



RPL Security

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
28/07/2024

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

Problem Statement

Problem Domain: Routing Protocol for Low Power and Lossy Networks (RPL) is a specific protocol that aims to control the data flow in networks with low power and high loss rates. These networks are commonly used in IoT applications, including smart cities, industrial automation, and environmental monitoring. Since different RPL networks contain ultra-sensitive data, it is paramount that their safety is considered, primarily because these networks are implemented in critical infrastructures.

Description of the Problem: Despite RPL being designed to reduce complexity, power consumption, and energy usage, the standard cannot be said to be highly resistant to security threats by intruders. These vulnerabilities include but are not limited to routing topology attacks such as rank attacks, wormhole attacks, sinkhole attacks, leakage of information, and denial of service attacks commonly referred to as DoS. This could result in disturbing operations, loss of data, and unauthorized access to the network's control; hence, the systems' availability and integrity will be threatened.

Significance of the Problem: The security of RPL-based networks is vital because they operate in areas where they support essential data and services. Threats include loss of confidentiality, theft of information, and disruption of an organization's activities. For instance, in smart grids, hackers can tamper with computer-controlled power systems, resulting in power blackouts or improper distribution of the available power, which has felt effects on the economy and society. Therefore, improving the security level of RPL is vital for the networks to function correctly.

Existing Solutions: Various security measures protect RPL, such as Cryptographic security, Secure critical management systems, and Intrusion detection systems. However, these solutions have some issues, such as energy consumption being significantly more than the original message's energy, additional computation being absorbed in the detection process, and many resources being required, which must be more suitable for LPLN networks. As a result, more than the existing solutions are needed to cover the needs related to the organization of effectively functioning RPL-based networks.

Justification for Research: Despite the existing efforts, more focus should be given to the efficient and lightweight security solution for RPL with a target operation within the resource constraints of LLNs. This research attempts to fill the gap by revealing fresh ideas that can improve security while positively impacting network resources' performance and utilization. Such research is essential since more and more IoT systems are being deployed in different fields, and the threats they face are rising.

Research Objectives

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:

1. To analyse the current or existing security vulnerabilities and attack vectors specific to RPL in low-power and lossy networks.
2. Propose or develop a lightweight security framework that utilizes cryptographic and non-cryptographic mechanisms to work effectively in resource-scarce settings.

3. Design an effective key management scheme that explicitly prevents RPL-based networks from being subjected to security breaches.
4. Implement, design, and develop an IDS capable of identifying different RPL-specific attacks in real-time while using fewer resources.
5. 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.

Literature Review

The IPv6-based Routing Protocol for Low-power and Lossy Networks (RPL) is currently one of the most widely used protocols in the IoT, especially because RPL is effective in managing resources that are often limited in the IoT context. However, it has several security threats, namely rank and version number attacks. This literature review analyses the recent trends for addressing and identifying these threats, whereas the main attention is paid to the methods based on machine learning, optimization, and lightweight security models.

Detection and Mitigation Techniques for RPL Attacks

Almusaylim et al. [1] consider ways to identify and counteract RPL rank and version number attacks, which are challenging as they disturb the routing structure and lead to extensive network fluctuations. This paper acknowledges that researchers have found that coping with an anomaly detection system with RPL is effective since such a system can detect abnormal patterns that depict such attacks. They present one that regulates the parameters according to the traffic and improves the detection of suspicious activity without significantly raising the false positive number.

In this respect, Yavuz et al., [2] consider using deep learning methods for detecting routing attacks in the IoT networks with a focus on RPL. Cao et al.'s study shows that through analysing those traffic, deep learning models can distinguish normal and malicious behaviours by learning those traffic patterns. That way, they demonstrate that such models provide high detection rates, and they propose a relatively solid approach to detecting a range of RPL-specific attacks such as rank and version number forgery.

Intrusion Detection Systems (IDS) and Optimization Techniques

Alzubi et al. [3] suggested the hybrid Intrusion Detection System (IDS) utilizing the Modified Binary Grey Wolf Optimisation Algorithm and Particle Swarm Optimization further to boost the intrusion detection rate in IoT networks. It is based on enhancing the selection of the characteristics connected with an attack to optimize IDS. The specifics of this work are presented in the following sentence: It is based on increasing the effectiveness of an IDS by optimizing the procedure for selecting the individual features that describe an attack. The research shows that this hybrid method outperforms other IDS approaches, attributed to its proper application in the LLC networks.

Proposing a modified version of the RPL protocol based on Machine Learning called QSec-RPL in conjecture with mobile IoT systems, Sharma et al. [4] suggest that its utilization can help detect version number attacks. This method employs reinforcement learning, which enables the system to learn about new attacks or patterns and how to handle them. This work further proposes the QSec-RPL, which can vastly reduce the attack impact through the fast detection of the attacker nodes and the denial, guaranteeing the PDR, LAS, DR, and Packet Delivery Ratio.

Lightweight Security Solutions

As for the further development and focus of Alsukayti and Singh [5], they also emphasize the need to solve the security problem in IoT networks more concretely in the context of the developing world with restricted educational and financial resources. They have created a minimalist framework using as few computational assets as possible to minimize the attacks against the RPL version number and the security required. Their solution also employs lightweight cryptography and heuristic techniques to identify malicious code because IoT devices have limited processing power and energy.

From the literature, Nandhini et al. [6] present an evaluation of the performance of the proposed Claim algorithm in detecting version attacks in RPL networks. It embraces testing the validity of a version number received from nodes, especially by the node that initiated the new version in the network, to prevent the network from being misguided on the topology condition. Their work also describes the effectiveness of Claim in different network settings and shows that even with a significantly higher number of messages, it does not negatively affect the overall detection accuracy while requiring minimal resources.

Conclusion

The related work suggests that research should focus on developing new security solutions for RPL based on the IoT environment's peculiarities. But when it comes to progression, there is what we have now as traditional methods of AI for speech recognition; there is deep learning, which is a new and improved method, optimization algorithms, and even new lightweight frameworks for this field. Based on the current findings, future research should aim to achieve a marked improvement in the efficacy of security while at the same time working under the limitations of low power and lossy networks.

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," 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 *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, pp. 209-215, Oct. 2021.