

Atheer Mohammed-Literature Review Report

by Iznan Hasbullah

Submission date: 27-Jul-2025 10:35PM (UTC+0800)

Submission ID: 2721160135

File name: Atheer_Mohammed-Literature_Review_Report.pdf (151.9K)

Word count: 705

Character count: 4110

Literature Review Report: ⁴Detection System for RPL Security

Introduction

The ²Internet of Things (IoT) has grown rapidly, but its security remains a major concern. The RPL protocol is widely used in IoT networks, yet it is vulnerable to Version Number Attacks (VNA) that disrupt routing and degrade performance. This literature review summarizes, analyzes, and compares six research papers addressing VNA detection in RPL-based IoT networks.

Summary of Research Papers

¹Paper 1: Distributed Monitoring Strategy

Mayzaud et al. (2017) proposed a distributed monitoring strategy to detect VNAs with high detection rates (>90%) and low false positives. The approach used passive monitoring nodes and Cooja simulations but required additional devices and was specific to RPL.

Paper 2: Lightweight Scheme

Alsukayti & Singh (2022) developed CDRPL, a lightweight collaborative scheme maintaining network stability and low overhead while detecting VNAs. It was tested only on VNAs in simulations, lacking real-world validation.

Paper 3: Detection and Mitigation

Almusaylim et al. (2020) introduced SRPL-RP, which detects and mitigates rank and VNAs with 98.17% accuracy in simulations. It lacked real-world testing and broader comparisons.

Paper 4: ML-LGBM

Osman et al. (2021) applied a LightGBM-based machine learning model to detect VNAs with 99.6% accuracy and low resource use, though it was not tested on actual IoT devices and risked overfitting.

Paper 5: Parent Supervision

Rouissat et al. (n.d.) proposed a lightweight parent supervision method reducing overhead and improving delivery, tested on a small 16-node simulated network focused only on VNAs.

Paper 6: Claim Algorithm

Nandhini et al. (2021) used a collaborative Claim algorithm improving detection, reducing latency by 87%, and increasing delivery by 86%. It was not tested on large-scale networks or evaluated for energy consumption.

Critical Analysis

These studies address VNA detection through innovative, lightweight designs with high accuracy and low overhead. However, they all rely heavily on simulations, lack real-world validation, focus narrowly on VNAs, and often omit energy-resource trade-off evaluations.

Connections

All studies focus on securing RPL in IoT networks, identifying VNAs as a significant threat. They propose lightweight, resource-efficient solutions tested mainly via simulation, assessing performance based on accuracy, overhead, and energy consumption.

Conflicts

The studies differ in monitoring (distributed vs. centralized), detection (rule-based vs. machine learning), scope (VNA only vs. multiple attacks), and level of application (parent-based vs. network-wide). Methodologies also vary between active and passive monitoring.

Synthesis Matrix

Study	Authors	Year	Research Design	Key Findings/Results	Methodology	Limitations
Distributed Monitoring	Mayzaud et al.	2017	Experimental	>90% detection, low false positives	Distributed monitoring, simulation	Extra devices, RPL-specific
CDRPL Scheme	Alsukayti & Singh	2022	Experimental	Stable network, low overhead	Modified RPL, simulation	Only VNA, simulated
SRPL-RP	Almusaylim et al.	2020	Experimental	98.17% accuracy, high delivery	Status tables, node isolation	No real-world testing
ML-LGBM	Osman et al.	2021	Experimental	99.6% accuracy, low memory use	LightGBM machine learning	Simulated only
Parent Supervision	Rouissat et al.	n.d.	Experimental	Lightweight, effective	Parent-child monitoring	Small network
Claim Algorithm	Nandhini et al.	2021	Experimental	87% latency reduction, 86% delivery	Claim algorithm, simulation	Limited scale, no energy analysis

References

- Almusaylim, Z. A., et al. (2020). *Detection and Mitigation of RPL Rank and Version Number Attacks in Smart Internet of Things*. <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., et al. (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., et al. (2021). *Version Attack Detection using Claim Algorithm in RPL based IoT Networks*. <https://doi.org/10.1109/ICOCSEC51865.2021.9591735>
- Osman, M., et al. (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, 83654–83665. <https://doi.org/10.1109/ACCESS.2021.3087175>
- Rouissat, M., et al. (n.d.). *Parent supervision lightweight solution against version number attacks for IoT networks*. <https://doi.org/>

Atheer Mohammed-Literature Review Report

ORIGINALITY REPORT

6%

SIMILARITY INDEX

2%

INTERNET SOURCES

6%

PUBLICATIONS

0%

STUDENT PAPERS

PRIMARY SOURCES

- | | | |
|---|--|----|
| 1 | Abhishek Verma, Virender Ranga. "Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review", IEEE Sensors Journal, 2020
Publication | 2% |
| 2 | Qais Al-Na'amneh, Walid Dhifallah, Rahaf Hazaymih, Laith Alzboon, Ayoub Alsarhan, Mohammed Alshinwan, Rabia Emhamed Al Mamlook. "chapter 8 Analysis for Detection and Mitigation of Version Number Modification Attack in the Internet of Things", IGI Global, 2025
Publication | 2% |
| 3 | S Kalyani, D Vydeki. "A Resource-Efficient Ensemble Learning Framework for Detecting Rank Attacks in RPL-Based IoT Networks", Journal of Economy and Technology, 2025
Publication | 2% |
| 4 | Nadia Alfrieihat, Mohammed Anbar, Shankar Karuppayah, Shaza Dawood Ahmed Rihan, Basim Ahmad Alabsi, Alaa M. Momani. | 1% |

"Detecting Version Number Attacks in Low Power and Lossy Networks for Internet of Things Routing: Review and Taxonomy", IEEE Access, 2024

Publication

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		