

# Chapter 4

## Impact of Decreased Rank Attack on Network Topology of RPL Using Contiki-NG

**Qais Al-Na'amneh**

 <https://orcid.org/0009-0008-3034-7693>


*Applied Science Private University,  
Jordan*

**Mohammed Almaiah**

 <https://orcid.org/0009-0008-9785-485X>

*University of Jordan, Jordan*

**Walid Dhifallah**

 <https://orcid.org/0000-0003-1368-9612>

*University of Gabes, Tunisia*

**Braa Qadoumi**

 <https://orcid.org/0000-0002-4753-7820>

*Applied Science Private University,  
Jordan*

**Rahaf Hazaymih**


*Jordan University of Science and  
Technology, Jordan*

**Ayoub Alsarhan**

 <https://orcid.org/0000-0001-9075-2828>

*Hashemite University, Jordan*

**Tasnim Al-Harasis**

 <https://orcid.org/0009-0004-7440-9850>

*Al Hussein Technical University, Jordan*

### ABSTRACT

*The Internet of Things (IoT) refers to the widespread use of smart objects connected to the internet. This innovative technology serves as the foundation for various intelligent gadgets, including smartphones, smart homes, and electric equipment. Furthermore, these devices are uniquely identified and automatically connected to the network. RPL emphasizes security due to the nature of objects and their restrictions, which might pose weaknesses for cyber-attacks. It is crucial to identify and*

DOI: 10.4018/979-8-3693-8014-7.ch004

*assess all potential assaults on this protocol, including the rank attack, which can significantly impact network performance and energy usage. The impact of rank assaults on the proactive IoT routing protocol, Low Power Lossy Network (RPL), is discussed in this study. It emphasizes the necessity of addressing these attacks concerning different scenarios preserving topology, avoiding communication delays, and reducing throughput. The proposed solution significantly decreases the impact of a decreased rank attack on network performance.*

## **I. INTRODUCTION**

A special attack in the RPL standard is the Decreased Rank Attack, which uses the rank property to produce a topology that is only partially sub-optimized (Ghaleb, 2023). A hostile actor announces a fictitious lower-rank value to trick nodes into choosing the attacker as their preferred parent on the path to the root. Although it isn't harmful in theory it can harm a network even more when combined with other attacks like selective forwarding or bypass attacks. The RPL Decreased Rank attack is assessed in this paper, and a Secure Objective Function (Sec-OF) is suggested to stop malevolent players from starting attacks. A significant threat to the RPL protocol inside the IoT 6LowPAN communication standard is the Decreased Rank attack (Aljaidi, 2023).

In addition to analyzing four mitigation and detection strategies, this work suggests modifying TRAIL to compute the downward trip time (DTT) for nodes. It presents a potential exploit utilizing nonlinear objective functions (NOFs) (Tolsma, 2021). There are three primary categories of rank attacks: worst-parent, raised rank, and decreased rank. Additionally, the article presents a potential vulnerability that might lead to network loops, let neighbors select a less-than-ideal parent, and deceive a node's rank. Although TRAIL does not stop decreasing rank attacks, it does guarantee a path from the root that increases in rank monotonically. It is less complicated for devices with limited resources and defends against higher-rank attacks than VeRA (Boudouaia, 2020).

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: [www.igi-global.com/chapter/impact-of-decreased-rank-attack-on-network-topology-of-rpl-using-contiki-ng/378746](http://www.igi-global.com/chapter/impact-of-decreased-rank-attack-on-network-topology-of-rpl-using-contiki-ng/378746)

## Related Content

---

### Quantum Cryptography: In Security Aspects

S. Venkata Lakshmi, Sujatha Krishnamoorthy, Mudassir Khan, Neeraj Kumar and Varsha Sahni (2021). *Limitations and Future Applications of Quantum Cryptography* (pp. 47-61).

[www.irma-international.org/chapter/quantum-cryptography/272364](http://www.irma-international.org/chapter/quantum-cryptography/272364)

### Preserving Data Privacy in Electronic Health Records Using Blockchain Technology

Sathiyabhama B., Rajeswari K. C., Reenadevi R. and Arul Murugan R. (2020). *Transforming Businesses With Bitcoin Mining and Blockchain Applications* (pp. 195-206).

[www.irma-international.org/chapter/preserving-data-privacy-in-electronic-health-records-using-blockchain-technology/238368](http://www.irma-international.org/chapter/preserving-data-privacy-in-electronic-health-records-using-blockchain-technology/238368)

### Cryptographic Techniques Based on Bio-Inspired Systems

Petre Anghelescu (2020). *Cryptography: Breakthroughs in Research and Practice* (pp. 99-119).

[www.irma-international.org/chapter/cryptographic-techniques-based-on-bio-inspired-systems/244908](http://www.irma-international.org/chapter/cryptographic-techniques-based-on-bio-inspired-systems/244908)

### Provable Security for Public Key Cryptosystems: How to Prove that the Cryptosystem is Secure

Syed Taqi Ali (2016). *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security* (pp. 317-341).

[www.irma-international.org/chapter/provable-security-for-public-key-cryptosystems/153082](http://www.irma-international.org/chapter/provable-security-for-public-key-cryptosystems/153082)

### Blockchain in Clinical Trials

Shaveta Malik, Archana Mire, Amit Kumar Tyagi and Arathi Boyanapalli (2021). *Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles* (pp. 278-292).

[www.irma-international.org/chapter/blockchain-in-clinical-trials/262706](http://www.irma-international.org/chapter/blockchain-in-clinical-trials/262706)