DOI: https://doi.org/10.57233/ihcfs.018

ISBN: 978-978-68-07775

BOOK OF PROCEEDINGS

IHCFS – 2025 WEBSITE: fos.fugusau.edu.ng

1ST INTERNATIONAL HYBRID CONFERENCE OF FACULTY OF SCIENCE

(A PUBLICATION OF FACULTY OF SCIENCE, FEDERAL UNIVERSITY GUSAU, NIGERIA)

COMPARATIVE EVALUATION OF RANK ATTACK VARIANTS IN STATIC, MOBILE AND HYBRID NETWORK ENVIRONMENT

Shamsuddeen Ismail Mohammad[1*], Faisal Ali Garba[2], Jameel Shehu Yalli[3], Yahaya Aliyu Mafindi[4], Aliyu Usman Shehu[5], Zara Sakanau[6],

Biometric Solutions, Human Capital Managers, Gombe, Nigeria[1]

Phoenyx Security, Kano, Nigeria[2]

Department of Computer Science, Federal University Gusau, Zamfara, Nigeria[3]

Information Technology Department, 3logy Limited, Abuja, Nigeria[4]

Department of Computer Science, Ibrahim Badamasi Babangida University, Lapai[5]

Department of Computer Science, Kaduna State University, Kaduna, Nigeria[6]

***Corresponding author:alifa2try@gmail.com**

ABSTRACT

Manipulating the RPL rank field remains a highly effective strategy for compromising IPv6 Low-Power and Lossy Networks (LLNs). Existing studies, however, usually analyse only one attack variant or a single mobility regime, providing limited guidance for practitioners. This work offers a comparative assessment of three rank-based attacks— Rank Decrease (low-rank lure combined with selective forwarding), Rank Increase (high-rank repulsion), and Worst Parent (malicious parent inflation)—across static, mobile, and hybrid (50% mobile) topologies. An open-source Python/SimPy simulator executes a full factorial design (3variants×3mobility regimes×3random seeds). The evaluation considers Packet-Delivery Ratio(PDR), average end-to-end delay(AE2ED), mean hop count, control-plane overhead, and approximate energy consumption.In static networks, RankDecrease reduces PDR by approximately 92%, Rank Increase by 42%, while WorstParent preserves delivery yet raises energy usage by about 10% owing to additional DIO traffic. Under full mobility, RankIncrease and WorstParent self-heal (PDR≈1.0), whereas RankDecrease still suppresses ~99% of packets; hybrid performance falls between these extremes.The study delivers (i) a systematic taxonomy that links attack semantics to observed impairments, (ii) the first side-by-side evaluation of all three variants under heterogeneous mobility, and (iii) design recommendations—dynamic rank-sanity checks and adaptive parent-switch thresholds—that mitigate each attack with minimal energy overhead.

Keywords: RPL, rank, mobility, IoT, routing

1.0 INTRODUCTION

Routing Protocol for Low-Power and Lossy Networks (RPL) organises Low Power and Lossy Networks (LLNs) into a Destination Oriented Directed Acyclic Graph (DODAG), where each node advertises a rank derived from hop count, Expected Transmission Count (ETX), or other metrics. Rank appears in every DODAG Information Object (DIO) message and drives parent selection, with Objective Function 0 (OF0) and Minimum Rank Hysteresis Objective Function (MRHOF) mapping link metrics into rank while reducing frequent parent changes. However, because RPL provides no cryptographic protection for rank, an insider can advertise false values—decreasing rank to attract traffic or increasing it to repel children and stretch paths. These manipulations lead to sub-optimal routing, loops, control-plane churn, and energy waste, and hybrid attacks combining rank decrease and selective forwarding worsen impact. Prior work generally studies one attack per scenario: Bang & Rao (2022) observed 7–13% Packet Delivery Ratio (PDR) loss under decreased rank in static and mobile networks; Bang & Rao (2023) compared decreased vs. increased rank in smart homes and found inflated control and

DOI: https://doi.org/10.57233/ihcfs.018

ISBN: 978-978-68-07775

BOOK OF PROCEEDINGS

energy overheads; Hkiri et al. (2024) studied decreased rank under mobility and reported stronger PDR degradation; Al Qaisi et al. (2024) evaluated three scenarios only on static grids; and Nejad et al. (2024) showed mobility amplifies rank manipulation by exposing parent-selection weaknesses. Countermeasures include ETX/metric-guards (Ghaleb et al., 2023), reputation-based filters such as LEACE (Rouissat et al., 2024), and intrusion-detection approaches like EMBOF-RPL and SVELTE, though most target only one variant and mainly static settings. Al Qaisi et al. (2024) notes no study compares decreased, increased, and worst-parent attacks across static, mobile, and hybrid deployments; our work fills this gap through tri-variant comparison, mobility-aware experimentation, unified metrics (PDR, AE2ED, hop count, control overhead, energy), and an open-source Python/SimPy model for reproducible exploration.

2.0 MATERIALS AND METHODS

We implemented the scenarios inpure Python using SimPy. SimPy offers a discrete-event kernel that is lightweight, deterministic, and easy to couple with custom energy or attack modules; a full 3600s run with 40 nodes completes in < 2s on a laptop, enabling hundreds of Monte-Carlo repetitions.Using SimPy thus lets us to sweep node count and attacker ratio quickly, inject mobility models directly in Python and export per-event logs that drive the energy model.We still align our parameters with those reported in recent Cooja studies to keep results comparable. Table 1 enumerates the network scenarios used for the experiments.

Table 1: Network Scenarios used for the experiments

Scenario	Topology & Node count	Mobility Model	Rationale
Static	30 nodes, random uniform placement in a 200 × 200m area	none	Baseline to isolate pure control-plane impact.
Mobile	30 nodes, same random start positions	Random-Waypoint, mean speed = 0.5 ms^{-1}, pause = 10s	Follows Prajisha and Vasudevan (2025) mobility parameters; emulates personnel-carried sensors.
Hybrid	1:3 mobile:static ratio (8 mobile, 22 static)	Mobile subset follows the same RWP model	Captures mixed industrial and wearable deployments.

2.1 Parameter Matrix

We vary one independent factor—the presence/absence of attackers—while keeping node count and simulation time fixed. Table 2 lists the concrete setting used for all three mobility regimes.

Table 2: Parameter Matrix used in the Simulation

Parameter	Value	Rationale
Node count *N*	30	Matches Prajisha and Vasudevan (2025) evaluation of MSecTrust (30-node LLN).
Attacker ratio	0% (baseline) or 10% (3 malicious nodes)	Keeps attacker density in line with the 1:10 ratio recommended for rank-attack benchmarks.
Simulation time	3600s	Long enough for steady-state parent selection and full traffic cycle. Matches Prajisha and Vasudevan (2025) simulation duration of MSecTrust
Random seeds	1,2,3	Captures run-to-run variability.

DOI: https://doi.org/10.57233/ihcfs.018

ISBN: 978-978-68-07775

BOOK OF PROCEEDINGS

IHCFS – 2025 WEBSITE: fos.fugusau.edu.ng

Area	200×200m	Provides average neighbour degree ≈ 6 at 50m range (consistent with Prajisha et al., (2025)).
Deployment	Random uniform	Avoids grid artefacts.
Mobility	see Section 5.2	Static / RWP / hybrid.
Radio range	50m	Same as Hkiri *et al*., (2024).

2.2 Performance Metrics

These definitions mirror the logic embedded in the custom PerformanceMonitor class and ensure that every mobility regime and attack variant is evaluated with exactly the same measurement pipeline.

Metric	Operational definition (as computed in our SimPy post-processor)
Packet-Delivery Ratio (PDR)	Ratio of data packets received by the sink to data packets generated at sources during the run.
Average End-to-End Delay (AE2ED)	Mean of individual packet latencies, where latency = (arrival time – creation time) for each successfully delivered packet.
Average Hop-count per Packet (AHP)	Total hop count accumulated by all delivered packets divided by the number of delivered packets. Each hop is counted when a forwarding node transmits the packet.
Control-plane overhead	Total number of DIO control packets transmitted network-wide in one simulation run. (DAO and DIS are not generated in our model and therefore not counted.)
Energy consumption (approx.)	Simple additive model:+ 0.25 u for every data-packet transmission, + 0.05u for every data-packet reception, and +0.10u for every DIO transmission. No idle listening, processing, or ACK cost is included.
Throughput	delivered packets × 64 bytes×8bits divided by the active traffic interval (first to last packet-creation timestamp), expressed in bits s^{-1}.

3.0 RESULTS AND DISCUSSIONS

3.1 Static Scenario

a. Rank Decrease (Table 3)

Selective forwarding combined with the low-rank lure devastates reliability: PDR falls from 1.00 to an average of 0.08, with one seed reaching complete delivery failure (0%). Because so few packets arrive, AE2ED and AHP lose diagnostic value—apparent “improvements” (e.g., 0s delay) reflect the near-empty denominator. Control traffic rises by ≈11%, driving a 13–24% energy increase, while throughput drops by three to five orders of magnitude.

Table 3: Rank Decrease vs. baseline (static scenario)

Metric	Baseline (Seed = 1)	Rank Decrease (Seed = 1)	Baseline (Seed = 2)	Rank Decrease (Seed = 2)	Baseline (Seed = 3)	Rank Decrease (Seed = 3)
PDR	1.00	0.04	1.00	0.20	1.00	0.00
AE2ED	0.0552	0.0553	0.1763	0.0856	0.1494	0.0000
AHP	1.00	1.00	3.28	1.57	2.77	0.00
Control Packets	90912	100862	106545	117191	95183	105124
Energy Used	9126.30	11295.10	14020.20	12848.95	10720.70	11400.45
Throughput	59904.00	16.87	1750528.00	86.94	740864.00	0.00

b. Rank Increase (Table 4).

PDR is highly seed-dependent: one run collapses to 0.04, one is unaffected, and one settles at 0.71. The variant therefore behaves nondeterministically in dense static meshes, but when PDR degrades it does so without inflating delay or hop count, confirming that most losses stem from route stretch and TTL expiry rather than loops. Control overhead and energy both rise by ≈12%, matching the fixed 5s interval of forged DIOs.

DOI: https://doi.org/10.57233/ihcfs.018

ISBN: 978-978-68-07775

BOOK OF PROCEEDINGS

IHCFS – 2025 WEBSITE: fos.fugusau.edu.ng

Table 4: Rank Increase vs. baseline (static scenario)

Metric	Baseline (Seed = 1)	Rank Increase (Seed = 1)	Baseline (Seed = 2)	Rank Increase (Seed = 2)	Baseline (Seed = 3)	Rank Increase (Seed = 3)
PDR	1.00	0.04	1.00	1.00	1.00	0.71
AE2ED	0.0552	0.0553	0.1763	0.1763	0.1494	0.1495
AHP	1.00	1.00	3.28	3.28	2.77	2.77
Control Packets	90912	100862	106545	117191	95183	105124
Energy Used	9126.30	11295.10	14020.20	15084.50	10720.70	11864.40
Throughput	59904.00	16.87	1750528.00	1750528.00	740864.00	208.75

c. Worst Parent (Table 5)

All reliability and latency metrics remain identical to baseline across seeds. The only penalties are an 11% increase in DIO traffic and a 9–12% rise in energy. The attacker's deliberate choice of a high-rank parent inflates overhead but is quickly corrected by RPL's periodic parent-check, explaining the lack of data-plane impact.

Table 5: Worst Parent vs. baseline (static scenario)

Metric	Baseline (Seed = 1)	Worst Parent (Seed = 1)	Baseline (Seed = 2)	Worst Parent (Seed = 2)	Baseline (Seed = 3)	Worst Parent (Seed = 3)
PDR	1.00	1.00	1.00	1.00	1.00	1.00
AE2ED	0.0552	0.0553	0.1763	0.1762	0.1494	0.1495
AHP	1.00	1.00	3.28	3.28	2.77	2.77
Control Packets	90912	100862	106545	117191	95183	105124
Energy Used	9126.30	10121.30	14020.20	15080.90	10720.70	11715.40
Throughput	59904.00	59904.00	1750528.00	1749504	740864.00	740864.00

3.2 Mobile Scenario

a. Rank Decrease (Table 6)

Mobility does not rescue delivery. PDR is ≤ 0.01 in every seed, showing that once victims are lured they continue to meet dropping parents even as the topology evolves. Control overhead grows by 10% and energy by 6–9%, while throughput collapses by six orders of magnitude.

Table 6: Rank Decrease vs. baseline (Mobile Scenario)

Metric	Baseline (Seed = 1)	Rank Decrease (Seed = 1)	Baseline (Seed = 2)	Rank Decrease (Seed = 2)	Baseline (Seed = 3)	Rank Decrease (Seed = 3)
PDR	1.00	0.00	1.00	0.00	1.00	0.01
AE2ED	0.0718	0.0590	0.0673	0.0500	0.0823	0.1279
AHP	1.30	1.10	1.21	1.00	1.51	2.26
Control Packets	142798	157443	139903	157998	145377	159780
Energy Used	15667.30	16551.55	15279.10	16641.10	16143.60	16814.00
Throughput	1816576.00	1.44	1818112.00	0.72	1812480.00	2.73

b. Rank Increase (Table 7).

Under continuous motion the Rank Increase (RI) attack does not affect delivery: PDR remains 1.00 for all three seeds. Mean delay and hop count climb only marginally (≤ 3%), indicating that the longer detours caused by the attacker's high-rank advertisement are quickly abandoned as nodes move. The main penalty is efficiency: forged DIOs push control traffic up by ~11% (e.g., 142798→157443 packets in Seed 1), which in turn raises network-wide energy consumption by 9–14%. Throughput is generally comparable with baseline but can

DOI: https://doi.org/10.57233/ihcfs.018

ISBN: 978-978-68-07775

BOOK OF PROCEEDINGS

IHCFS – 2025 WEBSITE: fos.fugusau.edu.ng

swing higher or lower depending on how long the initial parent-churn phase lasts (Seed 2 shows a slight gain, Seeds 1 and 3 a drop).

Table 7: Rank Increase vs Baseline (Mobile Scenario)

Metric	Baseline (Seed = 1)	Rank Increase (Seed = 1)	Baseline (Seed = 2)	Rank Increase (Seed = 2)	Baseline (Seed = 3)	Rank Increase (Seed = 3)
PDR	1.00	1.00	1.00	1.00	1.00	1.00
AE2ED	0.0718	0.0735	0.0673	0.0697	0.0823	0.0834
AHP	1.30	1.34	1.21	1.25	1.51	1.53
Control Packets	142798	157443	139903	157998	145377	159780
Energy Used	15667.30	17166.60	15279.10	17132.40	16143.60	17605.60
Throughput	1816576.00	259364.57	1818112.00	1819136.00	1812480.00	129499.43

c. Worst Parent (Table 8)

The Worst Parent (WP) variant shows an almost identical pattern to RI for mobile nodes. PDR stays at 1.00 and both AE2ED and AHP creep upward by about 2%. Because the attacker continually re-selects a high-rank parent, it triggers the same 11% bump in DIO transmissions and a corresponding 9–12% rise in energy. Throughput, however, tracks baseline much more closely than in the RI case, suggesting that WP's impact is confined almost entirely to control-plane overhead rather than data-plane congestion.

Table 8: Worst Parent vs. baseline (Mobile Scenario)

Metric	Baseline (Seed = 1)	Worst Parent (Seed = 1)	Baseline (Seed = 2)	Worst Parent (Seed = 2)	Baseline (Seed = 3)	Worst Parent (Seed = 3)
PDR	1.00	1.00	1.00	1.00	1.00	1.00
AE2ED	0.0718	0.0735	0.0673	0.0697	0.0823	0.0833
AHP	1.30	1.34	1.21	1.25	1.51	1.53
Control Packets	142798	157443	139903	157998	145377	159780
Energy Used	15667.30	17164.50	15279.10	17132.40	16143.60	17602.50
Throughput	1816576.00	1815552.00	1818112.00	1819136.00	1812480.00	1812480.00

3.3 Hybrid Scenario

a. Rank Decrease (Table 9)

Reliability remains poor (PDR 0–0.02) despite half the nodes being mobile, reinforcing that selective dropping is the decisive factor. The delay metric again becomes unreliable under heavy loss. Control and energy overheads rise modestly (5–10%), implying that most energy that would have been spent forwarding data is saved by early drops.

Table 9: Rank Decrease vs. baseline (Hybrid Scenario)

Metric	Baseline (Seed = 1)	Rank Decrease (Seed = 1)	Baseline (Seed = 2)	Rank Decrease (Seed = 2)	Baseline (Seed = 3)	Rank Decrease (Seed = 3)
PDR	1.00	0.00	1.00	0.02	1.00	0.01
AE2ED	0.0822	0.0600	0.0794	0.0617	0.0906	0.0821
AHP	1.49	1.11	1.44	1.09	1.66	1.39
Control Packets	115416	122552	128352	141548	127775	131435
Energy Used	13124.10	13119.35	14373.00	15005.75	14548.70	14033.65
Throughput	1817088.00	1.29	1819136.00	9.21	1817088.00	5.47

b. Rank Increase (Table 10)

Within the hybrid topology, the RankIncrease (RI) attack does not compromise reliability: PDR remains at 1.00 for all seeds. Nevertheless, the average end-to-end delay and mean

DOI: https://doi.org/10.57233/ihcfs.018

ISBN: 978-978-68-07775

BOOK OF PROCEEDINGS

hop count rise modestly—by approximately 2–4%—reflecting occasional route detours before nodes stabilise on acceptable parents. The forged high-rank advertisements also trigger additional DIO exchanges, producing an ~8% increase in control overhead and network-wide energy consumption.

Table 10: Rank Increase vs Baseline (Hybrid Scenario)

Metric	Baseline (Seed = 1)	Rank Increase (Seed = 1)	Baseline (Seed = 2)	Rank Increase (Seed = 2)	Baseline (Seed = 3)	Rank Increase (Seed = 3)
PDR	1.00	1.00	1.00	1.00	1.00	1.00
AE2ED	0.0822	0.0841	0.0794	0.0769	0.0906	0.0914
AHP	1.49	1.53	1.44	1.39	1.66	1.67
Control Packets	115416	122552	128352	141548	127775	131435
Energy Used	13124.10	13885.40	14373.00	15640.85	14548.70	14925.20
Throughput	1817088.00	1818112.00	1819136.00	202126.22	1817088.00	1818624.00

c. Worst Parent (Table 11).

The Worst Parent (WP) variant exhibits an almost identical performance profile. Packet delivery is fully maintained (PDR= 1.00), while latency and hop count show the same 2–4% uptick. Control-plane activity and energy usage likewise climb by roughly 8%, attributable to repeated parent reselection caused by the attacker's deliberate choice of high-rank neighbours. Thus, in the hybrid regime, both RI and WP impose an energy and overhead penalty without inflicting the severe reliability loss observed for RankDecrease.

Table 11: Worst Parent vs. baseline (Hybrid Scenario)

Metric	Baseline (Seed = 1)	Worst Parent (Seed = 1)	Baseline (Seed = 2)	Worst Parent (Seed = 2)	Baseline (Seed = 3)	Worst Parent (Seed = 3)
PDR	1.00	1.00	1.00	1.00	1.00	1.00
AE2ED	0.0822	0.0841	0.0794	0.0768	0.0906	0.0913
AHP	1.49	1.53	1.44	1.39	1.66	1.67
Control Packets	115416	122552	128352	141548	127775	131435
Energy Used	13124.10	13885.40	14373.00	15638.00	14548.70	14922.50
Throughput	1817088.00	1818112.00	1819136.00	1818624.00	1817088.00	1817600.00

4.0 CONCLUSION

This study delivers the first direct comparison of three rank-manipulation attacks—Rank Decrease, Rank Increase, and Worst Parent—across static, mobile, and hybrid deployments of the Routing Protocol for Low-Power and Lossy Networks (RPL). Using a lightweight Python/SimPy simulation framework, we evaluated each attack in terms of packet-delivery ratio, average end-to-end delay, hop count, control-plane overhead, and approximate energy consumption. Results show that Rank Decrease is the most harmful variant, reducing delivery by about 92% in static networks and continuing to suppress roughly 99% of packets under mobility, confirming its status as a critical reliability threat. In contrast, Rank Increase significantly affects only static scenarios, where it reduces delivery by 42% and slightly increases delay and hop count due to path stretching, but mobility enables natural route repair. Worst Parent does not reduce packet-delivery ratio or delay in any scenario yet consistently increases DIO transmission and energy consumption by about 10–12%, demonstrating that it is primarily an efficiency degradation attack. Overall, the findings highlight the need for defence mechanisms tailored to specific attack behaviours, such as rank-floor validation for Rank Decrease

and adaptive parent-switch and Trickle-control techniques to mitigate Rank Increase and Worst Parent.

REFERENCES

Al-Qaisi, L., Hassan, S., & Zakaria, N.H. (2024). *Performance evaluation of rank attack impact on routing protocol in low-power and lossy networks*. Indonesian Journal of Electrical Engineering and Computer Science, 36(1), 242-251.

Bang, A., & Rao, U. P. (2022). Impact analysis of rank attack on RPL-based 6LoWPAN networks in Internet of Things and aftermaths. *Arabian Journal for Science and Engineering,48*, 2489-2505.

Bang, A., & Rao, U. P. (2023). Performance evaluation of RPL protocol under decreased and increased rank attacks: A focus on smart home use-case. *SN Computer Science, 4*, 329.

Ghaleb, B., Al-Dubai, A., Hussain, A., Ahmad, J., Romdhani, I. I., & Jaroucheh, Z. (2023). Resolving the decreased rank attack in RPL's IoT networks. *IEEE Transactions/Conference Paper* (in press).

Hkiri, A., Karmani, M., Ben Bahri, O., Murayr, A. M., Alasmari, F. H., & Machhout, M. (2024). RPL-based IoT networks under decreased rank attack: Performance analysis in static and mobile environments. *Computers, Materials & Continua, 78*(1), 228-243.

Muzammal,S. M., Murugesan, R. K., Jhanjhi, N. Z., Humayun, M., Ibrahim, A. O., & Abdelmaboud, A. (2022). A trust-based model for secure routing against RPL attacks in Internet of Things. Sensors, 22(18), 7052. https://doi.org/10.3390/s22187052

Nejad, F. V., Sadeghi, M. M. G., & Rezvani, M. H. (2024). Analysis of decreased rank attack on RPL-based IoT networks. In *Proceedings of the 10th International Conference on Web Research* (pp. 40-47). IEEE

Prajisha, C., & Vasudevan, A. R. (2025). MSecTrust: A mobility-aware secure trust-based routing protocol for RPL-based Internet of Things. Journal of Network and Systems Management, 33, Article 40. https://doi.org/10.1007/s10922-025-09913-4.

Rouissat, M., Mohammed, B., Mokaddem, A., & Merahi, B. (2024). Exploring and mitigating hybrid rank attack in RPL-based IoT networks. *Journal of Electrical Engineering, 75*(3), 203-212.

Subhash, P. (2023). rankIMPACT: A study of rank attacks impact over RPL-based Internet of Things networks. In *IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)* (Workshop 3).

Zilberman, A., Dvir, A., & Stulman, A. (2025). *IPv6 RPL security vulnerabilities and mitigation techniques: A survey*. *ACM Computing Surveys*.