IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/46ICT/2025/4625525/
Vol. 2025 (35), Article ID 4625525

Performance Evaluation of a Modified RPL Routing Protocol Enabling Detection of Version Number and Rank Decrease Attacks in 6LoWPAN-based Wireless Sensor Networks*

Przemyslaw MACIEJKO and Jaroslaw KRYGIER

Military University of Technology, Faculty of Electronics, Warsaw, Poland

Correspondence should be addressed to: Przemyslaw MACIEJKO, przemyslaw.maciejko@wp.pl

* Presented at the 46th IBIMA International Conference, 26-27 November 2025, Ronda, Spain

Abstract

This paper presents mechanisms for detecting Version Number and Rank Decrease Attacks on a sensor network based on IEEE 802.15.4/6LoWPAN technology with the RPL routing protocol. In addition to detecting intruders carrying out the indicated attacks, the presented mechanisms also minimize the attack's effects. The tests of the developed solutions indicate high intruder detection efficiency, even with a significant number of simultaneously attacking nodes. Furthermore, using the developed mechanisms significantly reduces the energy consumption of network nodes during an attack, and minimizes signaling traffic.

Keywords: WSN, RPL, Version Number Attack, Rank Decrease Attack

Introduction

Wireless sensor networks (WSNs) are becoming commonplace in the era of the Internet of Things (IoT). Many WSNs utilize communication techniques that allow data to be transmitted to edge nodes via other intermediary nodes. Therefore, such networks require a routing protocol. Unfortunately, such a protocol can be a target for attacks against such networks. This paper is devoted to identifying the vulnerabilities of WSNs to selected attacks and to suggesting solutions for detecting such attacks.

The RPL protocol (Routing Protocol for Low-Power and Lossy Networks) (Winter, et al., 2012) was designed to meet the unique requirements of low-power and lossy networks, suitable for 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) (Montenegro et al., 2007), which are part of the IEEE 802.15.4 standard. RPL is a distance vector protocol, which means that route updates are regularly sent between neighboring nodes (Ghosh, 2017; Vasseur and Dunkels, 2010).

The RPL is based on Destination Oriented Directed Acyclic Graph (DODAG), whose basic element is the root node, from which subsequent branches of the tree are created. In relation to the sensor network, this node is most often the gateway from the sensor network to the external network. DODAG is built using a specific Objective Function (OF) that defines how routing metrics are calculated and manages the interconnection of nodes (the selection of parent and child nodes).

Cite this Article as: Przemyslaw MACIEJKO and Jaroslaw KRYGIER, Vol. 2025 (35) "Performance Evaluation of a Modified RPL Routing Protocol Enabling Detection of Version Number and Rank Decrease Attacks in 6LoWPAN-based Wireless Sensor Networks " Communications of International Proceedings, Vol. 2025 (35), Article ID 4625525, https://doi.org/10.5171/2025.4625525

The RPL uses three types of control messages: DIO (DODAG Information Object), DAO (DODAG Destination Advertisement Object), and DIS (DODAG Information Solicitation message). These are ICMPv6-based (Internet Control Message Protocol Version 6) information messages sent using IPv6 packets in IEEE 802.15.4 frames. The basic message used to build the DODAG structure is DIO. It carries information such as node rank, instance identifier supporting multiple independent structures, and DODAG version number.

Despite its many advantages, the RPL protocol is vulnerable to various attacks due to the lack of protective mechanisms in its implementation. These attacks can be divided into three main categories: attacks on topology, attacks on resources, and attacks on network traffic (Mayzaud, Badonnel and Chrisment, 2016).

Section II discusses several attacks, which the authors focused on. Section III reviews the literature, highlighting other authors' approaches to detecting similar attacks. Section IV presents proposed mechanisms for detecting selected attacks on the RPL protocol, developed by the authors. The results of the verification of the developed solutions are presented and discussed in Section V. The work is summarized in Section VI.

Selected Attacks on RPL Protocol

In order to understand the scope of this paper related to the evaluation of the effectiveness of the proposed attack detection mechanism in sensor networks based on 6LoWPAN technology and using the RPL routing protocol, this section provides a rough description of the principles of selected attacks on this type of network.

Version Number Attack

Attacks on network resources focus on exhausting a device's limited resources, such as energy or memory. They can be divided into direct and indirect attacks. The former involves generating unnecessary network traffic by an intruder to overload and degrade the network. Indirect attacks, such as the RPL protocol instance version number attack, focus on activities that lead to the generation of unnecessary traffic by other nodes in the network structure (Mayzaud, Badonnel and Chrisment, 2016). A malicious node executing this attack increments the DODAG version number in the DIO message to force other nodes to initiate a global routing tree repair process. Unauthorized initiation of this procedure leads to the reconstruction of the entire DODAG tree structure, thus causing excessive control traffic generation in the network, contributing to, among other things, delayed packet delivery or excessive energy consumption by individual nodes (Pongle and Chavan, 2015; Maciejko and Krygier, 2025).

Rank Decrease Attack

Another category of attacks against the RPL protocol are traffic-oriented attacks. These focus on disrupting, intercepting, or modifying data transmitted between nodes. They can be divided into eavesdropping attacks, which involve intercepting and analyzing network traffic, and appropriation attacks, in which the intruder overstates its performance or identifies itself as another node (Mayzaud, Badonnel and Chrisment, 2016). A downgrade attack is a type of appropriation attack. The intruder lowers its rank, thus assigning a more favorable route for forwarding packets. This forces sending nodes to change their parent nodes and default routes. Unauthorized changes to routing paths can have security implications for the network, potentially resulting in packet loss or disruption.

Related Work

The issue of attacks on sensor networks based on 6LoWPAN technology using the RPL protocol has been discussed in many publications over the last 10 years. This paper refers to only a few of these publications, which inspired the authors to develop their own solution, complementing the solutions described in these publications.

The concepts of mechanisms designed to detect version number attacks and rank attacks in RPL-based sensor networks were presented by Khalfoune and Beghdad (2024). They proposed a mechanism for detecting rank attacks that compares the current rank of a node with the rank of its parent, the previous rank of the node, the ranks of related nodes (nodes for which it is a parent), and the ranks of nodes having the same parent. They noted that in the

case of a node rank degression attack, the anomaly will be detected when this rank is less than the sum of the minimum rank of the sibling node and the threshold required to change the parent node. This solution is effective because it accounts for many dependencies in the sensor network structure. A comparative analysis of this solution with solutions from other researchers is also presented, demonstrating relatively high attack detection efficiency in specific network structures. The authors of this paper considered the conclusions from the research presented by Khalfoune and Beghdad (2024) to develop their own solution dedicated to network structures with a large number of nodes and specific types of attacks.

The issue of attacks on version numbers used in the RPL protocol was addressed by Nandhini, Srinath, Veeramanikandan and Malliga (2021). They analyzed existing solutions protecting the RPL protocol against such attacks and then presented the concept of a mechanism called Claim Algorithm. Verification of the version number of the RPL tree involves comparing the version number received by the verifying node with information obtained from its neighbors. Simulation results show that the proposed approach effectively mitigates the negative impact of such an attack; however, further improvements to this verification mechanism are needed for cooperating malicious nodes.

An interesting intrusion detection system designed specifically for IoT networks based on 6LoWPAN with the RPL protocol is the SVELTE system presented by Shahid Raza, Linus Wallgren, and Thiemo Voigt (2013). A key element of this system is the 6Mapper component, which periodically reconstructs the DODAG tree topology and analyzes the consistency of rank information in neighborhood relations. The results presented by Raza, Wallgren and Voigt (2013) indicate that the system demonstrated high effectiveness in detecting spoofed or altered information, sinkhole and selective forwarding attacks and low requirements for additional resources necessary for its implementation in the network.

Zahrah A. Almusaylim, NZ Jhanjhi, and Abdulaziz Alhumam (2020) also presented the SRPL-RP (Secure RPL Routing Protocol) mechanism, which is an extension of the RPL protocol designed to detect and prevent attacks on version and rank numbers. The system introduces an additional process for verifying routing information between nodes, specifically monitoring changes in version and rank numbers. It operates based on neighbor behavior and communication history, utilizing timestamp thresholds, monitoring tables, and anomaly detection thresholds. SRPL-RP also implements reputation rules, creates a blacklist of suspicious nodes, and dynamically isolates them. This solution also inspired the authors of this article due to its high attack detection effectiveness confirmed in various network structures

RPL Protocol Modifications - Attack Detection Mechanisms

Version Number Attack Detection Mechanism

Version number attacks affect the performance and efficiency of RPL-based networks. The mechanism presented in this section aims to protect against this attack by detecting unauthorized version number increments in DIO messages. The mechanism is inspired by the Claim Algorithm presented by Montenegro et al. (2007). It is based on verifying the correctness of DIO versions through neighbor voting. A node that receives a DIO message with a higher version number than the locally known one acts as a verifier and queries its neighbors for the current version. If the majority of sensors confirm the older version, the message sender is considered an intruder. The main advantages of this approach are low computational complexity and resistance to single false positives. However, for nodes with a small number of neighbors, the voting may not be reliable, which can lead to a decrease in the algorithm's effectiveness.

Fig. 1 shows the algorithm of the author's solution. The approach improves the effectiveness of attack detection through a series of verification steps. Each node performs the following steps:

- Verification of whether the sender of a DIO message is on the neighbor list of a given node;
- Analysis of the sent version of the DODAG tree instance – checking whether this parameter is greater than the current locally known value among neighbors;

- Identification of the sender – changes sent by the root are considered valid;
- Checking whether the new version is greater than the version known to the root node.

Fig 1. Version Number attack detection algorithm executed by each sensor node (Source (Own))

The presented solution, for detecting a Version Number attack does not require many neighbors. It distinguishes the master node from other nodes, and a simplified decision-making mechanism allows for a rapid response to attack detection. The DODAG message validation algorithm is run by all nodes present in the network structure. Once all conditions are met, the attack is detected by the sensor that performed the verification. For testing purposes, this is confirmed by logging the appropriate information by that node in the sensor's memory. Furthermore, upon detection

of an attack, the mechanisms responsible for global repair are immediately blocked to avoid excessive control traffic in the network. This blocking is implemented by the nodes that detected the attack by raising the appropriate flag in the RPL protocol source code upon detection, preventing the execution of instructions related to the global repair process.

Rank Decrease Attack Detection Mechanism

Rank Decrease attack protection relies on detecting a falsely lowered rank by an intruder and then blocking the process of changing the parent node by the node that received the DIO message. The following algorithm is characterized by low complexity and a simple decision-making process. Fig. 2 shows its logical flowchart. The presented Rank Decrease attack detection algorithm focuses on the node receiving DIO messages checking whether the newly received rank is lower than the previous one and comparing it with the average rank of neighboring nodes to exclude the possibility of a falsely reported attack in the event of a trusted sensor moving in the DODAG tree structure.

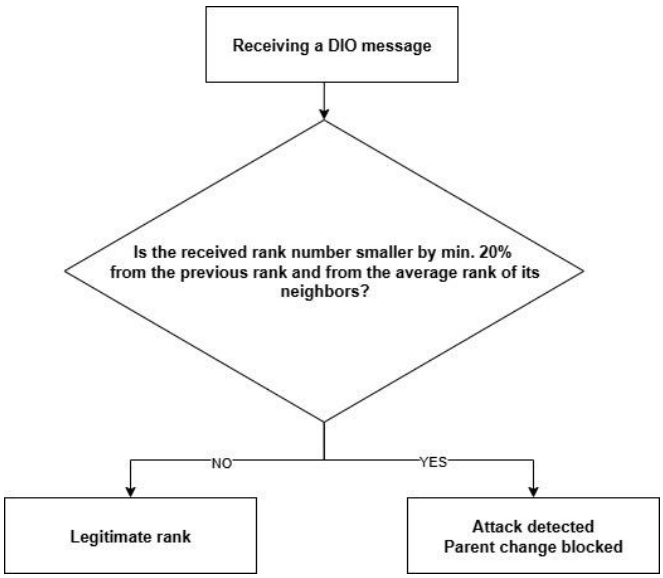

Fig 2. Rank Decrease attack detection algorithm executed by each sensor node (Source (Own))

Rank validation in DIO is performed by all nodes participating in a given DODAG instance. The authors assumed that an attack will be detected when a node's rank drops by at least 20% compared to the previous level, as well as the average rank of its neighbors. Nodes calculate their rank relative to the parent node, taking into account metrics such as hop count and link quality. Under stable communication conditions, where the network topology does not change frequently, the ranks of neighboring nodes should not differ significantly, and nodes in similar locations should have similar rank values. Almusaylim, Jhanjhi and Alhumam (2020) noted that a node's rank drop exceeding 20% of the average rank of its neighbors can be an indicator of a potential attack. Thus, this threshold was established based on empirical observations during tests of the SVELTE system published by Almusaylim, Jhanjhi and Alhumam (2020).

Experiments and Discussion of Results

As a reference point for evaluating the effectiveness of the modified RPL protocol, two different sensor network structures based on the Contiki OS operating system (Contiki-NG, 2025) were used, implementing the 6LoWPAN/IEEE802.15.4 protocol stack and containing modifications to the RPL protocol. Experiments were

conducted using the Cooja sensor network simulator, which simulates network conditions and emulates the Contiki OS operating system of individual sensors. Experiments related to latency and attack detection effectiveness were conducted on the network structure shown in Fig. 3. It consists of 50 nodes (one receiver marked in green and 49 senders marked in yellow) randomly distributed over a 300 m x 300 m area. It was assumed that the sensors would operate with a radio power sufficient for a 50 m range, and that communication would take place in open space. Attack detection performance was tested for four scenarios in which the number of attacking nodes increased. In each scenario, the percentage density of malicious nodes was 10%, 20%, 30%, and 40%. The location of intruders was randomized and changed in each simulation to obtain more reliable results. Analysis of attack detection latency was also performed for four scenarios in which the location of one intruder changed randomly.

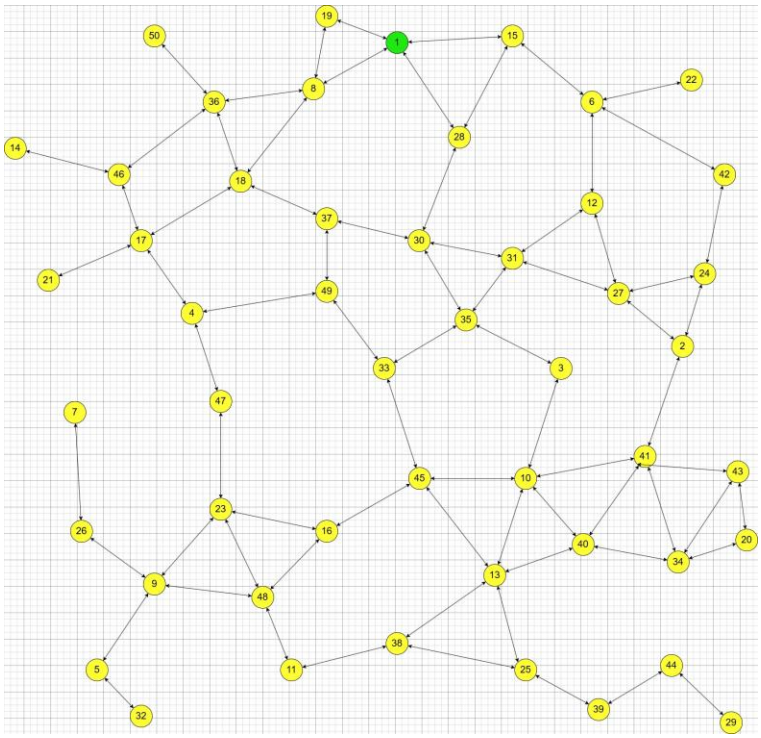

Fig 3. Network structure used to test the performance of attack detection mechanisms (Source (Own))

The impact of the applied attack detection mechanisms on selected performance measures of basic services in the sensor network was assessed in a network representing the distribution of sensors in a sample shopping mall, shown in Fig. 4, where sensors monitor air quality. In this network, packet delivery ratio (PDR), signaling traffic volume, and sensor energy consumption were assessed. Fig. 4 shows a network consisting of one receiver (S1), marked in green, and 22 transmitting sensors (S2–S23), marked in yellow.

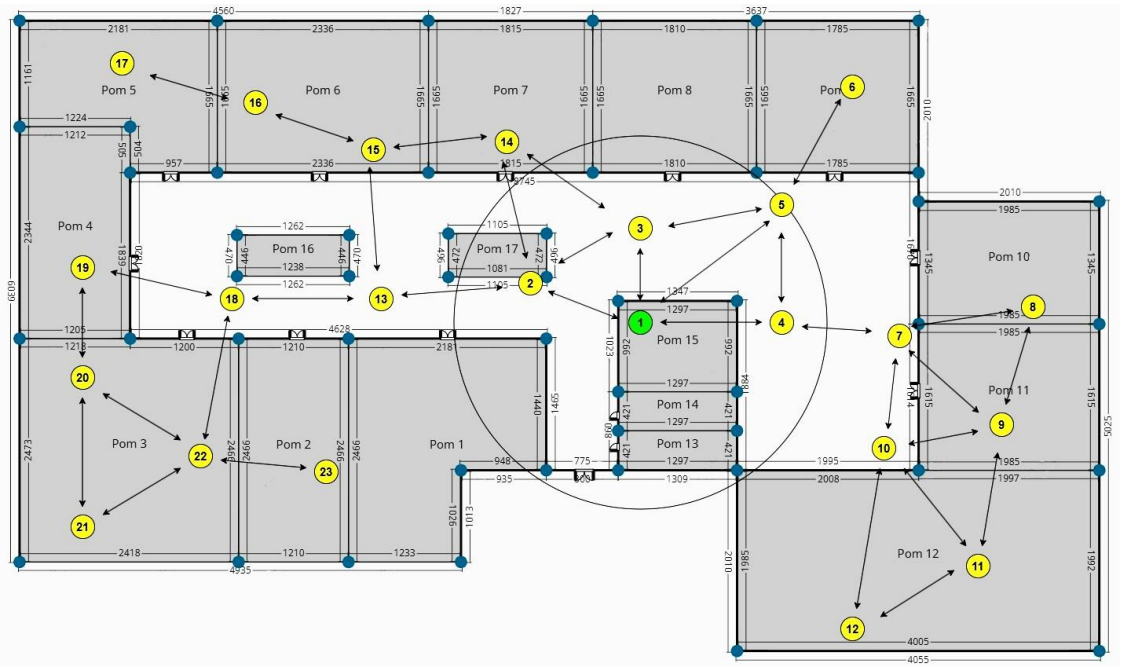

Fig 4. Network structure established on the example diagram of the shopping center (Source (Own))

In addition, three malicious nodes (S24 - S26) implementing Version Number and Rank Decrease attacks sequentially were added to the structure, as shown in Fig. 5. The intruders were marked in purple. Attacker S24 was placed in the direct radio range of the main sensor, as well as in the range of nodes S4 and S10. The other malicious nodes (S25 and S26) had a range of up to three and five senders, respectively.

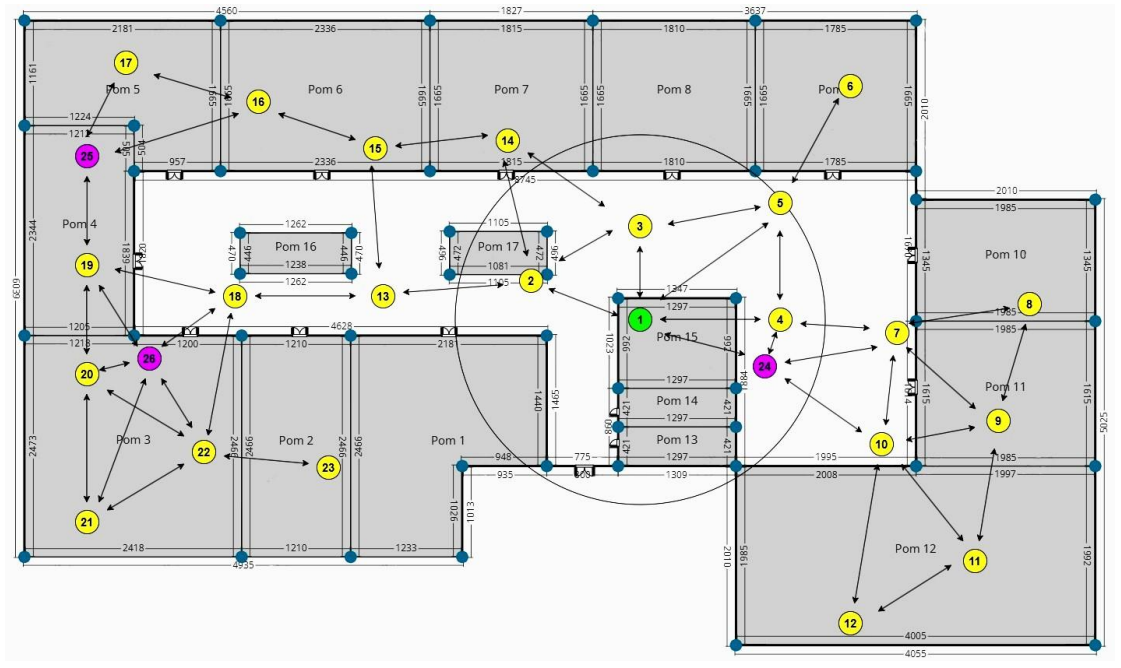

Fig 5. Network structure with malicious nodes (Source (Own))

Tests were conducted for a reference network structure without attacking nodes, a network structure with intruders carrying out Version Number and Rank Decrease attacks, and a network structure with intruders along with an implemented mechanisms to detect the attacks. Zolertia Z1 sensors based on the 16-bit MSP430F2617 microcontroller (Tracey, 2020), were used in the network. The devices are equipped with the IEEE 802.15.4-compliant receiver and have a radio range of 30 to 125 m, depending on the transmitting signals power (Tracey, 2020; Al-Suhail, Ghaida, Mehdi and Nikolakopoulos, 2017).

Impact of attack detection mechanisms on the packet delivery ratio

Fig. 6 presents a summary of the PDR obtained during tests of the assumed network scenarios. Analyzing the collected test results, it can be seen that the Version Number (VN) attack significantly affected packet loss. The PDR decreased by approximately 20 percentage points compared to the reference network. Implementing the proposed mechanism to detect this attack stabilized the packet loss rate, which remained close to the values from the reference network despite the active attack. In the case of the Rank Decrease (RD) attack, the PDR packet deliverability rate did not change significantly.

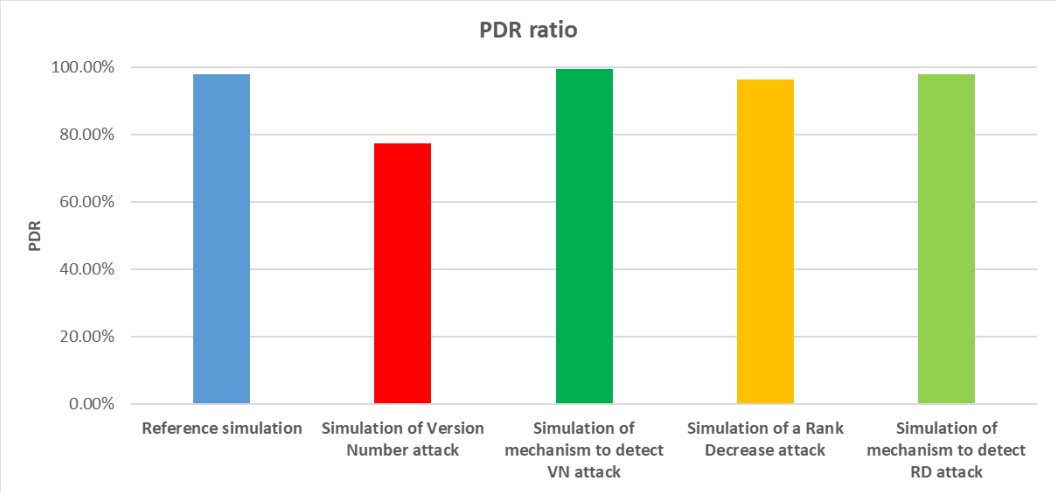

Fig 6. Packet delivery ratio (PDR) in assumed scenarios (Source (Own))

Impact of attack detection mechanisms on signaling overhead

The Version Number attack caused a several-fold increase in the number of DIO and DAO control messages sent, as shown in Fig. 7. The proposed solution, designed to detect this attack and mitigate its impact, resulted in the number of these control messages remaining essentially unchanged compared to the reference simulation. The noticeable increase in signaling traffic volume after implementing the attack detection algorithm is minimal and is visible for a few signaling messages.

A similar situation occurred with the Rank Decrease attack, although the increase in the number of DIO and DAO messages was not as large as with the Version Number attack. The presented Rank Decrease attack detection mechanism positively impacted the reduction of signaling traffic, minimizing the attack's impact. The number of DIO and DAO messages is significantly lower during the attack without our mechanisms, but slightly higher than in the reference network.

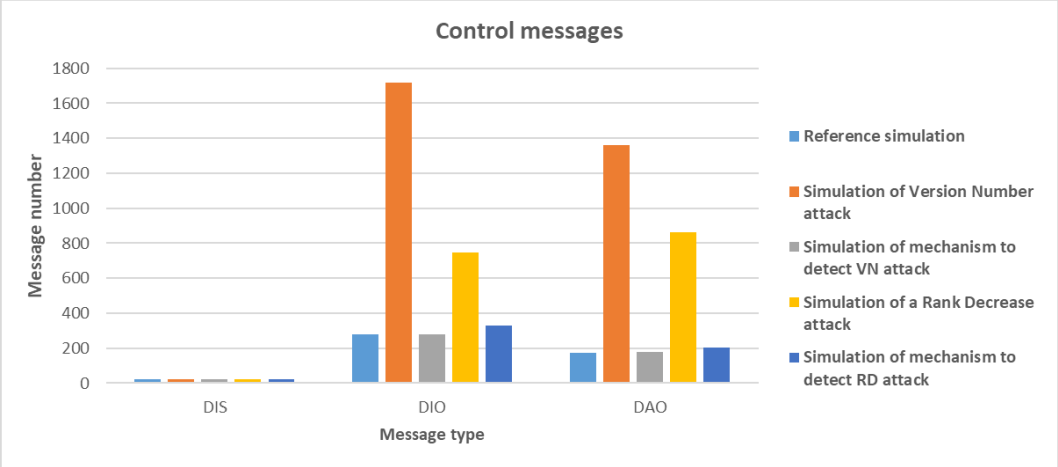

Fig 7. Number of control messages sent during testing of Version Number and Rank Decrease attack detection mechanism (Source (Own))

Impact of attack detection mechanisms power consumption of the sensors

Fig. 8 shows a graph of the average sensor power consumption during testing of the Version Number attack detection mechanism. As can be seen, the average power consumption of nodes after implementing the proposed solution is similar to the reference network. Furthermore, the attack did not isolate any node from the network structure, which can be observed when implementing the version number attack without the mechanism implemented. Due to redundant signaling, nodes S16-S18, as well as S21 and S23, were completely isolated from the network. It is worth noting that implementing the attack detection mechanism caused a slight increase in power consumption for some nodes. This phenomenon is most noticeable in the case of node S13, which serves as an indirect path to the source for six other senders. The difference in average power consumption after implementing the mechanism compared to the reference network is approximately 0.8 mW.

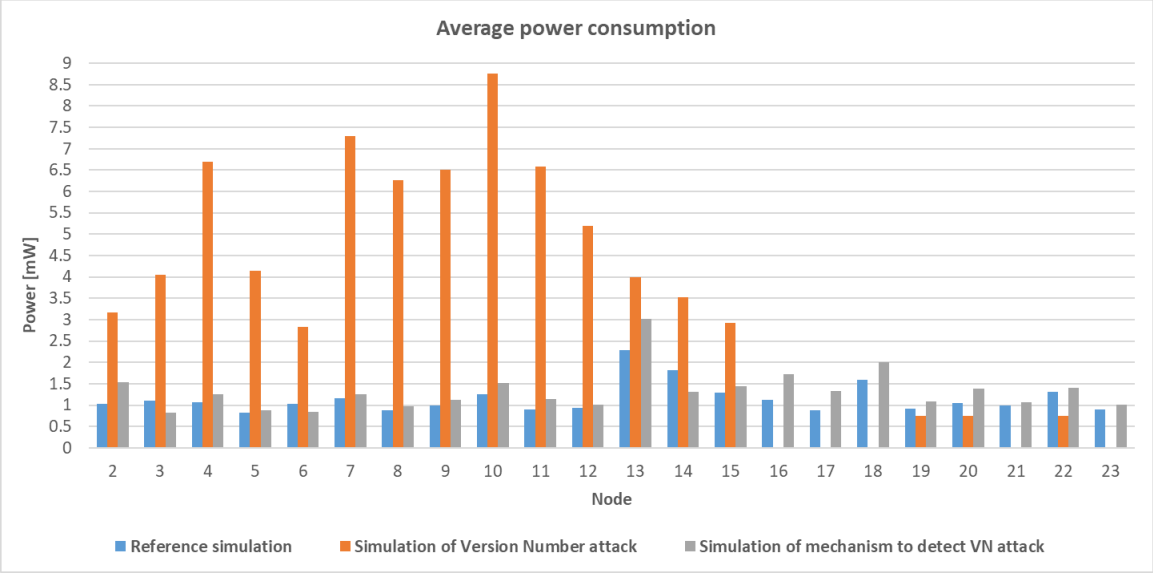

Fig 8. Average power consumption of the nodes during testing of Version Number attack detection mechanism (Source (Own))

Fig. 9 shows a graph of the average power consumption of the sensors during the Rank Decrease attack. The attack increased the power consumption of some sensors. Power consumption data was not collected for nodes S17, S21, and S23 due to their isolation from the network structure caused by the attack. This isolation occurred because both intruders were located in similar locations. This location caused two separate loops in the network at some point, and some sensors were cut off from the receiver. Implementing the Rank Decrease attack detection mechanism improved the performance of the RPL protocol by ignoring erroneously modified ranks by intruders. Measurement data was collected from all nodes. Despite the active attack, the average power consumption of nodes decreased and approached the reference results. The mechanism itself slightly affected the power consumption of nodes; for example, for node S13, the power consumption increased by approximately 0.3 mW compared to the reference simulation.

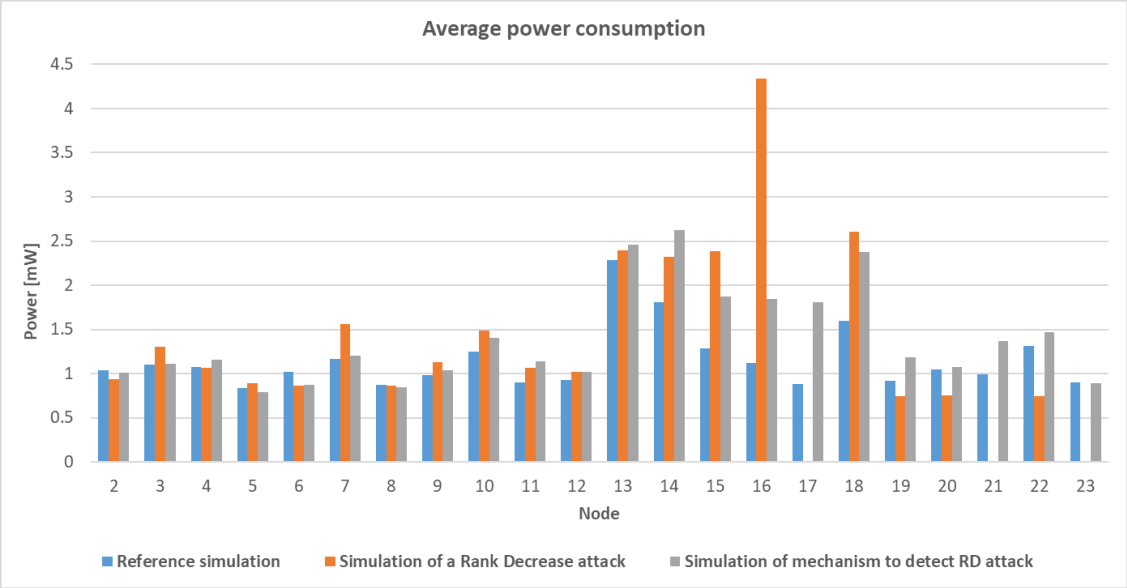

Fig 9. Average power consumption of the nodes during testing of Rank Decrease attack detection mechanism (Source (Own))

Accuracy and delay in attack detection

Based on the number of detected intruders, the percentage effectiveness is presented in Fig. 10. As can be seen, for attacker density of 10% and 20%, our mechanism correctly identified all intruders using Version Number and Rank Decrease attacks, achieving 100% detection accuracy.

With a higher number of attacking nodes, all malicious nodes were not correctly identified. For intruder density of 30% and 40%, the Version Number attack failed to detect one and four attackers, respectively, resulting in 93% and 80% effectiveness. The lack of full effectiveness was due to the large number of intruders, which prevented the mechanism from keeping up with identifying the version numbers contained in DIO messages.

In contrast, for intruder densities of 30% and 40%, in the case of the Rank Decrease attack, two and three attackers, respectively, were undetected, resulting in detection rates of 87% and 85%. Due to the large number of intruders, the mechanism based on comparing the obtained ranks with the ranks of its neighbors was unable to verify all malicious nodes.

Considering the complexity of the network structure used during testing, it can be concluded that the proposed solutions are highly effective in detecting these attacks.

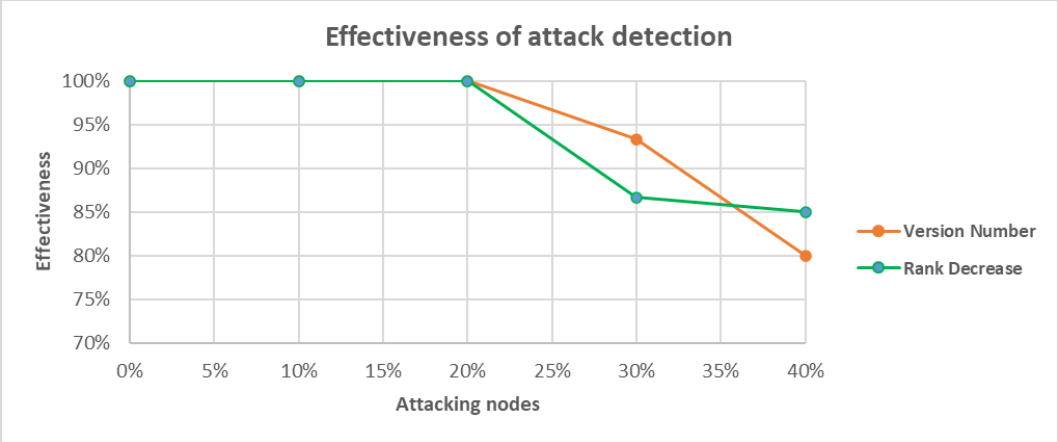

Fig 10. Effectiveness of Version Number and Rank Decrease attacks detection (Source (Own))

The detection latency of Version Number and Rank Decrease attacks was tested based on four scenarios in which a single intruder randomly changed its location. The latency of the mechanisms was determined based on the attack initiation timestamp, the receipt of the fake message by the legitimate node, and the attack detection. For the Version Number attack, the average detection time from its initiation was approximately 28 seconds, while the time to verify and detect the attack after the sensor received the DIO message was approximately 9 ms. The detection latency of the Rank Decrease attack from its initiation was approximately 11 seconds on average, and the time to verify the authenticity of the rank and detect the attack after the node received the DIO message was approximately 35 ms.

Conclusions

The paper demonstrates that WSNs with the RPL protocol are susceptible to Version Number and Rank Decrease attacks. The success of such attacks depends on the authentication of attacking nodes within the network. The authors propose solutions capable of detecting these attacks. The research indicates that these proposals not only allow for the detection of attacks but also for minimizing their effects by isolating the attacking nodes. These solutions require a slight modification of the RPL protocol.

Acknowledgment

This work was supported by Military University of Technology (Warsaw, Poland) Grant No UGB 22-058.

References

- Winter, T., Thubert, P., Brandt, A., Hui, J., Levis, P., Pister, K., Struik, R., Vasseur, J. P. and Alexander, R. (2012), 'RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks' RFC 6550, March 2012.
- Montenegro, G. et al. (2007), 'Transmission of IPv6 Packets over IEEE 802.15.4 Networks', RFC 4944, September 2007.
- Ghosh, R. K. (2017), 'Wireless Networking and Mobile Data Management', Singapore: Springer, 2017.
- Vasseur, J. P. and Dunkels, A. (2010), 'Interconnecting smart objects with IP: The next internet', Morgan Kaufmann, 2010.
- Mayzaud, A., Badonnel, R. and Chrisment, I. (2016), 'A Taxonomy of Attacks in RPL-based Internet of Things', Internation Journal of Network Security, vol. 18, no. 3, pp. 459-473, 2016.
- Pongle, P. and Chavan, G. (2015), 'A survey: Attacks on RPL and 6LoWPAN in IoT.', 2015 International conference on pervasive computing (ICPC), Pune, India, pp. 1-6, 2015. https://doi.org/10.1109/PERVASIVE.2015.7087034

- Maciejko, P. and Krygier, J. (2025), ‘Performance of RPL-based Wireless Sensor Networks Subjected to Selected Attacks.’, Communications of the IBIMA, vol. 2025, no. 335263, pp. 1-17, 2025. https://doi.org/10.5171/2025.335263
- Khalfoune, A. E. and Beghdad, R. (2024), ‘Securing RPL-Based Networks Against Version Number and Rank Attacks.’, Acta Informatica Pragensia, vol. 13, nr. 3, pp. 340-358, 2024. https://doi.org/10.18267/j.aip.234
- Nandhini, P. S., Srinath, P., Veeramanikandan, P. and Malliga, S. (2021), ‘Version Attack Detection using Claim Algorithm in RPL based IoT Networks: Effects and Performance Parameters Evaluation.’, 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, pp. 209-215, 2021. https://doi.org/10.1109/ICOSEC51865.2021.9591735
- Raza, S., Wallgren, L. and Voigt, T. (2013), ‘SVELTE: Real-time intrusion detection in the Internet of Things.’, Ad hoc networks, vol. 11, no. 8, pp. 2661-2674, 2013. https://doi.org/10.1016/j.adhoc.2013.04.014
- Almusaylim, Z. A., Jhanjhi, N. Z. and Alhumam, A. (2020), ‘Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP.’, Sensors, vol. 20, no. 21, pp. 1-25, 2020. https://doi.org/10.3390/s20215997
- Tracey, D. (2020), ‘A holistic architecture using peer to peer (P2P) protocols for the internet of things and wireless sensor networks.’, PhD Thesis: University College Cork, 2020.
- Al-Suhail, G., Ghaida, A., Mehdi, J. and Nikolakopoulos, G. (2017), ‘A practical survey on wireless sensor network platforms.’, Journal of Communications Technology, Electronics and Computer Science, vol. 13, pp. 23-30, 2017.
- Contiki-NG, ‘The OS for Next Generation IoT Devices.’, at https://www.contiki-ng.org/ (accessible: 29.09.2025)