

iSTIR-RPL: Trust-Aware Routing-State Protection Against Colluding Routing Table Overload Attack in Storing-Mode RPL

Faisal Ali Garba^{1*}, Sahalu Balarabe Junaidu², Yusuf Sahabi Ali², Abdussamad Imam Tanko³

¹Department of Computer Science, Sa'adatu Rimi College of Education, Kano, Nigeria

²Department of Computer Science, Ahmadu Bello University, Zaria, Nigeria

³Department of Mathematics, Ahmadu Bello University, Zaria, Nigeria

*Corresponding Author's Email: alifa2try@gmail.com

Received on: August, 2026 Revised and Accepted on: September, 2026

Published on: October, 2026

ABSTRACT

A memory exhaustion attack in the Internet Protocol version 6 (IPv6) Routing for Low Power and Lossy Networks (RPL) where attacking node inject fake Destination Advertisement Object (DAO) messages to saturate routing tables and isolate legitimate nodes is known by the name Routing Table Overload Attack (RTOA). Short-Interval Routing for RPL (STIR-RPL) is the only published countermeasure which provides zero measurable protection against RTOA and produced results similar to Baseline RPL (RFC 6550) when evaluated in this study. This paper proposes iSTIR-RPL, which addresses three fundamental deficiencies of STIR-RPL through three coordinated enhancements: (1) trust-aware routing-state admission using a three-tier pool system that allocates routing table capacity proportionally to verified, new-node, and suspicious nodes based on legitimate trust scores from iMSecTrust-RPL; (2) adaptive memory reservation that scales interval sizes continuously with trust level; and (3) suspicion-based routing-state control with colluding group detection. The proposed iSTIR-RPL eliminated node isolation completely across all evaluation runs, reduced routing table size by 69 to 72 percent relative to Baseline RPL (RFC 6550), and dropped DAO rejection events to zero, whilst maintaining statistically equivalent Packet Delivery Ratio to all comparison schemes (all $p > 0.05$) when evaluated across 180 simulation runs spanning three topologies, two RTOA variants, three attacker densities, and ten seeds per configuration. These results revealed that trust-conditioned routing-state admission is necessary and sufficient to prevent RTOA-induced node isolation in storing-mode RPL.

Keywords: IoT; trust-aware routing; memory exhaustion; security; iMSecTrust-RPL

1.0 INTRODUCTION

The standard routing protocol for IoT Smart Object Networks (SONs), standardised in Internet Engineering Task Force (IETF) Request for Comment (RFC) 6550 (Winter et al., 2012) is the Internet Protocol version 6 (IPv6) Routing Protocol for Low-Power and Lossy Networks (RPL). RPL has two modes of operations: storing mode of operation (MoP) and non-storing MoP. In storing-mode RPL, intermediate nodes maintain per-descendant routing state, creating a structural vulnerability that enables the Routing Table Overload Attack (RTOA). In RTOA a malicious node inject fabricated DAO messages to saturate routing tables at parent nodes, preventing legitimate nodes from registering their routes and causing node isolation (Tsao et al., 2015).

The proposed scheme STIR-RPL (Duroyon, Conti and Lal, 2021) which restructures routing table entries into address intervals to reduce memory consumption is the only published countermeasure specifically targeting RTOA in storing-mode RPL. However, STIR-RPL exhibits three fundamental deficiencies: it allocates routing table capacity without trust awareness, admitting all DAO senders regardless of behavioural history; it provides no adaptive memory management scaled to node trustworthiness; and it contains no detection mechanism for coordinated (colluding)

RTOA in which multiple attackers distribute their DAO floods to evade single-node rate detection. This study demonstrates empirically that these deficiencies cause STIR-RPL to provide zero measurable protection against RTOA under the evaluated conditions.

This paper proposes improved STIR-RPL (iSTIR-RPL), which addresses all three deficiencies through a three-tier trust pool system, adaptive interval sizing, and a suspicion-based colluding group detection mechanism. The proposed iSTIR-RPL receives trust scores from improved Mobility-Aware Secure Trust-Based Routing Protocol for RPL (iMSecTrust-RPL) (Garba et al., 2026) to condition routing-state admission decisions, enabling coordinated defence across both the trust plane and the routing-state plane when operating within the Trust-Aware Framework (TAF) (Garba, 2026). The remainder of this paper is organised as follows. Section 2 reviews related work. Section 3 describes the threat model and empirical failure of STIR-RPL. Section 4 presents the iSTIR-RPL design. Section 5 describes the simulation methodology. Section 6 presents and discusses results. Section 7 concludes the paper.

2.0 RELATED WORK

2.1 Routing Table Overload in Storing-Mode RPL

In IETF RFC 7416, Tsao et al. (2015) formally characterised RTOA and identified routing table

saturation through fabricated DAO flooding as a critical threat to storing-mode RPL deployments. Garba et al., (2025) carried out a subsequent simulation-based studies and confirmed that RTOA impact scales with attacker density and network size, producing complete communication failure in large networks at 20-30% attacker ratios.

2.2 STIR-RPL: The Only Published RTOA-Specific Countermeasure

Duroyon et al. (2021) proposed STIR-RPL as the first mechanism specifically designed to mitigate RTOA in storing-mode RPL. STIR-RPL restructures routing table entries by grouping destination addresses into contiguous intervals, reducing the number of table entries required. STIR-RPL however, lacked empirical validation under realistic adversarial conditions and contained no trust-awareness component, leaving the mechanism vulnerable to coordinated RTOA in which attackers distribute fabricated DAO destinations across the address space to circumvent interval compression.

2.3 Trust-Based Routing Defence for RPL

Prajisha and Vasudevan (2025) integrated Dempster-Shafer belief fusion with mobility awareness in MSecTrust-RPL to improve parent selection under Blackhole and Rank attacks. Whilst effective for

2.4 Positioning of iSTIR-RPL

forwarding-plane threats, MSecTrust-RPL operates at the routing decision plane and cannot prevent DAO flooding from exhausting routing table memory.

Garba et al. (2026) extended MSecTrust-RPL with bounded indirect trust fusion, load-balanced forwarding, and hysteresis-guarded parent switching through iMSecTrust-RPL, and provides trust scores used by iSTIR-RPL for pool-based admission decisions within TAF (Garba, 2026). Established work on recommender reliability in Bayesian reputation systems (Whitby et al., 2004) motivated the trust-bounding approach used in iMSecTrust-RPL. Simulation platforms for RPL trust research have been validated using Python-based discrete-event frameworks (Kauer, 2019; Shashidhar, Thanuja and Kunabeva, 2024; Dey & Ghosh, 2024). DAO rate-limiting (Wadhaj et al., 2020) represents a structural approach to RTOA mitigation but does not address colluding attackers that distribute load across multiple nodes. Airehrour, Gutierrez and Ray, (2019) and comprehensive RPL security surveys (Prajapati et al., 2025; Zilberman, Dvir and Stulman, 2025) confirm that no existing scheme provides unified defence against both trust-manipulation and routing-state exhaustion attacks.

Table 1: Comparison of RTOA Mitigation Approaches

Approach	Year	Mechanism	Colluding RTOA?	Trust Aware?	Key Limitation
STIR-RPL (Duroyon et al., 2021)	2021	Address interval clustering	No	No	No empirical validation; no trust; uniform-address attack bypasses compression
DAO Rate Limiting (Wadhaj et al., 2020)	2020	Per-node DAO rate cap	No	No	Colluding attackers distribute load; single-attacker focus only
MSecTrust-RPL (Prajisha & Vasudevan, 2025)	2025	D-S trust + parent selection	Partial	Yes	Operates at routing decision plane; cannot prevent DAO flooding
iMSecTrust-RPL (Garba et al., 2026)	2026	Bounded D-S; load balance; hysteresis	Partial	Yes	Same routing-decision-plane limitation; cannot control routing state memory
iSTIR-RPL (This Work)	2026	Three-tier trust pool; proportional suspicion; colluding group detection	Yes	Yes	Rank attack PDR deficit inherited from iMSecTrust-RPL (documented trade-off)

3.0 THREAT MODEL AND EMPIRICAL FAILURE OF STIR-RPL

3.1 Threat Model

This study considers RPL networks operating in storing mode. The attacker model assumes internal adversaries capable of two RTOA variants. In standard RTOA, individual malicious nodes inject fabricated DAO messages at high rates, exhausting the routing table of their parent node. In Colluding RTOA,

multiple coordinated attackers distribute their fabricated DAO messages across shared target parents, each sending at a moderate rate to evade single-node rate detection whilst collectively overwhelming available routing state.

3.2 Empirical Demonstration of STIR-RPL Failure

Table 2 presents mean isolated nodes and routing table size under Baseline RPL (RFC 6550) and baseline

STIR-RPL across all topology and attack combinations, averaged across ten seeds and three attacker densities (10%, 20%, 30%).

Table 2: Empirical Failure of STIR-RPL

Topology	Attack	Baseline RPL: Isolated Nodes	STIR-RPL: Isolated Nodes	Baseline RPL: Table Size	STIR- RPL: Table Size
Static	RTOA	4.47	4.47	2.97	2.97
Static	Colluding RTOA	2.17	2.20	2.97	2.97
Mobile	RTOA	3.50	3.50	3.57	3.58
Mobile	Colluding RTOA	1.77	1.77	3.57	3.58
Hybrid	RTOA	3.47	3.47	3.05	3.05
Hybrid	Colluding RTOA	1.77	1.70	3.05	3.05

Table 2 confirms that STIR-RPL produces results numerically identical to Baseline RPL (RFC 6550) across all topology and attack combinations. STIR-RPL's interval compression mechanism cannot prevent routing table exhaustion when attackers systematically inject DAO messages with destination addresses spanning the full interval space, bypassing compression entirely. This finding provides the empirical motivation for the trust-conditioned admission mechanism in iSTIR-RPL..

4.0 iSTIR-RPL DESIGN

iSTIR-RPL enhances STIR-RPL through three coordinated mechanisms. All three mechanisms feed detected malicious nodes into a shared attacker set, which is bidirectionally synchronised with iMSecTrust-RPL when operating within TAF (Garba, 2026).

4.1 Enhancement 1: Trust-Aware Routing-State Admission with Three-Tier Pool System

Rather than applying a single minimum trust threshold for binary admit-or-reject decisions, iSTIR-RPL implements a three-tier trust categorisation that assigns each requesting node to one of three memory pools based on its legitimate belief component $L(i,j)$ supplied by iMSecTrust-RPL (Garba et al., 2026):

Verified pool ($L(i,j) \geq 0.7$): reserved 60% of total routing table capacity. Nodes considered sufficiently observed and reliably forwarding.

New-node pool ($0.3 \leq L(i,j) < 0.7$): reserved 30% of capacity. Partially observed or borderline nodes.

Suspicious pool ($L(i,j) < 0.3$): reserved 10% of capacity. Nodes exhibiting predominantly malicious or suspicious forwarding behaviour.

A DAO request is rejected under two conditions: when the capacity of the relevant pool is exhausted, preventing any single trust category from consuming

resources reserved for other categories; or when the requesting node's suspicion score exceeds $SUSP_max = 5.0$, indicating coordinated DAO flooding behaviour regardless of trust classification.

4.2 Enhancement 2: Adaptive Memory Reservation with Proportional Interval Sizing

The available capacity within each pool is computed as $M_available(c) = \min(M_total - M_used_total, \max(0, M_total \times p(c) - M_used(c)))$, where $p(c)$ is the pool proportion for trust category c (0.60, 0.30, or 0.10) and $M_total = 30$ entries in the simulation configuration. Beyond pool-based admission control, interval size is allocated adaptively according to trust level:

Verified nodes: $interval_size = max_interval_size \times L(i,j)$, scaling continuously with trust up to a maximum of 256 address entries.

New nodes: fixed interval of 30% of maximum size ($256 \times 0.30 = 76$ entries).

Suspicious nodes: minimum interval of 4 address entries regardless of trust value.

4.3 Enhancement 3: Suspicion-Based Routing-State Control with Colluding Group Detection

To detect and mitigate Colluding RTOA, iSTIR-RPL introduces a continuous suspicion score $SUSP(j)$ for each node, computed after a minimum warm-up window of 5 seconds and 10 DAO messages. The DAO rate is computed as $\lambda(j) = DAO_count(j) / t_elapsed$. The RTOA rate threshold is set at $RTOA_RATE_THRESHOLD = SUSP_max \times 3 = 5.0 \times 3 = 15.0$ DAOs per second. The suspicion score is updated as:

$$If \lambda(j) > 15.0: SUSP(j) = SUSP(j) + 2.0 + (\lambda(j) - 15.0) \times 0.3 \quad \dots(1)$$

$$If \lambda(j) \leq 15.0: SUSP(j) = \max(0, SUSP(j) - 0.2) \quad \dots(2)$$

The fixed increment of 2.0 ensures any threshold-crossing event immediately raises concern. The

proportional term $(\lambda(j) - 15.0) \times 0.3$ ensures heavier flooding escalates suspicion faster, making the mechanism self-scaling. When $SUSP(j)$ reaches $SUSP_max = 5.0$, subsequent fake DAO messages from node j are rejected. Colluding RTOA detection: when two or more nodes simultaneously reach $SUSP_max$, iSTIR-RPL identifies them as a coordinated flooding group and blocks their combined entries collectively. This addresses the specific weakness of single-node rate detection.

4.4 Coordination with iMSeTrust-RPL via Shared Attacker Set

When iSTIR-RPL operates within TAF (Garba, 2026), it shares a bidirectional attacker set with iMSeTrust-RPL (Garba et al., 2026). Any node blocked by iSTIR-RPL's suspicion mechanism is simultaneously excluded from the parent candidate pool in iMSeTrust-RPL. Conversely, nodes flagged as Bad Mouthing Attack (BMA) or Ballot Stuffing Attack (BSA) attackers by iMSeTrust-RPL are treated as suspicious in iSTIR-RPL, restricting their routing-state allocation regardless of their Destination Advertisement Object (DAO) rate. This bidirectional coordination ensures that an attacker identified on either plane is automatically excluded by the complementary module.

5.3 Simulation Parameters

5.0 SIMULATION METHODOLOGY

5.1 Simulation Platform

All experiments were conducted using a custom-built Python-based discrete-event simulation environment. The simulator implemented core RPL operations including Destination Oriented Directed Acyclic Graph (DODAG) formation, parent selection, DAO/DODAG Information Object (DIO) message exchange, trust evaluation, and routing-table management. Python-based discrete-event simulation has been validated for RPL security research by Shashidhar et al. (2024), Dey and Ghosh (2024), and Kauer (2019), whose frameworks provided methodological precedent for the approach adopted here.

5.2 Network Topologies and Attacker Configurations

Three topologies were evaluated: static (all 30 nodes stationary), mobile (Random Waypoint 1-3 m/s, sink static), and hybrid (25% mobile, 75% static). Attacker ratios of 10%, 20%, and 30% of the total network population were evaluated across standard RTOA and Colluding RTOA attack variants.

Table 3: Simulation Parameters

Parameter	Value
Simulation coverage area	200 m × 200 m
Total nodes	30
Attacker ratios evaluated	10%, 20%, 30%
Transmission range	50 m
Simulation duration	60 minutes
Mobile-to-static ratio (hybrid)	1:3
Traffic model	CBR: 1 packet per 10 s per node
Packet size	127 bytes (IEEE 802.15.4)
Baseline link reliability	90%
Energy model	Battery: 1,000 ticks; Tx: 1 tick/pkt; Rx: 0.5 tick/pkt
Mobility model	Random Waypoint, 1-3 m/s
Seeds per configuration	10 independent random seeds
Total iSTIR-RPL evaluation runs	180 ($3 \times 2 \times 3 \times 10$)
Routing table capacity (M_total)	30 entries
Trust pool proportions	Verified: 60%; New-node: 30%; Suspicious: 10%
Suspicion threshold ($SUSP_max$)	5.0
RTOA rate threshold	15.0 DAOs per second

6.0 RESULTS AND DISCUSSION

6.1 Node Isolation Under RTOA and Colluding RTOA

Table 4 presents mean isolated nodes under all four defence conditions across three topologies, averaged across three attacker ratios and ten seeds per configuration.

Table 4: Mean Isolated Nodes Under RTOA and Colluding RTOA (averaged across 3 attacker ratios and 10 seeds)

Topology	Attack	Baseline RPL	STIR-RPL	iMSecTrust+STIR	iSTIR-RPL
Static	RTOA	4.47	4.47 (0%)	4.33 (-3%)	0.00
Static	Colluding RTOA	2.17	2.20 (worse)	2.33 (worse)	0.00
Mobile	RTOA	3.50	3.50 (0%)	2.93 (-16%)	0.00
Mobile	Colluding RTOA	1.77	1.77 (0%)	1.70 (-4%)	0.00
Hybrid	RTOA	3.47	3.47 (0%)	3.27 (-6%)	0.00
Hybrid	Colluding RTOA	1.77	1.70 (-4%)	1.90 (worse)	0.00

iSTIR-RPL achieves zero isolated nodes across all 180 evaluation runs. STIR-RPL produces results identical to Baseline RPL (RFC 6550). The iMSecTrust+STIR (Garba et al., 2026) integration reduces isolation marginally in some conditions but fails to eliminate it, and in some cases slightly worsens outcomes (e.g.,

static Colluding RTOA: 2.33 vs 2.17). This confirms that trust-based filtering of DAO senders alone is insufficient — a structural pool-based admission mechanism with rate-based suspicion scoring is required to prevent routing-state exhaustion under coordinated attack.

6.2 Routing Table Size and DAO Rejection

Table 5 presents mean routing table size and DAO rejection count under all four defence conditions, averaged across both attack types.

Table 5: Mean Routing Table Size and DAO Rejection Events Across Topologies and Defence Conditions

Topology	Defence	RT Size (mean)	vs Baseline RPL	DAO Rejected (mean)	vs Baseline RPL
Static	Baseline RPL	2.97	—	75	—
Static	STIR-RPL	2.97	0% (no improvement)	75	0%
Static	iMSecTrust+STIR	3.00	+1% (slightly worse)	61	-19%
Static	iSTIR-RPL	0.81	-73%	0	-100%
Mobile	Baseline RPL	3.57	—	41	—
Mobile	STIR-RPL	3.58	0% (no improvement)	41	0%
Mobile	iMSecTrust+STIR	3.49	-2%	35	-15%
Mobile	iSTIR-RPL	1.10	-69%	0	-100%
Hybrid	Baseline RPL	3.05	—	55	—
Hybrid	STIR-RPL	3.05	0% (no improvement)	53	-4%
Hybrid	iMSecTrust+STIR	3.14	+3% (slightly worse)	48	-13%
Hybrid	iSTIR-RPL	0.84	-72%	0	-100%

STIR-RPL (Duroyon et al., 2021) produces routing table sizes and DAO rejection counts virtually identical to Baseline RPL (RFC 6550) across all topologies, confirming its complete ineffectiveness under the evaluated attack conditions. iMsecTrust+STIR (Garba et al., 2026) reduces DAO rejections by 13-19% per topology through trust-based attacker filtering but does not reduce routing table size, demonstrating that fewer

DAO sources does not prevent table exhaustion when the surviving attackers flood at sufficient rates. iSTIR-RPL reduces routing table size by 69-73% and eliminates DAO rejection events entirely across all configurations.

6.3 Scalability with Increasing Attacker Density

Table 6: Mean Isolated Nodes by Attacker Ratio (averaged across attack types and topologies)

Attacker Ratio	Baseline RPL (Isolated Nodes)	iMsecTrust+STIR (Isolated Nodes)	iSTIR-RPL (Isolated Nodes)
10%	1.62	1.62 (0%)	0.00
20%	2.82	2.90 (worse)	0.00
30%	4.13	3.72 (-9.9%)	0.00

Node isolation under Baseline RPL and iMsecTrust+STIR scales directly with attacker density: from 1.62/1.62 at 10%, to 2.82/2.90 at 20% (iMsecTrust+STIR is worse), to 4.13/3.72 at 30%. iSTIR-RPL maintains zero isolation.

across all densities, demonstrating that the three-tier pool mechanism effectively absorbs increasing attacker pressure by restricting suspicious nodes to the 10% pool capacity regardless of their flooding rate.

6.4 Packet Delivery Ratio

Table 7: Mean PDR Under RTOA and Colluding RTOA (all differences $p > 0.05$)

Topology	Attack	Baseline RPL (%)	STIR-RPL (%)	iMsecTrust+STIR (%)	iSTIR-RPL (%)
Static	RTOA	74.5	74.5	73.0	76.2
Static	Colluding RTOA	70.1	71.0	67.5	72.0
Mobile	RTOA	24.6	24.6	22.0	24.0
Mobile	Colluding RTOA	18.4	18.8	17.8	20.7
Hybrid	RTOA	36.6	36.6	36.6	37.4
Hybrid	Colluding RTOA	38.4	36.9	34.9	37.0

No statistically significant PDR differences were found between iSTIR-RPL and any comparison scheme across all topology-attack combinations (all $p > 0.05$ by independent samples t-test). This confirms that iSTIR-RPL achieves its isolation and routing-table

benefits without imposing a packet delivery penalty, establishing that trust-conditioned routing-state management is compatible with RPL forwarding performance.

6.5 Summary of Key Results

Table 8: Summary of Key Results Across All Defence Conditions



Metric	Baseline RPL	STIR-RPL	iMSecTrust+STIR	iSTIR-RPL
Node isolation (static RTOA)	4.47	4.47 (0%)	4.33 (marginal)	0.00
Node isolation (static Colluding RTOA)	2.17	2.20 (worse)	2.33 (worse)	0.00
RT size — static	2.97	2.97 (0%)	3.00 (worse)	0.81 (-73%)
RT size — mobile	3.57	3.58 (0%)	3.49 (-2%)	1.10 (-69%)
RT size — hybrid	3.05	3.05 (0%)	3.14 (worse)	0.84 (-72%)
DAO rejections	High	High (identical)	Reduced 13-19%	0 (eliminated)
Isolation at 30% attacker density	4.13	—	3.72	0.00
PDR impact	Baseline	Equivalent	Slightly worse	Statistically equivalent

7.0 CONCLUSION

This paper presented iSTIR-RPL, a three-mechanism enhancement of STIR-RPL addressing the fundamental deficiencies of the only published RTOA-specific countermeasure for storing-mode RPL. The empirical demonstration that STIR-RPL provides zero measurable protection against RTOA — a finding not previously reported in the literature — establishes the necessity of the architectural changes introduced in iSTIR-RPL.

Evaluated across 180 simulation runs spanning three topologies, two attack variants, three attacker densities, and ten seeds per configuration, iSTIR-RPL eliminated node isolation completely, reduced routing table size by 69-73%, and dropped DAO rejection events to zero, whilst maintaining statistically equivalent PDR to all comparison schemes. The three-tier trust pool mechanism, adaptive interval sizing, and suspicion-based colluding group detection collectively provide a robust and scalable solution to routing-state exhaustion in storing-mode RPL. When integrated within TAF (Garba et al., 2026) via the shared attacker set with iMSecTrust-RPL (Garba et al., 2026), iSTIR-RPL contributes to a unified defence covering both the trust plane and the routing-state plane.

Future work includes physical testbed validation on Zolertia Re-Mote hardware, evaluation at larger network scales (50-150 nodes), adaptive trust threshold tuning, and extension to non-storing mode RPL variants.

ACKNOWLEDGEMENTS

This research was supported by the Tertiary Education Trust Fund (TETFund) Academic Staff Training and Development (AST&D) Local PhD Scholarship awarded to the first author through Sa'adatu Rimi College of Education (SRCOE), Kano, Nigeria.

REFERENCES

Airehrour, D., Gutierrez, J. A., & Ray, S. K. (2019). SecTrust-RPL: A secure trust-aware RPL routing

protocol for Internet of Things. *Future Generation Computer Systems*, 93, 860–876. <https://doi.org/10.1016/j.future.2018.03.021>

Dey, D., & Ghosh, N. (2024). iTRPL: An intelligent and trusted RPL protocol based on multi-agent reinforcement learning. *Ad Hoc Networks*, 163, 103586. <https://doi.org/10.1016/j.adhoc.2024.103586>

Duroyon, M., Conti, M., & Lal, C. (2021). STIR: Preventing routing table overload attacks in RPL-based IoT networks [Bachelor's thesis, Delft University of Technology]. TU Delft Repository. <https://resolver.tudelft.nl/uuid:03b45e33-2af2-48e7-8dd3-017eb7c99ef4>

Garba, F. A. (2026). Development of a trust-aware framework (TAF) for mitigating multi-vector routing attacks in RPL-based smart object networks [Doctoral dissertation, Ahmadu Bello University]. Department of Computer Science, ABU Zaria.

Garba, F. A., Junaidu, S. B., Ali, Y. S., & Tanko, A. I. (2026). iMSecTrust-RPL: A load-balanced, mobility-resilient trust management protocol for mitigating trust manipulation attacks in RPL-based IoT networks. Manuscript submitted for publication.

Garba, F. A., Yalli, J. S., Akande, J. O., Sagagi, I. T., Ibibo, J. T., Aliyu, A. S., & Adegoke, S. O. (2025). Performance evaluation of routing table overload attack in RPL-based IoT network. In *Proceedings of the 19th International Conference on Technology and Computing (ConNovate 2025): Intelligent, Secure and Sustainable Innovations for Connected World* (pp. 204–211). Nigeria Computer Society. <https://library.ncs.org.ng/download/performance-evaluation-of-routing-table-overload-attack-in-rpl-based-iot-network/>

Kauer, F. (2019). Scalable wireless multi-hop networks for industrial applications [Doctoral dissertation, Technische Universität Hamburg]. <https://doi.org/10.15480/882.2500>

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. arXiv:2501.10817.
<https://arxiv.org/abs/2501.10817>
- 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/s10922-025-09898-0>
- Shashidhar, P. K., Thanuja, T. C., & Kunabeva, R. (2024). Adaptive RPL routing optimisation model for multimedia data transmission using IoT. *Indian Journal of Science and Technology*, 17(5), 427–436. <https://doi.org/10.17485/IJST/v17i5.2785>
- Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A., & Richardson, M. (2015). A security threat analysis for the routing protocol for low-power and lossy networks (RFC 7416). Internet Engineering Task Force. <https://doi.org/10.17487/RFC7416>
- Wadhaj, I., Ghaleb, B., Thomson, C., Al-Dubai, A., & Buchanan, W. J. (2020). Mitigation mechanisms against the DAO attack on the routing protocol for low power and lossy networks (RPL-based networks). *IEEE Access*, 8, 43665–43675. <https://doi.org/10.1109/ACCESS.2020.2977476>
- Whitby, A., Jøsang, A., & Indulska, J. (2004). Filtering out unfair ratings in Bayesian reputation systems. In *Proceedings of the 7th International Workshop on Trust in Agent Societies (AAMAS 2004)* (pp. 106–117).
- Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Struik, R., Vasseur, J. P., & Alexander, R. (2012). RPL: IPv6 routing protocol for low-power and lossy networks (RFC 6550). Internet Engineering Task Force. <https://doi.org/10.17487/RFC6550>
- 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*. Advance online publication. <https://doi.org/10.1145/3708530>