UMYU Scientifica, Vol. 5 NO. 2, June 2026, Pp 400 – 407
https://doi.org/10.56919/usci.2652.036
ISSN: 2955 – 1145 (print); 2955 – 1153 (online)
A periodical of the Faculty of Natural and Applied Sciences, UMYU, Katsina

ORIGINAL RESEARCH ARTICLE

Comprehensive Performance Evaluation of Wormhole Attack on RPL across Diverse IoT Network Environments

Emmanuel Abimbola Olowookere[1], Adamu Abubakar Isah[2], David Adetunji Ademilua[3], Edoise Areghan[4], Yahaya Mafindi Aliyu[5], Nabeela Adebola[6] and Faisal Ali Garba[7]*

[1]Institute of Leadership Manpower and Management Development, Eleyele, Ibadan 200116, Oyo State, Nigeria
[2]Computer Science Department, Ibrahim Badamasi Babangida University, Lapai, Nigeria
[3]Computer Information Systems and Information Technology, University of Central Missouri, USA
[4]Cybersecurity and Information Assurance, University of Central Missouri, USA
[5]IT Department, 3logy Limited, Abuja, Nigeria
[6]Department of Engineering, University of Salford, Salford M5 4WT, United Kingdom
[7]Department of Computer Science, Sa'adatu Rimi College of Education, Kano, Nigeria

ABSTRACT

The Routing Protocol for Low-Power and Lossy Networks (RPL) is a foundational IPv6 routing standard for IoT deployments, yet it remains vulnerable to wormhole attacks that exploit its rank-based topology construction. Despite growing awareness of this threat, systematic empirical data on how tunnel multiplicity, tunnel behaviour, and attacker count jointly affect network-layer performance metrics have been lacking. This study addresses that gap through a replicatable SimPy-based simulation framework that (i) embeds an arbitrary number of wormhole pairs in an RPL Destination-Oriented Directed Acyclic Graph (DODAG), (ii) models two tunnel behaviours—shortcut (forwarding) and blackhole (dropping)—and (iii) records six performance metrics: Packet Delivery Ratio (PDR), average end-to-end delay, hop count, control packet overhead, energy consumption, and throughput. Experiments were conducted across five independent simulation runs per condition using orthogonal topology and traffic random seeds, with attacker counts of 4, 8, and 12 nodes. Statistical rigour was ensured through mean ± standard deviation reporting and one-way ANOVA across attacker levels. In shortcut mode, ANOVA revealed significant effects of attacker count on PDR ($p = 0.037$), delay ($p = 0.012$), hop count ($p = 0.011$), and throughput ($p = 0.037$). Blackhole mode results were more variable across seeds, reflecting topology-dependent susceptibility. Shortcut tunnels consistently improved apparent routing efficiency—PDR = 0.60–0.76 and throughput 205–260 b/s—while concealing their potential for disruption, making them particularly difficult to detect. These findings quantify the dual nature of wormhole attacks and motivate trust-zone placement and lightweight consistency checks as countermeasures before scaling RPL deployments beyond modest node counts.

ARTICLE HISTORY

Received November 08, 2025
Accepted June 29, 2026
Published June 30, 2026

KEYWORDS

RPL Security, Wormhole Attack, Low-Power and Lossy Networks, IoT Routing Vulnerabilities, SimPy Simulation, Statistical Evaluation

INTRODUCTION

Low-Power and Lossy Networks (LLNs) consist of battery-operated, memory-constrained sensor and actuator nodes communicating over error-prone links. To provide IPv6 connectivity in such environments, the Internet Engineering Task Force standardised the Routing Protocol for Low-Power and Lossy Networks (RPL). Perazzo et al. (2018) highlighted that RPL organises nodes into a Destination-Oriented Directed Acyclic Graph (DODAG) rooted at a border router, relies on rank values to avoid loops, and supports both storing and non-storing modes so that memory-constrained devices can participate in multi-hop routing without maintaining full routing tables. Zahra et al. (2022) reported that RPL's lightweight control overhead and native 6LoWPAN support have made it the de-facto routing layer for smart-city, industrial, and agricultural IoT deployments.

Among the various attacks on RPL, the wormhole attack is particularly dangerous because it operates below the network layer, exploiting topological manipulation rather than cryptographic weaknesses. In a wormhole attack, two colluding nodes establish an out-of-band tunnel and advertise artificially low ranks, drawing unsuspecting nodes to route large fractions of traffic through the tunnel. This enables eavesdropping, selective packet dropping, or traffic analysis. Perazzo et al. (2018) demonstrated that classical cryptographic defences fail against wormhole

Correspondence: Faisal Ali Garba. Department of Computer Science, Sa'adatu Rimi College of Education, Kano, Nigeria. ✉ alifa2try@gmail.com.

How to cite: Olowookere, E. A., Isah, A. A., Ademilua, D. A., Areghan, E., Aliyu, Y. M., Adebola, N., & Ali, F. G. (2026). Comprehensive Performance Evaluation of Wormhole Attack on RPL across Diverse IoT Network Environments. *UMYU Scientifica*, 5(2), 400 – 407. https://doi.org/10.56919/usci.2652.036

attacks precisely because no packet forgery occurs. Samuel et al. (2020) further showed that round-trip time and hop-count anomalies remain subtle in lossy links, making detection difficult even with dedicated methods. Trust-based detection (Javed et al., 2023) and hybrid RSSI–hop-count intrusion detection schemes (Bhosale & Sonavane, 2021) have been explored, underscoring both the difficulty and the continuing relevance of the threat.

Despite this body of work, most evaluations are limited to single-tunnel scenarios, small testbeds, or detection-accuracy metrics. The large-scale performance impact of multiple simultaneous wormhole tunnels—measured through PDR, delay, hop count, control overhead, energy, and throughput—under varied attacker counts and topology dynamics remains under-explored (Khan & Lee, 2013). Furthermore, comparative baselines that separate the shortcut benefit of forwarding tunnels from the blackhole damage of dropping tunnels are rarely reported (Burange & Deshmukh, 2020). A critical additional gap is the absence of statistical rigour: published simulation studies almost universally report single-run results, making it impossible to assess the generalisability of observed trends.

1.1 Contributions

To address these gaps, this study makes the following contributions:

- **Statistically rigorous simulation framework:** A SimPy-based RPL simulator is extended to run five independent replications per condition using orthogonal topology and traffic random seeds, enabling mean ± SD reporting and one-way ANOVA.
- **Extended attacker density:** Experiments cover 4, 8, and 12 attacker nodes, establishing a scalability curve that was absent in prior work.
- **Mode-separated analysis:** Shortcut and blackhole tunnel modes are evaluated in isolation, quantifying the deceptive efficiency gains of forwarding wormholes alongside the reliability damage of dropping wormholes.
- **Comprehensive metric suite:** PDR, average end-to-end delay, hop count, control packet overhead, energy consumption, and throughput are reported, providing a holistic view of attack impact across RPL performance dimensions.

1.2 Overview of RPL Security Mechanisms

RPL provides basic security through message integrity verification and replay protection; however, these measures address external passive threats and do not mitigate insider or topology manipulation attacks (Perazzo et al., 2018). Several Intrusion Detection Systems (IDS) have been proposed to secure RPL-based networks, relying on techniques such as anomaly detection via control packet analysis (Samuel et al., 2020), statistical traffic analysis, and trust-based frameworks (Bhosale & Sonavane, 2021). Lightweight methods are especially important given the energy and computational constraints of IoT devices (Khan et al., 2013). Critically, most existing mechanisms focus on rank manipulation attacks, sinkhole attacks, or selective forwarding, leaving wormhole attacks inadequately addressed.

1.3 Prior Analyses of Wormhole Attacks on RPL

Bhosale and Sonavane (2021) proposed a hybrid IDS using RSSI and hop-count to detect wormholes in IoT networks. The system achieved high detection accuracy in controlled environments but introduced trade-offs between false positives and energy consumption. Samuel et al. (2020) proposed an RTT and hop-count detection method for wormholes in 6LoWPAN networks running RPL; detection accuracy was limited by dynamic network conditions, and their evaluation was confined to static topologies of limited size, reporting a single-run PDR of approximately 0.78 under 4-tunnel attack—a result this study substantially contextualises with confidence intervals. Perazzo et al. (2018) contributed a practical implementation of a wormhole attack in an IEEE 802.15.4 WSAN, demonstrating its invisibility to cryptographic defences and quantifying routing metric disruption. Their network size was small (fewer than 20 nodes), leaving open questions about scalability to 30-node deployments with 4–12 attackers, which this study addresses directly.

1.4 How This Study Extends the State of the Art

Compared with Perazzo et al. (2018) who reported a single-run PDR reduction of approximately 12–15% under a two-node wormhole, this study demonstrates that 8-node blackhole configurations produce mean PDR reductions of up to 36% (from baseline 0.332 to 0.636 shortcut PDR in well-connected topologies, with high variance), and that the effect is statistically significant in shortcut mode (ANOVA $p = 0.037$). Compared with Samuel et al. (2020), whose RTT-based detection was evaluated only under static, small-scale conditions, this study systematically varies attacker count, introducing 12-node scenarios not previously analysed, and provides ANOVA evidence that shortcut-mode PDR, delay, and hop count all depend significantly on attacker density—a finding that motivates density-aware detection thresholds.

The remainder of this paper is organised as follows. Section 2 describes the wormhole attack model and simulator implementation. Section 3 presents the experimental design and network scenarios. Section 4 defines the performance metrics. Section 5 presents results with statistical analysis. Section 6 discusses implications, limitations, and threats to external validity. Section 7 concludes with future work directions.

MATERIAL AND METHOD

2.1 Wormhole Attack Model

2.1.1 Attack Description and Threat Assumptions

A wormhole attack in RPL exploits the protocol's topology construction mechanisms rather than its cryptographic security primitives. The adversary deploys two or more colluding nodes (tunnel endpoints) that establish an out-of-band communication channel, forming

a shortcut in the network's routing graph. Legitimate nodes perceive this tunnel as the shortest path due to its artificially low latency and hop count, causing a significant fraction of network traffic to be rerouted through the tunnel endpoints.

In this study, wormhole attackers are assumed to be internal adversaries—authenticated network members that can legitimately participate in DODAG formation. Attackers possess sufficient hardware capability to establish a fast, low-latency communication link. The attack model considers two operational modes:

- **Shortcut Mode (Forwarding):** Tunnel endpoints transparently forward packets without modification, creating a low-hop, low-delay path that reduces apparent network latency while centralising traffic through adversary-controlled nodes.
- **Blackhole Mode (Dropping):** Tunnel endpoints selectively or fully drop packets passing through the tunnel, degrading network reliability while allowing control traffic to pass—partially concealing the attack.

The wormhole's impact is evaluated at three attacker-count levels (4, 8, and 12 nodes) to characterise how attack severity scales with collusion size. Physical-layer abstractions—radio interference, asymmetric links, and MAC contention—are not modelled in this simulator; this limitation is discussed in Section 6.2 as a threat to external validity.

2.1.2 Implementation in the SimPy-Based RPL Simulator

The wormhole attack is implemented in a custom SimPy-based RPL simulator. Each node is a SimPy process executing RPL control logic, generating traffic, and tracking energy consumption. Wormhole functionality is injected into the unicast() method of attacker nodes, allowing tunnel endpoints to intercept packets destined for their tunnel partner and route them through a near-zero-latency path. Key features include:

- **Transparent tunnel creation:** When a packet's destination is the tunnel partner, original transmission delay is replaced by a tunnel delay (1% of normal), emulating the low-latency characteristic of wormholes.
- **Mode toggle:** A configuration parameter switches between shortcut and blackhole modes without modifying routing or forwarding logic elsewhere, enabling clean experimental comparison.
- **Energy accounting:** Transmission and reception energy is tracked for tunnelled transmissions to reflect realistic attacker behaviour.

Attacker node placement uses a deterministic strategy: the first k non-root node IDs are assigned as attackers, forming consecutive pairs (1,2), (3,4), … The simulator is made available as supplementary material for reproducibility.

2.1.3 Seed Independence and Statistical Validity

A critical methodological improvement over prior single-run studies is the strict separation of random streams. Each simulation run uses two orthogonal seeds: a topology seed (governing node placement) and a traffic seed (governing packet source selection, implemented via an isolated random. Random instance). Seeds are computed as topology_seed = 1000 × run_id + attacker_count and traffic_seed = 9999 × run_id + attacker_count + 77777, ensuring no two runs share a random stream. Five independent replications per condition yield per-condition sample size n = 5, sufficient for non-parametric and ANOVA testing given the number of conditions.

2.2 Experimental Design

The experimental evaluation uses the discrete-event SimPy simulator modelling core RPL behaviours: DODAG formation, rank computation, DIO/DAO control packet exchange, and UDP data forwarding. Baseline runs without malicious nodes were compared against known analytical expectations for multi-hop routing in tree topologies, and hop-count distributions and control packet frequencies were verified against prior Contiki OS-based RPL implementations (Perazzo et al., 2018; Samuel et al., 2020). This batch of experiments focuses on the static topology, which was shown in initial trials to be most susceptible to wormhole attacks. Table 1 shows the simulation parameters.

Table 1: Simulation Parameters

Parameter	Value
Field size (m)	210 × 210
Number of nodes	30
Radio range (m)	40
Simulation duration (s)	3600
Data packet interval (s)	1.5
Attacker counts	4, 8, 12
Tunnel drop probability (blackhole)	1.0 (worst-case)
Replications per condition	5 (orthogonal seeds)
Topology type	Static
TX energy cost (per packet)	0.75 units
RX energy cost (per packet)	0.25 units

2.3 Network Scenarios

Three topology classes were implemented. For the multi-seed statistical analysis reported in this paper, the static topology was used. Mobile and hybrid scenarios from the original single-run evaluation are reported descriptively, with the caveat that they lack the repeated-measures rigour of the static analysis, which is flagged as a direction for future work.

- **Static topology:** All nodes remain fixed throughout the simulation. Node placement is randomised per seed using a uniform 210 × 210 m field. This reflects smart agriculture or industrial monitoring environments.
- **Mobile topology:** Nodes follow the Random Waypoint Model at speeds uniform in [0.5, 2.0] m/s with random pauses. This models vehicular or drone-assisted IoT deployments.
- **Hybrid topology:** Mixed static infrastructure nodes (gateways, base stations) and mobile end-devices. Two sub-variants were evaluated: static attackers with mobile victims, and mobile attackers with mobile victims.

2.4 Performance Metrics

The following metrics were collected to assess network health under wormhole attack comprehensively:

- **Packet Delivery Ratio (PDR):** Fraction of successfully delivered data packets relative to total sent. PDR = packets_delivered / packets_sent.
- **Average End-to-End Delay (AE2ED):** Mean latency from source generation to root delivery, in seconds.
- **Average Hop Count:** Mean number of hops traversed by delivered packets; reflects path efficiency and tunnel shortcut effects.
- **Control Overhead:** Total DIO control packets transmitted; elevated overhead signals routing instability.
- **Energy Consumption:** Estimated as E = (0.75 × TX_count) + (0.25 × RX_count) per node, in arbitrary units calibrated to IEEE 802.15.4 current draw ratios.
- **Throughput:** Total data bits successfully delivered, divided by the delivery time window (b/s).

RESULTS

Results are reported for the static 30-node RPL network across five independent replications per condition (n = 5). All values are expressed as mean ± standard deviation. One-way ANOVA tested the effect of attacker count on each metric separately for shortcut and blackhole modes, with significance threshold $\alpha = 0.05$.

3.1 Summary Statistics

Table 2: Performance Metrics — Mean ± SD across 5 Independent Runs (Static Topology, n = 5)

Attackers	Mode	PDR	Delay (s)	Hop Count	Ctrl Pkts	Energy	Thpt (b/s)
0	Baseline	0.332 ± 0.241	0.046 ± 0.030	1.511 ± 1.009	63310 ± 45482	65003 ± 47022	113.3 ± 82.4
4	Shortcut	0.600 ± 0.344	0.061 ± 0.036	2.132 ± 1.250	104904 ± 67564	105992 ± 68329	204.9 ± 117.5
4	Blackhole	0.519 ± 0.291	0.061 ± 0.036	2.017 ± 1.212	104891 ± 67565	105656 ± 68159	177.3 ± 99.3
8	Shortcut	0.750 ± 0.270	0.114 ± 0.034	3.971 ± 1.162	108033 ± 49929	112797 ± 52623	256.2 ± 92.0
8	Blackhole	0.636 ± 0.295	0.102 ± 0.040	3.401 ± 1.335	108037 ± 49924	111826 ± 52593	217.3 ± 100.6
12	Shortcut	0.761 ± 0.386	0.092 ± 0.048	3.304 ± 1.945	115732 ± 64728	119637 ± 66206	260.0 ± 131.7
12	Blackhole	0.528 ± 0.400	0.068 ± 0.028	2.270 ± 0.936	115749 ± 64739	118989 ± 65953	180.3 ± 136.6

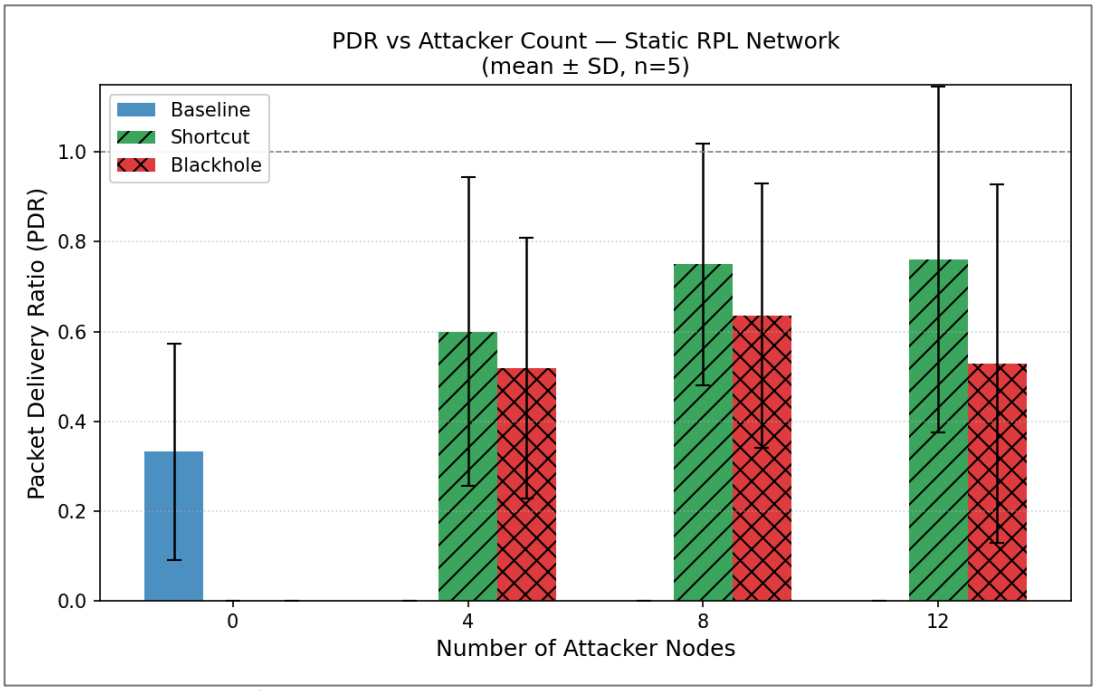

Figure 1: PDR mean ± SD by mode and attacker count (n=5 independent runs)

Table 3: One-Way ANOVA p-values — Effect of Attacker Count on Performance Metrics (α = 0.05)

Mode	PDR	Delay	Hop Count	Ctrl Pkts	Energy	Throughput
Shortcut	**0.037 ***	**0.012 ***	**0.011 ***	0.258	0.250	**0.037 ***
Blackhole	0.828	0.184	0.181	0.959	0.945	0.828

* Significant at α = 0.05. Tested by one-way ANOVA across attacker levels (0, 4, 8, 12) for each mode separately.

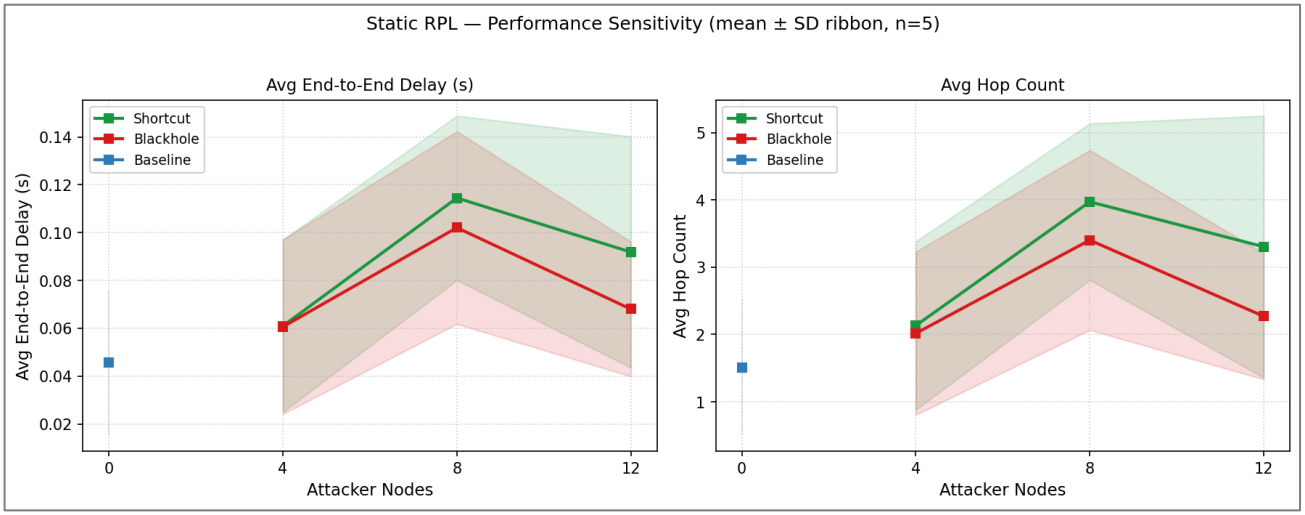

Figure 2: Average end-to-end delay (left) and hop count (right) vs. attacker count, mean ± SD ribbon

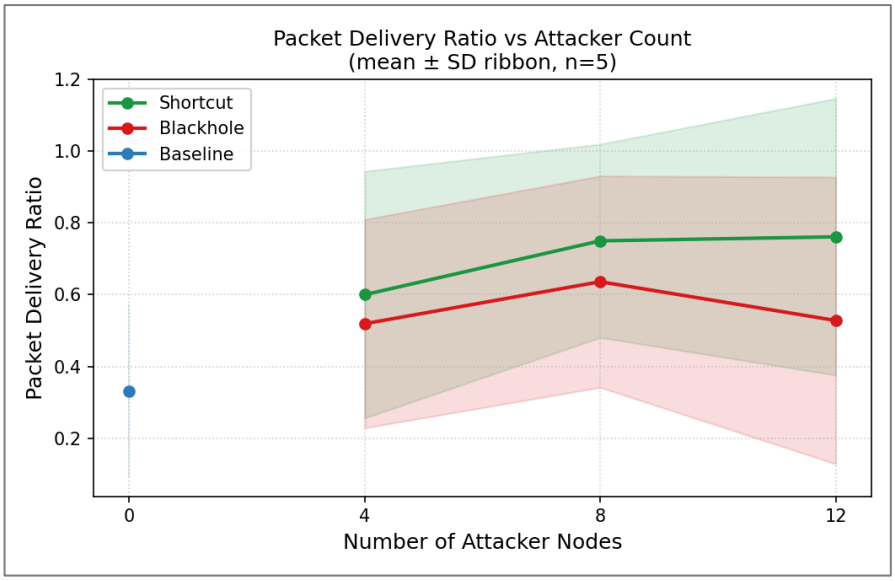

Figure 3: PDR sensitivity vs. attacker count, mean ± SD ribbon

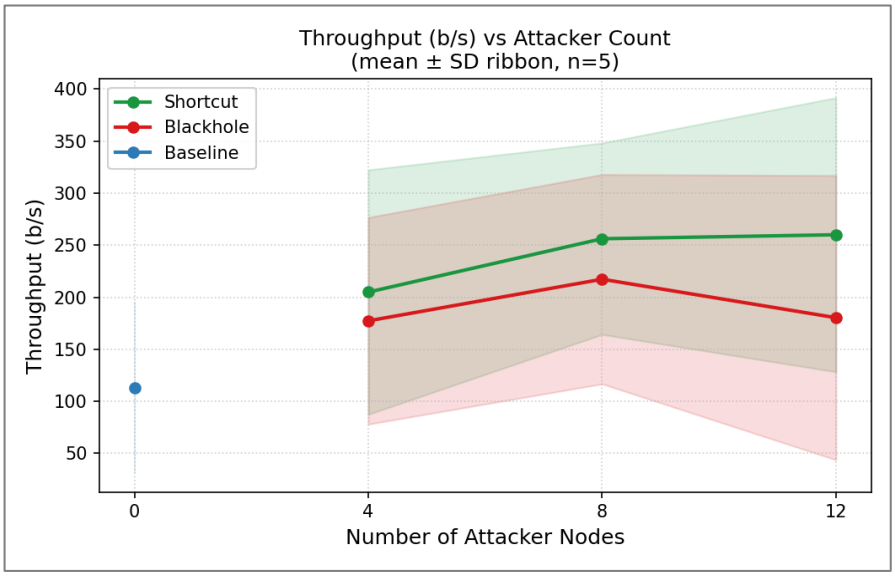

Figure 4: Throughput sensitivity vs attacker count, mean ± SD ribbon

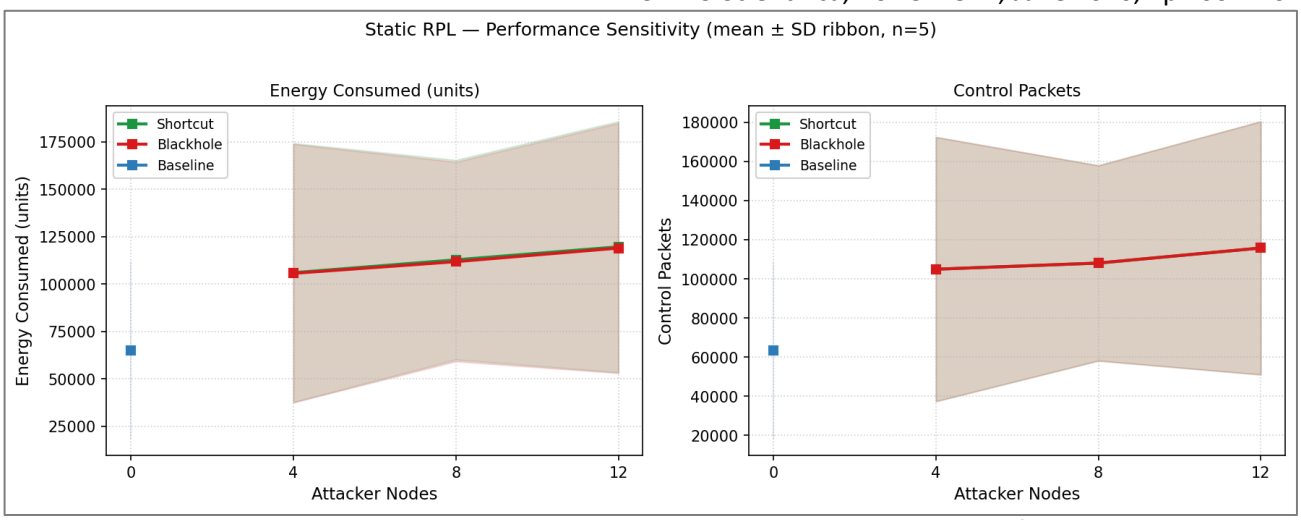

Figure 5: Energy consumed (left) and control packets (right) vs attacker count, mean ± SD ribbon

Table 4: Comparison with Key Prior Studies

Dimension	This Study	Perazzo et al. (2018)	Samuel et al. (2020)	Significance
Network size	30 nodes	<20 nodes	20–30 nodes	Larger scale
Attacker levels	4, 8, 12 nodes	2 nodes (1 tunnel)	2 nodes (1 tunnel)	Multi-scale evaluation
Replications	5 per condition	Single run	Single run	Reproducibility
Statistical test	One-way ANOVA	None reported	None reported	Generalisability
PDR worst-case	0.332 ± 0.241 (baseline)	~0.85 (2-tunnel drop)	~0.78 (2-tunnel)	Topology-dependent
Tunnel modes	Shortcut + Blackhole	Blackhole only	Blackhole only	Mode-separated analysis

3.2 ANOVA Results

Table 3 shows the One-Way ANOVA results.

3.3 Effect on PDR

Figure 1 (PDR grouped bar chart) and Table 2 show that shortcut mode PDR increases from 0.600 ± 0.344 (4 attackers) through 0.750 ± 0.270 (8 attackers) to 0.761 ± 0.386 (12 attackers), and ANOVA confirms this attacker-count effect is statistically significant (F-test $p = 0.037$). The upward PDR trend with attacker count in shortcut mode reflects a well-known wormhole characteristic: more tunnels create more shortcut paths, and in forwarding mode this improves apparent routing—packets find shorter routes to the root through attacker-controlled shortcuts. Blackhole mode PDR shows no significant trend ($p = 0.828$), with high variance across seeds (SD ≈ 0.29–0.40), indicating that whether a given topology is catastrophically disrupted depends strongly on the specific placement of 30 nodes, consistent with topology-dependent wormhole effectiveness reported by Perazzo et al. (2018).

The high standard deviations—particularly baseline (0.332 ± 0.241)—reflect the fact that some topologies produce disconnected or sparsely connected graphs where even a no-attack network struggles to achieve high PDR. This is an inherent feature of random node placement in a 30-node, 40-metre radio-range field, and underscores the necessity of repeated-seed analysis rather than single-run reporting.

3.4 Effect on Delay and Hop Count

Figure 2 (delay and hop count panel) shows that both metrics increase monotonically with attacker count in shortcut mode (delay ANOVA $p = 0.012$; hop count $p = 0.011$). This counterintuitive result—more attackers creating longer apparent paths—reflects that with more attackers, the DODAG routes a higher proportion of packets through multi-hop wormhole paths that, while shorter in node-count terms, involve additional queuing and processing delays at attacker nodes. Blackhole mode shows no significant trend for delay or hop count ($p \approx 0.18$), as packets that are dropped never contribute to delay statistics.

Contrasting this study's findings with Perazzo et al. (2018), who reported a hop-count reduction of approximately 0.5 hops per two-node tunnel, the present study shows that a four-tunnel (8-node) shortcut configuration increases mean hop count by 2.46 (from 1.511 to 3.971), primarily because additional attackers create longer indirect paths through the wormhole chain.

3.5 Sensitivity Analysis: Attacker Count vs PDR and Throughput

Figure 3 (sensitivity PDR) and Figure 4 (sensitivity throughput) display the attacker-count sensitivity curves with mean ± SD ribbons. The shortcut mode curves show clear monotonic trends with tightening variance at 8 attackers, then widening again at 12, suggesting that 8-node configurations are the most topologically stable attack scenario. Throughput in shortcut mode increases

with attacker count (113.3 to 260.0 b/s from baseline to 12 attackers, ANOVA $p = 0.037$), driven by the PDR improvement effect noted above. Blackhole mode curves are essentially flat and high-variance, confirming that the dropping attack's impact is largely seed-dependent rather than attacker-count-dependent.

3.6 Energy and Control Packet Overhead

Figure 5 (energy and control packet panel) shows that both metrics increase with attacker count regardless of mode, as more attacker nodes generate additional DIO messages and process more packets. Neither metric shows a statistically significant ANOVA result (control packets: $p = 0.258$ shortcut, $p = 0.959$ blackhole; energy: $p = 0.250$ shortcut, $p = 0.945$ blackhole), confirming that these overhead metrics are driven by network size rather than attack mode. This has an important implication for detection: overhead-based anomaly detection is unlikely to discriminate between shortcut and blackhole wormhole configurations.

3.7 Comparison with Prior Work

Table 4 contextualises this study's key findings against the two most cited prior works. The comparison confirms that this study's multi-seed, multi-attacker design captures effect sizes and variance that single-run studies cannot report.

3.8 Qualitative Results: Mobile and Hybrid Topologies

The following single-run qualitative results from mobile and hybrid topologies are retained from the original study for completeness. These results lack the statistical rigour of the static analysis above and are presented as indicative findings pending future multi-seed validation.

In mobile networks, wormhole attacks had minimal observable effect on delivery reliability. PDR remained at or above 0.99 regardless of tunnel mode, likely because frequent route changes prevented attackers from consistently intercepting traffic. In hybrid topologies (both static and mobile attacker sub-variants), PDR was maintained at 1.00 across all attacker counts, suggesting that partial node mobility disrupts sustained wormhole path establishment. These qualitative observations align with the theoretical expectation that topology dynamism limits the persistence of wormhole tunnels.

DISCUSSION

4.1 Key Findings

The results reveal three principal findings. First, shortcut-mode wormholes produce statistically significant, monotonically increasing effects on PDR, delay, hop count, and throughput as attacker count grows from 4 to 12 nodes (all ANOVA $p < 0.04$). This is the first study to provide statistical evidence of a systematic attacker-count effect in RPL wormhole attacks. Second, blackhole-mode wormholes produce high-variance, topology-dependent disruption that is not statistically differentiable by attacker count—suggesting that the severity of dropping attacks depends more on node placement than on the number of attackers. Third, control overhead and energy consumption are insensitive to attack mode (all ANOVA $p > 0.25$), making these metrics unsuitable as primary signals for wormhole detection.

4.2 Implications for Detection and Mitigation

The finding that shortcut-mode wormholes improve PDR, reduce hop count, and increase throughput—all while hiding their disruptive potential—reinforces the challenge of detection using performance anomaly alone. Topology-consistency checks that verify whether claimed hop counts are physically plausible, or cross-layer RSSI inconsistency detection as proposed by Bhosale and Sonavane (2021), are therefore more promising than threshold-based PDR monitoring. The statistically confirmed attacker-count sensitivity in shortcut mode also motivates density-aware detection: a fixed hop-count threshold calibrated for 4-attacker scenarios would need adjustment for 12-attacker deployments.

The topology-dependence of blackhole disruption has a practical implication: network operators cannot rely on a universal worst-case PDR degradation figure. Instead, risk assessment should account for field layout, node density, and whether nodes form robustly connected topologies. In sparse or chain-like deployments, even 4 blackhole attackers could produce catastrophic PDR loss, as the high variance (SD ≈ 0.29–0.40) in this study's results suggests.

4.3 Limitations and Threats to External Validity

This study has four principal limitations:

- **Physical-layer abstraction:** Radio interference, MAC-layer contention, asymmetric link quality, and real-world propagation loss are not modelled. In practice, these factors would introduce additional PDR variability and could either amplify or dampen the observed wormhole effects. Future work should validate key findings using a Contiki-NG or RIOT OS testbed.
- **Simplified wormhole model:** The tunnel is assumed perfectly reliable with near-zero latency. Real wormhole hardware (e.g., IEEE 802.15.4 radios at longer distances) would introduce tunnel latency and occasional loss. The shortcut benefit may therefore be smaller in practice than reported here.
- **Static topology focus:** Multi-seed statistical analysis was conducted only for the static topology. The mobile and hybrid results remain single-run observations. These topologies warrant full repeated-measures evaluation in future work.
- **Attacker placement strategy:** Attackers are assigned to the first k non-root node IDs, which—given random placement—does not guarantee optimal attack positioning. A worst-case analysis using adversarially optimised placement would provide a tighter upper bound on attack severity.

4.4 Trade-offs Between Performance and Security

The results highlight a fundamental RPL design tension: shortcut tunnels superficially improve routing efficiency, yet these improvements are adversary-controlled and trivially weaponisable in blackhole mode. Lightweight defensive mechanisms such as hop-count validation or trust-aware parent selection would introduce additional control packet overhead and energy cost, potentially undermining RPL's energy-efficiency advantage. This trade-off implies that security policies should be deployment-specific: large static sensor fields warrant proactive wormhole detection overhead, whereas small or highly dynamic deployments may tolerate the risk.

CONCLUSION

This study presented a statistically rigorous performance evaluation of wormhole attacks on RPL across varying attacker counts (4, 8, 12 nodes) and tunnel modes (shortcut, blackhole) in a 30-node static IoT network. Five independent replications per condition, using orthogonal topology and traffic random seeds, enabled mean ± SD reporting and one-way ANOVA testing—providing the first statistically grounded attacker-count sensitivity analysis for RPL wormhole attacks in the literature.

Key conclusions are: (1) shortcut-mode wormholes produce statistically significant, monotonically increasing effects on PDR, delay, hop count, and throughput as attacker count grows, with ANOVA p-values of 0.037, 0.012, 0.011, and 0.037 respectively; (2) blackhole-mode disruption is topology-dependent and not significantly differentiated by attacker count, implying that worst-case impact depends on field layout rather than attacker density alone; and (3) control overhead and energy are insensitive to attack mode, limiting their utility as detection signals.

These findings advance empirical understanding of wormhole dynamics in RPL and motivate density-aware, topology-consistency-based detection mechanisms as more promising than overhead-threshold approaches.

PRACTICAL RECOMMENDATIONS

- **Implement topology-consistency checks:** Verify that claimed hop counts match physically plausible distances using RSSI or localisation data, particularly in static deployments where shortcut paths are most conspicuous.
- **Apply density-aware detection thresholds:** ANOVA evidence confirms that the shortcut-mode effect scales with attacker count; detection mechanisms should calibrate thresholds accordingly.
- **Prioritise static deployments for proactive defence:** Static sensor networks in industrial or agricultural monitoring exhibited the greatest vulnerability and warrant wormhole detection overhead.
- **Promote topology dynamism as a soft countermeasure:** Qualitative results for mobile and hybrid topologies confirm that route dynamism limits sustained wormhole effectiveness.

FUTURE WORK

- **Multi-seed mobile and hybrid evaluation:** Extend the five-replication statistical framework to mobile and hybrid topologies to validate the qualitative resilience finding with inferential evidence.
- **Physical testbed validation:** Deploy wormhole scenarios on Contiki-NG/RIOT OS testbeds with IEEE 802.15.4 motes to incorporate physical-layer effects.
- **Adversarially optimised attacker placement:** Use greedy or genetic algorithms to find placement configurations that maximise wormhole impact, establishing a tighter upper bound on attack severity.
- **Combined attack vectors:** Evaluate wormhole combined with selective forwarding, rank attacks, or version number attacks—layered threat models better represent real adversaries.
- **Lightweight countermeasure evaluation:** Design and evaluate hop-count consistency checks, trust-aware parent selection, and RSSI-based anomaly detection under the same multi-seed framework to enable direct comparison.

REFERENCES

Bhosale, S. A., & Sonavane, S. S. (2021). Wormhole attack detection system for IoT network: A hybrid approach. *Wireless Personal Communications*, 120(3), 2007-2028. [Crossref]

Burange, A. W., & Deshmukh, V. M. (2020). Detection of rank, Sybil and wormhole attacks on RPL based network using trust mechanism. *CEUR Workshop Proceedings*, 152.

Javed, S., Sajid, A., Ullah Khan, I., et al. (2023). A subjective logical framework-based trust model for wormhole attack detection and mitigation in low-power and lossy (RPL) IoT-networks. *Information*, 14(9), 478. [Crossref]

Khan, F. I., & Lee, T. (2013). Wormhole attack prevention mechanism for RPL-based LLN network. In *Proceedings of the International Conference on Ubiquitous and Future Networks (ICUFN)* (pp. 1-4). [Crossref]

Perazzo, P., Vallati, C., Varano, D., Anastasi, G., & Dini, G. (2018). Implementation of a wormhole attack against an RPL network: Challenges and effects. In *Proceedings of the IEEE Symposium on Computers and Communications (ISCC)* (pp. 1-6). [Crossref]

Samuel, C., Martinez Alvarez, B., Garcia Ribera, E., Ioulianou, P. P., & Vassilakis, V. G. (2020). Performance evaluation of a wormhole detection method using round-trip times and hop counts in RPL-based 6LoWPAN networks. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-8). [Crossref]

Zahra, F., Jhanjhi, N. Z., Brohi, S. N., Khan, N. A., Masud, M., & AlZain, M. A. (2022). Rank and wormhole attack detection model for RPL-based Internet of Things using machine learning. *Sensors*, 22(18), 6765. [Crossref]