account for the stochastic variables of real-world deployments, such as the physical constraints of CC2420 radio transceivers, signal fading, and non-linear battery depletion cycles. Consequently, current security frameworks lack validation on physical Z1 motes within the MSP430 architecture. Without bridging this gap between simulation and reality, AI-driven security remains a theoretical exercise, potentially failing to maintain Quality of Service (QoS) when faced with the physical interference and hardware limitations of a live environment.

2. Research Objectives

The primary goal of this research is to develop and validate a resilient, AI-driven security framework for RPL-based IoT networks that functions effectively on physical hardware testbeds.

1. To analyze the impact of Version Number Attacks on the energy consumption and stability of RPL-based IoT networks:
 - To identify the key variables in DODAG reformation that lead to accelerated battery depletion in MSP430-based devices.
 - To quantify the relationship between attack frequency and the degradation of network-wide packet delivery ratios.
2. To evaluate the effectiveness of current machine learning models, specifically LightGBM, in detecting malicious DODAG updates within a resource-constrained environment:
 - To assess the computational overhead and RAM requirements of LightGBM when ported to limited-memory hardware.
 - To determine the detection accuracy of reduced-feature AI models in the presence of physical signal noise.
3. To design a lightweight security architecture that integrates AI-driven detection with protocol-aware mitigation strategies:
 - To develop a hybrid mechanism that utilizes Sequential Forward Selection to minimize the feature set for on-node processing.
 - To integrate mitigation logic that isolates rogue nodes without triggering redundant global repairs.
4. To validate the proposed framework using physical IoT hardware, such as Z1 motes, to bridge the current simulation gap in the literature:
 - To measure the framework's performance against real-world variables, including signal fading and CC2420 radio transceiver limitations.
 - To compare the empirical results of physical testbeds against traditional Cooja simulation data to identify divergence patterns.

5. To provide a set of implementation guidelines for deploying AI-security models on low-power IoT devices without compromising Quality of Service (QoS):
 - To establish a deployment blueprint for porting high-accuracy AI models to resource-constrained firmware.
 - To formulate recommendations for balancing security-driven computational load with the operational longevity of IoT networks.

3. Literature Review

- **Paper 1: Distributed Monitoring for Version Number Attacks (Mayzaud et al., 2017)** This study introduces a distributed monitoring architecture that utilizes high-order nodes for passive traffic analysis. By avoiding a centralized root-only detection model, the authors mitigate single-point-of-failure risks. Cooja simulations demonstrated detection rates above 90%; however, the methodology incurs a 15–20% communication overhead and a 5–10% increase in energy consumption. The requirement for specialized monitoring nodes remains a significant capital expenditure constraint.
- **Paper 2: Collaborative and Distributed RPL (Alsukayti & Singh, 2022)** The CDRPL scheme pivots toward "in-protocol" security, embedding detection logic directly into the standard RPL control messages. This approach effectively maintains QoS and ensures faster topology convergence after an attack. While the scheme reduces the need for external hardware, its reliance on simulation-only environments leaves its resilience against physical signal interference unverified.
- **Paper 3: The SRPL-RP Protocol (Almusaylim et al., 2020)** This research proposes a five-phase defense mechanism involving rank comparison, status tables, and timestamp verification. The protocol achieved an impressive 98.48% PDR and an average energy footprint of 1231.75 Joules. Despite its procedural depth, the study lacks a comparison with modern AI-driven models and remains limited by the absence of real-world hardware validation.
- **Paper 4: Machine Learning via LightGBM (Osman et al., 2021)** Osman et al. utilize the Light Gradient Boosting Machine to detect VN attacks with 99.6% accuracy. Through Sequential Forward Selection, they reduced the feature set from 113 to 17 variables. However, the reported execution time of 140.217 seconds and a RAM footprint of 347,530 bytes highlight a critical gap when compared to the 8KB RAM limits of standard IoT motes like the Z1.
- **Paper 5: Parent Supervision Mechanism (Rouissat et al., 2023)** This study presents a lightweight mechanism where parent nodes use DAO/DIO flags to

monitor children's version increments. Validation on simulated Z1 motes (MSP430-based) showed effective reduction of VNA impact. However, the 16-node topology used in the study is too small to accurately reflect the scaling challenges of dense smart city deployments.

- **Paper 6: The Claim Algorithm (Nandhini et al., 2021)** The Claim algorithm utilizes peer-based verification within the DODAG to confirm legitimate version changes, resulting in an 87% reduction in latency and an 86% enhancement in PDR. A critical limitation is the algorithm's vulnerability to coordinated attacks, where multiple rogue nodes collaborate to validate illegitimate version increments.

Critical Analysis

The current state of research demonstrates a clear shift from computationally heavy cryptography toward protocol-aware and data-driven solutions. While theoretical detection accuracy has reached maturity, the "Simulation Gap" remains the primary methodological obstacle. Reliance on the Cooja simulator (Rouissat et al., 2023; Nandhini et al., 2021) often abstracts away the complexities of signal fading and physical hardware constraints. Furthermore, most studies utilize small-scale topologies (10–20 nodes), which may not account for the non-linear overhead scaling found in industrial IoT applications.

Connections: Shared Research Trajectories All six reviewed papers identify RPL as the primary point of vulnerability and the VN attack as a destructive threat. There is a consistent push for lightweight designs to accommodate low RAM and energy footprints, with a universal reliance on metrics such as Packet Delivery Ratio (PDR) and control message overhead for validation.

Conflicts and Theoretical Divergence A fundamental philosophical divide exists between the distributed monitoring of Mayzaud et al. and the centralized/parent-to-root models of Rouissat et al. Furthermore, there is a distinct "Simulation vs. Reality" conflict regarding validation methodology. While rule-based algorithms (Nandhini et al.) provide deterministic transparency, they lack the adaptive flexibility of machine learning models (Osman et al.), which themselves face a significant "Complexity vs. Constraint" conflict given the resource limitations of physical motes.

4. Reference

- Almusaylim, Z. A., Alhumam, A., Mansoor, W., Chatterjee, P., & Jhanjhi, N. Z. (2020). Detection and mitigation of RPL rank and version number attacks in smart internet of things. *Preprints*.
<https://doi.org/10.20944/preprints202007.0476.v1>
- Alsukayti, I. S., & Singh, A. (2022). A lightweight scheme for mitigating RPL version number attacks in IoT networks. *IEEE Access*, 10, 111115–111133.
<https://doi.org/10.1109/ACCESS.2022.3215460>
- Mayzaud, A., Badonnel, R., & Chrisment, I. (2017). A distributed monitoring strategy for detecting version number attacks in RPL-based networks. *IEEE Transactions on Network and Service Management*, 14(2), 472–486.
<https://doi.org/10.1109/TNSM.2017.2705290>
- Nandhini, P. S., Srinath, P., Veeramanikandan, P., & Malliga, S. (2021). Version attack detection using claim algorithm in RPL based IoT networks: Effects and performance parameters evaluation. *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)*.
- Osman, M., He, J., Mohammed Mokbal, F. M., Zhu, N., & Qureshi, S. (2021). ML-LGBM: A machine learning model based on light gradient boosting machine for the detection of version number attacks in RPL-based networks. *IEEE Access*, 9, 83631–83645.
<https://doi.org/10.1109/ACCESS.2021.3086358>
- Rouissat, M., Belkheir, M., & Mokaddem, A. (2023). Parent supervision lightweight solution against version number attacks for IoT networks. *Journal of Reliable Intelligent Environments*.