Microwave Review
July 2025, Vol. 31, No. 1, pp. 58-62
DOI: 10.18485/mtts_mr.2025.31.1.10

Comparative Analysis of QoS Degradation in IoT Networks Caused by Hybrid Rank Attacks

Mohamed Achraf Boukhobza[1], Mehdi Rouissat[2,3], Mohammed Belkheir[1], Allel Mokaddem[1], Pascal Lorenz[4]

Abstract – **The Internet of Things (IoT) is a transformative technology applied across diverse domains, including manufacturing, environmental monitoring, home automation, and healthcare. It enables seamless interaction and data exchange between people, machines, and billions of interconnected devices, such as sensors, actuators, and services.**

Despite its advantages, IoT networks are highly vulnerable to various security threats. Cyberattacks targeting IoT systems can disrupt operations, compromise data integrity, and cause significant data loss. Addressing these challenges is particularly critical due to the large scale and resource constraints of IoT devices, necessitating robust and efficient security management.

This paper introduces a modified hybrid rank attack, evaluates its impact, and compares it to other hybrid rank attacks. The results demonstrate that the proposed attack severely degrades network Quality of Service, significantly affecting metrics such as overhead (increase of 390%), energy consumption (increase of 117%), Packet Delivery Ratio (decrease of 37%) and latency (increase of 95%).

Keywords – **IoT, RPL, QoS, Security, Rank Attacks**

I. INTRODUCTION

The Internet of Things (IoT) acts as a bridge to the expansive world of the Internet, with its core objective being to connect a wide variety of devices, from the simplest to the most complex [1,2]. It is considered as multidisciplinary framework that connects everyday objects to the internet, enabling smart and efficient services [3]. By integrating the physical and digital worlds, IoT introduces a new dimension where anyone can connect from any location. Sensors, a key component of IoT, collect environmental data and make adjustments when necessary [4, 5]. IoT is widely adopted across various domains to create new services or improve existing ones, with applications in transportation, environmental monitoring, healthcare, industrial automation, smart agriculture, public safety, and military operations, among others [6].

The core functionality of IoT hinges on its networks and the protocols that regulate them. Effective routing protocols play a vital role in ensuring reliable data transmission across these intricate networks. They optimize information flow while conserving resources and maintaining the security and Quality of Service (QoS) required for IoT applications [7]. Among these protocols, the Routing Protocol for Low-Power and Lossy Networks (RPL) stands out for its adaptability and suitability. RPL is specifically designed for constrained environments where devices are limited in processing, memory, and battery life. It structures the network as a Destination-Oriented Directed Acyclic Graph (DODAG), where devices choose one parent nodes based on an objective function. The rank metric is used to measure the distance between IoT nodes and the root node within the DODAG [8]. RPL-Contiki employs several control messages—DODAG Information Object (DIO), DODAG Information Solicitation (DIS) and DODAG Advertisement Object (DAO), to disseminate routing information and manage network routes. It supports multiple operational modes, including storing and non-storing modes, and incorporates mechanisms for loop prevention, local repairs, and mobility management [9, 10].

The IoT has emerged as the foundation of digital transformation in today's hyperconnected world, affecting almost every industry, from industrial automation to smart cities and healthcare. It is more important than ever to maintain the integrity and functionality of IoT networks as billions of devices connect and communicate with each other without interruption. But along with this expansion comes a growing risk: sophisticated cyberattacks are increasingly aiming for the very protocols that facilitate effective communication. Among these, hybrid rank attacks pose a threat that compromises security and performance in a subtle yet extremely disruptive way. The difficulty is that these attacks are dishonest; they use internal routing metrics to cause internal network instability. The resource limitations of IoT devices, which restrict their defensive capabilities, increase the urgency of addressing these threats. In IoT networks, devices are often publicly accessible and rely on wireless communication, making them vulnerable to security threats, which introduces challenges related to scalability, adaptability, and compatibility [8, 11]. RPL is particularly susceptible to attacks such as Rank, Sinkhole, and Wormhole attacks. These attacks jeopardize network integrity by altering routing information, diverting traffic through malicious nodes, and channelling data to unauthorized endpoints [12].

Hybrid attacks pose a significant threat to RPL-based IoT networks. In [13], a Hybrid Rank Attack (HRA) was introduced, combining two types of rank manipulation: the Decreased Rank Attack (DRA) and the Worst Parent Attack (WPA). In a DRA, a malicious node advertises a rank value lower than its actual rank, while in a WPA, the node

Article history: Received December 06,2024y; Accepted May 03, 2025

[1]Mohamed Achraf Boukhobza, Mohammed Belkheir and Mokaddem Allel are with LIMA Laboratory, Nour Bachir University Center El-Bayadh, Algeria, E-Mails: m.boukhobza@cu-elbayadh.dz, m.belkheir@cu-elbayadh.dz, a.mokaddem@cu-elbayadh.dz

[2]Mehdi Rouissat is with the institute of Technology, Nour Bachir University Center, El-Bayadh, and affiliated to [3] STIC Laboratory, University Aboubekr Belkaid, Tlemcen, Algeria, E-Mail: m.rouissat@cu-elbayadh.dz

[4]Psacal Lorenz is with Haute Alsace University, Mulhouse, France, E-mail: pascal.lorenz@uha.fr

announces a rank value higher than its own, deliberately disrupting the network topology by creating suboptimal paths. The HRA alternates between advertising decreased rank values and increased rank value. This dual strategy aims to destabilize the network by combining the effects of both attacks, forcing victim nodes to frequently switch their preferred parents. The hybrid attack introduces instability into the network topology through selecting the malicious node as the preferred parent during the decreased rank phase and replacing it during the increased rank phase. This constant parent-switching behavior exacerbates the attack's impact, significantly affecting network performance metrics such as message exchange rates, energy consumption, packet delivery ratio, latency, and memory usage.

Ensuring the dependability and security of IoT networks has become a global priority as they quickly grow to power smart homes, healthcare systems, and industrial environments. These networks serve as the digital foundation of contemporary infrastructure, but because of their intrinsic weaknesses, they are vulnerable to ever-more-advanced attacks. Among the most disruptive are rank-based attacks, which subtly compromise the effectiveness and stability of networks. Resolving these issues is essential to maintaining the expansion and confidence in IoT applications. By examining a novel hybrid rank attack that presents a serious risk to RPL-based IoT networks, this paper aids in this endeavor.

In this paper, a new variant of Hybrid Rank Attack is presented, based on Decreased Rank Attack (DRA) and Infinite Rank attack (IRA). The primary goal is to push the victim nodes to frequently switching their preferred parents while conducting continuous local repairs, to generate an excessive amount of unnecessary control messages throughout the network. This aims to drain node resources and degrade overall network performance. Additionally, it would significantly impact energy consumption, ultimately reducing the network's lifespan. The attack could also disrupt the DODAG topology and create routing inconsistencies within the network, potentially resulting in severe damage and complete communication failures. In this paper the hybrid Decreased Rank Attack - Worst Parent Attack is referred to as DICR Attack (Decreased Increased Rank Attack), while the hybrid Decreased Rank Attack - Infinite Rank Attack is referred to as DIFR (Decreased Infinite Rank Attack).

II. STUDIED TOPOLOGY

IoT devices are typically implemented using specialized operating systems (OSs) to accommodate their limited resources. Prominent examples include Contiki OS and TinyOS, both available as open-source platforms. In our work, we used Contiki 3.0 OS that includes the Cooja network simulator, a tool designed to simulate and evaluate RPL-based IoT environments under various configurations.

As depicted in Figure 1, a grid topology consisting of 25 nodes was configured for each simulation. Node 1 serves as the root of the DODAG. This topology was chosen for its flexibility, enabling the attacker to move between locations and assess the attack's impact from various perspectives. The analysis considers the number of hops required to reach the sink, all while maintaining a consistent neighbour count of four. In the first scenario, the malicious node is positioned one hop from the sink. In the second scenario, the malicious node is situated two hops away, while in the third scenario the malicious node is located three hops from the sink.

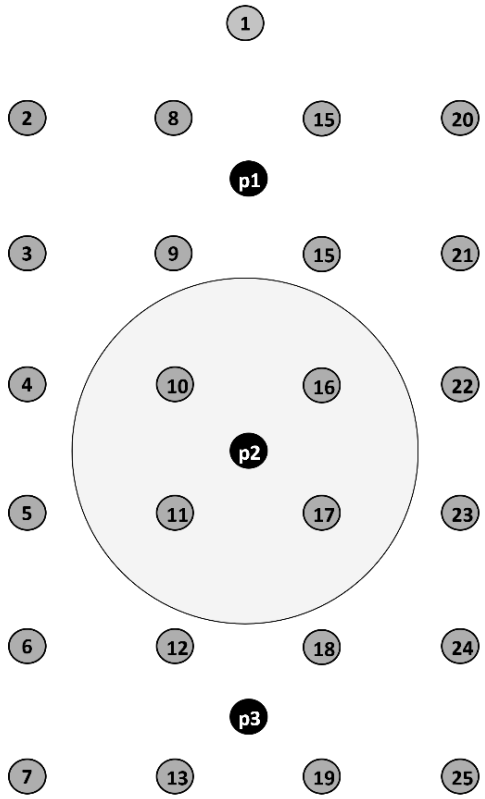

Fig.1. Studied Topology

TABLE 1
HARDWARE SPECIFICATION OF Z1 NODE

Parameter	Value
CPU idle current	0.426 mA
Current consumption in TX mode	17.4 mA
Current consumption in RX mode	18.8 mA
CPU power down current	0.020 mA
Maximum RAM size	8 kB
Maximum ROM size	92 kB
RTIMER_SECOND	32768 ticks /s

Each node was configured as a Zolertia Z1 mote, equipped with an MSP430 16-MHz MCU, 92KB of flash memory, 8KB of RAM, and a CC2420 transceiver. Across all experiments, the RPL protocol was used with the MRHOF objective function, employing ETX as the routing metric. Table 1 provides a summary of the key features of the used Z1 motes, while table 2 provide the configuration parameters used in all simulations. The setup involved configuring an RPL-UDP client on each non-sink RPL node to periodically transmit IoT data packets at an interval of approximately 30 seconds. All

transmitted data was ultimately received and processed by an RPL-UDP server operating at the sink node.

III. RESULTS AND DISCUSSION

Several network metrics were analyzed to comprehensively evaluate overall network performance, categorized as follows:

- QoS Performance: Latency and Packet Delivery Ratio (PDR).
- Network Overhead: Total RPL control packets (DIO, DAO, and DIS).
- Energy Efficiency: Energy consumption.
- Protocol Activity: Events such as preferred parent changes, local repairs, and loop occurrences.

These performance metrics were calculated using a clear methodology:

- PDR: Defined as the ratio of successfully received data messages at the sink node to the total messages transmitted by non-sink RPL nodes.
- Latency: Measured as the average time taken for data messages from RPL nodes to the sink, excluding lost or dropped messages.
- Control Overhead: Determined by counting all RPL control messages exchanged (generated and forwarded) across the network.

Energy Consumption: Computed based on experimental data from the powertrace script using the formula:

$$ConsumeEnergy = \frac{energest_{value} * current * voltage}{Rtimer\_Second} \quad (1)$$

Here, energest_value represents the total ticks for each energy mode, while Rtimer, current, and voltage were specific to the Z1 motes, as detailed in Table 2.

TABLE 2
SIMULATION PARAMETERS

Parameter	Values
Network layer Protocol	RPL
Operating System	Contiki 3.0.
Simulator	Contiki Cooja
Emulated nodes	Z1
MAC layer Protocol	IEEE 802.15.4
Radio model	UDGM
Simulation area	200 m × 200 m
Simulation time	20 minutes
Data transmission	1 Packet / 30s
Objective function	MRHOF
Malicious nodes	1
Legitimate nodes	24
TX range	50 m
Interference range	100 m

A. Overhead Results

The results in Table 3 demonstrate the significant impact of hybrid rank attacks on increasing network overhead. The DIFR attack caused a substantial rise in the generation of control packets, compared to DICR attack. The impact becomes higher when the malicious node is placed away from the sink. A Total overhead of 5969 messages is recorded in the DIFR arrack in the third scenario (S3) when the malicious node is placed 5 hops from the sink, where the DICR attack shows a total of 5797 messages for the same scenario. Compared to the attack free scenario, the overall control traffic surged by over 390% and 237 % in DIFR and DICR, respectively. The standard RPL protocol struggled to handle the attack, making it difficult to maintain protocol overhead at reasonable levels.

This increase was primarily due to the destabilizing effect of the attack, which caused network partitioning and frequent local repairs. These disruptions heightened DIO and DAO communications across various paths within the DODAG, ultimately reaching the sink node. Notably, DAO messages were the primary contributors to the overall rise in protocol overhead. For instance, in Scenario 3 (S3), the number of DAO messages increased to over 15 times that of the attack-free scenario. This dominance of DAO messages can be attributed to the frequent detachment and re-attachment of targeted RPL nodes, which reset their trickle timers and triggered the transmission of DIO and DAO messages at very short intervals, as table 4 depicts. These disruptions were often synchronized across multiple nodes, amplifying the attack's impact and extending its effects throughout the network. Based on table 4, the highest recorded timer rest is in the third scenario of the DIFR attack, where a total of 1980 timer resets is recorded, mainly because of parents switching.

B. Energy Consumption Results

Figure 2 illustrates the adverse impact of the DICR attack and the DIFR rank attacks on energy consumption. The results demonstrate that the DIFR has a more significant impact in all scenarios. Specifically, it results in total energy consumptions of 130.07 joules and 124.46 joules for the second and third scenarios, respectively, compared to 116.37 joules and 122.1 joules for the DICR attack. For both attacks, the second scenario exhibits the highest energy consumption.

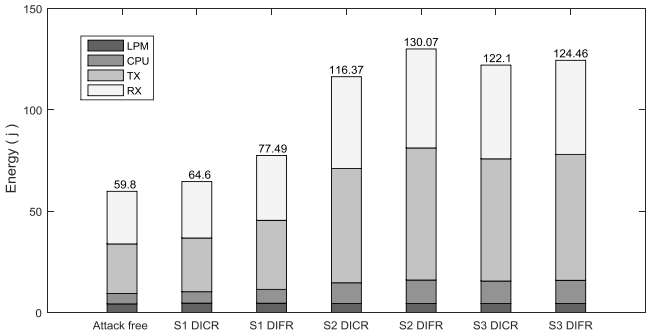

Fig.2. Energy Consumption Results of Hybrid Rank Attaks

Overall, the DIFR attack causes a noticeable increase in energy consumption, with an observed rise of 117% compared to the attack free scenario. These findings highlight the damaging effect of the DIFR attack, particularly when conducted in the middle of the topology. Such an increase in energy consumption at the RPL nodes would ultimately reduce the network's lifetime.

TABLE 3

NETWORK OVERHEAD RESULTS OF HYBRID RANK ATTACKS

Scenario		Sent Messages						Total
		Generated				Forwarded		
		DIS	DIO	DAO	No-Path DAO	DAO	No-Path DAO	
Attack free		24	573	249	59	808	80	1769
1 hop (S1)	DICR	25	549	252	49	877	99	1826
	DIFR	25	826	454	80	1233	128	2721
3 hops (S2)	DICR	26	1309	741	336	1764	339	4489
	DIFR	27	1858	888	513	1643	406	5308
5 hops (S3)	DICR	25	1749	958	753	1832	505	5797
	DIFR	25	2023	972	807	1685	482	5969

TABLE 4

NETWORK OVERHEAD RESULTS OF HYBRID RANK ATTACKS

	Attack free	DICR	DIFR	DICR	DIFR	DICR	DIFR
Infinite rank received	15	12	75	68	352	207	634
Changed preferred parent	41	49	80	336	523	753	806
Local repair	8	2	5	9	19	14	16
Loops	14	11	27	221	302	484	524
Total	78	74	187	634	1196	1458	1980

C. PDR and Latency Results

The Packet Delivery Ratio (PDR) quantifies the percentage of data packets successfully transmitted by network nodes and received at the root node, serving as a key indicator of the network's end-to-end link reliability. Conversely, latency measures the average time required for data packets to travel from the network nodes to the root node, considering only successfully received packets and excluding those that are lost or dropped.

TABLE 5

QOS PERFORMANCE RESULTS OF HYBRID RANK ATTACK SCENARIOS

Scenario		PDR (%)	Latency (Sec)
Attack-free		94,3	0,77
S1	DICR	95	0,80
	DIFR	93	1,01
S2	DICR	69,2	1,64
	DIFR	61,7	1,50
S3	DICR	60,3	0,73
	DIFR	59,1	0,80

Table 5 presents a comparative analysis of average delay values (in seconds) and the recorded PDR for the studied scenarios. Overall, the DIFR shows the lowest PDR, for instance a ratio of 59,1 % is recorded in the third scenario. Notably, the impact on the delivery ratio mirrors the pattern observed in overhead metrics. On the other hand, the latency shows the lowest value where the malicious node is placed in the middle of the network; scenario 2 of the attack. The increase in latency for is primarily attributed to packet collisions and congestion caused by the network's elevated overhead, particularly at the forwarder nodes.

The comparison with other hybrid rank attacks, including the DICR model and DRA, was carried out in order to confirm the importance of the suggested DIFR attack. The findings unequivocally demonstrate that, in comparison to these earlier models, DIFR causes more disruption in all measured parameters, including overhead, energy consumption, latency, and packet delivery ratio. Even when the malicious node is located further away from the sink, DIFR shows a wider destabilizing effect than DRA and DICR, which show localized effects. This increased disruption highlights the complexity of the attack and emphasizes how urgent it is to create stronger defenses. According to these results, DIFR is one of the most effective cutting-edge attack techniques assessed in RPL-based IoT environments.

The study's findings highlight the serious and extensive effects that hybrid rank attacks have on RPL-based IoT networks. Specifically, the proposed DIFR attack shows a significant decline in all important performance metrics, including an increase in overhead of 390% and an increase in energy consumption of 117%. Network congestion brought on by such high control message traffic eventually depletes node resources by causing frequent local repairs. The attack's efficacy in impairing the dependability of data transmission is demonstrated by the steady decline in the packet delivery ratio (up to 37%). Furthermore, real-time communication is compromised by the 95% latency spike, which is essential for critical applications like industrial monitoring and healthcare. These findings demonstrate the vulnerability of existing RPL

implementations to heightened threats in addition to validating the effectiveness of the novel hybrid attack. The attack's resilience is further supported by the impact's consistency across various node locations in the topology. The urgent need for cutting-edge security improvements to protect IoT infrastructure is highlighted by this study. IoT networks' dependability and durability are still seriously threatened in the absence of such safeguards.

IV. CONCLUSIONS

The IoT has experienced rapid expansion in recent decades, driving significant innovation and enabling highly integrated solutions. IoT services have become an essential part of daily life, and the number of IoT devices is expected to grow exponentially in the coming years. However, these devices are highly susceptible to various forms of cyberattacks. Identifying and addressing these threats is particularly challenging due to the sheer scale and diversity of IoT devices. IoT networks consist of heterogeneous devices and systems operating together, characterized by extensive interconnectivity and substantial data exchange. This dynamic environment presents significant security challenges, as safeguarding such networks becomes increasingly complex.

This paper presents a comprehensive analysis of a newly proposed hybrid rank attack, which builds upon the well-known Decreased Rank Attack (DRA) and Infinite Rank Attack (IRA). The primary objective of this hybrid attack is to destabilize the network by forcing victim nodes to frequently switch their preferred parents and repeatedly initiate local repairs. This behaviour leads to the generation of an excessive volume of unnecessary control messages across the network. The results reveal severe degradation in all key network metrics, highlighting the damaging impact of the proposed attack.

REFERENCES

[1] A. Hkiri, M. Karmani, O. B. Bahri, A. Mohammed Murayr, F. H. Alasmari, and M. Machhout, “RPL-Based IoT Networks under Decreased Rank Attack: Performance Analysis in Static and Mobile Environments,” *Computers, Materials & Continua*, vol. 78, no. 1, pp. 227–247, 2024, DOI:10.32604/cmc.2023.047087

[2] M. N. Bhuiyan, M. M. Rahman, M. M. Billah and D. Saha, "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, DOI: 10.1109/JIOT.2021.3062630

[3] F. Samie, L. Bauer and J. Henkel, "IoT Technologies for Embedded Computing: A Survey," *2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS)*, Pittsburgh, PA, USA, 2016, pp. 1-10., DOI: 10.1145/2968456.2974004

[4] H. Suo, J. Wan, C. Zou and J. Liu, "Security in The Internet of Things: A Review," *2012 International Conference on Computer Science and Electronics Engineering*, Hangzhou, China, 2012, pp. 648-651, DOI: 10.1109/ICCSEE.2012.373

[5] K. Prathapchandran, & T. Janani,"A Trust Aware Security Mechanism to Detect Sinkhole Attack in RPL-Based IoT Environment Using Random Forest – RFTRUST, " *Computer Networks*, vol. 198, 2021, DOI: 10.1016/j.comnet.2021.108413

[6] W.-T. Sung and Y.-C. Chiang, "Improved Particle Swarm Optimization Algorithm for Android Medical Care Iot Using Modified Parameters, " *Journal of Medical Systems*, vol. 36, no. 6, pp. 3755–3763, 2012, DOI: 10.1007/s10916-012-9848-9

[7] R. Yugha & S. Chithra, "A Survey on Technologies and Security Protocols: Reference for Future Generation IoT," *Journal of Network and Computer Applications*, vol. 169, 2020, DOI: 10.1016/j.jnca.2020.102763

[8] A. Wakili, S. Bakkali and A.E.H. Alaoui, "Machine Learning for QoS and Security Enhancement of RPL in IoT-Enabled Wireless Sensors", *Sensors International*, vol. 5, 2024, DOI: 10.1016/j.sintl.2024.100289

[9] H. Lamaazi & N.Benamar, "A Comprehensive Survey on Enhancements and Limitations of The RPL Protocol: A Focus on The Objective Function, " *Ad Hoc Networks*, vol. 96, DOI: 10.1016/j.adhoc.2019.102001

[10] M.E. Ekpenyong, D.E. Asuquo, I.J. Udo, S.A. Robinson and F.F. Ijebu, "IPv6 Routing Protocol Enhancements over Low-Power and Lossy Networks for IoT Applications: A Systematic Review," *New Review of Information Networking*, vol. 27, no. 1, pp. 30–68., 2022, DOI: 10.1080/13614576.2022.2078396

[11] A. Sharma, E. S. Pilli, A. P. Mazumdar and M. C. Govil, "A Framework to Manage Trust in Internet of Things," *2016 International Conference on Emerging Trends in Communication Technologies (ETCT)*, Dehradun, India, 2016, pp. 1-5, DOI: 10.1109/ETCT.2016.7882970

[12] J. Deogirikar and A. Vidhate, "Security Attacks in IoT: A Survey," *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, 2017, pp. 32-37, DOI: 10.1109/I-SMAC.2017.8058363

[13] M. Rouissat, M. Belkehir, M. Allel, A. Mokaddem, M. Bouziani and I.S. Alsukayti, "Exploring and Mitigating Hybrid Rank Attack in RPL-Based IoT Networks," *Journal of Electrical Engineering*, vol. *75, no.*3, pp. 204–213. DOI: 10.2478/jee-2024-0025