

RESEARCH PROPOSAL

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

Student Name: Mohammed Yahya Alghazwani

Course: AI800

Lecturer: Dr. Mohammed Anbar

Abstract

The rapid expansion of Internet of Things (IoT) networks introduces major security challenges, especially in routing protocols such as RPL. Version Number Attacks (VNA) are among the most critical threats affecting network stability. This research proposes a hybrid intrusion detection system combining lightweight techniques and machine learning to achieve both efficiency and accuracy. The system will be evaluated using simulation tools and performance metrics such as accuracy, energy consumption, and scalability. The proposed solution aims to provide a practical and efficient security model for IoT networks.

Chapter 1: Introduction

The Internet of Things (IoT) connects billions of devices across multiple domains. These systems operate under strict resource constraints, making security a major concern. The RPL protocol is widely used but lacks strong security mechanisms, making it vulnerable to attacks such as Version Number Attacks (VNA). These attacks manipulate routing information, causing instability and energy depletion.

Background

RPL organizes nodes in a DODAG structure. Control messages such as DIO, DAO, and DIS maintain routing. However, attackers exploit version numbers to trigger unnecessary repairs, leading to overhead and reduced performance.

Problem Statement

Existing IDS solutions either focus on lightweight efficiency or machine learning accuracy. Lightweight methods lack accuracy, while machine learning requires high resources. Most studies rely on simulation and lack real-world validation. A hybrid solution is needed to balance both aspects.

Research Objectives

Primary Objective:

Develop a hybrid IDS.

Specific Objectives:

- Analyze VNA
- Evaluate methods
- Design lightweight model
- Develop ML model
- Integrate system
- Evaluate performance

Research Scope

This research focuses on RPL-based IoT networks using simulation tools. Evaluation metrics include accuracy, energy consumption, and scalability.

Chapter 2: Literature Review

Several studies addressed IoT security. Distributed monitoring detects attacks effectively but requires extra nodes. Lightweight methods reduce overhead but lack accuracy. Optimization approaches improve feature selection. Machine learning models achieve high accuracy but require computational resources. Hybrid approaches aim to combine advantages but remain limited.

Additional studies show that deep learning and ensemble models improve detection accuracy, while blockchain-based methods enhance security trust. However, scalability and efficiency remain challenges.

Research Gap

There is a lack of integrated hybrid solutions that balance efficiency and accuracy. Most research focuses on single approaches and lacks real-world validation.

Chapter 3: Methodology

The research follows structured phases:

1. Data collection using Cooja simulation
2. Lightweight detection design
3. Machine learning model development
4. Hybrid integration
5. Performance evaluation

Expected Outcomes

- High detection accuracy
- Low energy consumption
- Improved network stability
- Scalable IDS

Gantt Chart

Month 1: Literature Review

Month 2: Design

Month 3: Implementation

Month 4: Testing & Report

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](#)