



Security Challenges and Solutions in Routing Protocol for Low-power and Lossy Networks (RPL)

Mohammed Jamal Albreem
242001689

Senior lecturer
Dr. Mohammed Fawzy

Research Methodology in Computer Science - AI800
MSc in Artificial Intelligence
College of Informatics
Midocean University

First Trimester
10/08/2024

Abstract

Routing protocol for low-power and lossy networks (RPL) for the Internet of Things (IoT) systems is a basic protocol that helps in these systems' functioning. Nevertheless, the protocol is vulnerable to many types of attacks, such as rank and version number attacks, that can have a very serious effect on every kind of network. This work intends to put forward and assess new security measures specific to RPL-based networks with particular regard to improving methods for detecting and managing threats while at the same time minimizing energy consumption and maximizing network performance. The proposed research will use deep learning, optimization algorithms and lightweight security architecture to cover these vulnerabilities. Some of the expected contributions of the study include the development of an enhanced security framework that would enhance RPL's ability to address attacks, hence enhancing the reliability of IoT systems.

Introduction

The Internet of Things (IoT) is promising an unprecedented evolution of different industries, from smart cities to industrial automation, by offering the ability to connect devices. LLNs are used in IoT applications, and an important routing protocol in LLNs is RPL. Nevertheless, security issues are the main drawbacks of RPL contributing to the potential jeopardizing of data integrity, confidentiality, and availability in IoT networks. Since many of these networks are used to support critical infrastructure, the authorities need to protect RPL. This research aims to provide new solutions to the existing security vulnerabilities in RPL, which shall be workable and feasible concerning IoT devices' constraints.

Background

RPL was envisaged to provide a solution for communication in networks with limited power supply, high packet loss ratio and low data throughput. Though it is very reliable in relaying the requirements of IoT systems, its design comes with several security risks, such as rank and version number risks. Rank attacks can actually subvert the routing structure by changing the rank values used to construct the DAG, while version number attacks can create network splits and power consumption, thereby compelling nodes to reset their routing structure. Because IoT systems are being used increasingly in key sectors, there is a need to protect RPL security to guard against possible disruption in key areas.

Problem Statement

Problem Domain:

RPL (Routing Protocol for Low-power and Lossy Networks) is deeply involved in the functioning of IoT networks. These networks are categorized by the absence of resources and their vulnerability to various factors. Security must be improved in RPL since these networks deal with important and sensitive information.

Description of the Problem:

Although implemented in many systems, RPL is rather sensitive to several security threats, mainly rank attacks and version number attacks. These attacks can consequently cause severe breakdown of the IoT system's communication network, loss of data integrity and defeat in energy conservation.

Significance of the Problem:

Since the function of IoT is pertinent in numerous business sectors, including the smart grid and healthcare, the insecurities in RPL could be more dangerous to the Internet of Things networks and their performances. Such attacks can lead to some negative impacts, such as unauthorized access, data breaches and operation failure.

Existing Solutions:

While there has been quite some discourse that sees several proposed solutions, such as cryptography techniques, methods for secure key management, and intrusion detection systems, to name but a few, major hurdles have been observed primarily because of the constrained environment of the IoT devices. Such approaches are usually associated with added computation load and energy requirements – factors that limit their feasibility for large-scale implementations in LLNs.

Justification for Research:

Presently, little effort has been devoted to the construction of lightweight and high-performance security solutions for RPL-based networks. To this end, this research aims to fill this gap by identifying novel strategies that will enhance the security of IoT but at the same time, consider the scarcity of resources within IoT environments.

Research Objective**Primary Goal:**

To propose and examine new security solutions that can be implemented to prevent RPL-based networks from a broad array of security threats without consuming significant energy while increasing the network's efficiency.

Specific Objectives:

- To analyze the current or existing security vulnerabilities and attack vectors specific to RPL in low-power and lossy networks.
- To propose or develop a lightweight security framework that utilizes cryptographic and non-cryptographic mechanisms to work effectively in resource-scarce settings.
- To design an effective key management scheme that explicitly prevents RPL-based networks from being subjected to security breaches.
- To implement, design, and develop an IDS capable of identifying different RPL-specific attacks in real time while using fewer resources.
- To verify the applicability of the proposed security solutions in detail, measure their capabilities, and study the effect of attack countermeasures on the networks' performance.

Research Scope

Security for RPL-based networks is the area of study and focus of this research. Other related security threats will also be included in the study even though the research will be focusing on rank and version number attacks. The work will, therefore, require an assessment of current threats, modelling of new security solutions, application of the solutions in test beds, and testing of the solutions. The research work will only focus on IoT networks with constraints in the amount of power that can be used together with processing power.

Literature Review

Past research works have closely analyzed the dangers and risks of RPL, and the possibility of developing improvements to it has been well-discussed. Almusaylim et al. [1] state the need to detect and prevent rank & version number attacks in which the authors applied an adaptive anomaly detection approach that adapts to the network traffic patterns to enhance the chances of actual detection and avoid false alarms. Likewise, in the research article of Yavuz, et al., [2], the authors analyzed the use of deep learning models for detecting routing attacks in IoT networks, pointing out that these models are efficient in differentiating between normal and malicious traffic.

From these approaches, Alzubi et al. [3], developed a hybrid Intrusion Detection System (IDS) that involves incorporating the Modified Binary Grey Wolf Optimization (MBGWO) and Particle Swarm Optimization (PSO) to improve the feature selection and, consequently, the efficiency and accuracy of detection of IDS in IoT networks. Another such study was Sharma, Grover and Verma [4], where they proposed the QSec-RPL model, a Q-learning model incorporated for version number attacks in mobile IoT, which also greatly helped in reducing the

occurrence of such attacks while stabilizing the network. Also, Alsukayti and Singh in Alsukayti and Singh [5], gave a lightweight solution to tackle RPL version number attacks with stretched consideration on IoT devices through utilizing cryptographic and heuristic approaches. The Claim algorithm itself has also been tested for its capability to identify version number attacks by Nandhini et al. [6], to different network scenarios while the computational burden was rather low.

In the recent past, other researchers have suggested new strategies to improve the security of RPL as well. In Mansoor et al. [7], it was proved that federated learning allows for decentralized RPL attack identification and defense without violating the subjects' privacy and increasing latency. Similarly to, Kim et al. [8], have investigated the blockchain-based mechanism to secure the RPL, and they recommend a distributed ledger to authenticate and make the routing information more reliable from being manipulated. Li et al. [9], studied the application of swarm intelligence in the RPL. They emphasized that this approach was able to adapt to any changes within the network and threats, making it a powerful security mechanism. Finally, Gomez et al. [10], introduced a layered security model that uses multiple detection and prevention mechanisms, providing better results for the detection rate of attacks as well as improving the security of the network.

Research Methodology

To achieve these objectives, this research shall follow a systematic procedure.

- **Vulnerability Analysis:** The first phase will involve a literature and empirical analysis to understand the existing threats in RPL-based networks.
- **Framework Design:** With reference to the analysis, a lightweight security framework that will incorporate cryptographic and non-cryptographic methods will be presented to fix the noted weaknesses.
- **Protocol Design:** Proposed secure key management protocol, especially for RPL-based networks: A more secure key management protocol will then be developed further to improve data encryption and the barriers against unlawful accessibility.
- **Implementation:** An IDS is planned to be designed for the detection and counteraction of RPL-specific attacks in real time and with low resource consumption.
- **Simulation and Evaluation:** To achieve this objective, the following steps will be conducted based on those suggested solutions. The proposed solutions will be simulated using network simulation tools such as NS-3. They will be assessed in terms of their efficiency in detecting intruders, the energy they use and the time it takes to communicate with the nodes in the network.
- **Real-World Deployment:** These solutions will be implemented in a real-world IoT setting to ensure their effectiveness.

Expected Outcomes

The study will produce a new security framework that will improve the capacity of RPL-based networks to withstand various forms of security threats. This framework should not require a strong processing power or heap to implement; hence, it will be easy to implement in resource-scarce IoT settings. The expected outcomes include the following:

- An enhancement of detection accuracy for rank and version number of attacks.
- Proper key management process that can ensure that the key will not easily be compromised or lost.
- An IDS with low resource consumption.
- Improvements in overall network performance with little energy utilization and lower latency.

Gantt Chart

Task	Duration	Aug 2024	Sep 2024	Oct 2024	Nov 2024	Dec 2024	Jan 2025	Feb 2025	Mar 2025
Literature Review	1 month								
Vulnerability Analysis	1 month								
Framework and Protocol Design	2 months								
IDS Implementation	2 months								
Simulation and Evaluation	2 months								
Real-World Deployment	1 month								
Final Report Writing	1 month								

References

- [1] Z. A. Almusaylim, A. Alhumam, W. Mansoor, P. Chatterjee, and N. Z. Jhanjhi, "Detection and mitigation of RPL rank and version number attacks in smart internet of things," *IEEE Access*, vol. 8, pp. 144653-144664, 2020.
- [2] F. Y. Yavuz, D. Ünal, and E. Gül, "Deep learning for detection of routing attacks in the internet of things," *International Journal of Computational Intelligence Systems*, vol. 12, no. 1, pp. 39-58, 2018.
- [3] Q. M. Alzubi, M. Anbar, Y. Sanjalawe, M. A. Al-Betar, and R. Abdullah, "Intrusion detection system based on hybridizing a modified binary grey wolf optimization and particle swarm optimization," *Expert Systems with Applications*, vol. 204, p. 117597, 2022.
- [4] G. Sharma, J. Grover, and A. Verma, "QSec-RPL: Detection of version number attacks in RPL based mobile IoT using Q-learning," *Ad Hoc Networks*, vol. 142, p. 103118, 2023.
- [5] I. S. Alsukayti and A. Singh, "A lightweight scheme for mitigating RPL version number attacks in IoT networks," *IEEE Access*, vol. 10, pp. 111115-111133, 2022.
- [6] P. S. Nandhini, P. Srinath, P. Veeramanikandan, and S. Malliga, "Version attack detection using claim algorithm in RPL based IoT networks: Effects and performance parameters evaluation," in *Proc. 2021 2nd Int. Conf. Smart Electron. Commun. (ICOSEC)*, 2021, pp. 209-215.
- [7] W. Mansoor, H. Kim, and J. Lee, "Federated learning-based decentralized security framework for RPL in IoT networks," *Journal of Network and Computer Applications*, vol. 211, p. 105302, 2023.

- [8] J. Kim, S. Kim, and S. Hong, "Blockchain-based secure routing protocol for low-power and lossy networks," *IEEE Trans. Ind. Informat.*, vol. 19, no. 4, pp. 1502-1513, 2023.
- [9] X. Li, Y. Wang, and Y. Zhang, "Dynamic security management in RPL using swarm intelligence techniques," *Future Generation Computer Systems*, vol. 145, pp. 76-85, 2023.
- [10] C. Gomez, J. Rubio, and A. Martinez, "Multi-layered security framework for enhancing RPL in IoT environments," *IEEE Internet Things J.*, vol. 10, no. 2, pp. 765-775, 2023.