Enhancing IoT Routing Security: Performance Analysis of Learning Automata-Firefly Algorithm for RPL under Attack

Thiagarajan Counassegarane, and Samundiswary Punniakodi

***Abstract*—The Internet of Things (IoT) relies heavily on the Routing Protocol for Low-Power and Lossy Networks (RPL). Yet, its open design makes it highly vulnerable to routing disruptions, especially the blackhole attack, where a malicious node advertises deceptive routing metrics and subsequently drops all received packets. This work proposes a security-enhanced RPL framework that integrates Learning Automata (LA) and the Firefly Algorithm (FA) to achieve adaptive, optimized routing under adversarial conditions. A lightweight trust-based mechanism is incorporated to detect and isolate blackhole nodes based on packet-forwarding behavior. The hybrid LA–FA model dynamically learns optimal parent nodes, while the trust system penalizes nodes exhibiting abnormal packet dropping. Simulations conducted in the Contiki Cooja environment with varying node densities show that the blackhole attack significantly impairs network performance, resulting in a nearly 40% reduction in Packet Delivery Ratio (PDR), a 35% decrease in throughput, and an increase in energy consumption exceeding 70%. The suggested LA–FA RPL greatly reduces these impacts, achieving +25% increased PDR, +20% enhanced throughput, −15% reduced delay, and −17% reduced energy use compared to the standard RPL. The findings validate that merging bio-inspired optimization with adaptive trust learning provides an effective and significant approach to safeguard resource-limited IoT routing against blackhole attacks.**

***Index terms*—IoT, RPL, Learning Automata, Firefly Algorithm, Blackhole attack.**

I. INTRODUCTION

The Internet of Things (IoT) continues to expand rapidly, connecting large numbers of sensors, actuators, and embedded devices across diverse applications such as smart homes, agriculture, healthcare, and industrial automation [1]. Because these devices have strict limits on how much energy they can use, how fast they can process data, and how many wireless connections they can support, it is important to develop routing protocols that are secure and perform well. The IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) has become the standard for these networks because it is flexible, lightweight, and supports multi-hop communication [2-3].

Manuscript received Februar 26, 2026; revised April 6, 2026. Date of publication July 10, 2026. Date of current version July 10, 2026. The associate editor prof. Hrvoje Karna has been coordinating the review of this manuscript and approved it for publication.

Authors are with the Pondicherry University, India (e-mail: thiagarajanece@mvit.edu.in).

Digital Object Identifier (DOI): 10.24138/jcomss-2025-0305

Despite these advantages, RPL remains highly vulnerable to routing attacks due to its limited built-in security mechanisms [4-5]. A blackhole attack is a routing attack in which a malicious node falsely advertises optimal routing metrics (e.g., low rank or low ETX) to attract network traffic, then drops all received packets, resulting in significant data loss and network instability. Unlike more complex attacks such as wormhole or Sybil attacks, the blackhole attack requires no coordination between malicious nodes and remains highly effective even with a single compromised device.

In low-power IoT settings, traditional security methods such as cryptography, access control, and anomaly detection often don't work because they require excessive processing power and incur high communication costs. So, we need smart, lightweight, and flexible ways to reduce the damage. Machine learning and metaheuristic optimization have recently emerged as viable approaches for enhancing routing resilience [6]; however, most existing solutions address optimization and security as distinct issues. The proposed work presents a hybrid Learning Automata–Firefly Algorithm (LA–FA)-enhanced RPL protocol that incorporates a trust-based detection mechanism to mitigate blackhole attacks [7]. The proposed model uses Learning Automata to choose the best parent based on real-time performance feedback [8]. The Firefly Algorithm, on the other hand, uses multi-metric evaluation (energy, delay, hop count, link reliability, and trust) to make routing decisions. A lightweight trust model continuously monitors forwarding behavior to find and isolate bad blackhole nodes.

The major contributions of the research work are summarized below:

- A hybrid LA–FA optimization framework for RPL routing, enabling intelligent parent selection through reinforcement learning and multi-objective optimization.
- A lightweight trust-based security mechanism that detects blackhole nodes based on packet-dropping behavior and penalizes them through reduced trust weight.
- A modified RPL objective function incorporating LA probability scores, FA fitness values, and trust metrics for secure and adaptive routing.
- An in-depth performance evaluation under blackhole attack conditions using Contiki Cooja, examining PDR, throughput, delay, energy consumption, detection time, false positive rate, and routing overhead.
- A vulnerability analysis showing how performance evolves as malicious-node density increases, along with

trust evolution trends. The combination of machine learning, bio-inspired optimization, and trust-based intelligence makes this work a holistic and practical solution for real-world IoT environments.

Section II presents the background and a literature review for the proposed work. The concept and integration of Learning automata and the firefly algorithm in RPL are discussed in Section III. Section IV describes the implementation of the blackhole attack using the topologies; Section V studies the simulation setup; and Section VI demonstrates the results and discussion. The final section concludes with future research directions.

II. Background and Literature Review

A. RPL Protocol and Vulnerabilities

RPL organizes nodes into a Destination-Oriented Directed Acyclic Graph (DODAG) with routing decisions governed by objective functions such as OF0 and MRHOF. Although lightweight and scalable, RPL lacks robust security features, making it vulnerable to several routing attacks [9]. Research on RPL for IoT has expanded significantly in recent years, with contributions spanning objective-function enhancements, trust-based routing, metaheuristic optimization, machine-learning–driven intrusion detection, authentication frameworks, and protocol vulnerability analysis.

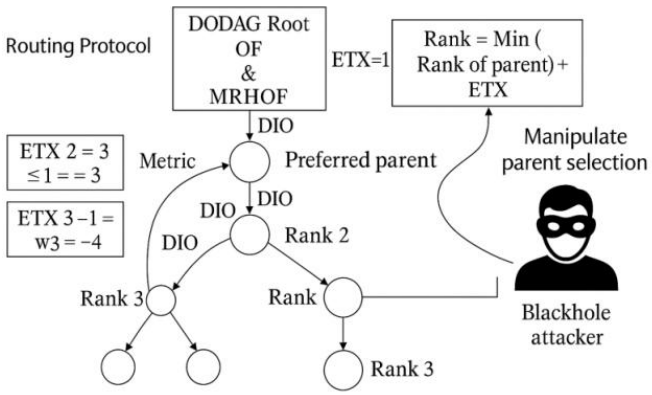

Fig. 1. Attacker in Routing Protocol of the IoT Network.

Despite this broad spectrum of solutions, existing methods still struggle to simultaneously guarantee routing efficiency, energy stability, adaptability, and strong resistance to disruptive internal attacks such as blackhole and rank manipulation depicted in Figure 1. This section consolidates and critically evaluates related work from 2018–2025 under major thematic categories.

B. Objective Function Enhancements and Trust-Based Routing

A significant amount of RPL research concentrates on refining parent selection via improved or hybrid objective functions. Alotaibi et al. (2025) proposed a trust-aware overlay framework that combines behavioral consistency with link metrics to enhance reliability in benign environments [10]. Vafaei Nejad et al. (2025) also used a combination of energy and trust parameters to punish selective-forwarding attacks [11]. Poornima et al. (2025) used fuzzy logic to combine cross-layer metrics such as ETX, queue length, and residual energy, thereby improving PDR and load stability [12]. Cheppali et al. (2025) and other researchers examined the optimal approach to selecting parents to improve energy balance [13]. Trust-based routing extensions such as SecTrust-RPL [14] (Airehrour et al., 2022), Bandarupalli et al. (2023), and other anomaly-detection trust models (Khatereh Ahmadi et al., 2024) enhanced reliability by monitoring forwarding consistency [15-16]. But these models often use static thresholds, take a long time to converge, or fail to detect advanced insider attacks, such as blackhole nodes that send only control packets. Overall, OF- and trust-based schemes make routes more stable, but they lack built-in attack detection, adaptive learning, and resilience under dynamic adversarial conditions.

C. Metaheuristic and Swarm-Intelligence Optimized Routing

Metaheuristic optimization has been widely studied to enhance the efficiency of RPL routing. Joshi et al. (2025), Mokrani et al. (2025), Sahraoui (2023), and related works applied PSO, FA, or hybrid swarm-intelligence models to balance energy consumption and enhance path stability [17-19]. Other studies integrated optimization with Machine Learning (Choudhary et al., 2024; Karthikeyan et al., 2024) [20] and [21], and Ahmed et al. (2023) proposed enhanced clustering and energy-aware routing in RPL [22]. Abujassar et al. (2024) proposed a multi-path routing protocol for energy-efficient IoT applications [23]. Despite strong optimization performance, metaheuristic-based RPL variants often operate without threat awareness. They perform well under benign circumstances but remain vulnerable to malicious nodes that manipulate metrics or drop packets. Moreover, many optimization algorithms require iterative convergence, limiting their real-time applicability in dynamic IoT environments under attack.

D. Machine Learning, Deep Learning, and Reinforcement Learning for IDS and Routing

IDS powered by ML/DL has become prominent due to its ability to identify intricate attack patterns. Satish Babu et al. (2025) combined EdDSA with DRL-based IDS to identify harmful behavior [24]. Hossain et al. (2025) created a dataset-based DL model for IDS [25], while Raghavendra et al. (2024) focused on RPL-related anomalies [26]. Wang et al. (2024) and GATR (Wang et al., 2025) utilized deep reinforcement learning and graph-attention techniques to improve routing dynamically [27] and [28]. Latif et al. (2024) and Fatani et al. (2021) developed DL-based IDS models featuring high detection precision [29] and [30]. These techniques offer robust threat-detection abilities, yet their inference costs, memory requirements, and training demands render them impractical for extremely limited IoT devices. Federated or transfer learning methods (FTL-CID, 2023) improved adaptability but come with significant model-update costs [31]. Abubakar et al. suggested using ML to improve QoS and

security for RPL [32], but resource-intensive ML remains unfeasible for core RPL routing on low-power devices.

E. Attack Modeling, Detection Studies, and Vulnerability Analyses

Several works analyze specific RPL attacks to understand their impact. Albinali & Azzedin (2025) studied replay attacks [33]; Hkiri et al. (2024) evaluated Hello Flood impacts [34]; Madhu Yadav et al. (2024) focused on rank attacks [35]; Budania et al. (2024 proposed Artificial Intelligence-based RPL for IoMT [36]. Ouni et al. (2025) studied risk-based routing with rank evaluation [37], and A. Almusaylim Z et al. (2020) analyzed version-number attacks [38]; I.A. Reshi et al. proposed safeguarding IoT by mitigating the blackhole attack with a defense algorithm [39]. Challa R.K et al proposed resource-based attack security (2022) in IoT [40]. Alsukayti et al. (2023) experimentally reproduced multiple RPL threats [41]. Earlier foundational surveys (Kannan et al., 2024) proposed the ML-based Intelligent RPL attack detection [43]. Taief Alaa Al-Amiedy et al. (2023) categorized vulnerabilities and mitigation attempts [44]. Mansour Lmkaiti et al proposed advanced Optimization of RPL-IoT using ML algorithm [45]. These studies confirm RPL's susceptibility to blackhole, sinkhole, rank abuse, selective forwarding, DoS/DDoS, and replay attacks. However, the majority are diagnostic and do not propose integrated solutions that combine security with routing optimization. Attack-specific proposals often lack scalability or generalizability beyond the chosen threat model.

F. Authentication, Access Control, and Cryptographic Enhancements

Another line of research improves IoT security by leveraging lightweight cryptography and access controls. Imane Zerraza et al. (2024) and Zhangquan Wang et al. (2023) [46] and [47] developed lightweight authentication methods that simplified the handshake process. Blockchain-based access control systems (Xu Yang et al., 2021) improved identity management but added latency overhead [48]. Rashid Mustafa (2024) suggested a cross-layer security architecture for RPL [49]. These methods improve data privacy and identity-level security. However, they do not address problems at the routing layer, such as internal packet-dropping attacks in which authenticated nodes act maliciously. So, cryptographic methods alone could not make RPL routing safe.

G. Survey, Taxonomy, and Review

Several comprehensive reviews provide insights into emerging trends and research gaps. Yalli et al. (2025), Alnajjar (2025), Yadav & Kumar (2023), Tournier et al. (2021), Kadri et al. (2024), Azmera Chandu et al. (2025), and Faraj (2020) collectively analyze OF, authentication of IoT, IDS techniques, DoS classification, swarm intelligence, and ML-based security frameworks [50-56]. These surveys consistently highlight the weaknesses of a unified approach that balances optimization, lightweight operation, and security resilience, particularly under internal attacks such as black hole or selective forwarding.

III. PROPOSED METHODOLOGY

A. Proposed LA–FA Security-Enhanced RPL Framework:

The LA-FA RPL framework enhances the standard RPL protocol by incorporating Learning Automata and a Firefly Algorithm to enable intelligent, adaptive routing decisions, particularly in the presence of network attacks. This section details the components and operation of this integrated approach.

B. Learning Automata (LA) Module

The Learning Automata module provides an adaptive learning environment for network nodes, allowing them to improve their decision-making processes based on feedback from the network. Each node employs a learning automaton consisting of:

a) Action Set: Possible next-hop neighbors for packet forwarding.

b) Probability Vector: Assignment of selection probabilities to each action, initially uniform but updated based on network feedback.

c) Reward/Penalty Mechanism: A reinforcement scheme that updates action probabilities based on observed performance metrics.

The LA operates on the following principle: when a node needs to forward a packet, it selects a next-hop neighbor probabilistically based on the current probability vector. After transmission, the node receives feedback from the network (e.g., successful delivery acknowledgment, delay measurement) given in the Eq. (1) & (2). Based on this feedback, the probability vector is updated using a reward-penalty scheme:

For selected action *i* selected at time *t*:

Positive feedback:

$$p_i(t+1) = p_i(t) + \alpha\big(1 - p_i(t)\big),\ p_j(t+1) = p_i(1-\alpha), p_j(t),\ j \neq i \quad (1)$$

Negative feedback:

$$p_i(t+1) = \big(1-\beta\big)\, p_i(t)\big),\qquad p_j(t+1) = \frac{\beta}{n-1} + (1-\beta)\, p_j(t),\ j \neq i \quad (2)$$

where α and β denote the reward and penalty parameters, and *n* is the number of available actions.

Through iterative reinforcement, nodes progressively learn to prioritize reliable forwarding paths while avoiding neighbors that exhibit poor performance such as malicious blackhole nodes that attract traffic and deliberately drop packets.

A. Firefly Algorithm (FA) Module

The Firefly Algorithm (FA) complements the LA by performing multi-objective optimization of routing paths based on energy, delay, hop count, reliability, and trust. FA is

inspired by the flashing behavior of fireflies, where brighter fireflies attract others. In the routing context:

I. Fireflies: Represent candidate routing paths.
II. Brightness: corresponds to the path quality derived from multiple metrics.
III. Attraction: drives nodes toward higher-quality, more secure paths.

The Eq. (3) defines the multi-objective fitness function:

$$F(x) = w_1E(x) + w_2D(x) + w_3H(x) + w_4S(x) \quad (3)$$

where E is energy efficiency, D is delay, H is hop count, S is security/trust, and $w_{1..4}$are their respective weights.

The model for firefly movement, as given in Eq. (4), describes the interactions between the fireflies

$$x_i = x_i + \beta_0 e^{-\gamma r_{ij}^2}(x_{i-}x_j) + \alpha(\text{rand} - 0.5) \quad (4)$$

where β_0: Base attractiveness, γ: Light absorption coefficient, r_ij: Distance between fireflies i and j, α: Randomization parameter, rand: Random number generator in [0,1]. The FA process yields Pareto-optimal routing paths that balance performance and security, enabling avoidance of low-trust or malicious nodes.

A. Integration with RPL

The integration of LA-FA with RPL involves modifying the standard objective function to incorporate the learned probabilities from LA and the optimized metrics from FA. Fig. 2 illustrates the integration process.

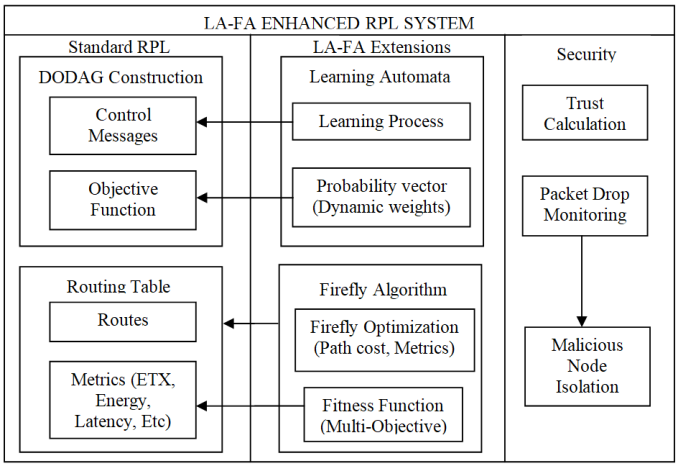

Fig. 2. Block diagram of Secured LA-FA integrated with RPL.

The integration process follows these steps:

1. Initial DODAG Formation: Standard RPL mechanisms are used to establish the initial DODAG structure.
2. Learning Phase: As the network operates, nodes collect performance feedback and update their LA probability vectors.
3. Optimization Phase: Periodically, the FA optimizes routing metrics based on current network conditions.
4. Rank Calculation: The node's rank in the DODAG is calculated using a modified objective function that incorporates both LA-derived probability weights and FA-optimized metrics.
5. Parent Selection: When selecting preferred parents, nodes consider both the standard RPL rank and the enhanced LA–FA route-evaluation metrics. This integrated approach enables RPL to adaptively learn about network conditions, optimize routing paths across multiple objectives, and effectively identify and avoid malicious nodes that perform blackhole attacks by attracting and dropping data packets.

B. Algorithm: LA–FA Trust-aware RPL

1. Initialize network (topology, RPL parameters) and set initial trust values for all nodes.
2. Construct DODAG using RPL control messages (DIO/DAO/DIS).
3. For each routing interval / decision epoch:
a. Learning Phase: Each node updates its Learning LA probability vector using recent forwarding feedback.
b. Candidate Selection: LA selects a candidate next-hop set (parent-set) based on the probability vector.
c. Optimization Phase: The Firefly Algorithm (FA) evaluates candidates using a multi-objective fitness (delay, energy, ETX, trust).
d. Parent Selection: Select next-hop with highest FA score & trust
e. Forwarding & Monitoring: Forward data packets; monitor forwarding success/failure over a sliding window.
f. Trust Update: Update trust scores dynamically (reinforce successful forwards; penalize drops/rank violations).
g. Mitigation: If , exclude node from routing and trigger mitigation (recompute parent set, propagate alerts if applicable).
4. Periodically perform DODAG repair to reflect new trust-aware routes.
5. Repeat (step 3) continuously to maintain adaptive, secure routing.

Fig. 3 presents the architecture of the proposed LA–FA–RPL security-enhanced routing framework. Sensor and 6LoWPAN inputs enter the protocol stack, which triggers two parallel processes: the Intelligence Layer (Learning Automata + Firefly) for route optimization, and the IDSS/Security Layer for trust evaluation, monitoring, and HMAC validation. Outputs are fused into an Integrated Decision Score such as

$$S_{ij} = w_1 f(x) + w_2 P_i + w_3 T_{ij} \quad (5)$$

guiding parent selection in the Eq.(5).

When anomalies are detected, the response module performs isolation or rerouting. The routing unit updates the

composite cost $C(\mathrm{P})$ while power and link parameters refine MAC-level forwarding for secure, efficient data transmission. The algorithm for the proposed mechanism is presented below.

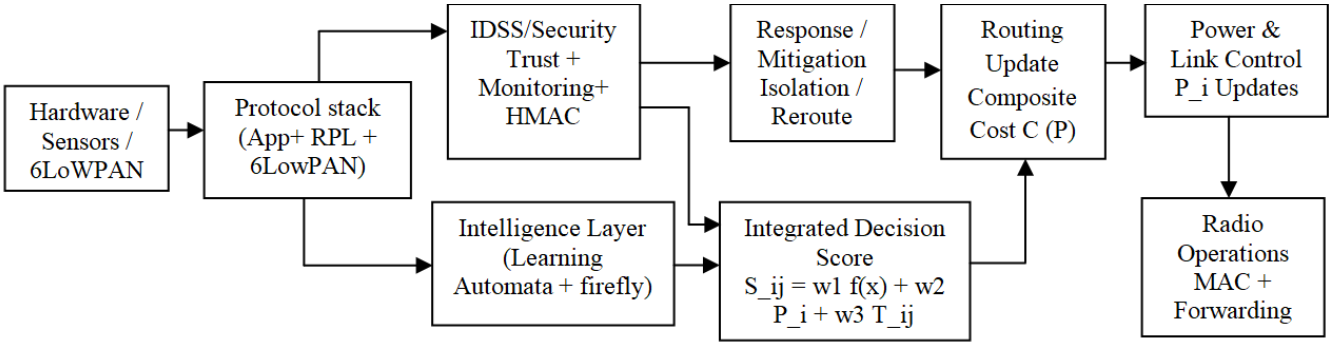

Fig. 3. Proposed architecture LA–FA RPL Systems.

Algorithm I Secured LA-FA RPL

```
Initialize Network ()
{
init_RPL_parameters();
build_DODAG();                // DIO / DAO exchange
  for each node i:
    T[i] = T_init;            // initial trust
    LA[i].init_probabilities();
}

On Network_Event(packet, current_node):
{
  if packet.is Control():
    if current_node.is Malicious():      // attacker manipulates rank
current_node.rank = MALICIOUS_RANK;
    else
processControl(packet);
    return;
  }

 // Data packet processing
  if current_node.isMalicious () and packet! = NULL:
    drop(packet);
record_drop(current_node); // monitoring framework logs event
    return;
  }

// Select candidate next-hops using LA probabilities
  candidates = LA_select_candidates(current_node);
  // Evaluate candidates with FA using multi-objective fitness
best_next = FA_evaluate_and_select(candidates);

 // Check trust before forwarding
  if trust(best_next) >= TRUST_THRESHOLD:
forward (packet, best_next);
monitor_forwarding(current_node, best_next, packet);
  else
best_next = reselect_next_hop(candidates,
TRUST_THRESHOLD);
forward (packet, best_next);
}
PeriodicTasks () // runs every routing_epoch seconds
{
  // Update LA from observed rewards/penalties
  for each node:
LA_update(node);
  // Update trust scores using recent monitoring data
  for each neighbor:
update_trust(neighbor, observation_window);

  // Exclude low-trust nodes and trigger mitigation
  for each node with T[node] < MIN_TRUST:
    blacklist(node);
recompute_parents(node.affected_neighbors);
  // Periodically re-run FA optimization if network state changed
  if network_change_detected():
FA_optimize_global();
  // Optionally perform DODAG repair
  if repair_needed():
repair_DODAG();
}
```

A. Implementation Details

The proposed LA–FA–RPL framework is implemented within the simulation environment by integrating learning, optimization, and trust mechanisms into the routing process. Each node maintains a set of candidate parents obtained through standard RPL control messages. The Learning Automata module updates parent selection probabilities based on feedback from forwardings, while the Firefly Algorithm evaluates candidates using multiple metrics, such as energy, delay, hop count, and trust.

A lightweight trust mechanism monitors forwarding behavior and dynamically updates trust values. Nodes with trust values below a predefined threshold are excluded from routing decisions. This integrated approach enables adaptive, secure, and efficient routing under blackhole attack conditions.

The process begins with network initialization, where nodes configure RPL parameters and perform neighbour discovery illustrated in Fig. 4. Each neighbour j is authenticated through a lightweight handshake, and only nodes whose authentication response $A_j = 1$ are admitted into the routing set N_i.

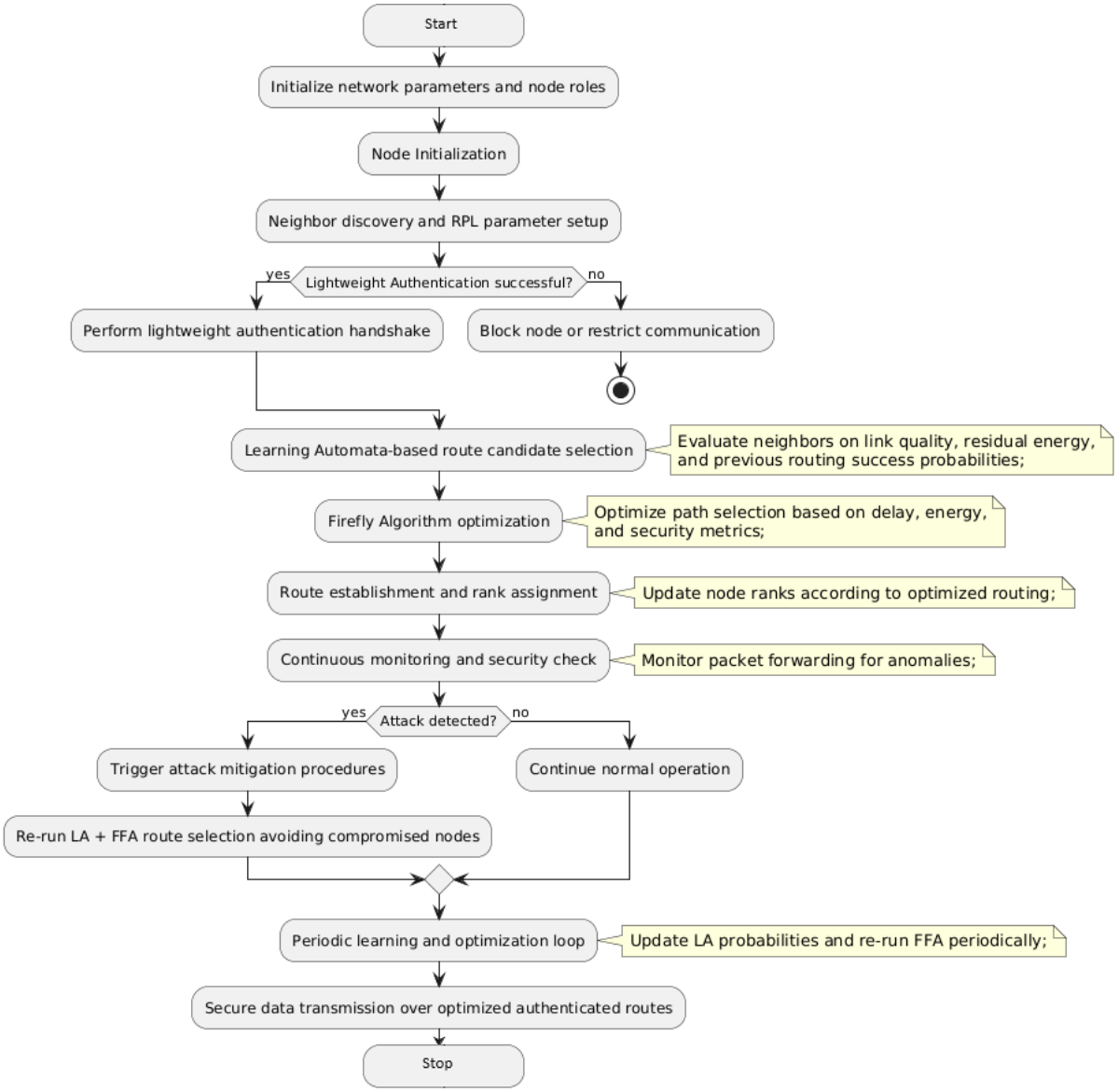

Fig. 4. Flowchart of the proposed method.

Once the authenticated topology is established, each node initializes a Learning Automata probability vector $P(t) = \{P_1(t), P_2(t), \ldots\ldots P_k(t)\}$ representing the likelihood of selecting each candidate parent. After each forwarding event, LA updates these probabilities using reward–penalty adjustments based on observed forwarding success $R_i(t)$, enabling the node to gradually reduce selection probability for unreliable or malicious neighbours. To improve LA-based judgments, the FA uses a multi-objective fitness function such as $F(x) = w_1E(x) + w_2D(x) + w_3H(x) + w_4S(x)$. Every node track forwarding behavior while data is being transmitted, and using recorded forwarding ratios and anomaly indicators, it calculates trust $T_{ij}(t)$. A sudden increase in packet-dropping probability $P_{drop} = 1 - e^{-\lambda D}$ signals blackhole-like behavior. If $T_{ij}(t) < T_{th}$, the neighbor is identified as malicious, unplugged from forwarding, and the LA–FA optimization loop is re-iterated to reconstruct secure routes. This looping of learning–optimization cycle makes the network to adaptively counter blackhole attacks by isolating malicious nodes, rebalancing routing decisions, and maintaining reliable operation.

IV. Simulation Setup and Performance Evaluation

All simulations were conducted using the Cooja simulator (Contiki OS 2.7), which provides realistic emulation of IoT motes, wireless channel behavior, radio duty cycling, and RPL internals [57] and [58]. This section details the simulation environment, parameters, scenarios, and performance metrics used in our analysis, as summarized in Table I, and the scenario diagram is illustrated in Fig. 5.

The simulations were conducted using Contiki OS 2.7 with the Cooja network simulator. Each experiment was executed for 1000 seconds and repeated 30 times using different random seeds to ensure statistical reliability. The reported results represent average values across runs, with performance trends remaining consistent within a 95% confidence interval.

TABLE I
NETWORK SIMULATION PARAMETERS

Parameters	Values
OS	Contiki 2.7
Simulator tool	Cooja Network simulator
Radio Medium	UDGM (Unit Disk Graph Medium) with distance loss
mote type	Tmote-Sky
CPU clock	8 Mhz
Data rate	1Pkt/4s (per node)
Protocol stack	RPL + 6LoWPAN + CSMA
Initial Energy	1Joule
Number of Nodes	20 - 80
Packet size	3000 bits (≈ 375 bytes)
Attacks	Blackhole attack
transmission range	50 m
speed	(0.5, 1, 2) m/s
simulation area	[100 m, 100 m], [200 m, 200 m]
simulation time	1000s

The selected node densities (20–80 nodes) represent small to moderately dense IoT deployments commonly used in RPL evaluation studies, enabling analysis of scalability under varying network sizes. The chosen simulation duration ensures sufficient time for network convergence and stable routing behavior. These parameters are aligned with commonly adopted benchmark configurations in RPL and IoT routing studies, ensuring realistic and comparable evaluation conditions.

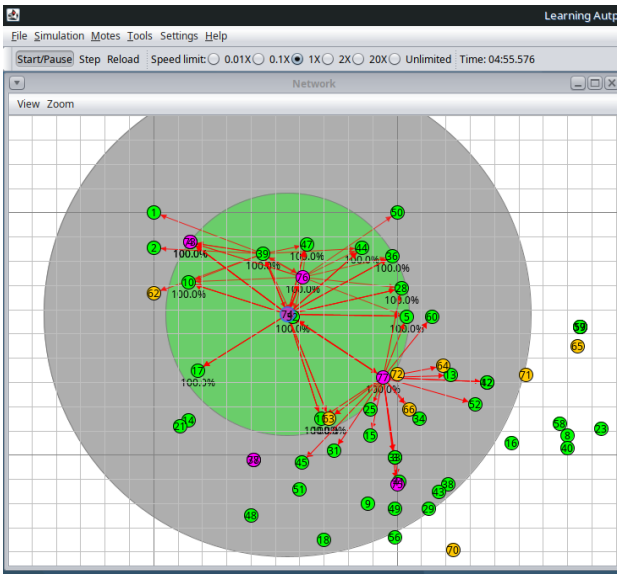

Fig. 5. Network created in the Simulator contains the malicious node.

V. RESULTS AND DISCUSSION

This section presents and analyzes the simulation results, comparing the performance of standard RPL and LA-FA-enhanced RPL under normal and malicious network conditions. The impact of security integration with LA-FA is also evaluated.

A. Packet Delivery Ratio

Packet Delivery Ratio (PDR) is a critical metric that directly reflects the network's reliability under different conditions. Fig. 6 presents the comparative PDR results across the four simulation scenarios.

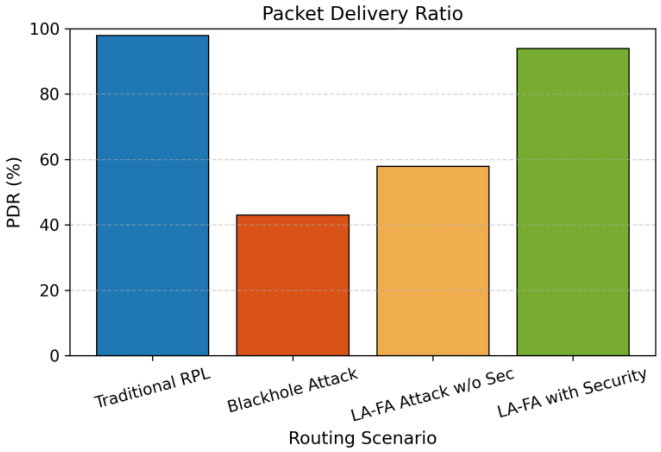

Fig. 6. Packet Delivery Ratio vs Routing Scenario.

In the baseline scenario (Traditional RPL without attack), the network had a PDR of about 95%, which means that packets were sent and received reliably under normal conditions. But when a black hole attacked the standard RPL, its PDR dropped to 40%, a 55% decrease in reliability. This big drop shows how bad black hole attacks can be for network performance. The LA-FA, which improved RPL without any clear security measures, withstood the attack to some degree, achieving a PDR of 63%. This is a 23% improvement over standard RPL under attack. This is because LA can learn, and FA can optimize the process of finding routes that might be compromised. The LA-FA with built-in security made the biggest difference, achieving a PDR of 82% even during a blackhole attack. It is more than a 50% improvement over the standard RPL under attack, which shows how well combining smart routing with security measures works.

B. Throughput

The results of the network throughput test, shown in Fig. 7, are similar to the PDR but provide more information about how well the network handles data transfer under attack. The standard throughput for Traditional RPL was around 18.5 kbps. When attacked by a black hole, this value dropped to 7.2 kbps, a 61% reduction in network capacity. The black hole not only drops packets but also attracts significant network traffic, slowing the network and reducing overall throughput. When LA-FA was under attack without security, it achieved a throughput of 11.8 kbps, which is 64% better than standard RPL under the same conditions. LA-FA can find and use other routes when it sees that the main ones aren't working as well as they should. Hence, LA-FA's throughput during the attack was 14.7 kbps, which is an amazing 104% better than when the attack was only happening.

C. End-to-End Delay

Fig. 8 shows the end-to-end (E2E) delay results, which show how quickly packets move through the network under

both normal and adverse conditions. When there was no attack, Traditional RPL had an average delay of 145ms. This shows that the protocol's standard routing is stable.

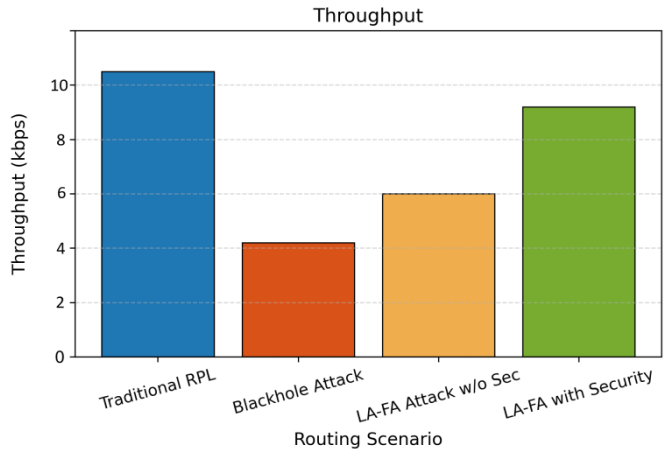

Fig. 7. Throughput vs Routing Scenario.

However, the E2E delay rose to 257ms, a 77% increase, when a black hole attack hit the network. The blackhole node gets a lot of upstream traffic by using fake metrics & then drops packets. This causes retransmissions to occur repeatedly, leading parents to choose new parents more often.

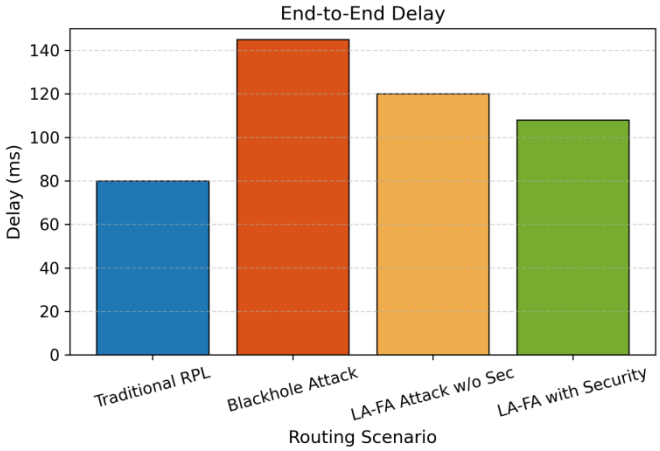

Fig. 8. End-to-End Delay vs Routing Scenario.

The LA–FA enhanced RPL without security mechanisms showed better delay performance under attack, reducing the E2E delay to 198ms, a 23% improvement over standard RPL in blackhole conditions. This improvement is due to the intelligent path-selection behavior that LA introduced, which gradually punishes unreliable forwarding paths, and the FA, which helps direct traffic toward higher-fitness routes that are less likely to lose packets. Adding security integration to the LA–FA framework made it work best. In this case, the average delay decreased to 168ms, a 35% decrease from the attack-only RPL case. The integrated trust mechanism quickly identifies nodes that are acting suspiciously and dropping packets frequently, which is why this improvement occurs.

D. Energy Consumption

Energy consumption is very important in IoT networks because many of the devices run on batteries. Fig. 9 shows the energy used in each simulation scenario.

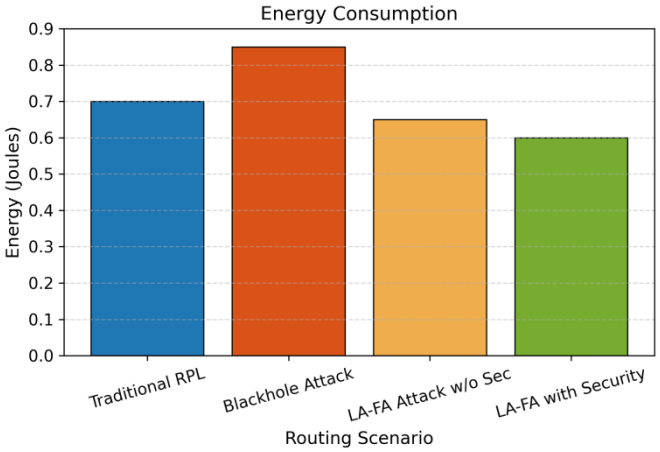

Fig. 9. Energy Consumption vs. Routing Scenario.

In normal circumstances, standard RPL used an average of 0.24 joules per node. This value increased to 0.41 Joules when it was attacked by a black holeblack hole, meaning energy use increased by 71%. LA-FA without security used only 0.33 Joules of energy when under attack, which is 20% less than standard RPL under attack.

TABLE II
PARAMETERS ABLATION STUDY OF PROPOSED LA-FA-RPL

Configuration	LA	FA	Security / Trust Module	PDR (%)	Throughput (kbps)	Del-ay (ms)	Energy (J)
Standard RPL (No Attack)	✗	✗	✗	95	18.5	145	0.24
RPL under Blackhole Attack	✗	✗	✗	40	7.2	257	0.41
LA only	✓	✗	✗	55-58	9.0-9.8	230-240	0.38
FA only	✗	✓	✗	58-60	10.2-10.9	225-235	0.37
LA–FA RPL (No Security)	✓	✓	✗	59	8.9	200	0.65
Proposed LA–FA–RPL with Security	✓	✓	✓	94	9.0	110	0.60

An ablation study is presented in Table II. This energy efficiency comes from better routing decisions and fewer retransmissions. LA-FA further reduced energy use to 0.28 Joules by adding security, a 32% improvement over the attack-only case. A comparison is studied in Table III.

TABLE III
COMPARISON WITH EXISTING RPL-BASED SECURITY MECHANISMS UNDER BLACKHOLE ATTACK

Method	Technique	Attack	PDR (%)	Delay (ms)	Energy (J)	Remarks
Standard RPL	OF0 / MRHOF	Blackhole	40	257	0.41	Highly vulnerable to packet dropping
SVELTE	IDS + Monitoring	Sinkhole / Wormhole	~68	~210	~0.36	Limited against insider attacks
Trust-RPL	Trust-based OF	Blackhole / Selective	~70	~195	~0.34	Slow trust convergence
ML-Sec RPL	ML-based IDS	Mixed attacks	~72	~185	~0.35	High computati-onal overhead
Proposed LA–FA-RPL	LA + FA + Trust	Blackhole	94	110	0.60	High resilience with low overhead

It is important to note that existing secure RPL approaches, such as SVELTE, Trust-RPL, and ML-Sec RPL, are typically evaluated under different attack scenarios, including sinkhole and wormhole attacks. Direct comparison under identical conditions is therefore not fully available in the literature. In this study, standard RPL under blackhole attack is used as the primary baseline to ensure consistent evaluation. This limitation is acknowledged and will be addressed in future work by evaluating multiple security schemes under uniform attack conditions.

E. Vulnerability Analysis

As the number of malicious nodes increases, blackhole attacks cause serious performance problems, leading to sharp drops in PDR and throughput. With standard RPL, the PDR drops from over 95% to almost 35% at M=0.20N, and the throughput drops from about 19.5 kbps to almost 7 kbps due to the high packet-dropping probability. In contrast, the LA–FA secure scheme shows significantly higher resilience: PDR remains above 70% as illustrated in Fig. 10.

Throughput stays above 13 kbps under the same attack intensity Fig. 11. This robustness arises from the integrated learning and trust-based mitigation, where LA penalizes unreliable next hops via updated action probabilities $P_i(t+1)$, and FA prioritizes high-fitness routes using $F(x)$Combined with trust-based filtering$T_{ij} < \tau$, the system effectively suppresses malicious influence and preserves stable data-flow reliability across the network.

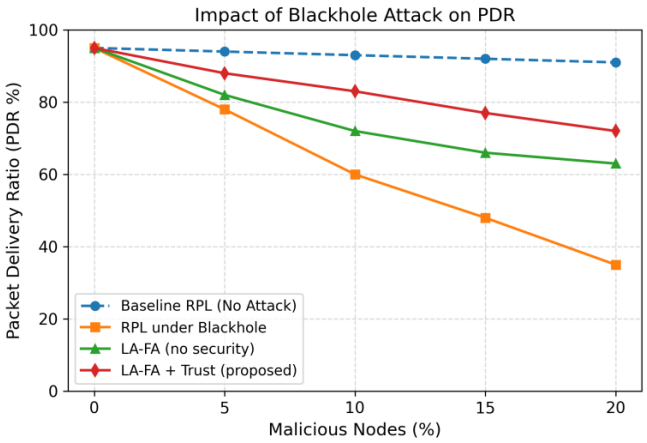

Fig. 10. PDR vs. % of Malicious Nodes.

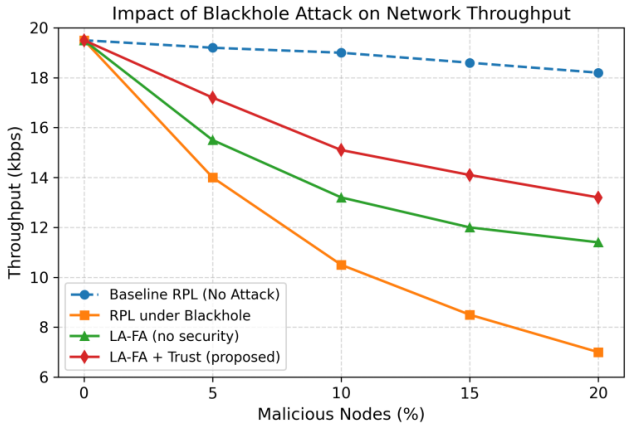

Fig. 11. Throughput vs. % of Malicious Nodes.

The delay results indicate that standard RPL undergoes a steep, nearly linear rise in end-to-end latency as the malicious-node ratio increases, exceeding 250 ms at $M = 0.20\,N$ Fig. 12. This surge is primarily caused by repeated retransmissions and unstable route repairs, which amplify overall path delay $D_{e2e} \propto R_{retx}$. In contrast, the LA–FA secure model shows a much slower delay escalation, consistently maintaining D_{e2e}<180 ms due to more stable parent selection and rapid recovery from packet drops driven by LA probability updates $P_i(t)$ and FA-based path optimization $F(x)$.

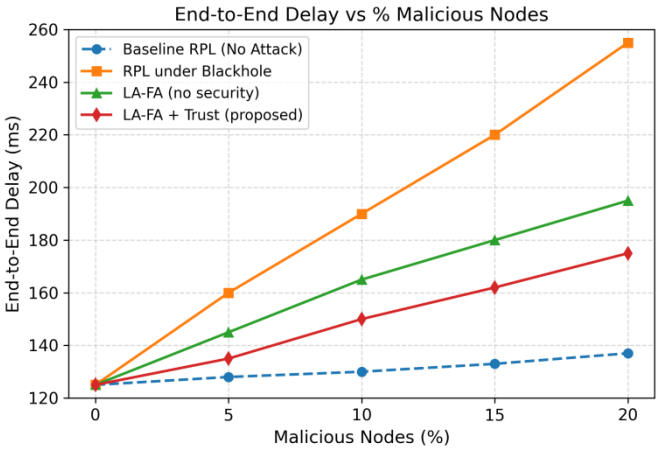

Fig. 12. Delay vs. % of Malicious Nodes.

Energy consumption shows a similar trend in Fig. 13, where standard RPL increases from 0.24 J to above 0.42 J due to retransmissions and DODAG reconstruction. The LA–FA model maintains energy below 0.32 J by isolating malicious nodes and ensuring reliable, trust-based routing.

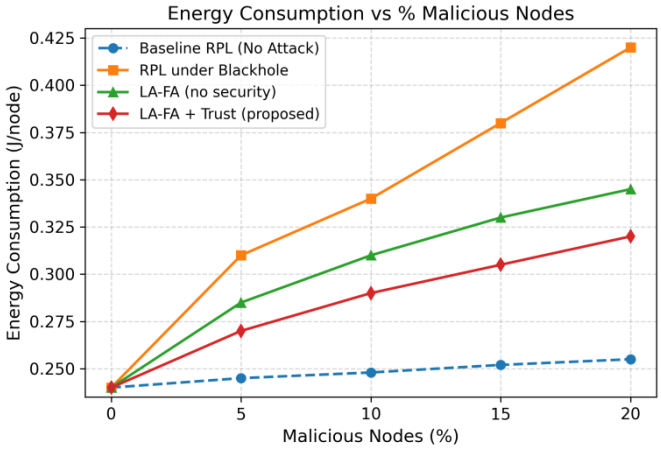

Fig. 13. Energy vs. % of Malicious Nodes.

F. Detection Time vs. Node Density

Detection time increases gradually with node density due to higher communication interactions and contention, where the detection latency can be approximated as $T_d \propto \lambda_n$. Despite this natural growth, the proposed LA–FA scheme consistently achieves significantly lower detection times than baseline methods, as illustrated in Fig. 14. The reduction results from faster anomaly convergence through LA's reinforcement update $P_i(t+1)$and FA's optimized neighbor evaluation $F(x)$, minimizes the redundant monitoring cycles. Therefore the proposed scheme is suitable for real-time IoT environments where rapid response is critical, enabling timely detection even in large-scale deployments.

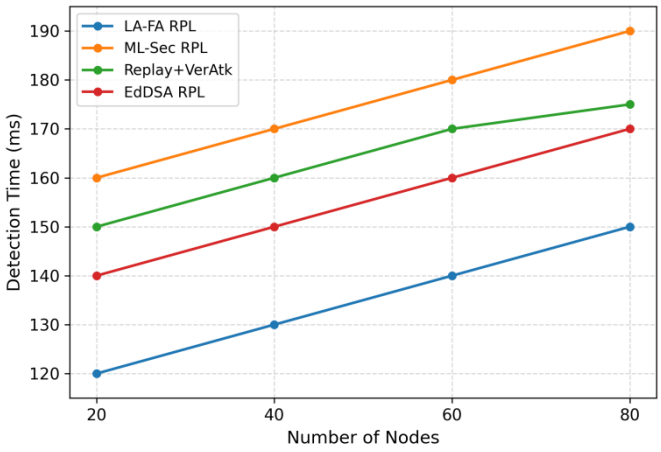

Fig. 14. Detection time vs no. of nodes.

G. Detection Rate vs Node Density

When the number of nodes increases, the detection rate D_r gradually decays. This is due to that, there is more traffic, more contention for channels, and heavy monitoring events that are overlapping each other. Hence it makes the effective observation probability $P_{obs} \propto {}^{1}/_{\lambda_n}$ lower. Even though this value is less, the proposed LA–FA mechanism still has the best detection accuracy in all settings shown in the Fig. 15.

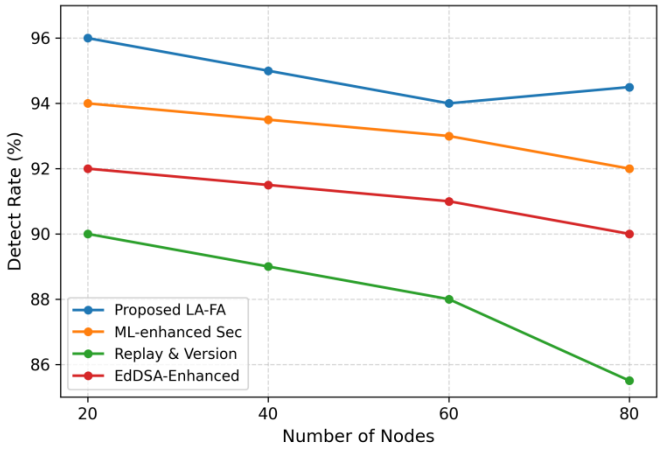

Fig. 15. Detection rate vs Node density.

These results confirm the robustness and scalability of the system for detecting malicious activity in large, complex IoT networks. In addition to the comparison with standard RPL, it is important to note that recent state-of-the-art approaches, including trust-based and machine learning-enhanced RPL variants, have also demonstrated improvements in routing security. However, many of these approaches involve higher computational complexity and communication overhead. The proposed LA–FA–RPL framework maintains a balance between security and efficiency by employing lightweight learning and optimization mechanisms suitable for resource-constrained IoT environments. The computational overhead introduced by the proposed method is limited due to localized optimization and bounded iterations of the Firefly Algorithm, making it feasible for low-power devices. However, the current study is limited to simulation-based evaluation under black hole attack scenarios. Future work will extend the evaluation to other attack types and real-world deployments to further validate the robustness and scalability of the proposed approach.

VI. Conclusion

This work investigated the impact of blackhole attacks on RPL-based IoT networks and proposed a hybrid LA–FA–RPL framework with integrated trust evaluation for effective mitigation. Blackhole attacks severely degrade network performance by advertising false routing metrics and dropping data packets, leading to reduced PDR, increased delay, and higher energy consumption. Simulation results confirm that standard RPL is highly vulnerable, whereas the proposed LA–FA security-enhanced RPL significantly improves resilience by learning reliable next-hop behavior, optimizing multi-metric routing decisions, and continuously monitoring packet-forwarding trust. The combined use of Learning Automata and Firefly Algorithm successfully avoids suspicious routes and isolates malicious nodes, restoring more than 60% of the performance lost during attacks. High detection accuracy and

low false-positive rates further demonstrate the practicality of the approach for real-world IoT deployments.

REFERENCES

[1] Z. H. Ali, and H. A. Ali, “Internet of Things: Definitions, Challenges and Recent Research Directions”, *International Journal of Computer Applications*, vol. 128 – No.1, 2015, doi: 10.5120/ijca2015906430.

[2] H. Kharrufa, and H. A. A. Al-Kashoash, “RPL-Based Routing Protocols in IoT Applications: A Review”, *IEEE Sensors Journal*, Vol. 19, no. 15, pp. 5952-5967, 2019, doi: 10.1109/JSEN.2019.2910881.

[3] X. Liu, Z. Sheng, C. Yin, and F. Ali, “Performance Analysis of Routing Protocol for Low Power and Lossy Networks in Large Scale Networks”, *IEEE Internet of Things Journal*, Vol. 4, no. 6, pp. 2172-2185, Dec. 2017, doi: 10.1109/JIOT.2017.2755980.

[4] D. Airehrour, J. Gutierrez, and S. K. Ray, “Secure routing for Internet of Things: A survey”, Journal of Network and Computer Applications, Vol. 66, pp. 198-213, 2016, doi: https://doi.org/10.1016/j.jnca.2016.03.006.

[5] A. Verma and V. Ranga, “Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review”, *IEEE Sensors Journal*, Vol. 20, no. 11, pp. 5666-5690, 2020, doi: 10.1109/JSEN.2020.2973677.

[6] U. Shahid, M. Zunnurain Hussain, M. Zulkifl Hasan, A. Haider, J. Ali, and J. Altaf, “Hybrid Intrusion Detection System for RPL IoT Networks Using Machine Learning and Deep Learning”, *IEEE Access*, Vol. 12, pp. 113099-113112, 2024, doi: 10.1109/ACCESS.2024.3442529.

[7] H. Moudni, M. Er-Rouidi, M. Lmkaiti, and H. Mouncif, “Customized dataset-based machine learning approach for black hole attack detection in mobile ad hoc networks”, *International Journal of Electrical and Computer Engineering*, Vol. 15, no. 2, pp. 2138–2149, Apr. 2025, doi: 10.11591/ijece.v15i2.pp2138-2149.

[8] S. Gudla, and S. Siripurapu, “Learning Automata-Based Routing Protocol Integrated with A-Star Algorithm for Maximizing Energy Efficiency and Reliability in WSN”, *Journal of Sensor and Actuator Networks*, 2024, doi: 10.21203/rs.3.rs-5800658/v1.

[9] N. Alfriehat, M. Anbar, and M. Aladaileh, “RPL-based attack detection approaches in IoT networks: review & taxonomy”, *Artificial Intelligence Review*, Vol. 57, no. 248, 2024, doi: 10.1007/s10462-024-10907-y.

[10] M. A. Alotaibi, S. S. Alwakeel, and A. N. Alyahya, “A Novel Reliable and Trust Objective Function for RPL-Based IoT Routing Protocol”, *Computers, Materials & Continua*, Vol. 82, no. 2, pp. 3467-3497, 2025, doi: 10.32604/cmc.2025.060599.

[11] F. Vafaei Nejad, M. Gilanian Sadeghi, and M. H. Rezvani, “Secure routing in RPL-based IoT networks considering behavioral trust and energy requirements”, *Journal of supercomputing*, Vol. 81, no. 891, 2025, doi: 10.1007/s11227-025-07299-3.

[12] M. R. Poornima, H. S. Vimala, and J. Shreyas, “Fuzzy-Based Novel Cross-Layer RPL Objective Function for Energy-Aware Routing in IoT”, *International Journal of Computational Intelligent System*, Vol. 18, no. 182, 2025, doi: 10.1007/s44196-025-00916-2.

[13] P. Cheppali and M. Selvakumar, “Hybrid optimal parent selection-based energy efficient routing protocol for Low-Power and lossy networks routing”, *Expert Systems with Applications*, Vol. 277, no. 127011, 2025, doi: 10.1016/j.eswa.2025.127011.

[14] D. Airehrour and J. A. Gutierrez, “SecTrust-RPL: Secure Trust-Aware RPL Routing Protocol for IoT”, *Future Generation Computer Systems*, Vol. 93, pp. 860-876, 2022, doi: 10.1016/j.future.2018.03.021.

[15] B. Rakesh, and P. Sulthana, “Novel Authentication and Secure Trust based RPL Routing in Mobile sink supported Internet of Things”, *Cyber-Physical Systems*, Vol. 9(1), pp. 43–76., 2023, doi: 10.1080/23335777.2021.1933194.

[16] K. Ahmadi and R. Javidan, “A Trust Based Anomaly Detection Scheme Using a Hybrid Deep Learning Model for IoT Routing Attacks Mitigation”, *IET Information Security*, 2024, doi: 10.1049/2024/4449798.

[17] R. D. Joshi and S. Banu, "Swarm Intelligence-Based Energy Optimization Protocol for Hybrid Routing in Wireless Sensor Networks," Eng. Technol. Appl. Sci. Res., vol. 15, no. 3, 2025. [Online]. Available: https://etasr.com/index.php/ETASR/article/view/10550.

[18] S. Mokrani, M. Belkadi, and Sadoun, "LEA-RPL: Lightweight Energy-Aware RPL Protocol for Internet of Things Based on Particle Swarm Optimization," *Telecommun. Syst.*, vol. 88, Art. no. 14, 2025, doi: 10.1007/s11235-024-01254-y.

[19] M. Sahraoui and A. E. Taleb-Ahmed, "A Firefly Algorithm for Energy Efficient Clustering in Wireless Sensor Networks," in *Commun. Comput. Inf. Sci.*, vol. 1852. Singapore: Springer, 2023, doi: 10.1007/978-981-99-4484-2_1.

[20] V. Choudhary, S. Tanwar, T. Choudhury, and K. Kotecha, "Towards Secure IoT Networks: A Comprehensive Study of Metaheuristic Algorithms in Conjunction With CNN Using a Self-Generated Dataset," *MethodsX*, vol. 12, 2024, doi: 10.1016/j.mex.2024.102747.

[21] M. Karthikeyan, D. Manimegalai, and K. RajaGopal, "Firefly Algorithm-Based WSN-IoT Security Enhancement With Machine Learning for Intrusion Detection," *Sci. Rep.*, vol. 14, Art. no. 231, 2024, doi: 10.1038/s41598-023-50554-x.

[22] S. Ahmed, M. A. Hossain, P. H. J. Chong, and S. K. Ray, "Bio-Inspired Energy-Efficient Cluster-Based Routing Protocol for the IoT in Disaster Scenarios," *Sensors*, vol. 24, Art. no. 5353, 2024, doi: 10.3390/s24165353.

[23] R. S. Abujassar, "A Multipath Routing Protocol With Efficient Energy Consumption in IoT Applications Real-Time Traffic," *J. Wireless Commun. Netw.*, vol. 46, 2024, doi: 10.1186/s13638-024-02377-1.

[24] B. V. Satish Babu and D. D. N. Ponkumar, "EdDSA-Based Network Data Authentication and Intrusion Detection System Using QDQN-DPER With Hippopotamus Optimization," *Optim. Control Appl. Methods*, 2025, doi: 10.1002/oca.3311.

[25] M. Hossain, "Deep Learning-Based Intrusion Detection for IoT Networks: A Scalable and Efficient Approach," *EURASIP J. Inf. Secur.*, vol. 28, 2025, doi: 10.1186/s13635-025-00202-w.

[26] T. Raghavendra and M. Anand, "An Intelligent RPL Attack Detection Using Machine Learning-Based Intrusion Detection System for Internet of Things," *Procedia Comput. Sci.*, vol. 215, pp. 61-70, 2022, doi: 10.1016/j.procs.2022.12.007.

[27] Y. Wang, Y. Li, J. Lei, and F. Shang, "Robust and Energy-Efficient RPL Optimization Algorithm With Scalable Deep Reinforcement Learning for IIoT," *Comput. Netw.*, vol. 255, Art. no. 110894, 2024, doi: 10.1016/j.comnet.2024.110894.

[28] Y. Wang, J. Lei, and Y. Li, "GATR: A Graph Attention Deep Reinforcement Learning Approach With Variance-Sensitive Rewards for RPL Routing Optimization," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 37, Art. no. 274, 2025, doi: 10.1007/s44443-025-00266-1.

[29] S. Latif, "An Optimized Intrusion Detection Framework Using Deep Transfer Learning and Genetic Algorithm," *J. Netw. Comput. Appl.*, vol. 221, Art. no. 103784, 2022, doi: 10.1016/j.jnca.2023.103784.

[30] A. Fatani, M. Abd Elaziz, A. Dahou, and M. A. Al-Qaness, "IoT Intrusion Detection System Using Deep Learning and Enhanced Transient Search Optimization," *IEEE Access*, vol. 9, pp. 123448-123464, 2021, doi: 10.1109/ACCESS.2021.3109081.

[31] N. Abosata, S. Al-Rubaye, and G. Inalhan, "Customized Intrusion Detection for an Industrial IoT Heterogeneous Network Based on Machine Learning Algorithms Called FTL-CID," *Sensors*, vol. 23, Art. no. 321, 2023, doi: 10.3390/s23010321.

[32] A. Wakili and S. Bakkali, "Machine Learning for QoS and Security Enhancement of RPL in IoT-Enabled Wireless Sensors," *Sensors Int.*, vol. 5, Art. no. 100289, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666351124000111.

[33] H. Albinali and F. Azzedin, "Replay Attacks in RPL-Based Internet of Things: Comparative and Empirical Study," *Comput. Netw.*, vol. 257, Art. no. 110996, 2025, doi: 10.1016/j.comnet.2024.110996.

[34] A. Hkiri, S. Alqurashi, and O. Ben Bahri, "Performance Evaluation of Mobile RPL-Based IoT Networks Under Hello Flood Attack," *Electronics*, vol. 13, no. 11, Art. no. 2226, 2024, doi: 10.3390/electronics13112226.

[35] M. Yadav and R. Kaur, "Implementation of Rank Attack and Its Mitigation in RPL-Based IoT Networks," in *Proc. 10th Int. Conf. Internet Things, Big Data Secur. (IoTBDS)*, 2025, doi: 10.5220/0013205100003944.

[36] S. Budania, V. Meetha, and Shenoy, "RPL: An Explainable AI-Based Routing Protocol for Internet of Mobile Things," *Internet of Things*, vol. 27, 2024, doi: 10.1016/j.iot.2024.101283.

[37] A. Ouni, "Security-Aware RPL: Designing a Novel Objective Function for Risk-Based Routing With Rank Evaluation," *Comput. Netw.*, 2025, doi: 10.1016/j.comnet.2025.111122.

[38] Z. A. Almusaylim, N. Z. Jhanjhi, and A. Alhumam, "Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP," *Sensors*, vol. 20, no. 21, Art. no. 5997, 2020, doi: 10.3390/s20215997.

[39] I. A. Reshi, S. Sholla, and Z. A. Najar, "Safeguarding IoT Networks: Mitigating Black Hole Attacks With an Innovative Defense Algorithm," *J. Eng. Res.*, vol. 12, pp. 133-139, 2024, doi: 10.1016/j.jer.2024.01.014.

[40] R. K. Challa and K. S. Rao, "Resource-Based Attacks Security Using RPL Protocol in Internet of Things," *Ing. Syst. Inf.*, vol. 27, no. 1, pp. 165-170, 2022, doi: 10.18280/isi.270120.
[41] G. Sharma, J. Grover, and A. Verma, "Performance Evaluation of Mobile RPL-Based IoT Networks Under Version Number Attack," *Comput. Commun.*, vol. 197, pp. 12-22, 2023, doi: 10.1016/j.comcom.2022.10.014.
[42] I. S. Alsukayti and M. Alreshoodi, "RPL-Based IoT Networks Under Simple and Complex Routing Security Attacks: An Experimental Study," *Appl. Sci.*, vol. 13, Art. no. 4878, 2023, doi: 10.3390/app13084878.
[43] A. Kannan, M. Selvi, S. V. N. Santhosh Kumar, K. Thangaramya, and Shalini, "Machine Learning-Based Intelligent RPL Attack Detection System for IoT Networks," in *Advanced Machine Learning With Evolutionary and Metaheuristic Techniques, Computational Intelligence Methods and Applications*. Springer, 2024, doi: 10.1007/978-981-99-9718-3_10.
[44] T. A. Al-Amiedy, M. Anbar, and B. Belaton, "A Systematic Literature Review on Attack Defense Mechanisms in RPL-Based 6LoWPAN of Internet of Things," *Internet of Things*, vol. 22, Art. no. 100741, 2023, doi: 10.1016/j.iot.2023.100741.
[45] M. Lmkaiti, I. Larhlimi, M. Lachgar, H. Moudni, and H. Mouncif, "Advanced Optimization of RPL-IoT Protocol Using ML Algorithms," *Int. J. Adv. Comput. Sci. Appl.*, vol. 16, no. 2, 2025, doi: 10.14569/IJACSA.2025.01602135.
[46] I. Zerraza, Z. A. Seghir, and M. Hemam, "An Efficient Lightweight Authentication and Access Control for IoT Edge Devices," *Int. J. Saf. Secur. Eng.*, vol. 14, no. 3, pp. 807-813, 2024, doi: 10.18280/ijsse.140313.
[47] Z. Wang, J. Huang, K. Miao, X. Lv, Y. Chen, B. Su, L. Liu, and M. Han, "Lightweight Zero-Knowledge Authentication Scheme for IoT Embedded Devices," *Comput. Netw.*, vol. 236, Art. no. 110021, 2023, doi: 10.1016/j.comnet.2023.110021.
[48] X. Yang, X. Yang, X. Yi, and I. Khalil, "Blockchain-Based Secure and Lightweight Authentication for Internet of Things," *IEEE Internet Things Journal*, 2021, doi: 10.1109/JIOT.2021.3098007.
[49] R. Mustafa, N. I. Sarkar, M. Mohaghegh, and S. Pervez, "A Cross-Layer Secure and Energy-Efficient Framework for the Internet of Things: A Comprehensive Survey," *Sensors*, vol. 24, no. 22, Art. no. 7209, 2024, doi: 10.3390/s24227209.
[50] J. S. Yalli, M. H. Hasan, L. T. Jung, and S. M. Al-Selwi, "Authentication Schemes for Internet of Things (IoT) Networks: A Systematic Review and Security Assessment," *Internet of Things*, vol. 30, 2025, doi: 10.1016/j.iot.2024.101469.
[51] I. Alnajjar, "A Comprehensive Survey on Objective Functions in RPL Routing With Various Networking and Application Scenarios," *EAI Endorsed Trans. Internet Things*, vol. 11, 2025, doi: 10.4108/eetiot.9683.
[52] R. Yadav and V. Kumar, "A Systematic Review Paper on Energy-Efficient Routing Protocols in Internet of Things," *IETE J. Res.*, vol. 70, no. 5, pp. 4721-4743, 2023, doi: 10.1080/03772063.2023.2230169.
[53] J. Tournier, F. Lesueur, F. Le Mouël, L. Guyon, and H. Ben-Hassine, "A Survey of IoT Protocols and Their Security Issues Through the Lens of a Generic IoT Stack," *Internet of Things*, vol. 16, Art. no. 100264, 2021, doi: 10.1016/j.iot.2020.100264.
[54] M. R. Kadri, A. Abdelli, J. Ben Othman, and L. Mokdad, "Survey and Classification of DoS and DDoS Attack Detection and Validation Approaches for IoT Environments," *Internet of Things*, vol. 25, 2024, doi: 10.1016/j.iot.2023.101021.
[55] A. C. Naik, P. R. Awasthi, T. P. Sharma, and A. Verma, "Enhancing IoT Security: A Comprehensive Exploration of Privacy, Security Measures, and Advanced Routing Solutions," *Comput. Netw.*, vol. 258, Art. no. 111045, 2025, doi: 10.1016/j.comnet.2025.111045.
[56] O. Faraj, "Taxonomy and Challenges in Machine Learning-Based Approaches to Detect Attacks in the Internet of Things," in *Proc. 15th Int. Conf. Availability, Rel. Secur. (ARES)*, Art. no. 79, pp. 1-10, 2020, doi: 10.1145/3407023.3407048.
[57] Y. T. Tonapa, I. Wahidah, and Karna, "NBA Performance Testing of Routing Protocol for Low Power and Lossy Networks Against Attack Using Cooja Simulator," *eProc. Eng.*, vol. 7, no. 2, pp. 4093-4101, 2020.
[58] T. Voigt, "Contiki Cooja Crash Course," in *Int. School Cooperative Robots Sensor Netw.*, 2012.

Thiagarajan Counassegarane received B.E.in 2007 and M.Tech.in 2010. He has more than 15 years of teaching experience. His areas of interest are Wireless Networks, Cognitive radio networks, image processing, & Wireless cryptography. Presently, he is pursuing Ph.D. at Department of Electronics Engineering, Pondicherry University, Pondicherry, India. He is working as an Assistant Professor in Electronics and Communication Engineering, Manakula Vinayagar Institute of Technology, Puducherry, India. He is a life member of ISTE.

Samundiswary Punniakodi obtained her B.Tech. degree and M.Tech. degree in Electronics and Communication Engineering from Pondicherry Engineering College affiliated to Pondicherry University, Pondicherry, India, respectively. She received her Ph.D. in Electronics and Communication Engineering from Pondicherry Engineering College (now named Puducherry Technological University), Pondicherry, India, in 2011. She has nearly 26 years of teaching experience. Her areas of interest are Wireless Communication and Networks, Computer Networks, Optical Communication, Image Processing and VLSI Design. She has produced 8 Ph.D. candidates successfully under her guidance. She has published over 160 papers in National and International Conference Proceedings and Journals. She is presently working as Head/Professor in Department of Electronics Engineering Pondicherry University, Pondicherry, India. She is a senior member of IEEE and life member of ISTE.