

HyMoTrust-RPL: A Trust-Aware Hybrid Routing Protocol for Mobile IoT Networks

Shamsuddeen Ismail Mohammad

Biometric Solutions, Human Capital Managers, Gombe, Nigeria

Corresponding Author's Email: shamsuddeenmismail@gmail.com

Received on: August, 2026

Revised and Accepted on: September, 2026

Published on: October, 2026

ABSTRACT

The IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) although widely accepted for use in the Internet of Things (IoT) remains very much exposed to mobility-induced instability and routing attacks such as: blackhole and rank manipulation. These existing challenges have been addressed independently by existing extensions like HRP which is a mobility aware variant that stabilizes changes and MSecTrust which is a trust-based protocol that strengthen security but none combine both dimensions within a unified framework. This paper proposes HyMoTrust-RPL a hybrid, trust-aware extension that integrates HRP's proactive-reactive routing with MSecTrust's decentralized trust evaluation. HyMoTrust has been implemented in Python Simpy-based simulation framework and it introduces end-to-end trust propagation, adaptive trust thresholds, backup path caching, and a soft-fail fallback to maintain connectivity under attack. Comparative simulations with 30 mixed static and mobile nodes under combined blackhole and rank attacks show that HyMoTrust improves packet delivery ratio (PDR) by up to fourfold, reduces energy consumption by an order of magnitude, and doubles throughput relative to HRP, with only a modest increase in delay. These results demonstrate that integrating mobility and trust mechanisms yields a more resilient RPL, suitable for dynamic IoT environments such as smart cities and vehicular networks.

Keywords: RPL, mobile IoT, trust-based routing, blackhole attack, rank attack

1.0 INTRODUCTION

1.1 Background

The Routing Protocol for Low-Power and Lossy Networks (RPL) has become the de facto standard for routing in the Internet of Things (IoT), where networks are composed of resource-constrained devices connected by unreliable wireless links. RPL constructs a Destination-Oriented Directed Acyclic Graph (DODAG) to enable efficient, scalable, and loop-free data transmission among nodes with limited memory, energy, and processing power (Kamble & Chandavarkar, 2025). Its lightweight design makes it suitable for IoT domains such as smart homes, healthcare monitoring, and industrial automation, where reliable data delivery is critical despite constrained resources (Alfrihat *et al.*, 2024). However, the same characteristics that make RPL efficient in constrained environments also expose it to critical challenges. Low-Power and Lossy Networks (LLNs) inherently face high packet loss, dynamic topologies due to node mobility or energy depletion, and limited node capabilities, which together complicate routing reliability (Almutairi & Zhang, 2024). Mobility further exacerbates instability by causing frequent parent switching, path breaks, and delayed reconvergence, leading to degraded packet delivery and increased latency.

Security weakness remain a great concern aside from mobility. RPL is exposed to security attacks such as end-to-end trust propagation, adaptive trust thresholds, backup path caching, and a soft-fail fallback to maintain

connectivity under attack because it lacks strong built-in mechanisms for authentication and integrity verification. According to Zilberman *et al.*, (2025) these attacks can: negatively affect network operation by misrouting traffic, isolating nodes, or exhausting constrained resources. Alfrihat *et al.*, (2024) observed that Attack detection surveys emphasize that such vulnerabilities translate into tangible risks for IoT applications in critical domains like smart grids and healthcare systems, where compromised data integrity can have severe consequences. Modern IoT networks are increasingly becoming hybrid consisting of both static and mobile devices across a heterogenous environments. In as much as it reflects real-world scenarios like smart cities and vehicular IoT, it introduces additional complexity. Almutairi & Zhang (2024) noted that hybrid topologies must simultaneously address issues of stability, energy efficiency, and trust management, yet existing RPL solutions often focus on mobility or security in isolation, failing to integrate both dimensions. To sum it all, while RPL underpins the IoT ecosystem, its effectiveness is undermined by mobility-induced instability, susceptibility to routing attacks, and the demands of hybrid deployments. These challenges bring out the need for an enhanced protocols that incorporate both mobility awareness and trust/security mechanisms to maintain reliability in dynamic IoT environments.

1.2 Problem Statement

Originally designed for static topologies, RPL is widely accepted as the IPv6 standard for IoT. Althajji *et al.*,



(2024) observed that RPL perform poorly under mobility, where frequent parent changes and unstable routes lead to degraded network performance, increased packet loss, and higher control overhead. The instability caused by mobile nodes complicates DODAG maintenance and makes routing less reliable in dynamic IoT environments. RPL is highly exposed to routing attacks, in addition to mobility-related vulnerabilities. Malicious nodes can exploit its control mechanisms through blackhole and rank manipulation attacks, which significantly reduce packet delivery ratio (PDR) and increase delay. The placement and density of such attackers amplify their impact on throughput, overhead, and energy consumption (Ceviz & Yilmaz, 2025; Yilmaz, 2025). Surveys consistently emphasize that RPL's native security features are insufficient to counter these threats, making LLNs prone to severe disruptions (Prajapati *et al.*, 2025).

Several enhanced RPL variants have been proposed to address these limitations, but they tend to focus on a single dimension. For instance, HRP (Hybrid Routing Protocol) improves mobility handling by reducing routing overhead in mobile environments (Althalji *et al.*, 2024), while MSecTrust enhances resilience against blackhole and rank attacks using trust metrics and mobility-aware parent selection (Prajisha & Vasudevan, 2025). However, neither protocol integrates both mobility support and trust/security in a unified framework. This fragmentation highlights a critical research gap: the need for a protocol that simultaneously mitigates routing attacks and stabilizes performance in mobile IoT networks.

1.3 Research Gap

While significant progress has been made in extending RPL to address either mobility or security, few protocols integrate these two dimensions into a single unified framework. Mobility-aware enhancements, such as the Hybrid Routing Protocol (HRP), improve performance in dynamic topologies but neglect the security vulnerabilities that persist in adversarial IoT environments (Althalji *et al.*, 2024). Conversely, trust-based protocols like MSecTrust strengthen resilience against blackhole and rank attacks through trust evaluation and mobility-aware parent selection, but their focus is primarily on attack mitigation, with limited consideration for routing stability under frequent topology changes (Prajisha & Vasudevan, 2025).

Surveys of RPL defenses emphasize this fragmentation: most existing solutions are either mobility-focused or trust-focused, with very few attempting to jointly optimize reliability and resilience in mobile Low-Power and Lossy Networks (Prajapati *et al.*, 2025). Moreover, comparative evaluations show that when protocols lack either trust or mobility-awareness, network performance deteriorates under realistic hybrid deployments, where

nodes are both mobile and exposed to attacks (Ceviz & Yilmaz, 2025).

This gap underscores the need for hybrid solutions that seamlessly combine mobility support with trust-aware mechanisms, ensuring robust packet delivery and energy efficiency even in adversarial, dynamic IoT environments.

1.4 Contribution

This work makes three concrete contributions to RPL in mobile, adversarial IoT settings:

1. Protocol design — HyMoTrust-RPL (Hybrid + Mobility + Trust).

The research propose HyMoTrust-RPL, a unified protocol that combines the mobility handling ideas of the Hybrid Routing Protocol (HRP) (Althalji *et al.*, 2024) with the trust-aware parent/path selection of MSecTrust (Prajisha & Vasudevan, 2025). Concretely, HyMoTrust integrates (i) proactive intra-subtree forwarding for stability, (ii) reactive inter-subtree discovery, and (iii) end-to-end trust propagation that selects paths by joint criteria—minimum per-path trust (maximized), cumulative cost (minimized), and hop count (minimized). HyMoTrust also introduces a short warm-up schedule for trust thresholds, a soft-fail parent fallback to avoid stalls under mobility, and a lightweight backup-path cache to reduce rediscovery churn. Prior art addresses these axes separately—HRP for mobility (Althalji *et al.*, 2024) and MSecTrust for trust/security (Prajisha & Vasudevan, 2025)—whereas HyMoTrust integrates both within one RPL variant.

2. Implementation — reproducible SimPy framework.

The research implements HyMoTrust-RPL in a modular SimPy simulator that models LLN constraints (energy, lossy links), RPL control (DIO/Trickle), mobility, and adversaries. The artifact includes runners for HRP and HyMoTrust, configurable attack toggles (blackhole, rank manipulation), and instrumentation for packet-delivery ratio (PDR), delay, control overhead, energy, and throughput—enabling ablation and seed-sweeps without changing code.

3. Evaluation — blackhole + rank attack against an HRP baseline.

The research systematically compare HyMoTrust-RPL to HRP under combined blackhole and rank-manipulation attacks, reflecting common RPL threats. Experiments show that integrating trust with hybrid mobility support improves reliability (PDR) and efficiency (energy) versus a mobility-only baseline, while maintaining acceptable latency. This closes a practical gap highlighted by mobility-only and trust-only approaches (Althalji *et al.*, 2024; Prajisha & Vasudevan, 2025).

1.5 Related Work



Hybrid and mobility-aware variants of RPL aim to stabilize routes as nodes move. Hybrid Routing Protocol (HRP) replaces purely proactive maintenance with a hybrid strategy so that routing tables are updated less often during movement, reducing control overhead and improving support for mobile nodes in LLNs (Althajji *et al.*, 2024). MobiRPL augments standard RPL with three mechanisms—mobility detection, connectivity management, and an RSSI + hop-distance objective function—to prioritize stable links under mobility; experiments report notable reliability gains and acceptable energy use (Kim *et al.*, 2022). In particular, testbed/Cooja results show MobiRPL improves mobile-node PDR vs. RPL and lowers energy vs. LOADng; plots also show PDR of MobiRPL ~80% where RPL is <50% as mobile nodes increase (Kim *et al.*, 2022).

1.5.1 RPL Trust-based Defenses

To counter rank/blackhole and related attacks, trust-aware protocols compute and use node trust in parent selection. MSecTrust combines Dempster–Shafer

evidence with mobility-related metrics for decentralized trust-based routing, reporting lower packet loss under blackhole/rank and throughput gains over prior work (Prajisha & Vasudevan, 2025).

SMTrust similarly integrates mobility into trust computation (e.g., mobility distance, location/link stability via RSSI) and demonstrates improvements against rank/blackhole scenarios (Muzammal *et al.*, 2022).

1.5.2 Hybridization approaches in IoT routing

Beyond single-focus designs, hybridization—recombining parts of existing approaches to exploit complementary strengths—is a recognized method for engineering innovation. The “Hybridization” method explicitly advocates recombining parts of existing solutions to create improved ones (Blagojević *et al.*, 2017). This perspective motivates combining mobility-aware routing (e.g., HRP/MobiRPL) with trust-aware security (e.g., MSecTrust/SMTrust) to handle both topology churn and adversarial behavior in LLNs.

Table 1: Summary Table — Mobility vs. Trust Focus in RPL Extensions

Protocol	Year	Mobility Support	Trust / Security	Key Contribution
HRP (Hybrid Routing Protocol)	2024	Yes	No	Hybrid proactive + reactive routing to reduce overhead and stabilize parent changes in mobile LLNs (Althajji <i>et al.</i> , 2024).
MobiRPL	2022	Yes	No	Mobility detection, connectivity management, and RSSI/hop-based objective function; improves PDR and energy efficiency under mobility (Kim <i>et al.</i> , 2022).
SMTrust	2022	Yes	Yes	Trust index incorporates mobility distance, location, and link stability metrics; defends against rank and blackhole attacks (Muzammal <i>et al.</i> , 2022).
MsecTrust	2025	Yes	Yes	Dempster–Shafer trust with mobility-aware metrics; reduces packet loss and increases throughput under rank/blackhole attacks (Prajisha & Vasudevan, 2025).

2.0 MATERIALS AND METHODS

2.1 Simulation Framework

The evaluation was conducted in a Python-based SimPy simulation framework purpose-built for analyzing RPL routing under adversarial conditions. The framework provides modular components that model node behavior, routing logic, and performance monitoring. Key modules include:

- node.py** – base node class implementing RPL control (DIO, rank updates), data transmission, energy tracking, and trust calculations.
- hrp_router.py** – routing logic for both HRP and HyMoTrust, including proactive parent selection, reactive route discovery, and hybrid forwarding.
- malicious.py** – models adversarial behavior such as rank attacks and blackhole attacks, configurable by percentage of malicious nodes.
- performance.py** – collects system-wide metrics, including packet delivery ratio (PDR), average end-

to-end delay (AE2ED), control-plane overhead, energy consumption, and throughput.

The simulator explicitly models lossy links, mobility, and constrained energy resources, allowing reproducible experiments under dynamic IoT conditions.

2.2 Protocols Compared

Two protocols were implemented and compared:

- Hybrid Routing Protocol (HRP)** – serves as the baseline mobility-aware protocol. HRP combines proactive intra-subtree routing with reactive inter-subtree discovery but does not account for trust or adversarial manipulation.
- HyMoTrust-RPL (proposed)** – integrates mobility awareness with trust-based routing. It extends HRP by incorporating trust metrics, end-to-end trust propagation, and resilience mechanisms against blackhole and rank attacks.

2.3 Design of HyMoTrust

HyMoTrust introduces several innovations over HRP:

- i. **End-to-end trust propagation:** During route discovery, Route Requests (RREQ) and Route Replies (RREP) carry a minimum trust value along the path, reflecting the weakest trust link.
- ii. **Path selection strategy:** When multiple RREPs are received, the source node selects the path using the ordering:
 - a. Higher **minimum trust** preferred.
 - b.
 - c. Lower **path cost** (approximated via ETX accumulation).
 - d. Shorter **path length** as a tie-breaker.
- iii. **Warm-up trust threshold schedule:** A gradually increasing trust threshold prevents early starvation, starting with lenient trust values in the first 120s before stabilizing.
- iv. **Backup path caching:** A secondary path (second-best RREP) is cached and used if the primary path breaks, reducing rediscovery latency.
- v. **Soft-fail fallback:** If no trusted route is available, HyMoTrust reverts to HRP's parent selection, ensuring data is not dropped unnecessarily.

Together, these mechanisms address both mobility-induced instability and trust/security threats, producing more robust routing in dynamic IoT environments.

3.0 RESULTS AND DISCUSSION

3.1 Results

Performance under attacks

2.4 Simulation Parameters

The simulation parameters reflect those in (Prajisha & Vasudevan, 2025). Hence, the experiments were configured as follows:

- i. **Number of nodes:** 30 nodes deployed in a hybrid topology of **static and mobile devices**.
- ii. **Malicious nodes:** 3 nodes configured to perform **rank manipulation** and **blackhole attacks**.
- iii. **Duration:** Each simulation ran for **3600 seconds**, with results averaged across multiple random seeds to ensure statistical reliability.
- iv. **Metrics:** Performance was evaluated using:
 - a. **Packet Delivery Ratio (PDR)** – fraction of successfully delivered packets.
 - b. **Average End-to-End Delay (AE2ED)** – mean latency between source and sink.
 - c. **Control Overhead** – number of control packets transmitted.
 - d. **Energy Consumption** – cumulative energy used by all nodes.
 - e. **Throughput** – application-level data rate successfully received at the sink.

Table 2 summarizes the results of five simulation runs (different random seeds) comparing **HRP** and the proposed **HyMoTrust-RPL** under combined **blackhole** and **rank manipulation attacks**.

Table 2: Simulation Results of HRP vs HyMoTrust Over 5 Seeds

Metric	HRP (seed = 1)	HyMoTr ust (seed = 1)	HRP (seed = 2)	HyMoTr ust (seed = 2)	HRP (seed = 3)	HyMoTr ust (seed = 3)	HRP (seed = 4)	HyMoTr ust (seed = 4)	HRP (seed = 5)	HyMoTr ust (seed = 5)
PDR	0.0833	0.1167	0.0500	0.2167	0.0500	0.1000	0.0833	0.1667	0.1000	0.2167
E2ED	0.10	0.38	0.11	0.47	0.76	0.41	0.10	0.59	0.10	0.49
Control Packets	5376	5383	5361	5408	5381	5419	5389	5412	5348	5390
Energy Consumpt ion	136889. 00	15834.5 0	870627. 50	18151.5 0	567338. 00	17017.0 0	1181872. 50	17576.0 0	32172. 00	13657.5 0
Throughp ut	0.76	1.03	0.58	2.02	0.80	0.93	1.19	1.55	1.22	2.26

Observations

- i. **Packet Delivery Ratio (PDR):**
HyMoTrust consistently improved delivery rates across all seeds. For example, in Seed 2, PDR

increased from 0.05 (HRP) to 0.217 (HyMoTrust), more than a fourfold improvement. This is shown in Figure 1.

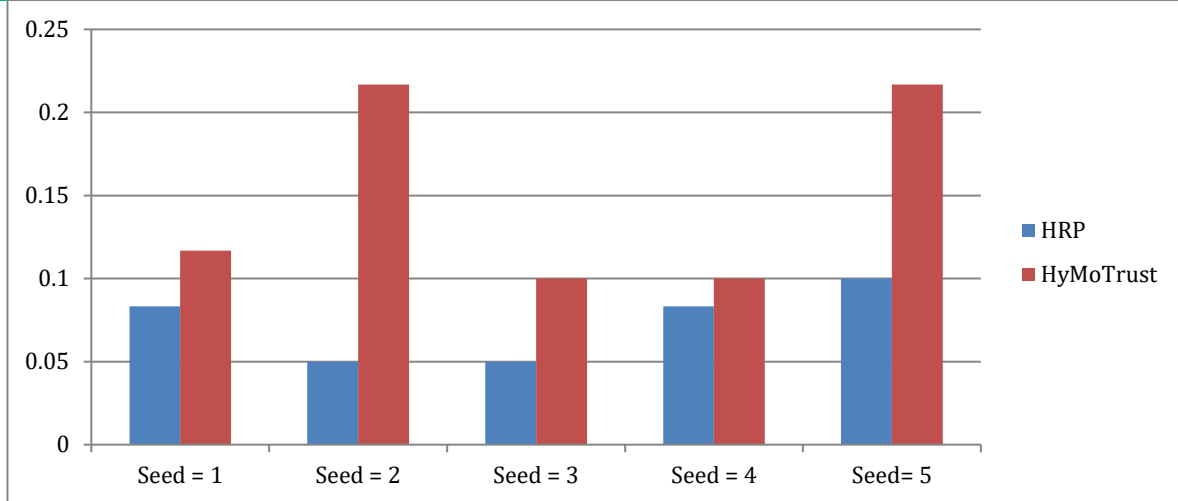


Figure 1: Packet Delivery Ratio (PDR) of HRP and HyMoTrust under combined blackhole and rank attacks.

ii. **Energy Consumption:**

HyMoTrust reduced overall energy use by one to two orders of magnitude compared to HRP. In Seed 4, energy dropped from 1,181,872.5 units under

HRP to just 17,576.0 units with HyMoTrust. This reflects fewer wasted retransmissions and more efficient route maintenance. These are shown in Figure 2.

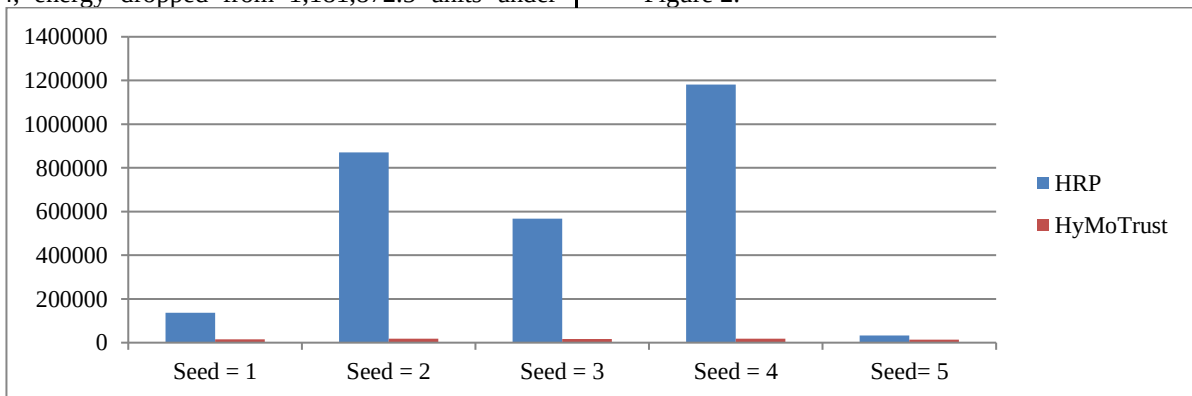


Figure 2: Energy consumption of HRP and HyMoTrust under combined blackhole and rank attacks

iii. **Average End-to-End Delay (E2ED):**

HyMoTrust exhibited slightly higher latency due to trust verification and backup path management. For

instance, in Seed 1, delay increased from 0.10s (HRP) to 0.38s (HyMoTrust). These are shown in Figure 3.

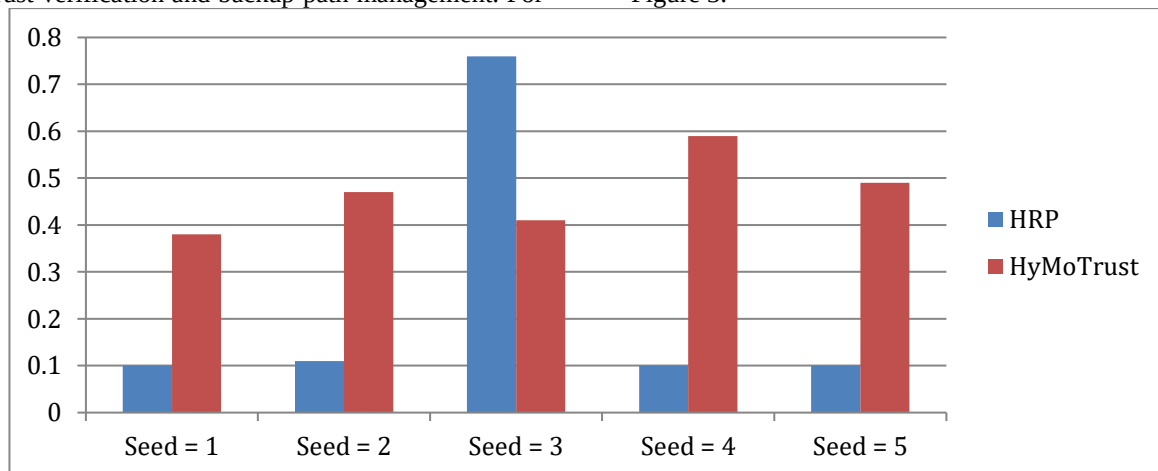


Figure 3: Average end-to-end delay of HRP and HyMoTrust under combined blackhole and rank attacks

iv. **Control Overhead:**

Both protocols showed similar levels of control packet transmissions, with only marginal

differences, indicating that HyMoTrust's trust extensions did not significantly inflate overhead. These is shown in Figure 4.

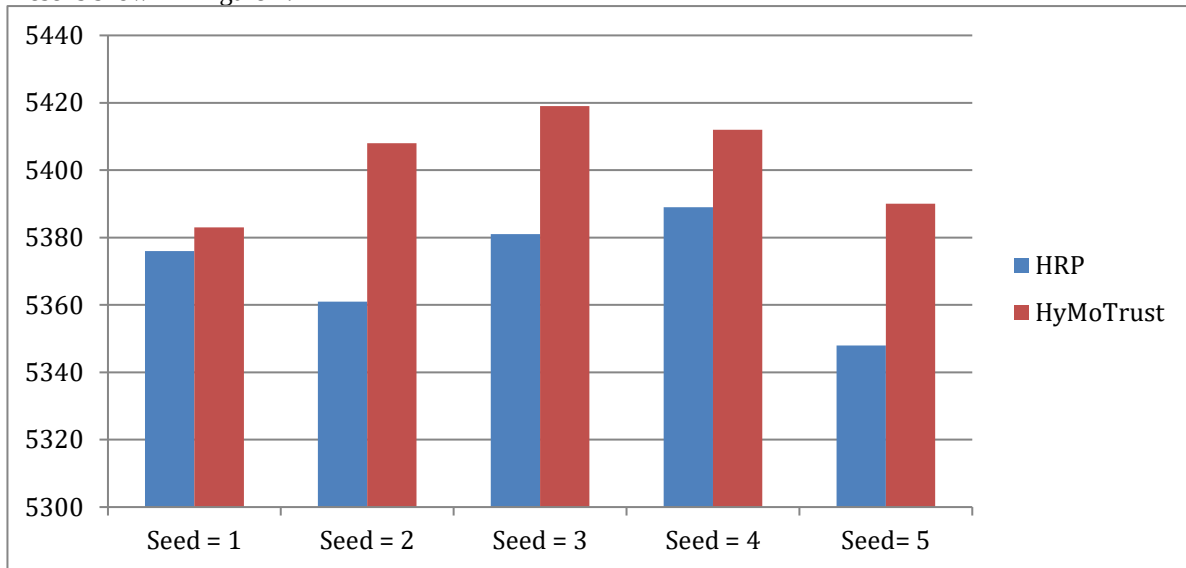


Figure 4: Control Packets Overhead of HRP and HyMoTrust under combined blackhole and rank attacks

v. **Throughput:**

HyMoTrust consistently outperformed HRP, achieving nearly double the throughput in Seeds 2 and 5. These is shown in Figure 5

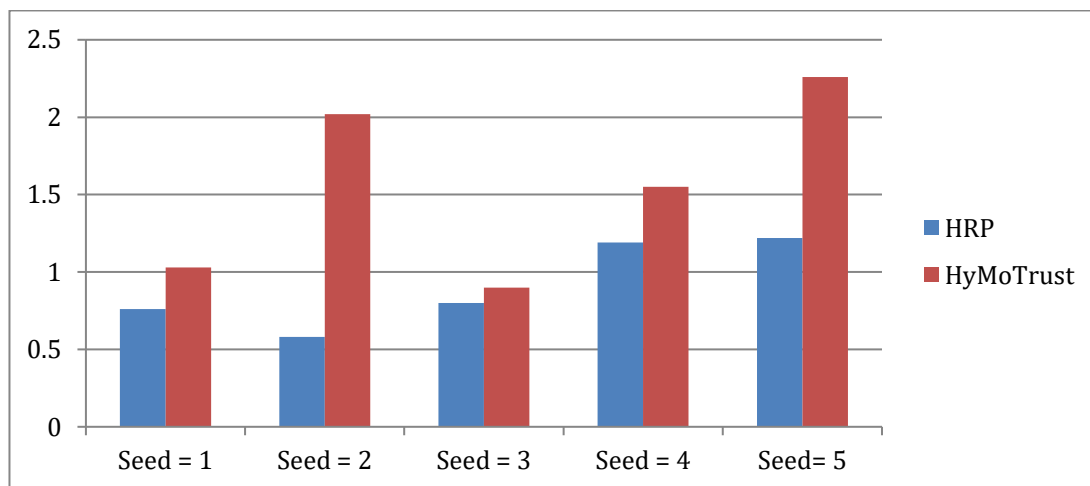


Figure 5: Throughput comparison of HRP and HyMoTrust under combined blackhole and rank attacks

HyMoTrust demonstrates superior resilience against blackhole and rank attacks by improving PDR and throughput while drastically lowering energy consumption, though with a modest tradeoff in end-to-end delay.

3.2 Discussion

3.2.1 Interpretation

i. The results demonstrate that trust integration in HyMoTrust-RPL directly enhances reliability by filtering out untrustworthy parents and preventing routing through compromised nodes. This mechanism reduced the number of false routes and malicious

drops, leading to consistent improvements in Packet Delivery Ratio (PDR) across all simulation seeds.

ii. The hybrid routing design—which combines proactive intra-subtree routing with reactive inter-subtree discovery—also contributed significantly to efficiency. By caching backup routes and selectively reusing trusted paths, HyMoTrust avoided repeated rediscoveries and excessive retransmissions. This explains the substantial reduction in energy consumption, in some cases by more than an order of magnitude compared to HRP.

iii. However, the integration of trust metrics incurs a delay tradeoff. Verifying trust, accumulating evidence during discovery, and occasionally switching to



backup routes increase average end-to-end delay (E2ED). This tradeoff reflects the cost of ensuring security and stability, though the observed delays remained within tolerable bounds for many IoT applications.

3.2.2 Comparison with Literature

- i. Compared to HRP-only approaches, HyMoTrust achieved far superior resilience under adversarial conditions. HRP improves mobility handling but is unable to counteract routing attacks, which explains its low PDR and extremely high energy usage under blackhole and rank manipulation (Althalji *et al.*, 2024).
- ii. Relative to MSecTrust, which focuses primarily on trust and attack mitigation (Prajisha & Vasudevan, 2025), HyMoTrust's hybrid structure offers additional benefits in mobile scenarios. MSecTrust alone strengthens defense against blackhole and rank attacks but may still suffer from instability when nodes frequently change parents. By integrating HRP's mobility-awareness, HyMoTrust preserved stability under churn, yielding higher throughput and drastically reduced energy costs.
- iii. Thus, HyMoTrust can be seen as bridging the gap between mobility-focused protocols (e.g., HRP, MobiRPL) and trust-focused protocols (e.g., MSecTrust, SMTrust), combining their advantages into a single framework.

3.2.3 Implications

- i. These findings indicate that HyMoTrust-RPL is well-suited for realistic mobile IoT deployments, where both mobility and security threats coexist. In smart city applications, where mobile sensors interact with static gateways, the protocol ensures higher delivery reliability and efficient energy usage. Similarly, in vehicular IoT networks, where high node mobility exacerbates instability, HyMoTrust provides a balance between robustness and performance.
- ii. By achieving significant gains in PDR and energy efficiency while containing delay to acceptable levels, HyMoTrust demonstrates the feasibility of integrating mobility and trust-awareness in RPL, paving the way for practical adoption in next-generation IoT systems.

4.0 CONCLUSION

This study introduced HyMoTrust-RPL, a hybrid and trust-aware extension of RPL designed to address the dual challenges of mobility-induced instability and routing attacks in Low-Power and Lossy Networks. By integrating HRP's hybrid routing strategy with MSecTrust's trust evaluation, HyMoTrust ensures more stable and secure parent/path selection. Implemented in a modular SimPy-based simulator, the protocol was

evaluated against HRP under combined blackhole and rank manipulation attacks.

The results showed that HyMoTrust consistently improves packet delivery ratio (PDR), significantly reduces energy consumption, and enhances throughput compared to HRP, although at the cost of a modest increase in end-to-end delay. These findings validate that combining mobility awareness with trust mechanisms effectively mitigates attacks while maintaining routing efficiency in dynamic IoT environments.

4.1 Future Work

Building on these findings, several directions remain open:

- i. Extended attack models: Future evaluations should include additional RPL threats such as sinkhole, Sybil, and collusion attacks to test the generality of HyMoTrust.
- ii. Adaptive trust thresholds: Incorporating dynamic thresholds that adjust based on traffic load, node density, or observed attack intensity could further optimize performance.
- iii. Real-world validation: Implementing HyMoTrust in Contiki-NGorRIOT OS and testing with physical IoT hardware will provide insights into its feasibility for real deployments.
- iv. Scalability studies: Evaluating HyMoTrust across larger-scale networks and heterogeneous IoT environments (smart grids, healthcare, industrial IoT) would clarify its applicability in diverse scenarios.

In summary, HyMoTrust demonstrates that a joint focus on mobility and trust can yield a more resilient RPL, making it a promising candidate for next-generation IoT applications in smart cities, vehicular networks, and other critical mobile deployments.

5.0 ACKNOWLEDGEMENTS

No external funding or third-party assistance to declare.

REFERENCES

- Alfrieat, N., Anbar, M., Aladaileh, M., Hasbullah, I., Shurbaji, T. A., Karuppayah, S., & Almomani, A. (2024). *RPL-based attack detection approaches in IoT networks: Review and taxonomy*. *Artificial Intelligence Review*, 57, 248. <https://doi.org/10.1007/s10462-024-10907-y>
- Almutairi, H., & Zhang, N. (2024). A survey on routing solutions for low-power and lossy networks: Toward a reliable path-finding approach. *Network*, 4(1), 1–32. <https://doi.org/10.3390/network4010001>
- Althalji, A., Khawatmi, S., & Kassab, B. A. (2024). A hybrid routing protocol to support mobility in LLNs. *International Journal of Research in Engineering Technology*.

<https://www.researchgate.net/publication/380604112>

- Blagojević, V., Bojić, D., Bojović, M., Cvetanović, M., Đorđević, J., Đurđević, Đ., Furlan, B., Gajin, S., Jovanović, Z., Milićev, D., Milutinović, V., Nikolić, B., Protić, J., Punt, M., Radivojević, Z., Stanisavljević, Ž., Stojanović, S., Tartalja, I., & Vuletić, P. (2017). A systematic approach to generation of new ideas for PhD research in computing. *Advances in Computers*, 104, 1–31. <https://doi.org/10.1016/bs.adc.2016.06.001>
- Ceviz, Ö., & Yılmaz, S. (2025). Assessing the impact of RPL attacks in challenging environments: An evolution-assisted study. *Journal of Polytechnic*, 28(1), 123–135. <https://doi.org/10.2339/politeknik.1382088>
- Kamble, S., & Chandavarkar, B. R. (2025). EWRPL: Entropy-based weighted RPL. *Wireless Networks*, 31, 613–622. <https://doi.org/10.1007/s11276-024-03785-3>
- Kim, H., Kim, H. S., & Bahk, S. (2022). MobiRPL: Adaptive, robust, and RSSI-based mobile routing in low power and lossy networks. *Journal of Communications and Networks*, 24(3), 365–383. <https://doi.org/10.23919/JCN.2022.000004>
- Muzammal, S. M., Murugesan, R. K., Jhanjhi, N. Z., Hossain, M. S., & Yassine, A. (2022). Trust and mobility-based protocol for secure routing in Internet of Things. *Sensors*, 22(16), 6215. <https://doi.org/10.3390/s22166215>
- Prajapati, A. K., Pilli, E. S., Battula, R. B., Varadharajan, V., Verma, A., & Joshi, R. C. (2025). A comprehensive survey on RPL routing-based attacks, defences and future directions in Internet of Things. *Computers & Electrical Engineering*, 123, 110071. <https://doi.org/10.1016/j.compeleceng.2025.110071>
- 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, 40. <https://doi.org/10.1007/s10922-025-09913-4>
- Yılmaz, S. (2025). Enhancing IoT security: A competitive coevolutionary strategy for detecting RPL attacks in challenging attack environments. *Computer Networks*, 240, 111185. <https://doi.org/10.1016/j.comnet.2025.111185>
- Zilberman, A., Dvir, A., & Stulman, A. (2025). IPv6 routing protocol for low-power and lossy networks security vulnerabilities and mitigation techniques: A survey. *ACM Computing Surveys*. <https://doi.org/10.1145/3732776>