

Course Title: Research Methodology in Computer Science

Course Code: AI800

Weighting: 20%

Lecturer: Dr. Mohammed Anbar

Hand-out Date: 6 July 2024

Hand-in Date: 27 July 2024

Hand-in Method: Online Submission via E-Learning.

Assignment Report: Securing RPL-Based IoT Networks: An Adaptive and Energy-Efficient Approach to Mitigating Version Number Attacks in Large-Scale Deployments

Student ID: 242001474

Student Name: Ali Mohamed

Table of contents:

- Problem Statement
- Objectives:
- References

- **Problem Statement**

Networks associated with the Internet of Things (IoT) as well as particularly those utilizing the Routing Protocols for Low-Power and Lossy Networks (RPL) are the subject of concern [1, 2]. The challenges of safeguarding low-resource devices in massively distributed networks—an increasingly significant topic for industrial control, smart cities, and healthcare systems—are covered in this topic.

The particular issue at hand is that version number assaults can be launched against IoT networks based on RPL [3, 4]. Because these attacks raise the version number on purpose, they use RPL's global repair mechanism to make the Destination-Oriented Directed Acyclic Graph (DODAG) rebuild itself when it's not needed [5, 6]. This results in increased network overhead, rapid battery depletion of IoT devices, issues with channel availability, and potential routing loops [2, 4]. The size of contemporary IoT deployments and the resource limitations of IoT devices exacerbate the difficulty.

Given the growing number of IoT deployments, this issue is quite important. Version number assaults have the potential to seriously shorten the lifespan of a network, interfere with regular operations, and jeopardize data integrity [3, 5]. The potential impact of such attacks increases rapidly as IoT networks become more and more essential to vital infrastructure, such as industrial control systems, smart grids, and healthcare monitoring [1, 6]. The sustained expansion, dependability, and public confidence in IoT networks depend heavily on their capacity to maintain efficiency and security. In IoT-dependent industries, failing to fix this vulnerability could result in large financial losses, privacy violations, and even hazards to public safety.

In the context of growing IoT deployments, this topic is quite important. Attacks using version numbers can drastically shorten the lifespan of a network, interfere with regular operations, and jeopardize the integrity of data [3, 5]. With the growing integration of IoT networks into vital infrastructure, such as industrial control systems, smart grids, and healthcare monitoring, the potential consequences of such assaults are increasing dramatically [1, 6]. The ability to maintain internet of things networks securely and effectively is essential for them to keep expanding, remaining trustworthy, and earning the confidence of the

general public. Industry sectors that depend on IoT could suffer significant financial losses, privacy infringements, and even threats to the general population if this vulnerability is not patched.

Despite these contemporary treatments, there remains a pressing need for additional research. Because comprehensive comparison studies are lacking, there are questions about the relative effectiveness and efficiency of present approaches [1, 2, 3, 5, 6]. The continuous evolution of IoT technology and attack vectors has resulted in this gap, making it difficult for academics to perform comprehensive and current comparisons. Solutions that effectively strike a compromise between security and the energy limitations of Internet of Things devices are conspicuously lacking [4, 5], an important consideration that has been disregarded in the rush to implement strong security measures. Furthermore, many recommended approaches lack thorough real-world testing or fail to account for interaction with broader security frameworks [6], primarily because of the difficulty and expense of putting up large-scale IoT testbeds.

The rapidly evolving nature of IoT threats and the expanding scope of IoT installations necessitate the need for more flexible, energy-efficient, and scalable security solutions [4, 6, 7]. Our research aims to fill in these gaps by: Comparing and contrasting all of the solutions that are currently in use in order to provide a precise standard for further study. Creating an innovative security architecture that is energy-aware and can adjust to the resource limitations of various Internet of Things devices. Putting our idea into practice and testing it in an actual Internet of Things setting to show its usefulness and efficacy. Combining our strategy with more comprehensive IoT security frameworks to provide a comprehensive defense against a range of threats. This research is unique in that it takes a comprehensive approach, integrating the creation of an adaptable, energy-efficient security framework with a detailed examination of current solutions. Our effort intends to greatly enhance the field of IoT security, especially in the context of RPL-based networks confronting version number threats, by filling up important research gaps and emphasizing practical application.

Objectives:

Enhanced Investigation Goal: Developing, implementing, and evaluating a comprehensive, energy-efficient, and flexible solution for version number attack detection and mitigation in RPL-based IoT networks would help to increase the security and resilience of large-scale IoT installations.

Comparison Analysis: To stop version number attacks in RPL-based IoT networks, conduct a thorough assessment of the most recent iterations of claim algorithms, machine learning models, lightweight schemes, and distributed monitoring techniques. This will lay the groundwork for future development by highlighting significant advantages and disadvantages of the present approaches.

Adaptive Detection Mechanism: To Design and build a detection mechanism that can adjust its parameters based on network conditions and attack patterns. This target aims to improve the accuracy and efficiency of attack detection while addressing the lack of context-aware solutions in the techniques now in use.

Energy-efficient Mitigation: To Provide and put into action a method of energy-efficient mitigation that successfully thwarts version number attacks and lessens the impact on Internet of Things devices with limited funding. Reaching a compromise between energy efficiency and security is critical in Internet of Things networks, and this objective satisfies that demand. Create an Integrated Security Framework to allow the suggested approach to be easily integrated with other RPL network security mechanisms. This goal attempts to solve the current lack of integration in available solutions by developing a comprehensive security approach.

Practical Assessment: To Put the suggested solution into practice and assess it in various practical IoT implementations. The aforementioned goal fills the need in the comprehensive field testing of current solutions and will yield significant understanding on the pragmatic suitability of our methodology. **Scalability Analysis:** Look into and measure how scalable the suggested solution is in extensive IoT networks that have thousands of nodes. By addressing the shortcomings in the scalability studies of existing methods, this goal will show that the solution is viable for large-scale IoT deployments.

Recommendations for Standardization: To Create recommendations based on evidence for possible RPL standard modifications that would strengthen the

standard's built-in defense against version number attacks. This goal seeks to overcome the dearth of standardization initiatives in the literature and make a lasting contribution to IoT network protocols.

Fast Recovery Mechanism: After a version number assault has been identified and countered, develop, put into practice, and assess a fast recovery mechanism that can promptly return the network to normal. This goal is to provide network resilience and reduce the long-term effects of attacks.

This study is essential to safeguarding the growing field of Internet of Things implementations. Our goal is to increase the security, efficiency, and reliability of IoT systems dramatically by tackling the critical vulnerability of version number attacks in RPL-based networks. We will close the gap between academic research and practical application with our all-encompassing strategy, which combines theoretical study with practical execution and evaluation. Our solution is viable for resource-constrained IoT devices in large-scale deployments since it focuses on energy efficiency and scalability. Furthermore, this research has the ability to influence the direction of IoT network protocols in the future and leave a lasting legacy in the area by potentially aiding standardization efforts.

A thorough evaluation of the versions number attack solutions currently in use with one another. A cutting-edge, flexible, and energy-saving version number attack detection and mitigation system. Factual information about how well the suggested solution works and how it affects actual Internet of Things deployments. Metrics for scaling IoT network security on a big scale. Improvements that should be made to the RPL standard to protect it from version number attacks. Quick recovery for network restoration following an attack. Additions to the corpus of knowledge on IoT security through presentations at international conferences and publications in journals of significant influence.

References

- Almusaylim, Z. A., Alhumam, A., Mansoor, W., Chatterjee, P., & Jhanjhi, N. Z. (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., Badonnel, R., & Chrisment, I. (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., Srinath, P., Veeramanikandan, P., & Malliga, S. (2021). Version Attack Detection using Claim Algorithm in RPL based IoT Networks: Effects and Performance Parameters Evaluation. *Proceedings - 2nd International Conference on Smart Electronics and Communication, ICOSEC 2021*, 209–215. <https://doi.org/10.1109/ICOSEC51865.2021.9591735>
- Osman, M., He, J., Mokbal, F. M. M., Zhu, N., & Qureshi, S. (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., Universitaire Nour Bachir El Bayadh Mohammed BELKHEIR, C., Universitaire Nour Bachir El Bayadh Allel Mokaddem, C., Center Nour Bachir, U., Bachir, N., & Allel Mokaddem, A. (n.d.). Parent supervision lightweight solution against version number attacks for IoT networks. <https://doi.org/>