



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
05/07/2024

Paper Summaries and Critical Analysis:

Paper 1: The paper titled "Detection and Mitigation of RPL Rank and Version Number Attacks in Smart Grid Applications" and conducted **by** Almusaylim et al. [1].

- Summary

Objectives: The primary focus of this research is to identify and mitigate Rank and Version Number attacks in the context of smart grid systems using the Routing protocol for Low power and lossy networks (RPL) protocol.

Methods: To find and stop these assaults, the research combines a variety of security techniques, including trust-based methods and intrusion detection systems.

Key Findings: The proposed methods significantly improve the security of smart grid applications by efficiently identifying and thwarting Rank and Version Number assaults.

- Critical Analysis

Strengths: The study presents a comprehensive strategy that incorporates a number of detecting techniques. Moreover, it utilizes these techniques in an actual situation, guaranteeing the significance and usefulness of the results.

Weaknesses: The methodology's complexity might lead to increased computing cost, which might limit its applicability in resource-constrained Internet of things (IoT) contexts.

Paper 2: The paper titled “Deep Learning for Detection of Routing Attacks in the Internet of Things” and conducted **by** yavuz et al. [2].

- Summary

Objectives: In order to detect routing attacks in IoT networks, this study proposes to use a deep-learning-based approach that focuses on decreasing rank, hello-flood, and version number modification assaults.

Methods: The research effort creates IoT attack datasets using the Cooja simulator and trains deep learning models to identify these threats.

Key Findings: demonstrates the effectiveness of deep learning in boosting IoT security by successfully achieving high accuracy and precision in identifying the designated routing attacks.

- Critical Analysis

Strengths: Large-scale IoT networks could benefit from this strategy due to its high accuracy and scalability. Deep learning makes it possible to handle large datasets and complex attack patterns efficiently.

Weaknesses: The method requires a large amount of computer power during training; hence it might not be practical in many Internet of Things scenarios. Furthermore, depending solely on simulation data may limit the applicability of the findings to actual situations.

Paper 3: The paper titled “Intrusion Detection System Based on Hybridizing a Modified Binary Grey Wolf Optimization and Particle Swarm Optimization” and conducted **by** Alzubi et al. [3].

- Summary

Objectives: The goal of the research is to improve intrusion detection in Internet of Things (IoT) networks by presenting a hybrid optimization approach.

Methods: The study combines Modified Binary Grey Wolf Optimization (MBGWO) with Particle Swarm Optimization (PSO) to improve the performance of an Intrusion Detection System (IDS).

Key Findings: The hybrid approach outperforms the classic methods in terms of false positive rate and detection accuracy.

- Critical Analysis

Strengths: By combining the best aspects of both optimization strategies, the hybrid algorithm improves detection performance. It also shows fewer false positive rates when compared to other approaches.

Weaknesses: Higher computing expenses could result from the hybrid algorithm's complexity. Moreover, a thorough comparison with other cutting-edge techniques is absent from the study.

Paper 4: The paper titled “QSec-RPL: A Lightweight Secure Routing Framework for IoT” and conducted **by** Sharma et al. [4].

- Summary

Objectives: Explains Q-Learning method (QSec)-RPL, a simplified architecture designed to defend the RPL protocol against many types of routing attacks.

Methods: Utilizes both cryptographic techniques and trust-based mechanisms to bolster the security of RPL.

Key Findings: QSec-RPL effectively mitigates several routing attacks while maintaining low overhead, making it suitable for resource-constrained IoT devices.

- Critical Analysis

Strengths: The framework minimizes computational and communication overhead because it is designed for contexts with limited resources. It provides extensive security features and handles several attack vectors.

Weaknesses: Relying too much on cryptographic techniques could cause latency and increase energy consumption, which could have an impact on how well IoT networks function.

Paper 5: The paper titled “A Lightweight Scheme for Mitigating RPL Version Number Attacks in IoT Networks” and conducted **by** Singh and Alsukayti [5].

- Summary

Objectives: The vulnerability of RPL to Version Number (VN) attacks—which can cause frequent topology changes in IoT networks—is discussed in the study. Collaborative and Distributed RPL (CDRPL), the suggested remedy, improves RPL's resistance to VN attacks while requiring the least amount of overhead.

Methods: CDRPL adds a distributed and cooperative security model to RPL while requiring little changes to its fundamental operations. Simple node-local processing is used, with no need for extra entities or needless connection cost. The technique seeks to identify and stop both simple and sophisticated VN attacks.

Key Findings: The outcomes of the experiments show that CDRPL effectively detects and mitigates VN assaults while preserving network stability, managing traffic overhead, enhancing QoS, and using less energy. CDRPL provides better performance with less processing needs than other methods.

- Critical Analysis

Strengths: This lightweight solution shows scalability and efficacy in small and large network environments, needing minimum changes to the current RPL protocol. The efficiency of the suggested solution has been confirmed by extensive experimental evaluations.

Weaknesses: The research lacks thorough comparisons of computational complexity and communication overhead with all currently available methods. Although countering VN assaults is essential, it might overshadow other possible RPL weaknesses.

Paper 6: The paper titled "Version Attack Detection using Claim Algorithm in RPL-based IoT Networks: Effects and Performance Parameters Evaluation" and conducted **by** Nandhini et al. [6].

- Summary

Objectives: This research introduces a claim-based approach for identifying and mitigating VN attacks with the goal of strengthening the security of RPL networks. The study evaluates the suggested solution's effects and performance indicators in several IoT network scenarios.

Methods: Using the claim-based algorithm described in the study, nodes confirm assaults by comparing version numbers from neighbors and looking for differences. It evaluates and contrasts network performance under various attack scenarios with the baseline.

Key Findings: The outcomes show how well the claim-based method detects and lessens the effects of VN attacks on network performance. Even in the face of attacks, the system preserves energy usage and packet delivery ratio stability while guaranteeing robust network functioning.

- Critical Analysis

Strengths: The claim-based technique reduces interference with network operations during attack detection and mitigation while providing a methodical way to identify VN attacks. It also includes a thorough assessment of network performance across various attack scenarios.

Weaknesses: The approach's verification process may result in an increase in overhead. Nevertheless, comprehensive comparisons of the suggested solution's efficiency and scalability with other current approaches are absent from the paper.

Connections and Conflicts:

Connections: Several papers [1], [2] and [4] focus on securing the RPL protocol against routing attacks, highlighting its critical role in IoT security. The use of deep learning [2] and hybrid optimization algorithms [3] indicates a trend towards leveraging advanced computational methods for intrusion detection. Both papers [5] and [6] aim to strengthen the security of RPL-based IoT networks by mitigating VN attacks. Each solution prioritizes maintaining network stability and performance while addressing security issues.

Conflicts: Paper [2] emphasizes the use of deep learning, while Paper [4] favors lightweight solutions, emphasizing the trade-off between detection accuracy and computational efficiency. Paper [3] introduces a hybrid approach that aims to balance these factors, albeit with added complexities. Papers [5] and [6] focus on different approaches: CDRPL prioritizes minimal modifications and lightweight processing, whereas the claim-based algorithm involves more extensive verification processes, potentially increasing overhead.

Summary Table:

Publication Year	Author(s)	Methodology	Key Findings	Limitations
2023	Sharma et al. [4]	Cryptographic, Trust-based methods	Effective and lightweight security for RPL	Latency and additional energy consumption
2023	Nandhini et al. [6]	Claim-based algorithm	Successful detection and mitigation of VN attacks, maintains network performance	Potential overhead due to verification process, limited scalability analysis
2022	Alzubi et al. [3]	MBGWO, PSO	Improved detection accuracy and lower false positive rate	Increased computational costs
2022	Singh and Alsukayti [5]	Collaborative and Distributed RPL (CDRPL)	Effective detection and mitigation of VN attacks with lightweight processing	Limited comparison with other solutions, focus only on VN attacks
2020	Almusaylim et al. [1]	IDS, Trust-based methods	Effective detection and mitigation of RPL attacks	Increased computational overhead
2018	yavuz et al. [2]	Deep learning, Cooja simulator	High accuracy and precision in detecting routing attacks	High computational resources required, reliance on simulations

- **RPL:** Routing protocol for Low power and lossy networks.
- **IoT:** Internet of things.
- **MBGWO:** Modified Binary Grey Wolf Optimization.
- **PSO:** Particle Swarm Optimization.
- **IDS:** Intrusion Detection System.
- **CDRPL:** Collaborative and Distributed RPL.
- **VN:** Version Number.

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, doi: 10.20944/preprints202007.0476.v1.
- [2] furkan yavuz, F. Yusuf YAVUZ, D. Ünal, and E. Gül, "Deep Learning for Detection of Routing Attacks in the Internet of Things," 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 Syst Appl*, vol. 204, Oct. 2022, doi: 10.1016/j.eswa.2022.117597.
- [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, Apr. 2023, doi: 10.1016/j.adhoc.2023.103118.
- [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, doi: 10.1109/ACCESS.2022.3215460.
- [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 *Proceedings - 2nd International Conference on Smart Electronics and Communication, ICOSEC 2021*, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 209–215. doi: 10.1109/ICOSEC51865.2021.9591735.