Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.047087

ARTICLE

# RPL-Based IoT Networks under Decreased Rank Attack: Performance Analysis in Static and Mobile Environments

**Amal Hkiri[1,*], Mouna Karmani[1], Omar Ben Bahri[2], Ahmed Mohammed Murayr[2], Fawaz Hassan Alasmari[2] and Mohsen Machhout[1]**

[1]Physic Department, Electronics and Micro-Electronics Laboratory, Faculty of Sciences of Monastir, Monastir, 5000, Tunisia

[2]Department of Science and Technology, College of Ranyah, Taif University, P.O. Box 11099, Taif, 21944, Saudi Arabia

*Corresponding Author: Amal Hkiri. Email: hkiriamalfsm@gmail.com

Received: 24 October 2023 Accepted: 07 December 2023 Published: 30 January 2024

## ABSTRACT

The RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) protocol is essential for efficient communication within the Internet of Things (IoT) ecosystem. Despite its significance, RPL's susceptibility to attacks remains a concern. This paper presents a comprehensive simulation-based analysis of the RPL protocol's vulnerability to the decreased rank attack in both static and mobile network environments. We employ the Random Direction Mobility Model (RDM) for mobile scenarios within the Cooja simulator. Our systematic evaluation focuses on critical performance metrics, including Packet Delivery Ratio (PDR), Average End to End Delay (AE2ED), throughput, Expected Transmission Count (ETX), and Average Power Consumption (APC). Our findings illuminate the disruptive impact of this attack on the routing hierarchy, resulting in decreased PDR and throughput, increased AE2ED, ETX, and APC. These results underscore the urgent need for robust security measures to protect RPL-based IoT networks. Furthermore, our study emphasizes the exacerbated impact of the attack in mobile scenarios, highlighting the evolving security requirements of IoT networks.

## KEYWORDS

RPL; decreased rank attacks; mobility; random direction model

## 1 Introduction

The Internet of Things (IoT) serves as the gateway to the vast realm of the Internet. Its primary aim is to establish connectivity between all types of devices, ranging from the smallest to the most intricate [1]. Leveraging its wireless capabilities and contextual awareness, IoT finds applications in domains like smart cities [2] and healthcare [3] monitoring by employing cost-effective and energy-efficient devices. Yet, many devices within the IoT realm are resource-constrained, requiring solutions that are lightweight, secure, and adaptable for mobility [4]. One example is 6LoWPAN, an adaptation layer within the IoT architecture, designed to function on devices with limited resources [5]. The IoT landscape requires the development of streamlined applications to facilitate communication among constrained nodes within restricted networks. 6LoWPAN operates across the network and data link layers, optimizing the transmission of IPv6 packets in networks with resource limitations [5]. Due

to the associated overhead, conventional routing methods like Adhoc On-Demand Distance Vector (AODV) [6], Open Shortest Path First (OSPF) [7], and Dynamic Source Routing (DSR) [8] are not advisable for use in such constrained networks. RPL introduced by the Internet Engineering Task Force (IETF) within the ROLL group, offers an efficient routing solution for intelligent IP devices in the context of 6LoWPAN [9]. Numerous Internet of Things (IoT) applications with limited resources, such as agriculture [10], remote area monitoring [11], military deployments, and the healthcare sector [12] employ the RPL protocol. It has solidified its status as the protocol of choice at the network layer, emerging as a prominent routing solution within low-power and lossy networks (LLNs). As the Internet of Things (IoT) continues to interconnect billions of devices, a critical need has arisen to confront the array of threats targeting IoT [9]. The proliferation of resource-constrained devices alongside the prevalence of lossy networks amplifies the scope of potential vulnerabilities within the IoT landscape. Recent years have seen a surge in attacks on IoT networks, with adversaries exploiting not only the communication channels but also the vulnerabilities presented by compact devices themselves [13]. Even 6LoWPAN, though not immune, faces security challenges, leaving it susceptible to exploitation, an issue that holds significant consequences, particularly within lossy networks. RPL exhibits susceptibility to attacks that exploit aspects of network topology, traffic patterns, and resource allocation. This research focuses on routing attacks with a particular emphasis on the decreased rank attack within the context of RPL-based 6LoWPAN [14]. In the context of RPL-based IoT networks, the concept of "Rank" plays a crucial role by offering a relative assessment of the quality of paths to the intended destination. What distinguishes the Decreased Rank attack is its exclusive association with the RPL standard, making it one of the most formidable threats to the network's routing efficiency and energy utilization. The importance of addressing Decreased Rank attacks lies in the fundamental objectives of upholding network security and stability. These attacks provide malicious actors with the means to manipulate traffic within the RPL network by altering their priority status, resulting in reduced data throughput and undesirable communication delays. Furthermore, these attacks pose significant risks to the security and privacy of IoT networks. They can lead to data exposure and interception by diverting traffic and causing delays, as well as unauthorized data access by manipulating routing paths, directly undermining privacy [15,16]. This dual impact on network performance is of paramount significance, especially when considering the inherent resource limitations of IoT devices. Detecting such routing attacks in the context of RPL-based 6LoWPAN presents notable challenges, primarily due to the dynamic nature of IoT networks [17]. While our work primarily focuses on analyzing the performance of the RPL protocol under decreased rank attacks within static and mobile environments, it's worth noting that the privacy-preserving mechanisms discussed in [18,19] serve as illustrative examples of how privacy can be safeguarded in network operations, a matter of utmost importance in the broader context of IoT network security.

## 2 Contributions

This study offers valuable insights into the impact of the decreased rank attack on RPL-based networks. It achieves this through a meticulous analysis, quantifying changes in performance metrics, including Packet Delivery Ratio (PDR), Average End-to-End Delay (AE2ED), throughput, Expected Transmission Unit (ETX), and Average Power Consumption (APC). These metrics provide a holistic view of how the attack affects various aspects of network operation, shedding light on its consequences. The study's consideration of both static and mobile network environments extends the applicability of its findings to diverse scenarios, offering a more comprehensive assessment. The novel inclusion of the Random Direction Mobility Model (RDM) within the decreased rank attack scenarios adds an innovative dimension. Additionally, this study investigates node scalability, ranging from 10 to 40 nodes, addressing potential scalability challenges and delving into the attack's impact as the network

size fluctuates. This multidimensional analysis enhances our understanding of the implications of the decreased rank attack in RPL-based networks, providing valuable insights for network practitioners and researchers. Moreover, most works in the literature even the recent ones comely use the COOJA simulator Contiki version 2.7 as a simulation tool. In this manuscript, we used the COOJA simulator version 3.0, which has different and recent features compared to other versions including the update of platforms and bug fixes. Furthermore, with its in-depth examination of the decreased rank attack and its specific focus on details, this research serves as a critical resource in fortifying the security and improving the performance of RPL-based IoT networks, especially in the face of evolving challenges. It contributes to bridging the knowledge gap regarding the impact of the decreased rank attack on RPL networks, supporting the development of more effective security strategies and protocols for IoT environments.

This paper is structured into several key sections, each contributing to a comprehensive exploration of the subject matter. In Section 3, we delve into the core RPL specifications, shedding light on the attack utilized in this study and offering insights into mobility within the RPL framework. Building upon this foundation, Section 4 provides a thorough review of pertinent research, both in scenarios involving RPL with and without attacks and across both static and mobile environments. Section 5 is dedicated to detailing the specific setups used in our simulations and the subsequent performance evaluations. The experimental outcomes and a comparative analysis are unveiled in Section 6, allowing for a deeper understanding of the results. Finally, in Section 7, we end the paper by summarizing our findings and charting a course for future research endeavors in this domain.

## 3 Background

This segment delves into the RPL protocol, a prominent choice for LLNs. Additionally, it furnishes an overview of the decreased rank attack within the context of RPL-based 6LoWPAN networks.

### *3.1 RPL Overview*

The RPL protocol was devised to meet the specific challenges presented by low-power and lossy networks (LLNs) within the expansive landscape of IoT [9]. As the IoT continues to expand, the necessity for effective communication among resource-constrained devices becomes increasingly pivotal. RPL stands as a foundational solution that addresses these challenges, all while optimizing energy usage and maintaining a high degree of adaptability. Its approach to efficient routing is rooted in a combination of energy conservation and scalability, making it an essential protocol for LLNs. The topology of the RPL network is structured as a Directed Acyclic Graph (DAG), which may be further segmented into one or more Destination Oriented Acyclic DAGs (DODAGs). Each sink node, within the network corresponds to a DODAG. Additionally, RPL enables three types of traffic flows; point-to-point (P2P), multipoint-to-multipoint (MP2MP), and point-to-multipoint (P2MP) [20]. RPL employs four values to maintain and identify its topology. The first parameter is RPLInstanceID, which serves as the identifier for one or more Destination-Oriented Acyclic Graphs (DODAGs). In cases where several InstanceIDs exist within the same network, each one defines a distinct set of DODAGs that are independently optimized for various Objective Functions (OFs). These DODAGs collectively form an RPL Instance, with all DODAGs in that instance using the same OF. The second parameter is DODAGID, a unique identifier for each individual DODAG. When combined with RPLInstanceID, it provides a unique designation for a specific DODAG within the network. The third parameter is VersionNumber, which increments when a DODAG root reconstructs a DODAG.

It can be employed to distinguish different versions of a DODAG when combined with InstanceID and DODAGID. The final parameter is Rank, which identifies the position of an individual node within a DODAG. It is determined based on the node's relationship to the DODAG root during classification within a specific DODAG Version [9].

ICMPv6 control messages are pivotal in optimizing RPL's performance in low-power and lossy IoT networks. They are fundamental for establishing and maintaining efficient routing paths, which are crucial in such network environments. Among these messages, the DODAG Information Solicitation (DIS) message is proactive, allowing nodes to gather information about the DODAG root and its configuration parameters. This empowers nodes to identify potential parent nodes, enhancing routing path optimization. On the other hand, the DODAG Information Object (DIO) message periodically broadcasts essential configuration information from the DODAG root. It ensures all network nodes share a synchronized understanding of the DODAG's structure, including version details and node ranks. The Destination Advertisement Object (DAO) message enables non-root nodes to broadcast their presence, facilitating parent-child relationships within the DODAG. This supports the establishment of efficient routing paths and sustains network connectivity. The Destination Advertisement Acknowledgment (DAO-ACK) message validates successful parent-child relationships and accurate routing path configurations. Objective functions (OF) within the RPL protocol dynamically adjust route selection criteria, considering metrics like energy efficiency, latency, link quality, and reliability [21]. In RPL, communication within a Destination-Oriented Directed Acyclic Graph (DODAG) involves two main types of routes: upward routes for data transmission from leaf nodes to the root, and downward routes for control information and updates from the root to the network endpoints. These bidirectional routes ensure efficient communication and network management. Furthermore, RPL offers three operational modes for low-power and lossy networks: storing, non-storing, and hybrid modes. Storing mode uses specific nodes with more resources as storing nodes to maintain routing information. Non-storing mode dynamically makes routing decisions without local storage, suitable for larger networks with resource-constrained nodes. Hybrid mode combines elements of storing and non-storing, accommodating networks with mixed resource capabilities. The choice of mode depends on factors like network size and node constraints. An integral component of RPL's energy-efficient approach is duty cycling, which alternates nodes between active and sleep states to manage energy resources. While RPL includes inherent security mechanisms, vulnerabilities like rank manipulation and selective forwarding should be addressed. Configurable parameters, including Trickle timer intervals, minimum hop rank increase, and path cost, allow fine-tuning RPL's performance to specific network conditions [21].

### *3.2 Decreased Rank Attack*

The Decreased Rank Attack is a strategically orchestrated exploitation of the RPL protocol's rank-based routing mechanism, designed to compromise the integrity and performance of IoT networks. It is a type of traffic attack targeting RPL [14]. The attack strategy unfolds through distinct phases. It initiates with the deliberate selection of a particular network node as the target for compromise, utilizing vulnerabilities, weak security mechanisms, or code injection to gain unauthorized access. Once control is established, the attacker manipulates the node's rank by intentionally lowering it, misleading the network into placing it lower in the hierarchy than its actual position [14]. This manipulated rank then entices legitimate nodes during parent selection, leading them to favor the compromised node. Consequently, routing choices are diverted, enabling the attacker to direct traffic through suboptimal paths. The impact is profound and multi-faceted. Disrupted routing hierarchy results in inefficiencies, degraded performance manifests as reduced PDR and AE2ED and heightened power consumption emerges from compromised nodes participating in suboptimal routing. Moreover,

the attack raises significant security concerns, as unauthorized control over network nodes can lead to unauthorized data access manipulation. These cumulative consequences underscore the need for robust countermeasures to safeguard the integrity and security of RPL-based IoT networks against the Decreased Rank Attack [14]. To enhance the comprehension of the Decreased Rank Attack process, Fig. 1 illustrates a flowchart detailing the key steps involved in this attack. It begins with the attacker's meticulous selection of a target node, exploiting security vulnerabilities to gain unauthorized access. Once in control, the attacker manipulates the node's rank to appear lower in the hierarchy, enticing legitimate nodes to choose it as a parent. This diverts routing decisions, leading to traffic being routed through less optimal paths, causing inefficiencies and degraded performance, including reduced Packet Delivery Ratio (PDR) and increased Average End-to-End Delay (AE2ED). Additionally, compromised nodes in suboptimal routing increase power consumption. The attack concludes when the attacker achieves their goals, significantly affecting the network's efficiency and stability.

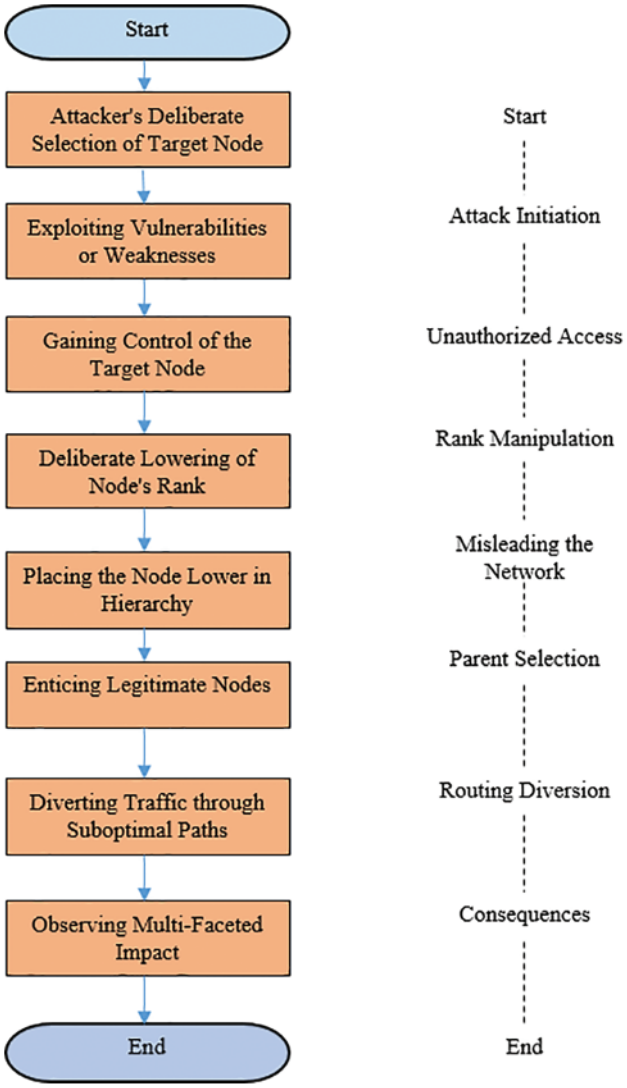


**Figure 1:** Decreased rank attack flowchart

### *3.3 Mobility and RPL*

The RPL protocol holds significant prominence in establishing efficacious communication pathways within Internet of Things (IoT) networks particularly in resource-constrained environments. By employing a hierarchical framework termed a Destination-Oriented Directed Acyclic Graph (DODAG), it optimizes energy utilization and ensures dependable data routing from source nodes to sink nodes [9]. However, the ubiquity of mobile nodes in IoT networks introduces dynamism to network topology. These mobile entities, encompassing vehicular units and unmanned aerial vehicles, engender frequent alterations in connectivity patterns, thereby posing intricate challenges to sustaining stable communication pathways as nodes undergo intermittent connectivity or traverse within the network [22]. Regrettably, the inherent dynamism of mobile IoT networks fosters vulnerabilities susceptible to exploitation by potential adversaries. Security breaches, including selective forwarding, black-hole attacks, and spoofing, attain heightened impact due to the uncertainty inherent in node positions and the fluid network configurations engendered by mobility. The correlation between mobility and security attacks exacerbates the repercussions of malevolent actions. For instance, a mobile malicious node may adroitly evade detection while traversing through the network, thus compounding the efficacy of attack identification and subsequent mitigation [23]. Given this intricate symbiosis, meticulous analysis of RPL's comportment under both attack scenarios and node mobility emerges as a critical imperative. This evaluative undertaking furnishes discernment into the dynamic interplay between RPL's operational performance and its security attributes within the intricate environment of IoT ecosystems. By scrutinizing key metrics, encompassing packet delivery ratios, latency profiles, energy consumption patterns, route stability indices, and convergence times, researchers can unearth the protocol's tenacity against security breaches and its adaptability to the flux of network dynamics catalyzed by mobility. A deep understanding of how RPL handles these interconnected challenges influences the development of protocol extensions that leverage mobility insights. These extensions are designed to address emerging security threats while maintaining communication pathways even in the dynamic context of modern IoT applications. Categorized by [24], mobility models exhibit a binary division with Sink-based models and Non Sink-based models constituting the two primary categories. Further subdivision of the latter yields two distinct subcategories: synthetic and Trace-based models. Notably, synthetic models encompass two sub-classes, namely, entity mobility models and group-based mobility models. Within the realm of Entity mobility models, a dual categorization emerges giving rise to Human-based models and Object-based models. The Human-based models undergo additional bifurcation differentiating between Macroscopic and Microscopic variants. Noteworthy is the classification of the object-based mobility models within which the accidental and intentional models are positioned. These models are conventionally tailored to represent object movements, while still accommodating the utilization of human or group-based models. Furthermore, the intentional mobility models unveil a tripartite categorization, encompassing Mobility models with spatial dependency, Mobility models with temporal dependency, and Mobility models with geographical restrictions. Haut du formulaire.

## 4 Related Work

Numerous studies within the literature have been dedicated to investigating the implications of the decreased rank attack on the RPL protocol, particularly in static environments. These investigations delve into the potential vulnerabilities and disruptions caused by this attack type on the network's performance and reliability. In their research, authors in [25] demonstrated that a change in rank value has a significant impact on network performance. They examined a scenario involving Wireless Sensor Networks (WSNs) using power line communication, where a node' changes. This resulted in

the emergence of loops between child nodes and their parent node, ultimately causing an unstable network topology. Authors [26] analyzed the influence of four distinct rank attacks on both RPL performance and network topology. Their findings indicate that the parameters most significantly affected are the delivery ratio, node count, the DIO messages, and network delay. In their work [27], the authors introduced a novel rank-based attack strategy where the attacker deliberately sends false rank and routing metric values into the network, intensifying the impact of the attack. This maneuver compels neighboring nodes to establish routing paths through the node executing the attack. In a separate study [28], researchers examined the consequences of rank attacks on spoofed IP addresses. However, it is worth noting that this particular investigation does not differentiate between the impacts of increased and decreased rank attacks. In [29], the authors presented both a practical and simulated implementation of RPL, featuring tailored adjustments designed to support the needs of the Advanced Metering Infrastructure (AMI) within the context of Smart Grid (SG) applications, which have distinct wireless sensor network (WSN) routing requirements. They assess the performance of RPL by conducting experiments with 140 nodes in a wireless sensor testbed (IoT-LAB) and simulated scenarios with 1000 nodes using the Cooja simulator. These evaluations were carried out to gauge RPL's performance in networks of medium and high node densities. To gauge RPL's effectiveness, the authors employ two routing metrics for the selection of paths: ETX and HOP Count (HC). These metrics play a pivotal role in assessing RPL's performance across key factors, including network latency, PDR, control traffic overhead, and power consumption. In their study conducted in [30], the authors examined the effect of three specific attacks on RPL networks: Increase Number attack, Hello Flooding attack, and Decrease Rank attack. They further explored the repercussions of these attacks in scenarios involving multiple attackers and over time. The outcomes of their simulations demonstrated that these attacks could significantly disturb network performance. Notably, the rise in the attackers' number primarily affects, E2ED, network throughput and PDR.

Extending the investigation to dynamic settings, the literature also encompasses studies focusing on the decreased rank attack's impact within a mobile environment. Recognizing the unique challenges posed by mobility, researchers have explored how nodes' changing positions and intermittent connections can exacerbate the effects of the attack. Authors in [31] provided a comprehensive review of routing protocols designed for Low-Power and Lossy Networks (LLNs), with a specific focus on RPL and its relevant mobility extensions. The authors conducted simulations of RPL and its extensions using Cooja under various conditions employing the Random Waypoint Model (RWP). Their findings led to a classification of these protocols into two groups. The first group, although more responsive to mobility, suffers from poorer performance due to their substantial control of traffic requirements. Conversely, the second group includes less responsive protocols with lower control traffic, leading to superior overall performance. This underscores the adverse impact of control traffic on maintaining routing tables in LLNs, which operate at low data rates and face spectrum usage limitations. Authors in [32] assessed RPL's performance across three distinct configurations: network scalability, multiple sinks, and mobility models. They employed two distinct scenarios for their evaluation. The first scenario was based on group models, where they arbitrarily selected the RPG and Nomadic Model. In contrast, for the entity models, they opted for three specific models: Random Walk (RWK), Random Waypoint (RWP), and Self-Similar Least Action Walk (SLAW). On the other side, authors of [33] conducted comprehensive testing of RPL and assessed its performance within real-world IoT applications. Their evaluation encompassed a range of scenarios that considered various application requirements and challenges. These scenarios involved factors such as node mobility, outdoor and indoor environments, and deployment constraints. In [34], authors assessed the impact of two IoT routing attacks including the decreased rank attack and DIS attack when a mobile attacker

is involved, aiming to provide a thorough evaluation in comparison to scenarios involving a static attacker. They compared these attacks with regard to PDR and average power consumption. Through simulations, the authors found that when the attacking node exhibits mobility, there is an average power consumption increase of 36.6% and a 14% reduction in PDR compared to situations where the attacking node remains stationary. In [35], Ibrahim et al. assessed the impact of the RPL rank attack using the standard RPL protocol, evaluating it in both static and mobile environments. Their findings reveal that the rank attack exerts a more pronounced influence on RPL performance in mobile environments, whereas its effect is diminished in static environments. Authors in [14] examined the impact of the rank attack on RPL. They also conducted extensive simulations across four different network topologies, which encompassed two variations of grid topologies, a random topology, and a random topology featuring mobile nodes. In [36], the authors explored the network performance of the RPL protocol, employing it within static networks to manage power consumption while maintaining network topology Quality of Service (QoS). Furthermore, they delved into RPL's behavior within a mobile context, assessing its performance with the Random Waypoint (RWP) mobility model and quantifying its power consumption. To gauge the effects of these models and their power usage, they conduct a comparative analysis between the static model and the RWP model, both utilizing the RPL routing protocol. In their work presented in [37], the authors examined the RPL's performance in the context of a smart home network topology. Their study included a systematic analysis where they illustrated how each type of rank attack variant and the location of the attacking node within the network topology could potentially degrade network performance. Moreover, in [38], the researchers provided an extensive examination of the rank's influence on RPL networks. They conducted thorough experimental analyses across four distinct RPL network topologies and assessed the consequences of the rank attack. To ensure a comprehensive evaluation of the rank attack's impact, the authors utilized both grid-based and randomized variations of network topologies. Within the grid context, the topology was further categorized into grid corner and grid center, dependent on the location of the sink node. Meanwhile, in consideration of mobility, the random topology was subdivided into two variations: one with stationary nodes and the other involving mobile nodes. Table 1 provides an overview of pertinent research and highlights its distinctions from existing literature that has explored the effects of the decreased rank attack on the RPL network in both static and mobile environments.

**Table 1:** Comparative overview of prior research and the current study

| Related work | Year | Performance metrics | Simulator | Mobility support | Attack |
|---|---|---|---|---|---|
| [25] | 2010 | Stabilization time, DIOs generated | NS2 | No | No |
| [26] | 2013 | Number of affected nodes, E2ED, throughput, PDR, number of DIO messages generated | Cooja 2.5 | No | Yes |
| [27] | 2016 | PDR, DIOs generated, percentage of network nodes converged, E2ED | Cooja | No | Yes |
| [31] | 2016 | Control traffic, data traffic ratio, CPU usage, radio usage, PDR, delay | Cooja | Yes | No |
| [27] | 2017 | PDR, E2ED | Cooja 2.7 | No | Yes |

(Continued)

**Table 1 (continued)**

| Related work | Year | Performance metrics | Simulator | Mobility support | Attack |
|---|---|---|---|---|---|
| [32] | 2018 | Control traffic overhead, energy consumption, PDR, number of hops, ETX | Cooja | Yes | No |
| [29] | 2019 | Control traffic overhead, PDR, ETX, latency, average power consumption | Cooja | No | No |
| [33] | 2019 | Throughput, latency, PDR, average power consumption. | Cooja | Yes | No |
| [34] | 2020 | PDR, average power consumption | Cooja | Yes | Yes |
| [35] | 2020 | Control overhead, preferred parent changes, convergence time, energy consumption, lifetime | Cooja 3.0 | Yes | Yes |
| [30] | 2022 | Throughput, latency, PDR, average power consumption | Cooja 3.0 | No | Yes |
| [14] | 2022 | Packets received, control message count, inter-packet time, average power consumption | Cooja 2.7 | Yes | Yes |
| [36] | 2023 | Node power, control traffic overhead, ETX, hop count, PDR | Cooja 2.7 | Yes | No |
| [37] | 2023 | Packet overhead, average inter-packet time, PDR, average power consumption | Cooja 2.7 | Yes | Yes |
| [38] | 2023 | PDR, delay, throughput, ETX, interval DIO rate, energy cons, beacon interval, DAO rate, preferred parent change | Cooja 3.0 | No | Yes |
| This paper | 2023 | PDR, throughput, E2ED, ETX, average power consumption | Cooja 3.0 | Yes | Yes |

In the landscape of research on the RPL protocol within IoT networks, our paper distinguishes itself in several crucial aspects. First and foremost, we introduce an innovative dimension by incorporating the Random Direction Mobility Model (RDM) and elevating network density as key elements of our study. Unlike many prior works that have not explored the implications of RDM or increased network density, our research delves into uncharted territory, providing a unique perspective on RPL's performance. Furthermore, we conduct a thorough examination of RPL, utilizing an extensive range of performance metrics such as Packet Delivery Ratio (PDR), Average End to End Delay (E2ED), throughput, Expected Transmission Count (ETX), and average power consumption. This multifaceted evaluation ensures a comprehensive understanding of RPL's strengths and limitations under varying conditions. What sets our paper apart is the seamless integration of the decreased rank attack into both static and mobile environments. While other studies have considered these elements individually, our work uniquely combines them, offering insights into the complex challenges that IoT networks face in the presence of this attack. Lastly, our use of Cooja 3.0, a more advanced version of the simulator, provides enhanced accuracy and reliability for our experiments, setting our research on a firm foundation. In summary, our paper contributes significantly to the field by providing a

fresh perspective, a wider array of performance metrics, a novel combination of attack and mobility scenarios, and the advantage of an updated simulator version, all of which amplify the importance of securing IoT networks in the evolving landscape.

## 5 Simulation Setups and Performance Evaluation

### *5.1 Simulation Setups*

In this section, we outline our proposed scenarios, which encompass both stationary and mobile nodes. Additionally, we provide insights into the specifics of the mobility models employed for this experiment. We utilize the Random Direction Mobility model (RDM) to mitigate the impact of density waves and maintain consistent neighbour numbers per node during simulations. The RDM model, introduced in references [24] and [39], addresses the uneven distribution of mobile nodes within the Random Waypoint (RWP) model [24]. In RDM, nodes initially select both a random direction and speed and start moving in the chosen direction at the selected speed until reaching the simulation boundary. At this point, a new direction and speed are determined, and the process iterates. Notably, a significant challenge in handling the behavior of mobile nodes when they approach simulation boundaries is addressed by variations such as the Random Direction with Reflection and Random Direction with Wrap Around models. The unique attribute of the RDM model is that nodes determine random directions rather than random positions and temporarily halt at boundaries, ameliorating the issue of node accumulation at the simulation center. Consequently, node distribution across the simulation area achieves greater uniformity over time. For our experimental setup, we leveraged the Cooja simulator, a cycle-accurate platform built in Java, renowned for its ability to emulate Off-The-Shelf Internet of Things (IoT) devices [40]. This simulator seamlessly operates within the Contiki operating system (OS), meticulously designed to cater to the complexities of resource-constrained IoT-embedded devices [41]. Our research and analyses were carried out using the Zolertia One (Z1) IoT platform, a product developed by Zolertia R [42]. This platform features the energy-efficient Texas Instruments MSP430 Micro-Controller (MCU) as its Central Processing Unit (CPU), complemented by the Chipcon CC2420 radio module for wireless communication [42]. An essential aspect of our experiments was the consideration of mobility, which was facilitated by incorporating a dedicated mobility plugin into the Cooja simulator. This expansion of capabilities allowed us to effectively simulate mobile IoT applications. For generating patterns of movement among mobile nodes, we harnessed BonnMotion, an open-source Java-based software developed at the University of Bonn in Germany [43]. This tool empowered us to generate and meticulously assess mobile ad hoc applications. Our approach began with defining the network scenarios under examination and the specific simulation metrics in use. The experimental setup involved using the Z1 platform, which boasts specific hardware features. The platform's Micro-Controller Unit (MCU) is the MSP430, while the transceiver used is the CC2420. The operational voltage range for the MCU falls within the range of 1.8 V to 3.6 V, and for the transceiver, it is 2.1 V to 3.6 V. The platform is designed to operate effectively within a temperature range of 40°C to +85°C. The clock frequency is limited to a maximum of 16MHz. In different operational modes, the platform exhibits varying power consumption. In the MCU's active mode, the current consumption is 2 mA, while in the low-power mode, it reduces significantly to just 0.5 μA. During radio transmission, the platform consumes 17.4 mA, and when in IDLE mode, it draws 426 μA. The current consumption is higher during radio reception, at 18.8 mA. In the Off mode, the platform's current consumption is the lowest, at 0.1 μA. These hardware specifications played a crucial role in our experiments, ensuring the accurate simulation and assessment of IoT devices under various conditions [42].

### *5.2 Network Configurations*

Based on the information presented in Table 2, a series of simulation scenarios were executed within a 10000 $m^2$ environment to comprehensively study RPL's performance under various mobility patterns. The network configuration included varying numbers of sensor nodes: 10, 20, 30, and 40, all governed by a singular gateway node. The simulation employed Z1 motes, as mentioned before, and utilized the UDP transport layer protocol, along with the IEEE 802.15.4 PHY and MAC layers. Communication was facilitated through a radio medium modeled as a unit disk graph, with a transmission range established at 50 m. To assess network robustness, the experiment introduced dynamic elements by designating 10%, 20%, 30%, and 40% of the nodes as attackers. Furthermore, 60% of the nodes were set as mobile, moving at a consistent speed of 1 to 2 m/s. Data packets, each sized at 30 bytes, were transmitted at intervals of 60 s, enabling a comprehensive analysis of the network's performance and resilience under the specified conditions. The simulations extended for one hour, allowing for an accurate observation of the network's actual performance.

**Table 2:** Simulation setups

| Settings | Values |
|---|---|
| Transmission range | 50 m |
| Dimension area | 10000 $m^2$ |
| Sensor nodes' number | 10, 20, 30, 40 |
| Attacker nodes' number | 10%, 20%, 30%, 40% |
| Mobile nodes' number | 40% |
| Radio medium | Unit disk graph medium |
| Transport layer protocol | UDP |
| PHY and MAC layer | IEEE 802.15.4 |
| Node velocity | 1 to 2 m/s |
| Data packet sending interval | 60 s |
| Simulation time | h |

### *5.3 Performances Metrics*

The simulation was conducted with the primary objective of comprehending the repercussions of the deceased rank attack within two distinct environmental contexts: static and mobile settings. The assessment pertained to the effect of this attack on the network's operational efficiency. The evaluation criteria encompassed key performance indicators, including throughput, PDR, E2ED, ETX and APC, renowned for their paramount relevance and responsiveness in gauging network performance.

The PDR is a fundamental quantitative measure characterizing the efficacy of data transmission and quantifies the ratio of successfully conveyed data packets to the total dispatched packets within the network. This parameter is mathematically encapsulated by the following formula [30]:

$$\text{PDR} = \frac{P_{received}}{P_{Generated}} * 100 \tag{1}$$

where $P_{received}$ and $P_{Generated}$ represent the total number of packets received by the sink node and the total number of packets generated by the source nodes, respectively.

The E2ED refers to the time interval that elapses between the initiations of data transmission from a source node to its eventual reception at the destination node. It is given using the following Eq. 2 [30]:

$$\text{E2ED} = Time_{receiver} - Time_{sent} \text{ (ms)} \tag{2}$$

where $Time_{receiver}$ is the value of the timestamp when the packet is received at the destination node. While $Time_{sent}$ is the value of the timestamp when the packet is transmitted from the source node.

Throughput quantifies the speed at which data is successfully transmitted through a network, often expressed in Kilos bits per second (kbps) or packets per second (PPS) [30].

$$\text{Throughput} = \frac{Total\ received\ Data}{Simulation\ Time} \text{ (kbps)} \tag{3}$$

where "Total Received Data" refers to the quantity of successfully received data at the destination node during the simulation. "Simulation Time" is the duration of the simulation.

ETX serves as a metric within wireless ad hoc networks for estimating the expected number of transmissions required for a packet to successfully traverse a link between two nodes. It helps quantify the reliability of a link by considering factors such as packet loss and interference. The ETX calculation employs the PDR, where the reciprocal of the PDR yields the ETX value as shown in the formula below [29]:

$$\text{ETC} = \frac{1}{PDR} = \frac{P_{Generated}}{P_{received}} \tag{4}$$

The average power consumption (APC) refers to the mean rate at which energy is consumed by simulated nodes within a network over a specific duration. It is a vital metric for assessing the energy efficiency of networked devices and their impact on battery life. The APC is calculated using the following equation [30]:

$$\text{APC} = \frac{Energest_{value} * I * V}{Rtimer_{second} * Runtime} \text{ Mw} \tag{5}$$

$Energest_{value}$ refers to the energy consumption value obtained from the Energest module in Contiki. It provides information about energy consumption by various components such as the CPU, radio, and other peripherals. I and V represent respectively the current (in amperes) consumed by the node and the voltage (in volts) supplied to the node. $Rtimer_{second}$: Refers to the time (in seconds) of the Rtimer module, which is a real-time timer module in Contiki. *Runtime* depicts the total runtime of the simulation (in seconds).

## 6 Experiment Outcomes and Comparative Study

Within this section, we present the findings derived from our thorough experiments.

### *6.1 Packet Delivery Ratio (PDR)*

Figs. 2a and 2b depict the PDR under decreased rank attack in two distinct environments: the static environment in (a) and the mobile environment in (b). The primary focus of these visualizations is to analyze the impact of varying parameters on the PDR. Specifically, the number of nodes and the percentage of attackers have been manipulated to discern their effects on network performance. In Fig. 2a, corresponding to the static environment, the PDR is depicted with respect to the number of nodes (10, 20, 30, 40) and varying percentages of attackers (up to 40%). A noteworthy observation

is that the PDR demonstrates a decline when compared to the baseline scenario without attacks. Moreover, an intriguing trend surfaces when the nodes' number escalates: the PDR experiences a decrease. This trend accentuates the sensitivity of the network's PDR to changes in node density. Concurrently, in Fig. 2b, within the mobile environment, a similar analytical framework is applied. The PDR is plotted against the identical parameters of node count and attacker percentage. Notably, the graph displays analogous tendencies as its static counterpart, reflecting the PDR's response to the interplay between node count, attacker presence and network mobility. Furthermore, both figures consistently reveal the influence of attacker prevalence on the PDR. The percentage of attackers correlates with a decrease in the PDR, underscoring the disruptive nature of attacks on network reliability. As the attacker percentage increases, the PDR steadily diminishes, underscoring the critical importance of robust security measures in maintaining desirable PDR levels. Fig. 3 provides a representation of the dynamics of PDR, in specific scenarios, emphasizing the significance of network configuration and security considerations in governing data transmission reliability.

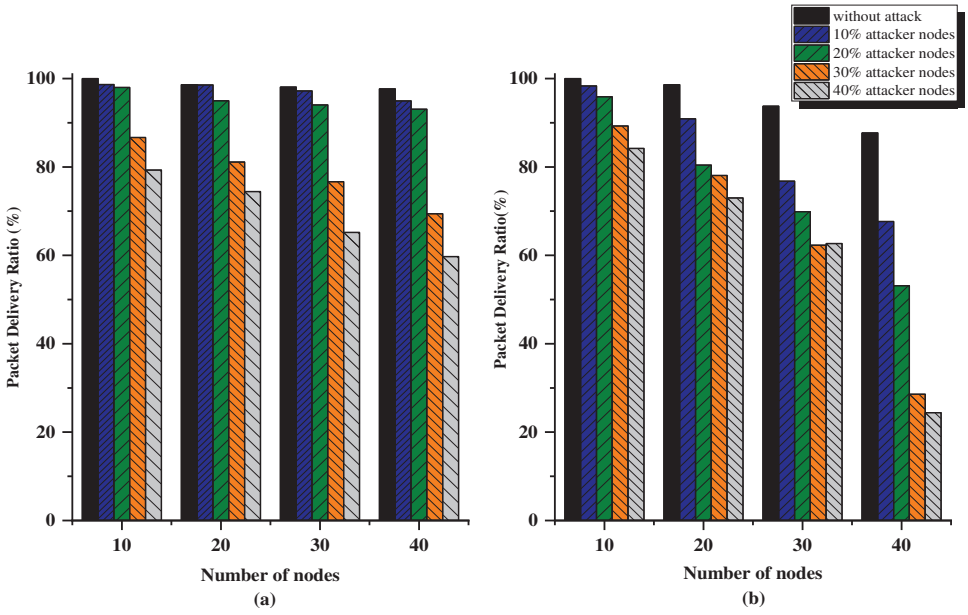


**Figure 2:** PDR in (a) static (b) mobile environment under decreased rank attack

The decline in PDR under a decreased rank attack within a network utilizing the Random Walk mobility model is attributed to interconnected factors. First, the disruption of routing paths emerges as a pivotal influence. The inherently erratic and unpredictable movement patterns characteristic of the Random Walk model interact with nodes possessing artificially lowered ranks, resulting in suboptimal routing decisions and the subsequent misrouting or loss of packets. Furthermore, the model's dynamic nature complicates the establishment of reliable communication paths, accentuated by the intrusion of nodes with compromised ranks. Consequently, the PDR diminishes due to increased inefficiencies and disruptions in data transmission. The attack's effect on the network's resilience is noteworthy, impeding the adaptability required for coping with dynamic scenarios. The compromised routing paths underscore the vulnerabilities within routing mechanisms and stress the importance of secure protocols. This reduction in PDR stands as an evident marker of the attack's effectiveness in undermining communication integrity. In response, devising robust security measures and adaptive

routing strategies becomes imperative to counteract the impacts of the decreased rank attack and to sustain dependable data delivery within the intricacies of the Random Walk mobility model.

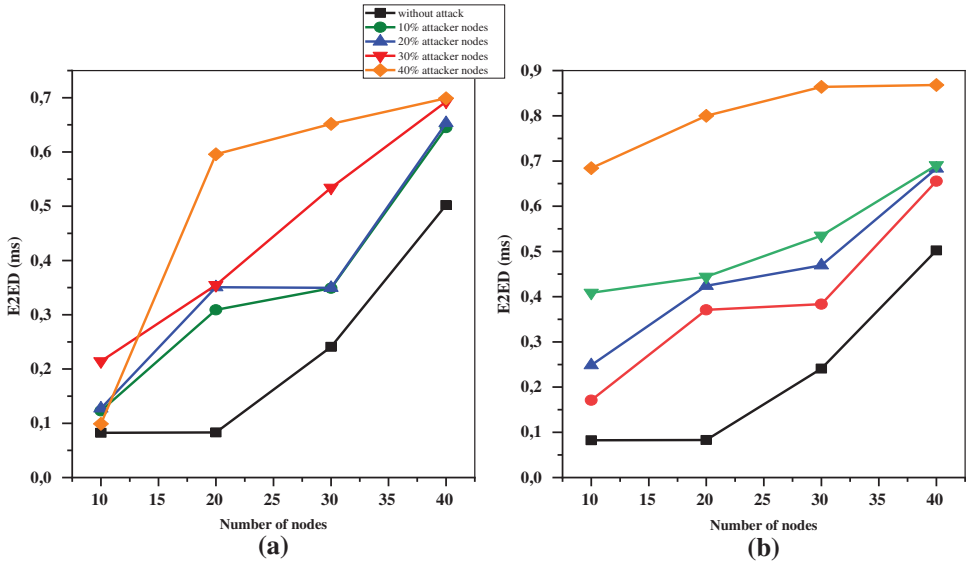


**Figure 3:** E2ED (a) static (b) mobile environment under decreased rank attack

### *6.2 The End-to-End Delay*

In Figs. 3a and 3b, both depicted as line charts, a comprehensive analysis E2ED is presented in a static and a mobile environment respectively in (3a) and (3b). The primary intent of these visualizations is to explore the influence of varying parameters on the E2ED metric. In Fig. 3a, which corresponds to the static environment, the E2ED is plotted against varying numbers of nodes (10, 20, 30, 40) and different percentages of attackers (10%, 20%, 30%, 40%). One notable observation is the discernible increase in E2ED compared to the baseline scenario without attacks. Notably, the network devoid of attacks attains the lowest E2ED value, indicating its performance in ensuring fast and efficient data delivery. Moreover, when the nodes' number increases, E2ED increases. This pattern highlights the network's sensitivity to changes in node density. Additionally, the influence of attacker nodes becomes evident. As the percentage of attackers increases, a parallel rise in E2ED becomes apparent. This trend emphasizes how attackers negatively affect data transmission efficiency. In addition, the analysis of Fig. 3b reveals similar findings within a mobile environment. The line chart compares the performance of E2ED under different parameters including node count and attacker percentage. Similar to the static scenario, the consistent behavior of E2ED in response to mobility dynamics is highlighted by the persistent overarching trends. Ultimately, graphs cohesively elucidate the intricacy of E2ED within both environments. They underscore the effects of node density and attacker presence on network performance, accentuating the imperative of robust security measures and adaptive routing strategies. Importantly, the findings delineate that the network featuring 40% attacker nodes attains the highest E2ED value, underscoring the acute vulnerability of compromised networks to protracted end-to-end delays.

The increased E2ED resulting from the decreased rank attack within a network employing the Random Walk mobility model has implications for communication efficiency, network robustness, and security vulnerabilities. This effect highlights how node movement patterns, compromised routing

paths, and data transmission integrity are intricately connected. Firstly, higher E2ED values indicate disruptions in communication routes due to compromised routing during an attack. In scenarios where nodes exhibit movement, under the Random Walk model compromised routes further complicate establishing pathways. Secondly, the attack weakens the network's adaptive resilience by introducing compromised nodes. This erosion of adaptability is reflected in the elevated E2ED, exposing limitations in dynamic scenarios and sustaining reliable data transmission. Thirdly, the amplified E2ED serves as a prominent indicator of the attack's success in tampering with network communication. This underscores vulnerabilities within routing mechanisms, emphasizing the necessity for fortified protocols to avert unauthorized interference. Moreover, the impact is palpable on user experience, with extended E2ED leading to delayed data delivery, especially critical in real-time applications. As a result, it becomes more crucial to implement security measures and routing strategies to ensure data transmission integrity within the Random Walk mobility model.

### *6.3 Throughput*

Fig. 4 comprises a diagram, illustrating the throughput performance in distinct scenarios. The x-axis of the diagram delineates the varied nodes' number (going from 10 to 40), while the y-axis represents the throughput values. The diagram is divided into two sections: Without attack and under decreased rank attack for both static and mobile environments. RA stands for the static network's decreased rank attack, whereas MRA corresponds to the decreased rank attack in the mobile network. Simulation results show that static networks without attack exhibit the highest throughput values underscoring the significance of stability and the absence of malicious interference. When mobility or decreased rank attacks are introduced, a reduction in throughput becomes evident. This is also evident for both static and mobile environments, reaffirming the effect of mobility and compromised routing on data throughput.

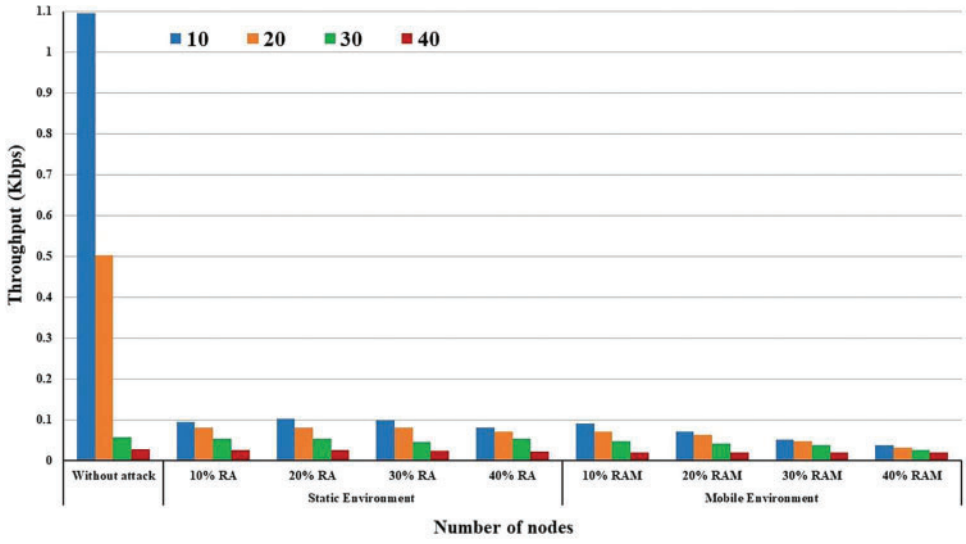


**Figure 4:** Throughput within a static and mobile environment under decreased rank attack

The reduction in throughput when the of nodes number increases in the presence of both the decreased rank attack and a Random Walk mobility model is a result of an intricate interplay of factors. The larger network size leads to heightened interference and contention for the wireless medium, causing more packet collisions and retransmissions. Additionally, the complex routing

paths in larger networks introduce inefficiencies, necessitating longer paths and more hops for communication. The impact of compromised routing decisions due to the decreased rank attack further exacerbates this issue, contributing to higher latency and increased retransmissions. Due to its random nature, the Random Walk mobility model introduces variability in link qualities and affects throughput consistency. Furthermore, increased channel utilization, due to more nodes, intensifies traffic, adding to the retransmission load and reducing effective throughput. The combination of these factors results in diminished throughput, impacting the quality of service and highlighting the need for robust routing, security mechanisms and congestion control strategies to mitigate the challenges posed by larger networks with mobility and attacks.

### *6.4 Expected Transmission Count (ETX)*

Fig. 5 depicts a comprehensive overview of how the ETX metric changes in response to variations in the number of nodes and percentages of attacker nodes for both static and mobile environments. As shown in Fig. 5, with an increase in the number of nodes, the ETX values also increase. This indicates that as the network grows in size, the overall transmission count required for successful packet delivery rises. The observed behavior remains consistent regardless of the variations in the percentage of attacker nodes. Furthermore, Fig. 6 illustrates another important observation. Regardless of the number of nodes, when the percentage of attacker nodes increases, the ETX values rise. This indicates that the presence of attacker nodes affects the overall link quality and reliability. Both static and mobile environments exhibit this behavior, suggesting that attacker nodes have a consistent effect regardless of node mobility. The figure also highlights a noteworthy point. At the maximum values of 40 nodes and 40% attacker nodes, the ETX reaches its peak. This indicates that the network experiences its highest transmission count requirement under these conditions. The graph visually demonstrates the influence of both the network density and the presence of attacker nodes on ETX values. Lastly, the figure draws attention to the impact of node mobility on the network. It is evident that mobility affects the behavior of the network and consequently the ETX metric. This insight underscores the importance of considering mobility when analyzing and optimizing network performance.

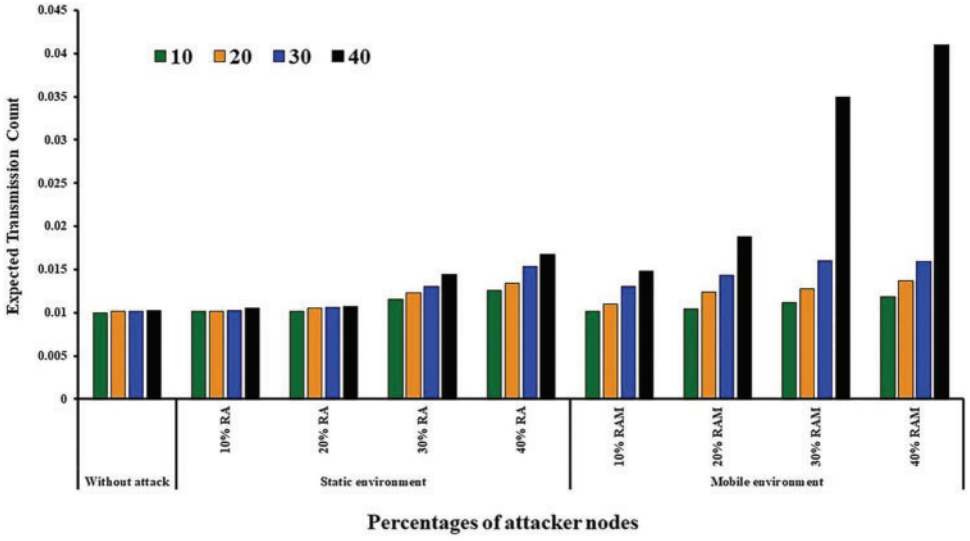


**Figure 5:** ETX within static and mobile environments under decreased rank attack

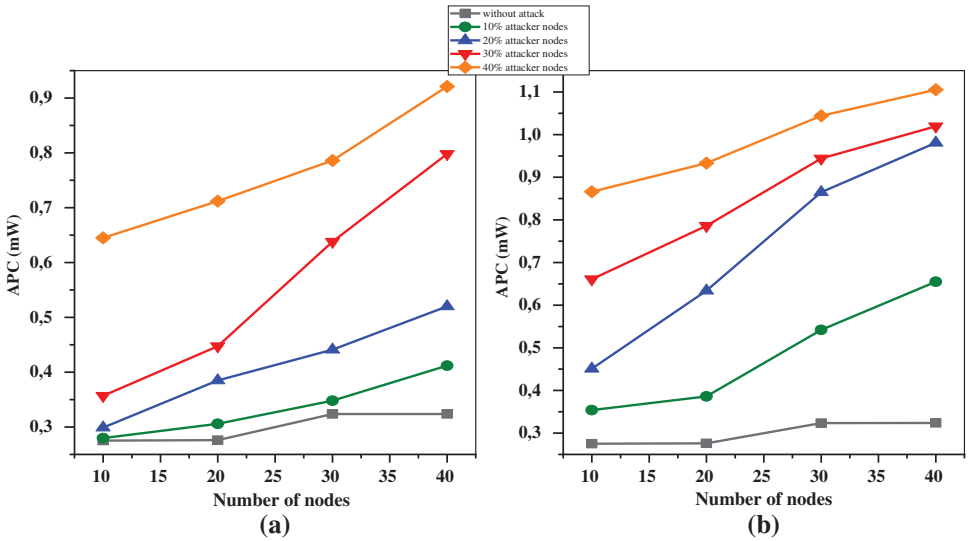


**Figure 6:** APC (a) static (b) mobile environment under decreased rank attack

The observed increase in ETX values when nodes' number in the network was augmented under the decreased rank attack within a random direction mobility model can be attributed to a combination of factors. Firstly, the rise in network density introduces heightened interference and traffic. With more nodes contending for the wireless medium, collisions become more likely, leading to increased packet loss and retransmissions. This, in turn, adversely affects the overall link quality and prompts an increase in ETX values. Secondly, the larger network size introduces longer communication paths and a greater number of potential points of failure. Consequently, the reliability of individual links decreases, necessitating more retransmissions to ensure packet delivery which increases the ETX values. Thirdly, the random direction mobility model accentuates the instability of link conditions due to frequent node movements. As nodes shift around the network, link quality fluctuates, requiring additional retransmissions for successful communication, further contributing to higher ETX values. Lastly, the compounded effects of the decreased rank attack aggravate the challenges posed by the previous factors. The attackers' deliberate degradation of link quality amplifies the impact of interference, mobility, and network size, ultimately resulting in the observed increase in ETX values. The combination of these factors underscores the complexity of wireless network behavior and the multi-faceted nature of the observed outcomes.

### *6.5 Average Power Consumption (APC)*

Fig. 6 presents the APC in two distinct network scenarios: (a) a static environment and (b) a mobile environment, both under the decreased rank attack. An interesting observation in both scenarios is that the average power consumption increases when varying the total number of nodes and the percentage of attacker nodes. In the static environment depicted in Fig. 6a, the average power consumption increases as the number of nodes and percentage of attacker nodes increase. Similarly, in Fig. 6b, representing the mobile environment, a parallel behavior emerges, but with a significant impact. In Fig. 6b, we can observe that the APC goes up from 0.8, to 1.1 mW when 40% of attacker nodes are present. Additionally, in Fig. 6a it rises from 0.6 to 0.9 mW for the same percentage. Consequently, when compared to a static network, mobile networks exhibit a significant rise in average power usage. This figure provides valuable insights into the interplay among network parameters, attacker nodes,

and mobility, shedding light on their combined influence on average power consumption during a decreased rank attack.

The observed rise in average power consumption within a random direction mobility model network as both the number of nodes and the percentage of attacker nodes increase can be attributed to a confluence of factors. Firstly, the expanded network size ushers in heightened network activity, with more nodes engaging in data transmission and processing, demanding increased power resources. Secondly, the larger node population amplifies the possibility of interference and collisions, necessitating retransmissions that consume additional power. Thirdly, the malicious activities of attacker nodes including generating fake traffic or disrupting network operations, contribute to power consumption by compelling legitimate nodes to counteract the effects of the attack. Fourthly, the inherent overhead of managing node mobility in such a network, involving routing table updates and dynamic topology adjustments contributes to elevated energy usage. Furthermore, dynamic routing path changes induced by node mobility, increase power consumption as nodes establish and maintain new routes, often influenced by attacker nodes. Moreover, the mobility itself, with nodes constantly adapting to changing positions, can be energy-intensive due to power adjustments for maintaining connectivity. Additionally, the heightened contention for channel access among an increased node count leads to delays and retransmissions, further elevating power usage. Lastly, as the network grows in complexity, efficient resource allocation becomes more challenging, necessitating additional computational efforts and communication, which consume power resources.

## 7 Conclusion

This study undertook a comprehensive evaluation of RPL's performance under diverse scenarios, shedding light on its limitations in adapting to changing network topologies and mobility challenges. We specifically investigated RPL's behavior in static and mobile settings, employing the random direction mobility model (RDM) while subjecting it to the decreased rank attack. Our analysis encompassed variations in node quantities and the percentage of malicious nodes in both static and mobile environments, gauged through five key metrics: Average End-to-End Delay (AE2ED), throughput, Packet Delivery Ratio (PDR), Expected Transmission Count (ETX), and average power consumption (APC). In the presence of a decreased rank attack operating within RDM, various facets of network performance undergo notable alterations. Primarily, the Packet Delivery Ratio experiences a decline, signifying an increased rate of lost or undelivered packets. Simultaneously, Expected Transmission Count values rise, reflecting the heightened need for packet retransmissions and additional hops due to the attack-induced routing disruptions. Average End-to-End Delay registers an increase, attributable to delays introduced by the attack, affecting routing decisions and data transmission. Throughput decreases as a consequence of the attack's interference with data flow, resulting in greater packet loss and retransmissions. Lastly, average power consumption tends to surge due to increased energy expenditure on packet transmissions and retransmissions, primarily as packets follow longer paths. These findings underscore the perturbing effect of a decreased rank attack and underscore the critical importance of implementing robust security measures, particularly in dynamic and mobile network environments, to safeguard against such disruptions. In summary, this study provides crucial insights into the challenges faced by RPL-based IoT networks and the tangible impact of the decreased rank attack. These findings have significant implications for the development of protective measures and the long-term resilience of IoT networks in the face of ever-evolving threats. Our future goal is to expand on the insights from this research to create an anomaly intrusion detection system. This system will be designed to identify internal attacks by continuously monitoring specific performance parameters sensitive to such attacks within a mobile environment.

**Acknowledgement:** The authors would like to acknowledge the Deanship of Graduate Studies and Scientific Research, Taif University for funding this work.

**Funding Statement:** The authors received no specific funding for this study.

**Author Contributions:** The authors confirm contribution to the paper as follows: Study concept, data analysis, and writing: Hkiri, A.; writing review and editing: Karmani, M., Ben Bahri, O.; draft manuscript preparation: Murayr, A. H., AlAsmari, H. F., Machhout, M. All authors reviewed the results and approved the final version of the manuscript.

**Availability of Data and Materials:** All data generated or analysed during this study are included in this article and are available from the corresponding author upon reasonable request.

**Ethics Approval:** All authors confirm that accepted principles of ethical and professional conduct have been followed. Additionally, this article does not contain any studies with human participants or animals performed by any of the authors.

**Conflicts of Interest:** The authors declared that they have no conflicts of interest to report regarding the present study.

## References

[1] M. N. Bhuiyan, M. M. Rahman, M. M. Billah and D. Saha, "In Internet of things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10474–10498, 2021.

[2] M. M. Kamruzzaman, "Key technologies, applications and trends of Internet of Things for energy-efficient 6G wireless communication in smart cities," *Energies*, vol. 15, no. 15, pp. 5608, 2022.

[3] M. H. Kashani, M. Madanipour, M. Nikravan, P. Asghari and E. Mahdipour, "A systematic review of IoT in healthcare: Applications, techniques, and trends," *Network and Computer Applications*, vol. 192, pp. 103164, 2021.

[4] V. A. Thakor, M. A. Razzaque and M. A. Khandaker, "Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities," *IEEE Access*, vol. 9, pp. 28177–28193, 2021.

[5] Z. Yang and C. H. Chang, "6LoWPAN overview and implementations," in *Proc. of EWSN*, Beijing, China, pp. 357–361, 2019.

[6] M. Singh and S. Kumar, "A survey: Ad-hoc on demand distance vector (AODV) protocol," *International Journal of Computers and Applications*, vol. 161, pp. 38–44, 2017.

[7] A. Verma and N. Bhardwaj, "A review on routing information protocol (RIP) and open shortest path first (OSPF) routing protocol," *International Journal of Future Generation Communication and Networking*, vol. 9, no. 4, pp. 161–170, 2016.

[8] A. R. Zarzoor, "Enhancing dynamic source routing (DSR) protocol performance based on link quality metrics," in *Proc. of ISemantic*, Semarangin, Indonesia, pp. 17–21, 2021.

[9] A. K. Darabkh, M. Al-Akhras, N. J. Zomot and M. Atiquzzaman, "RPL routing protocol over IoT: A comprehensive survey, recent advances, insights, bibliometric analysis, recommendations, and future directions," *Journal of Network and Computer Applications*, vol. 207, pp. 103476, 2022.

[10] A. Vangala, A. K. Das, V. Chamola, V. Korotaev and J. J. P. C. Rodrigues, "Security in IoT-enabled smart agriculture: Architecture, security solutions and challenges," *Cluster Computing*, vol. 26, no. 2, pp. 879–902, 2023.

[11] D. Bhattacharjee, T. Acharya and S. Chakravarty, "Energy efficient data gathering in IoT networks with heterogeneous traffic for remote area surveillance applications: A cross layer approach," *IEEE Transaction Green Communication and Networking*, vol. 5, no. 3, pp. 1165–1178, 2021.
[12] S. J. Ramson, S. Vishnu and M. Shanmugam, "Applications of Internet of Things (IoT)–an overview," in *Proc. of ICDCS*, Coimbatore, India, pp. 92–95, 2020.
[13] N. A. M. Alhammadi and K. H. Zaboon, "A review of IoT applications, attacks and its recent defense methods," *Journal of Global Scientific Research*, vol. 7, no. 3, pp. 2128–2134, 2022.
[14] A. Bang and U. P. Rao, "Impact analysis of rank attack on RPL-based 6LoWPAN networks in Internet of Things and aftermaths," *Arabian Journal for Science and Engineering*, vol. 48, no. 2, pp. 2489–2505, 2023.
[15] F. Song, Q. Zheng, D. Liu, J. Zhang, X. Lin *et al.,* "Privacy-preserving task matching with threshold similarity search via vehicular crowdsourcing," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 7, pp. 7161–7175, 2021.
[16] F. Song, Q. Zheng, D. Liu, J. Zhang, X. Lin *et al.,* "Privacy-preserving keyword similarity search over encrypted spatial data in cloud computing," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6184–6198, 2021.
[17] T. A. Al-Amiedy, M. Anbar, B. Belaton, A. A. Bahashwan, I. H. Hasbullah *et al.,* "A systematic literature review on attacks defense mechanisms in RPL-based 6LoWPAN of Internet of Things," *Internet of Things*, vol. 22, pp. 100741, 2023.
[18] C. Zhang, X. Luo, J. Liang, X. Liu, L. Zhu *et al.,* "POTA: Privacy-preserving online multi-task assignment with path planning," *IEEE Transactions on Mobile Computing*, vol. 18, pp. 1–13, 2023.
[19] C. Zhang, C. Hu, T. Wu, L. Zhu and X. Liu, "Achieving efficient and privacy-preserving neural network training and prediction in cloud environments," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, pp. 4245–4257, 2022.
[20] G. Sharma, J. Grover and A. Verma, "Performance evaluation of mobile RPL-based IoT networks under version number attack," *Computer Communications*, vol. 197, pp. 12–22, 2023.
[21] O. Gaddour and A. Koubaa, "RPL in a nutshell: A survey," *Computer Networking*, vol. 56, no. 14, pp. 3163–3178, 2012.
[22] K. Subash and L. Arockiam, "A survey on issues and challenges in RPL based routing for IoT," *Annals of the Romanian Society for Cell Biolog*, vol. 25, pp. 501–510, 2021.
[23] A. Verma and V. Ranga, "Security of RPL based 6LoWPAN networks in the Internet of Things: A review," *IEEE Sensors Journal*, vol. 20, no. 11, pp. 5666–5690, 2020.
[24] B. Safaei, A. Mohammadsalehi, K. T. Khoosani, S. Zarbaf, A. M. H. Monazzah *et al.,* "Impacts of mobility models on RPL-based mobile IoT infrastructures: An evaluative comparison and survey," *IEEE Access*, vol. 8, pp. 167779–167829, 2020.
[25] W. Xie, M. Goyal, H. Hosseini, J. Martocci, Y. Bashir *et al.,* "Routing loops in dag-based low power and lossy networks," in *Proc. of AINA*, Perth, Australia, pp. 888–895, 2010.
[26] A. Le, J. A. Lasebae, A. Vinel, Y. Chen and M. Chai, "The impact of rank attack on network topology of routing protocol for low-power and lossy networks," *IEEE Sensor Journal*, vol. 13, no. 10, pp. 3685–3692, 2013.
[27] A. Rehman, M. M. Khan, M. A.Lodhi and F. B. Hussain, "Rank attack using objective function in RPL for low power and lossy networks," in *Proc. of CIICS*, Sharjah, United Arab Emirates, pp. 1–5, 2016.
[28] K. K. Rai and K. Asawa, "Impact analysis of rank attack with spoofed IP on routing in 6LoWPAN network," in *Proc. of IC3*, Noida, India, pp. 1–5, 2017.
[29] S. A. Abdel-Hakeem, A. A. Hady and H. kim, "RPL routing protocol performance in smart grid applications based wireless sensors: Experimental and simulated analysis," *Electronics*, vol. 8, no. 2, pp. 186, 2019.
[30] H. Amal, K. Mouna and M. Mohsen, "The routing protocol for low power and lossy networks (RPL) under attack: Simulation and analysis," in *Proc. of IC_ASET*, Hammamet, Tunisia, pp. 143–148, 2022.
[31] A. Oliveira and T. Vazao, "Low-power and lossy networks under mobility: A survey," *Computer Networking*, vol. 107, pp. 339–352, 2016.

[32] H. Lamaazi, N. Benamar and A. J. Jara, "RPL-based networks in static and mobile environment: A performance assessment analysis," *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 3, pp. 320–333, 2018.
[33] H. Kharrufa, N. Salman, M. Lei and A. H. Kemp, "A performance evaluation of RPL in mobile iot applications: A practical approach," *IFAC-PapersOnLine*, vol. 52, no. 24, pp. 312–317, 2019.
[34] M. Christopher, G. Baraq, M. G.M.Safwan, J. Zakwan and A. B. A. Saleh, "The impact of mobile DIS and rank-decreased attacks in Internet of Things networks," *International Journal of Advanced Engineering and Technology*, vol. 10, no. 2, pp. 66–72, 2020.
[35] S. Ibrahimy, H. Lamaazi and N. Benamar, "RPL assessment using the rank attack in static and mobile environments," in *Proc. of 2020 Int. Conf. on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)*, Sakheer, Bahrain, pp. 1–6, 2020.
[36] C. S. Sanaboina and P. Sanaboina, "Impact of mobility on power consumption in RPL," arXiv:2305.05308, 2023.
[37] A. Bang and U. P. Rao, "Performance evaluation of RPL protocol under decreased and increased rank attacks: A focus on smart home use-case," *SN Computer Science*, vol. 4, no. 4, pp. 326, 2023.
[38] I. S. Alsukayti and M. Alreshoodi, "RPL-based IoT networks under simple and complex routing security attacks: An experimental study," *Applied Sciences*, vol. 13, no. 8, pp. 4878, 2023.
[39] T. Camp, J. Boleng and V. Davies, "A survey of mobility models for ad hoc network research," *Wireless Communications and Mobile Computing*, vol. 2, no. 5, pp. 483–502, 2002.
[40] C. Thomson, I. Romdhani, A. Al-Dubai, M. Qasem, B. Ghaleb *et al.,* "Cooja simulator manual," Edinburgh Napier University, Edinburgh, 2016.
[41] Y. B. Zikria, M. K. Afzal, F. Ishmanov, S. W. Kim and H. Yu, "A survey on routing protocols supported by the Contiki Internet of Things operating system," *Future Generation Computer Systems*, vol. 82, pp. 200–219, 2018.
[42] I. N. R. Hendrawan and I. G. N. W. Arsa, "Zolertia Z1 energy usage simulation with Cooja simulator," in *Proc. ICICoS*, Semarang, Indonesia, pp. 147–152, 2017.
[43] A. Bothe and N. Aschenbruck, "BonnMotion 4-taking mobility generation to the next level," in *Proc. of IPCCC*, Austin, TX, USA, pp. 1–8, 2020.