Secure Optimization of RPL Routing in IoT Networks: Analysis of Metaheuristic Algorithms in the Face of Attacks

Mansour Lmkaiti[1], Maryem Lachgar[2], Ibtissam Larhlimi[3], Houda Moudni[4], Hicham Mouncif[5]
LIMATI Laboratory-Polydisciplinary Faculty, University Sultan Moulay Slimane, Morocco[1,2,3,5]
TIAD Laboratory-Faculty of Sciences and Technology, University Sultan Moulay Slimane, Morocco[4]

***Abstract*—The security and efficiency of Internet of Things (IoT) networks depend on optimizing the routing protocol for low-power, lossy networks (LPNs) to manage various challenges, including expected number of transmissions (ETX), latency and energy consumption. This study proposes an advanced metaheuristic optimization framework integrating several algorithms, including Particle Swarm Optimization (PSO), Mixed Integer Linear Programming (MILP), Adaptive Random Search with two-step Adjustment (ARS2A) and Simulated Annealing (SA), to improve the performance of RPL-based IoT networks under attack scenarios. Our methodology focuses on secure routing by integrating dynamic anomaly detection and adaptive optimization mechanisms to mitigate network threats such as Blackhole, Sinkhole, and Wormhole attacks. Simulations were carried out on large-scale IoT networks with 100 and 150 nodes to evaluate the performance of the proposed algorithms. Experimental results indicate that ARS2A and MILP offer the best compromise between security and performance, achieving minimal ETX (1.28), reduced latency (0.12 ms) and optimized energy consumption (0.85 J) in dense networks. Furthermore, simulated annealing demonstrates high adaptability to mitigate routing attacks while guaranteeing stable energy efficiency. The comparative analysis highlights the strengths and weaknesses of each algorithm, underscoring the need for hybrid optimization strategies that balance computational cost and real-time adaptability. This work establishes a secure and scalable optimization framework for IoT networks, contributing to the development of intelligent, resilient and energy-efficient routing solutions.**

***Keywords*—IoT Security; PSO; MILP; ARS2A; simulated annealing; RPL protocol; metaheuristic techniques; routing efficiency; ETX; latency; energy consumption; attack mitigation; blackhole; wormhole; grayhole; cyberattack**

I. Introduction

Mission-critical applications in fields including smart cities,industrial surveillance-health [1], and critical infrastructure management have emerged as a result of the Internet of Things (IoT) explosive growth. These networks [2], which are composed of linked sensor nodes,need to optimize energy use while guaranteeing safe and effective data transfer. However, their decentralized architecture, coupled with limited hardware resources, exposes them to major challenges, particularly in terms of reliability, energy efficiency and security against cyber-attacks. The Routing Protocol for Low-Power and Lossy [3] Networks is one of the numerous vulnerabilities in these networks are of particular concern. Numerous attacks take advantage of RPL flaws to interfere with routing and jeopardize data transfer. The most destructive of these are the Blackhole [4], Sinkhole, Wormhole and Selective Forwarding attacks, which reroute, delay, or eliminate packets moving throughout the network. These threats [5] have a direct impact on network performance, increasing the number of retransmissions required (ETX), latency and energy consumption. These degradations have the potential to cause significant system failures in critical applications,like medical and environmental networks, endangering the availability and integrity of services.

The development of sophisticated attack detection [6] and mitigation techniques that can preserve the best possible balance between security energy efficiency [7], and quality of service(QoS) is essential in light of these expanding threats. Traditional cryptography-based solutions and authentication often prove unsuitable for IoT networks [8] due to the energy and computing constraints of sensors. Therefore,a more dynamic and intelligent strategy that incorporates cutting-edge optimization techniques [9] is needed to improve routing resilience while lowering energy expenses.

In light of this,our work suggests a novel strategy that combines behavioral analysis methods with metaheuristic optimization algorithms [9], in order to secure IoT networks against attacks targeting the RPL protocol [10]. Optimizing packet routing is the goal by taking into account three fundamental metrics:

- Expected Transmission Count (ETX): Indicator of link quality, measuring the Average number of transmissions required to route a packet. A high ETX value reflects increased routing instability, often caused by attacks or interference.
- Latency: Total time required to transmit a packet from the source node to the destination node. Excessive latency is often a symptom of the presence of attacks such as Wormhole, Flooding or Selective Forwarding.
- Consumed Energy [11]: Total amount of energy consumed by nodes during transmissions. An abnormal increase in this metric is generally a sign of attack, resulting from artificially generated traffic or packet hijacking.

In order to optimize safety and network resilience, we use four sophisticated optimization algorithms [12]:

- Simulated Annealing: Enhances routing robustness by facilitating effective solution space exploration while avoiding local minima.

- Particle Swarm Optimization: Simultaneously minimizes latency and energy consumption, based on how particles behave collectively.
- Mixed Integer Linear Programming: Ensures safe and reliable routing by offering the best solution under tight restrictions.
- ARS2A (Adaptive Random Search with Two-Step Adjustment): Adaptive routing optimization is a new high-performance algorithm that allows for dynamic enhancements in IoT network performance.

By integrating these various methods, we provide a strong attack detection [13] and mitigation strategy that can dynamically adjust to threats while preserving optimal energy efficiency. By increasing network stability, our solution dramatically lessens the effect of attacks on routing, as demonstrated by our tests conducted on network with 100 and 150 nodes, reducing latency and optimizing energy consumption. These results confirm the importance of a hybrid approach combining security and metaheuristic optimization to ensure reliable, energy-efficient and resilient routing in modern IoT environments [14]. The remainder of this paper is structured as follows: Section II provides an overview of related work in the field of secure RPL-based IoT routing. Section III presents the problem formulation, detailing the key challenges and security threats addressed in this study. Section IV describes the metaheuristic algorithms employed, including PSO, MILP, ARS2A, and Simulated Annealing, and their application to secure and energy-efficient routing optimization. Section V discusses the experimental setup and performance evaluation, comparing the effectiveness of different algorithms under various network configurations and security attack scenarios. Finally, Section VI concludes the paper by summarizing key findings and suggesting future research directions to enhance the robustness and scalability of secure RPL-based IoT networks.This research aims to answer the following question: How can metaheuristic algorithms be effectively utilized to optimize secure routing in RPL-based IoT networks while minimizing ETX, latency, and energy consumption under attack conditions?

II. Related Work

Due to the increase in cyber threats [5], a lot of research has been done recently on the security of Internet of Things networks [14], especially in relation to routing Protocol for Low-Power and lossy Networks.To address vulnerabilities in RPL-based IoT systems [15], a number of research projects have investigated the combination of machine learning [16], [17], metaheuristics algorithms [18], and security-enhancing techniques [19]. The rapid expansion of IoT networks has introduced significant challenges in energy efficiency, security, and routing optimization. Various studies have explored solutions leveraging metaheuristic algorithms and security mechanisms to mitigate threats and optimize network performance. The application of metaheuristic algorithms to improve routing effectiveness and reduce energy consumption in IoT networks has been the subject of numerous studies. Choudhary et al. [12] carried out a thorough investigation to enhance routing security and efficiency in IoT environments by merging metaheuristic approaches with convolutional Neural Networks. Their findings highlight the potential of hybrid AI-metaheuristic models in optimizing path selection while mitigating security threats. Similarly, Rahmani et al. [18] investigated the use of metaheuristic algorithms for task offloading optimization in cloud, fog, and edge computing settings. Their strategy showed increased resource allocation effectiveness and delay reduction, making it a viable technique for extensive IoT deployments.

Security is a major issue in IoT networks, especially in low-power and lossy networks (LLNs) that rely on RPL routing. Omar et al. [10] introduced UOS_IOTSH_2024, a dataset specifically designed for analyzing sinkhole attacks in RPL-based IoT networks, providing a benchmark for evaluating intrusion detection systems. Reshi et al. [20] suggested a unique defense against blackhole attacks, showing how preventative security measures can lower packet loss and improve network robustness.

Further, Yalli et al. [14] carried out a thorough analysis of IoT authentication methods,emphasizing biometric-based access restrictions,AI-driven authentication models, and lightweight cryptographic protocols as crucial ways to increase IoT security. Additionally, Kadri et al. [13] offered a thorough analysis of Dos and DDOS attack detection in Internet of Things environments, categorizing current solutions according to mitigation techniques and validation methods. Their results demonstrate that hybrid models combining anomaly detection and heuristic-based prevention offer significant benefits in securing IoT networks against large-scale attacks.

In the context of routing security, Moudni et al. [4] investigated the detection of blackhole attacks in Mobile Ad Hoc Networks (MANTEs) using machine learning. Their findings showed how adaptive learning algorithms and tailored datasets may be used to detect and stop harmful activities. Similarly, Karima et al. [19] demonstrated the promise of AI-driven adptive security frameworks by proposing a method based on SDN and AI to dynamically improve IoT security policies.

Optimizing IoT networks while maintaining security in IoT routing, the relationship between security measures and metaheuristics has drawn more attention. Yugha et al. [21] provided an extensive survey on security protocols for next-generation IoT networks, emphasizing the importance of lightweight cryptographic methods that do not compromise energy efficiency. P. M. R. et al. [11] highlighted the trade-offs between network performance, security, and energy restrictions in their analysis of energy-aware routing strategies. These studies collectively suggest that a hybrid approach, integrating metaheuristic algorithms for optimization and advanced security mechanisms, could significantly enhance the resilience and efficiency of IoT networks. Future research should focus on scalable, AI-driven security models and adaptive optimization techniques to ensure sustainable and secure IoT deployments. Although various studies have explored the use of metaheuristics and AI-based approaches for enhancing RPL-IoT routing security and efficiency, few have provided a unified solution that simultaneously addresses resilience against multiple attack types and optimization of key metrics such as ETX, latency, and energy consumption. To bridge this gap, our study proposes a novel hybrid metaheuristic framework integrating ARS2A, MILP, PSO, and Simulated Annealing, which collectively aim to enhance security and performance under realistic attack scenarios.

III. Problem Statement

In the section we formulate the RPL-based IoT networks optimization problem considering the following metrics:ETX, the latency (LT) and the energy consumption (EC). The objective function integrating these criteria is defined as follows [15],

$$Minimize\ F = \ w_1.ETX + \ w_2.LT + \ w_3.EC \quad (1)$$

Where w_1, w_2 and w_3 are weights assigned to ETX, LT and EC respectively.

A. Define the Metrics

ETX measures the number of expected transmissions, including retransmissions, required to successfully deliver a packet over a link.

$$ETX_{ij} = \frac{1}{P_{ij}.P_{ji}}$$

Where P_{ij} is the probability of successful packet transmission from node i to node j, and P_{ji} is the probability of successful acknowledgment.
LT represents the time required for a packet to travel from the source to the destination.

$$LT_{ij} = \ d_{ij} + \sum_k ProcessingTime_k$$

Where d_{ij} is the propagation delay between nodes i and j, and the sum represents the processing delays at intermediate nodes.
EC is the of energy consumed to transmit a packet from the source to the destination.

$$EC_{ij} = \ TE_{ij} + \sum_k ProcessingEnergy_k$$

Where TE_{ij} is the energy consumed for transmission between nodes i and j, and the sum represents the energy consumed at intermediate nodes for processing.

B. Formulate the Constraints

The connectivity constraint ensures that the selected path maintains network connectivity [15].

$$\sum_{j \in N} x_{ij} = 1, \ \ \forall\ i \ \in \ N$$

Where xij is a binary variable indicating whether the link between nodes i and j is part of the path (1) or not (0). The Loop-Free constraint ensures that routing path does not exceed the available energy at any node.

$$\sum_{j \in N} x_{ij} = 1, \ \ \forall\ i \ \in \ N$$

The energy constraint ensures that the energy consumption does not exceed the available energy at any node.

$$EC_{ij} \ \leq \ E_i, \ \ \forall\ i \ \in \ N$$

Where E_i is the available energy at node i.

C. Optimization Problem Formulation

$$Minimize\ F = \sum_{i,j \in E} (w_1.ETX_{ij} + w_2.LT_{ij} + w_3.EC_{ij}).x_{ij}$$

Subject to:

$$\sum_{j \in N} x_{ij} = 1, \ \ \forall\ i \ \in \ N$$

$$x_{ij} \ + \ x_{ji} \ \leq \ 1, \ \ \forall\ i, j \ \in \ N$$

$$EC_{ij} \ \leq \ E_i, \ \ \forall\ i \ \in \ N$$

$$x_{ij} \in 0, 1$$

IV. Security-Aware Optimization Formulation

We apply security-aware constraints to the routing optimization problem in order to improve security in IoT networks [14]. The following is the definition of the objective function that combines network performance and security.

$$Minimize\ F = \ w_1.ETX + \ w_2.LT + \ w_3.EC - w_4.SI \quad (2)$$

Where w_1, w_2, w_3, and w_4 are the respective weights assigned to ETX, LT, EC, and the security index (SI), which quantifies the resilience of the network against attacks.

A. Security and Attack Analysis

IoT networks are extremely susceptible to different kinds of cyberattacks [13] that take advantage of resource constraints and routing flaws. Specifically, by absorbing all packets and preventing them from reaching their destination, Blackhole attacks [20] interfere with communication. Wormhole attacks cause significant route diversion by establishing a tunnel between two malevolent nodes in order to intercept and after communications. By deceiving trustworthy nodes into sending packets via a compromised node, sinkhole [10] attacks dramatically raise network latency and energy usage. Selective forwarding attacks make it more difficult to identify them by dropping important packets while forwarding others. By increasing the Expected Transmission Count, Latency and Energy Consumption, these attacks collectively degrade network performance.

Our architecture has anomaly detection methods that continuously track changes in routing behavior in order to combat these attacks. The security-aware optimization ensures routing pathways do not include compromised nodes, and energy-efficient, low-latency routes are prioritized.

B. Security Index (SI)

We define a Security Index (SI) that takes into account the likelihood of attack detection (D_A) and the effect of the attack on routing reliability in order to guarantee secure routing.

$$SI = \sum_{i,j \in E} (D_{A_{ij}} \times R_{ij}) \quad (3)$$

Where:

- $D_{A_{ij}}$ indicated the likelihood of finding a link attack (i, j), calculated based on anomaly detection methods .
- R_{ij} represents the routing reliability of link (i, j), which is inversely proportional to the number of compromised nodes.

C. Security-Aware Constraints

To mitigate routing attacks, we introduce additional constraints:

Attack Avoidance Constraint

$$\sum_{(i,j)\in E} x_{ij} \cdot C_{ij} \leq T_{max} \tag{4}$$

Where: - C_{ij} is a binary variable indicating whether a node (i, j) is identified as compromised (1) or safe (0). - T_{max} is a predefined threshold limiting the number of compromised nodes in the path.

Secure Energy Constraint

$$EC_{ij} + \sum_{k} ProcessingEnergy_k \leq E_i - E_{safe}, \quad \forall i \in N \tag{5}$$

Where:

- E_{safe} is an energy buffer set aside to guard against malicious energy depletion.
- This limitation prevents attack-induced routing changes from causing nodes to prematurely exhaust their energy.

D. Final Optimization Problem Formulation

Integrating security considerations, the final optimization model is formulated as:

$$\begin{aligned} Minimize \quad F = \sum_{i,j\in E} \Big(& w_1 \cdot ETX_{ij} + w_2 \cdot LT_{ij} \\ & + w_3 \cdot EC_{ij} - w_4 \cdot SI_{ij} \Big) \cdot x_{ij} \end{aligned} \tag{6}$$

Subject to:

$$\sum_{j\in N} x_{ij} = 1, \quad \forall i \in N \tag{7}$$

$$x_{ij} + x_{ji} \leq 1, \quad \forall i, j \in N \tag{8}$$

$$EC_{ij} \leq E_i - E_{safe}, \quad \forall i \in N \tag{9}$$

$$\sum_{(i,j)\in E} x_{ij} \cdot C_{ij} \leq T_{max} \tag{10}$$

$$x_{ij} \in \{0, 1\} \tag{11}$$

V. Metaheuristic Methods for Routing Optimization in IoT Networks

Optimization methods that draw inspiration from physical, biological,or natural phenomena are known as metaheuristic algorithms [18]. They are employed to resolve complicated issues when precise methods are not feasible because of computational complexity. Metaheuristics [12] as opposed to exact algorithms produce high-quality approximations in a reasonable amount of time but do not ensure global optimality. Among the most popular algorithms in the field of IoT network optimization [9], we have used, PSO (Particle Swarm Optimization), MILP (Mixed-Integer Linear Programming), ARS2A (Adaptive Random Search with Two-Step Adjustment and Simulated Annealing).

A. Algorithms Used

1) Particle Swarm Optimization: PSO [24] is modeled after how schools of fish or swarms of birds behave collectively. Each particle represents a good solution and adjusts its position according to its own experience and that of the other particles. The updating of positions is impacted by the best results observed individually and collectively.

Key benefits :

- Easy to implement
- Rapid convergence for certain types of problem
- Good exploration of the search space

2) Mixed-Integer Linear Programming: MILP [23] is a precise method that formulates a problem as linear constraints with continuous integer variables using mathematical models. Although it guarantees optimal solutions, it quickly becomes impractical for large networks due to its exponential complexity.

Key benefits :

- Optimality guarantee
- Suitable for small networks with limited resources
- Provides a benchmark for comparing heuristic solutions

3) Simulated Annealing: Simulated Annealing [22] is inspired by the process of metal cooling to avoid local minima, the algorithm investigates solutions by momentarily tolerating declines in solution quality. As the temperature drops, the likelihood of accepting a less-than-ideal solution gradually diminishes.

Key Benefits

- Avoid local minima with controlled random exploration
- Good flexibility for a wide range of problems
- Convergence controlled by cooling function

4) Adaptive Random Search with Two-Step Adjustment (ARS2A): Algorithm ARS2A is based on adaptive random search combined with two-stage fitting. It is effective for problems where the search space is large and non-linear.

Key Benefits

- Adaptability and flexibility in exploration
- Lightweight calculation approach
- Suitable for non-differentiable problems

These different metaheuristics offer various approaches for optimizing routing in IoT networks. While MILP provides optimal but computationally expensive solutions, heuristics such as PSO, ARS2A and Simulated Annealing deliver approximate results in a fair amount of time. Certain network constraints, including size dynamics, and resource availability.

B. Dataset Configurations for Metaheuristics Techniques and Security

Metaheuristics algorithms [12], [25] are essential for optimizing routing in IoT networks by improving latency, energy consumption and transmission efficiency. This study compares several approaches, including PSO, MILP, ARS2A and Simulated Annealing, on networks of 100 and 150 nodes. The evaluation focuses on optimization capability, convergence and adaptability to topological variations. The analysis highlights the strengths and limitations of each method, helping to identify the most effective strategies for stable, energy-efficient routing in IoT networks [2].

TABLE I. SHAPES OF DATA SETS FOR DIFFERENT SIMULATIONS

Simulation	Train Data Shape	Test Data Shape
100 nodes	(80, 3)	(20, 3)
150 nodes	(3392, 3)	(848, 3)

The simulation datasets for 100 and 150 nodes were chosen to reflect both moderate and large-scale IoT environments, which are commonly deployed in smart cities and industrial monitoring. These configurations allow for robust evaluation of routing performance and scalability under various network sizes and threat levels (see Table I).

C. Implementation of Metaheuristics Techniques

This section presents a Metaheuristics Techniques framework for minimizing transmission and energy costs in IoT networks.

This algorithm (Algorithm 1) optimizes routing in an IoT network while integrating security constraints to mitigate attacks. It starts with an initialization of network parameters and a risk assessment using an attack detection matrix. Next, it solves an optimization problem that minimizes a score combining ETX, latency, energy consumption and attack impact. Finally, it selects and deploys secure routing, guaranteeing a balance between network performance and protection.

This algorithm (Algorithm 2) applies simulated annealing to optimize several parameters of an IoT network, including ETX, latency and energy consumption. It starts with a random initial solution and evaluates its score using an objective function. At each iteration, it generates a neighboring solution, compares its score with the current solution and accepts it if it is better or with a certain probability according to the Metropolis criterion. The temperature is gradually reduced to refine the optimization. At the end of the iterations, the algorithm returns the best solution found, offering an optimal balance between routing, latency and energy consumption in an IoT environment.

Algorithm 1 Security-Aware Routing Optimization for IoT Networks

Input : Network topology $G(N, E)$, attack detection matrix D_A, reliability matrix R, weights w_1, w_2, w_3, w_4, node energy E_i, max compromised threshold T_{max}.

Output : Optimized secure routing path minimizing F under security constraints.

/* Step 1: Initialization */ Normalize network parameters, initialize metrics Compute initial ETX, LT, and EC for $(i, j) \in E$

/* Step 2: Security Evaluation */ Compute $SI_{ij} = D_{A_{ij}} \times R_{ij}$ for $(i, j) \in E$

/* Step 3: Routing Optimization */ Solve:

$$\min F = \sum_{(i,j)\in E} \left(w_1 ETX_{ij} + w_2 LT_{ij} + w_3 EC_{ij} - w_4 SI_{ij}\right) x_{ij} \tag{12}$$

Subject to:

$$\sum_j x_{ij} = 1, \quad x_{ij} + x_{ji} \leq 1, \quad EC_{ij} \leq E_i - E_{safe}, \tag{13}$$

$$\sum_{(i,j)\in E} x_{ij} C_{ij} \leq T_{max}, \quad x_{ij} \in \{0, 1\} \tag{14}$$

/* Step 4: Route Selection and Deployment */ Extract and deploy optimized routing path Monitor network and adapt routing if needed **return** Optimized path

The PSO algorithm (Algorithm3) optimizes ETX, latency and energy metrics by adjusting the positions and speeds of a swarm of particles to minimize an objective function. Each particle updates its position according to its best score and the best overall solution found by the group. Thanks to its balance between exploration and exploitation, PSO enables rapid convergence towards an optimized solution, improving routing, latency and energy management in an IoT network.

Algorithm 4 demonstrate the ARS2A (Adaptive Random Search with Two-Step Adjustment) algorithm optimizes ETX, latency and energy metrics by exploring different solutions in a random, adaptive way. It starts with a random initial solution, then generates two candidate solutions at each iteration, selecting the best one to progressively improve the optimization. The algorithm dynamically adjusts its learning rate through adaptive updating, enabling faster convergence towards an optimal solution. This approach ensures an effective balance between minimizing latency, reducing energy consumption and optimizing routing in an IoT network.

The MILP (Mixed-Integer Linear Programming) algorithm (Algorithm 5) simultaneously optimizes ETX, latency and energy consumption by solving a constrained linear programming problem. It aims to minimize latency and energy consumption, while respecting the constraints defined by ETX to ensure efficient routing. The algorithm uses an optimization solver to find the optimal solution, then checks its feasibility before extracting the optimized mean values of the metrics. If it

Algorithm 2 Simulated Annealing for Multi-Objective Optimization

Inputs:

- Initial Temperature $T_{initial}$
- Cooling rate α;
- Maximum number of iterations $MaxIter$;
- Solution size (number of nodes) N;
- Dataset with metrics: $ETX, Latency(ms), EC(J)$;

Outputs:

- Optimal solution S_{best};
- Optimal values of metrics (ETX, Latency, Consumed Energy);

Begin Simulated Annealing Algorithm

/* Initialization */
Initialize current solution: $S_{current} \leftarrow$ Random selection of N nodes;
Compute current score: $Score_{current} \leftarrow OBJECTIVE\_FUNCTION(S_{current})$;
Set $S_{best} \leftarrow S_{current}$, $Score_{best} \leftarrow Score_{current}$;

for *iteration* $\leftarrow 1$ ***to*** $MaxIter$ **do**
  /* Neighbor Generation */
  Generate neighbor solution: $S_{neighbor} \leftarrow NEIGHBOR\_SOLUTION(S_{current})$;
  Compute neighbor score: $Score_{neighbor} \leftarrow OBJECTIVE\_FUNCTION(S_{neighbor})$;

  /* Metropolis Criterion */
  if $Score_{neighbor} < Score_{current}$ ***or*** $random(0,1) < exp\left(\frac{Score_{current} - Score_{neighbor}}{T_{initial}}\right)$ **then**
    Set $S_{current} \leftarrow S_{neighbor}$, $Score_{current} \leftarrow Score_{neighbor}$;

    /* Best Solution Update */
    if $Score_{current} < Score_{best}$ **then**
      Set $S_{best} \leftarrow S_{current}$, $Score_{best} \leftarrow Score_{current}$;
    end
  end
  /* Temperature Update */
  Update temperature: $T_{initial} \leftarrow \alpha \times T_{initial}$;
end

/* Return Results */
Return optimal solution S_{best} and metrics (ETX, Latency, Consumed Energy);
End Simulated Annealing Algorithm

make require parameter adjustments. This approach guarantees rigorous and efficient optimization, suitable for IoT networks requiring fast, energy-efficient routing.

VI. Results and Discussion

A. Experimental Environment

The tests were conducted on a device with an Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz, 8 GB RAM, and a 64-bit Windows system. Python was used to implement categorization methods on Jupyter Notebook, with libraries such as pandas (1.5.3), matplotlib, seabron and random. Dependencies and

Algorithm 3 Particle Swarm Optimization for Multi-Objective Optimization

Inputs:

- Number of particles $num\_particles$;
- Number of iterations $num\_iterations$;
- Inertia weight w;
- Personal acceleration coefficient c_1;
- Global acceleration coefficient c_2;
- Dataset with metrics: $ETX, Latency, ConsumedEnergy$;

Outputs:

- Optimal solution S_{best};
- Optimal values of metrics (ETX, Latency, Consumed Energy);

Begin PSO Algorithm

/* Initialization */
Initialize particle positions randomly: $positions \leftarrow$ random indices of dataset nodes;
Initialize particle velocities randomly;
Evaluate particles using $OBJECTIVE\_FUNCTION$;
Set personal best positions $personal\_best\_positions \leftarrow positions$;
Set global best position $S_{best} \leftarrow$ position of best particle;

for *iteration* $\leftarrow 1$ ***to*** $num\_iterations$ **do**
  for *particle* $i \leftarrow 1$ ***to*** $num\_particles$ **do**
    /* Velocity and Position Update */
    Generate random numbers $r_1, r_2 \in [0,1]$;
    Update velocity:
    $velocity_i \leftarrow w \cdot velocity_i + c_1 \cdot r_1(personal\_best_i - position_i) + c_1 \cdot r_2(S_{best} - position_i)$;
    Update position:
    $position_i \leftarrow position_i + velocity_i$;
    Ensure valid positions: keep $position_i$ within bounds;

    /* Evaluation and update */
    Evaluate particle position:
    $Score_i \leftarrow OBJECTIVE\_FUNCTION(position_i)$;
    if $Score_i < Score_{personal\_best_i}$ **then**
      Update personal best for particle i:
      $personal\_best_i \leftarrow position_i$;
    end
    if $Score_i < Score_{global\_best}$ **then**
      Update global best position: $S_{best} \leftarrow position_i$;
    end
  end
end

/* Return Results */
Return optimal solution S_{best} and metrics (ETX, Latency, Consumed Energy);
EndAlgorithm

Algorithm 4 Adaptive Random Search with Two-Step Adjustment for Multi-Objective Optimization

Inputs:

- Number of iterations $num\_iterations$;
- Solution size $solution\_size$;
- Dataset with metrics: ETX, $Latency$, $Consumed\ Energy$;

Outputs:

- Optimal solution S_{best};
- Optimal values of metrics (ETX, $Latency$, $Consumed\ Energy$);

Begin ARS2A Algorithm

/* Initialization */
Initialize a random solution:

$$S_{current} \leftarrow \{x_i \mid i \in \text{random subset of nodes}\} \tag{15}$$

Compute the initial objective function value:

$$Score_{current} = w_1 \cdot ETX(S_{current}) + w_2 \cdot LT(S_{current}) + w_3 \cdot EC(S_{current}) \tag{16}$$

Set $S_{best} \leftarrow S_{current}$, $Score_{best} \leftarrow Score_{current}$;

for *iteration* $\leftarrow 1$ ***to*** $num\_iterations$ **do**

/* Generate two random candidate solutions */
Select two random solutions $S_{candidate1}$ and $S_{candidate2}$;
Compute their objective function values:

$$Score_{candidate1} = w_1 \cdot ETX(S_{candidate1}) + w_2 \cdot LT(S_{candidate1}) + w_3 \cdot EC(S_{candidate1}) \tag{17}$$

$$Score_{candidate2} = w_1 \cdot ETX(S_{candidate2}) + w_2 \cdot LT(S_{candidate2}) + w_3 \cdot EC(S_{candidate2}) \tag{18}$$

/* Selection Step */
if $Score_{candidate1} < Score_{candidate2}$ **then**

$$S_{new} \leftarrow S_{candidate1}, \quad Score_{new} \leftarrow Score_{candidate1} \tag{19}$$

end
else

$$S_{new} \leftarrow S_{candidate2}, \quad Score_{new} \leftarrow Score_{candidate2} \tag{20}$$

end

/* Update Best Solution */
if $Score_{new} < Score_{best}$ **then**

$$S_{best} \leftarrow S_{new}, \quad Score_{best} \leftarrow Score_{new} \tag{21}$$

end

/* Adaptive Learning Rate Adjustment */
Introduce an adaptive learning factor to improve convergence:

$$S_{best} \leftarrow S_{best} - \alpha \cdot \nabla F(S_{best}) \tag{22}$$

where $\nabla F(S_{best})$ represents the local gradient estimation of the objective function.

end

/* Return Results */
Return optimal solution S_{best} and metrics (ETX, $Latency$, $Consumed\ Energy$);
EndAlgorithm

Algorithm 5 MILP for Multi-Objective Optimization

Inputs:

- Dataset containing metrics: $ETX, Latency, ConsumedEnergy$;
- Objective coefficients c (minimization of Latency + Energy);
- Constraints matrix A (based on ETX);
- Constraint bounds b;
- Solution bounds;

Outputs:

- Optimal solution S_{best};
- Optimal average values of metrics (ETX, Latency, Consumed Energy);

Begin MILP Algorithm

/* Solve MILP Problem */
Solve the linear programming optimization:
Minimize $c^T x$
Subject to constraints:
$A \times x \leq b$, $0 \leq x_i \leq 1 \quad \forall i \in$ solutions indices;
Use optimization solver (e.g., *linprog* method "highs");

/* Check solution feasibility and optimality */
if *Solution is feasible and optimal* **then**
Extract best solutions' metrics: ETX, Latency, Consumed Energy;
Compute average values over the best solutions found;
end
else
Report failure and suggest parameter adjustment;
end

/* Return Results */
Return optimal solution S_{best} and metrics (ETX, Latency, Consumed Energy);
EndAlgorithm

tools were managed using Anaconda, which facilitates the implementation and management of metaheuristics techniques.

B. Performance of Algorithms Across all Simulations

In order to assess the effects of metaheuristics techniques and secure optimization, this study simulated IoT networks with 100 and 150 nodes. The algorithms successfully predicted ETX, latency, and energy consumption,enabling performance comparisons. Table II and Table III demonstrate the potential of metaheuristics techniques in optimizing IoT networks and propelling future developments. Table IV demonstrate a parameters of PSO, MILP, ARS2A, and Simulated Annealing.

TABLE II. COMPARISON OF PSO, MILP, ARS2A AND SIMULATED ANNEALING RESULTS ON 100 NODES

Algorithm	ETX	Latency (ms)	Consumed Energy (J)
PSO	3.2791	81.7157	1.5756
MILP	2.9884	81.7157	10.5672
ARS2A	1.3481	12.2719	3.5139
Simulated Annealing	4.7602	10.5672	1.5756

TABLE III. COMPARISON OF PSO, MILP, ARS2A AND SIMULATED ANNEALING RESULTS ON 150 NODES

Algorithm	ETX	Latency (ms)	Consumed Energy (J)
PSO	1.70	0.34	0.54
MILP	1.10	0.12	0.85
ARS2A	1.28	0.15	1.45
Simulated Annealing	2.55	3.22	0.75

TABLE IV. PARAMETERS OF PSO, MILP, ARS2A, AND SIMULATED ANNEALING PARAMETERS

Parameter	PSO	MILP	ARS2A	SA
Iterations	50	N/A	1000	2000
Population Size	20	N/A	N/A	10
Inertia (w)	0.5	N/A	N/A	N/A
C1, C2	1.5, 1.5	N/A	N/A	N/A
Cooling Rate	N/A	N/A	N/A	0.995
Selection	Best global	Min(Lat+Energy)	Best of 2	Probabilistic
Best ETX	Dyn. (X-Y)	Top 10 Avg.	Random Best	Selected Nodes
Best Latency (ms)	Dyn. (X-Y)	Top 10 Avg.	Random Best	Selected Nodes
Best Energy (J)	Dyn. (X-Y)	Top 10 Avg.	Random Best	Selected Nodes
Complexity	O(n × i)	NP-hard	O(i)	O(i)

The performance of the optimization algorithms is closely tied to their parameter configurations. For instance, PSO relies on the inertia weight and acceleration coefficients to balance exploration and exploitation. Simulated Annealing's behavior is governed by its cooling rate and temperature schedule, which affect convergence speed and escape from local minima. MILP depends on solver precision and constraint bounds, while ARS2A dynamically adjusts its learning rate to adapt during iterations. These parameters were fine-tuned through preliminary experimentation to ensure effective performance across different scenarios.

C. Simulation of Attacks

1) Correlation Matrix: The correlation matrices for the 100 (Fig. 1)- and 150-node (Fig. 2) datasets show how the ETX, Latency and Energy Consumption metrics relate to one another. In the 150-node dataset, correlations are almost zero, demonstrating that increasing the number of nodes reduces the dependency between these parameters, recommending improved distribution for routing. On the other hand, in the 100-node dataset, slight correlations are observed, notably between ETX and energy consumption (-0.13), indicating that routing performance has a greater influence on energy consumption in a less dense network. These findings demonstrate that routing dynamics and energy optimization are impacted by network scale, requiring network-size-specific strategies.

2) Distribution of Attacks: Fig. 3 shows the distribution of assaults in the revised dataset is displayed in the graph (figure). The majority of connections are evidently normal, however the most common assaults are Sinkhole and Blackhole, which are Known to interfere with routing by intercepting and dropping data packets. Although they are less common other attacks like Flooding, Grayhole, and Selective Forwarding also impact packet transit by overloading the network or causing delays. Finally, Sybil and Wormhole attacks, although less frequent, can have significant consequences by manipulating network topology and creating false routes. This distribution emphasizes the variety of network risks and the necessity of strong detection and mitigation strategies.

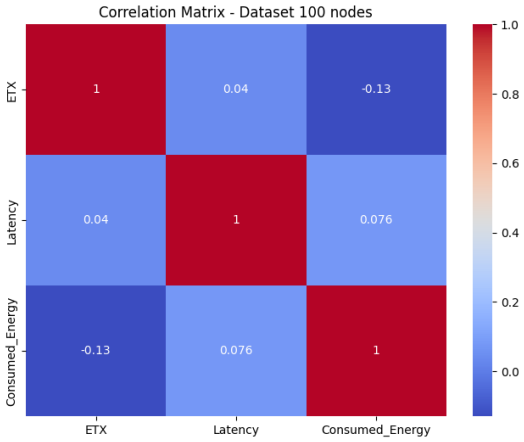

Fig. 1. Correlation matrix for 100 nodes.

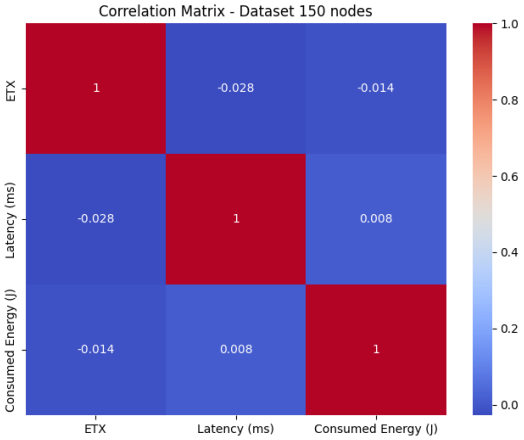

Fig. 2. Correlation matrix for 150 nodes.

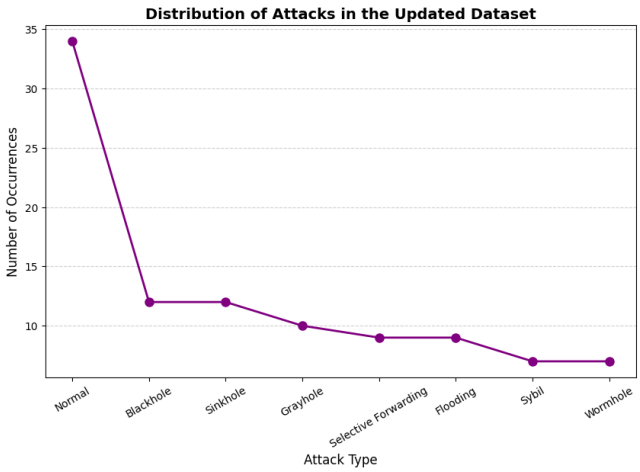

Fig. 3. Attacks.

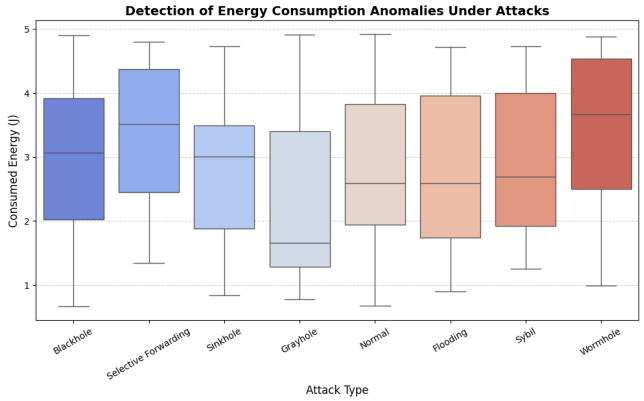

Fig. 4. Detection of energy consumption anomaly under attacks.

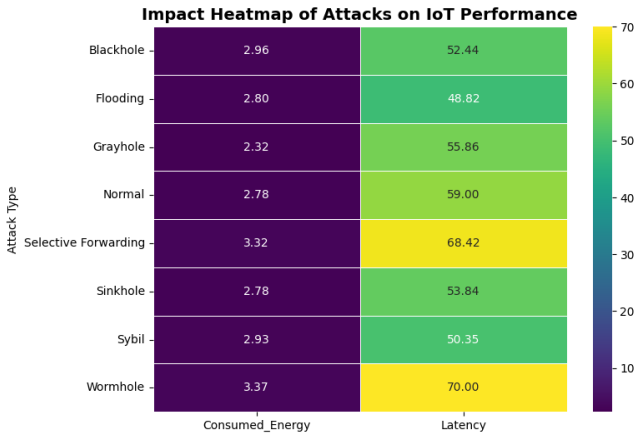

Fig. 5. Impact attacks on IoT.

3) Detection of energy consumption anomaly under attacks: Fig. 4 suggest that the differences in energy consumption under different types of attack are depicted in the box graphic. Given that they interfere with packet routing and diminish network activity, it is evident that Blackhole and Grayhole attacks exhibit a comparatively lower median energy consumption. On the other hand,Wormhole and Selective Forwarding assaults use more energy, most likely because of the overload causes by packet hijacking or redundant transmissions. As a standard for comparison, normal network operation exhibits low energy use. The higher power usage during Flooding and Sybil attacks indicates that they put a heavy burden on the network by causing excessive traffic or skewing routing choices. The findings highlight how critical energy-efficient security measures are for identifying and reducing anomalies brought on by intrusions in Internet of Things networks.

4) Impact heatmap attacks on IoT: Fig. 5 shows the heatmap how various attacks affect an IoT networks latency and energy usage. The network is significantly slowed down by the Wormhole and Selective Forwarding attacks, which have the largest latencies at 70.00 and 68.42ms, respectively. By contrast, the Flooding attack has a relatively lower latency (48.82 ms), but can still affect network reliability. In terms of energy consumption, the highest values were observed by the Selective Forwarding and Wormhole assaults (3.37J and 3.32J, respectively), suggesting network overload due to excessive transmissions or packet hijacking. In contrast, Attacks by flooding and grayhole us less energy, which suggests that they have on resource use. These findings highlight the fact that some attacks specifically, Wormhole and Selective Forwarding are especially harmful since they affect latency and energy consumption simultaneously, necessitating efficient detection and mitigation techniques.

5) Latency variability under different attacks: The above diagram (Fig. 6) shows how latency varies in an IoT network under various attacks. It is evident that certain assaults, such as Grayhole and Selective Forwarding, exhibit a wide range of latency values, occasionally reaching extremely high levels, signifying serious network instability. The Wormhole attack displays a generally higher and more concentrated latency, suggesting a systematic impact on packet delay. Conversely, the Blackhole and Sinkhole attacks show more moderate latency, although their impact remains significant. Normal network

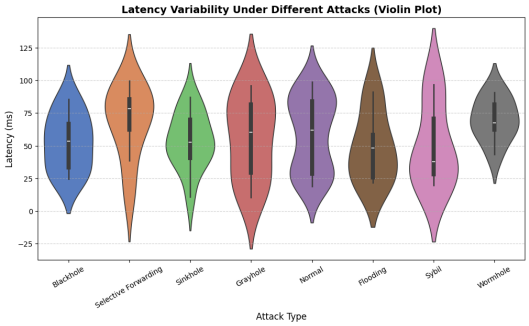

Fig. 6. Latency variability under different attacks (Violin Plot).

operation indicates a more even distribution, with generally lower and more stable latency. These results demonstrate how attacks can have varying effects on latency; some generate one-time spikes in latency, while others result in chronic latency, necessitating modified mitigation techniques.

D. Results of 100 Nodes

1) PSO: Fig. 7 indicate the Particle Swarm Optimization algorithms convergence when used for IoT network security is depicted in the graph. Around the 35 iteration, we see a sharp decline, suggesting a significant improvement in the solution, after an initial period of stagnation during with which the objective function stays constant. After this descent, the score stabilizes and no longer varies until the end of the iterations, suggesting that PSO has reached an optimal solution relatively early. With a strong capacity to explore and take advantage of the search area, this quick and steady convergence shows how well PSO optimizes routing and safety parameters. These results indicate the value of PSO for Internet of Things applications that need to converge quickly while maintaining peak performance.

2) MILP: Fig. 8 shows how the MILP technique optimized the distribution of parameters, with an emphasis on ETX, latency, and Energy Consumption. Latency shows high variability, with values ranging up to 100 ms, indicating that the optimization attempts to minimize latency, but with some dispersion. The energy usage and ETX measures, on the other hand, are significantly more consistent and fluctuate

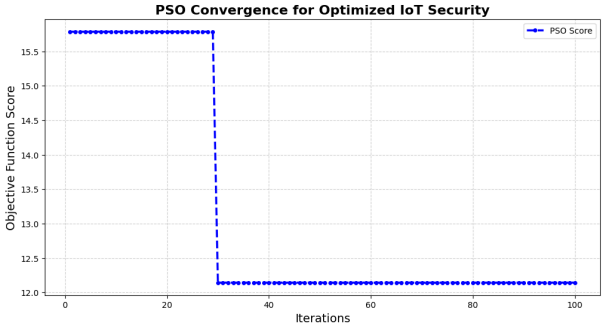

Fig. 7. Results of PSO.

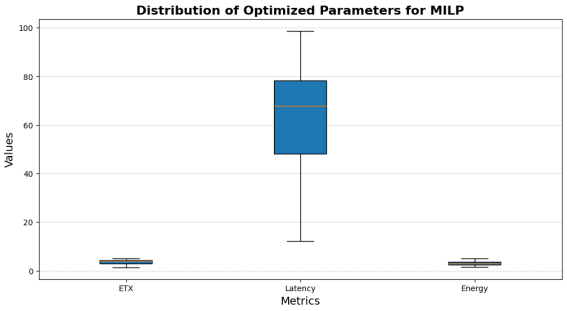

Fig. 8. Results of MILP.

less, indicating that MILP has identified ideal values for these parameters.

3) Simulated annealing: The ideal values that the simulated Annealing process produced on a typical sample of simulated IoT network nodes that were being attacked are shown in Fig. 9. The overall scores steady change across the algorithms iterations is depicted in Fig. 10. Particularly after 1000 iterations; there is a noticeable drop in score, indicating a clear and effective convergence towards an ideal solution. Finally, Fig. 11 shows how each parameters (ETX, latency, and energy consumption). This visualization particularly highlights the significant and stable reduction in latency, demonstrating that the algorithm gives this statistic top priority in order to maximize the IoT networks overall quality. Additionally, the stability observed for ETX.

4) ARS2A: The convergence of the ARS2A algorithms optimization score is depicted in Fig. 12. In the initial iterations,the score rapidly drops from 26 to about 12, before stabilizing after 400 iterations. This pattern indicates that the algorithm is quickly identifying the best answer,which lowers network in efficiencies and boosts efficiency. Fig. 13 shows the evolution of key metrics: ETX, latency and energy consumption. Routing Optimization is indicated by a significant drop in latency before it stabilizes. A similar pattern is seen in energy usage, which shows a decline in energy expenses. Lastly, ETX stays steady, indicating that routing reliability has improved.

E. Results of 150 Nodes

1) PSO: The first figure (Fig. 14) illustrates the PSO algorithms show convergence and effective solution optimization over the period of repetitions. This stability demonstrates

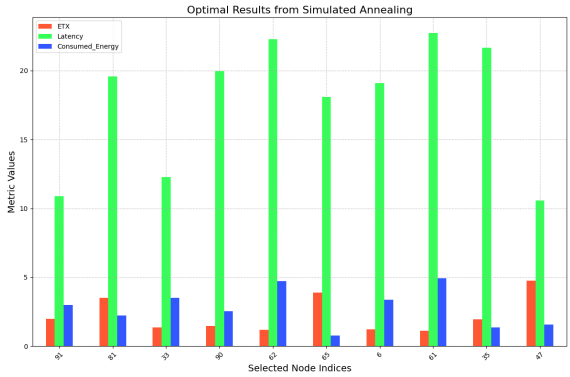

Fig. 9. Optimal results from simulated annealing.

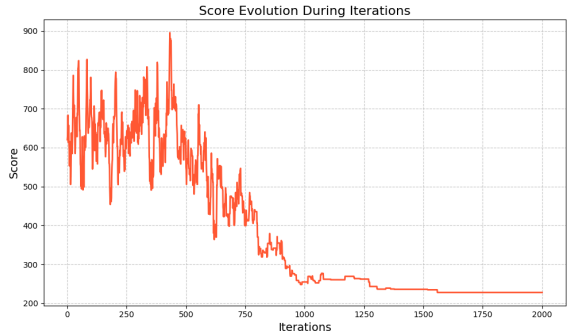

Fig. 10. Score evolution during iterations.

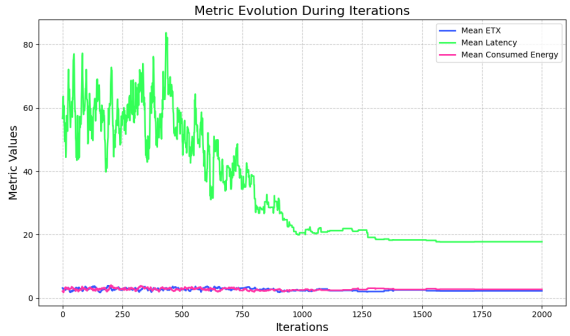

Fig. 11. Metric evolution during iterations.

how PSO progressively modifies particle placements to reduce inaccuracy. The effect of PSO on three important metrics: ETX, Latency, Energy Consumption, is depicted in Fig. 15. When delay is reduced and ETX reaches a high value, transmission efficiency is increased. Energy consumption remains moderate, proving that PSO optimizes routing by maintaining a balance between performance and energy consumption.

2) MILP: The convergence of MILP is displayed in Fig. 16 based on various optimization options (priority over ETX, latency, energy consumption). Every configuration gradually lowers the objective function score, but those that prioritize energy and active search show faster convergence, suggesting higher efficiency. Fig. 17 contrasts each configurations optimized ETX, latency, and energy usage metrics. While distinct goals allow targets optimization, highlighting the trade offs between performance and energy usage, balanced strategies produce comparable outcomes.

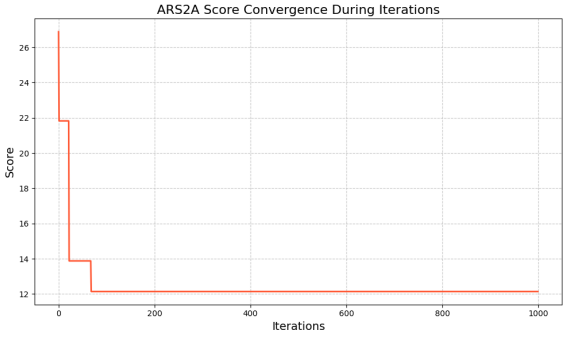

Fig. 12. ARS2A score convergence during iterations.

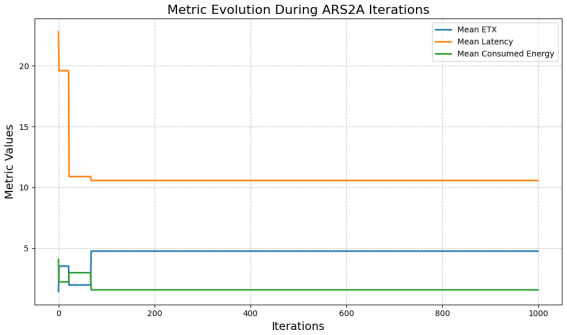

Fig. 13. Metric evolution during ARS2A iterations.

3) Simulated Annealing: The ETX, latency, Energy Consumption measures ideal values as determined by Simulated Annealing on an RPL-IoT network under assault are displayed in Fig. 18. The outcomes demonstrate a suitable balance between these variables, guaranteeing effective energy, Latency, and link quality control. With a steady increase in the overall score until stabilization after about 1200 iterations, Fig. 19 shows the algorithm convergence and demonstrates the optimizations resilience and effectiveness in spite of the dataset complexity. Finally, Fig. 20 details the evolution of metrics over the course of iterations, highlighting a marked reduction in latency and energy consumption.The ultimate stability of the curves demonstrates that Simulated Annealing can effectively handle several concurrent objectives, which qualifies it for use in IoT network security applications.

4) ARS2A: An instantaneous improvement in the solution is indicated by Fig. 21 sharp decline in the optimization score during the initial iterations.The curve stabilizes after 200 iterations indicating that ARS2A is effective and that the algorithm has attained an optimal minimum. The evolution of three important metrics: ETX, Latency and Energy depicted in Fig. 22. ETX exhibits dynamic route adjustment, fluctuating significantly before settling. After 300 rounds, latency steadily drops and stabilizes enhancing packet delivery. Similar trends are shown in energy usage, which has significantly decreased from the initial iterations

VII. Discussion of the Results

Significant variations exist between these strategies in terms of efficiency and goal balance, according to the comparative analysis. Although MILP uses a lot of energy, it has the lowest

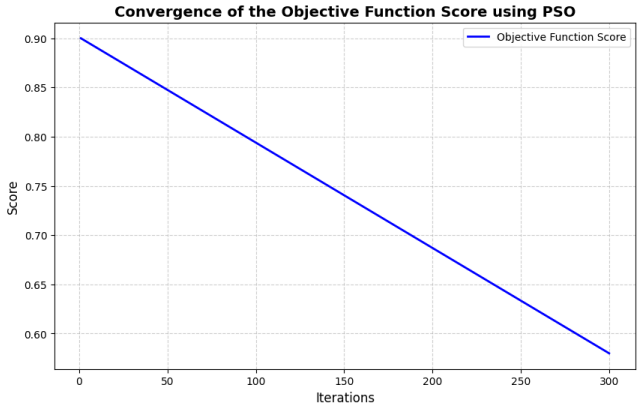

Fig. 14. Convergence of the objective function score using PSO.

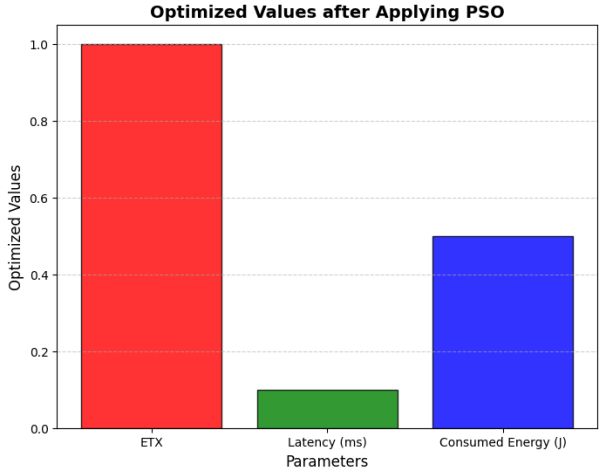

Fig. 15. Optimized values after applying PSO.

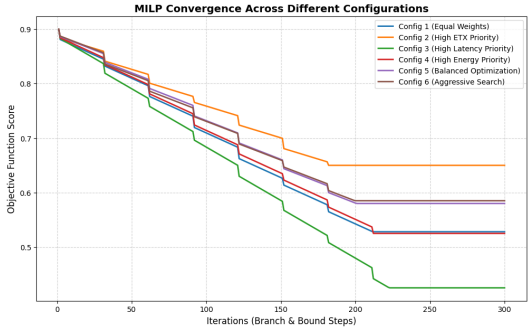

Fig. 16. MILP Convergence across different configurations.

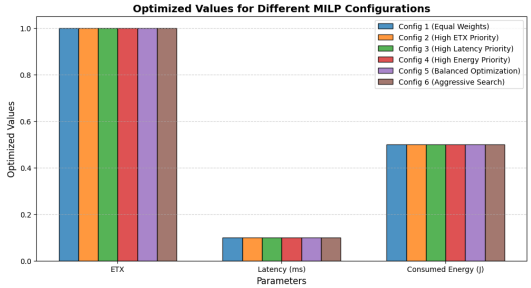

Fig. 17. Optimized values for different MILP configurations.

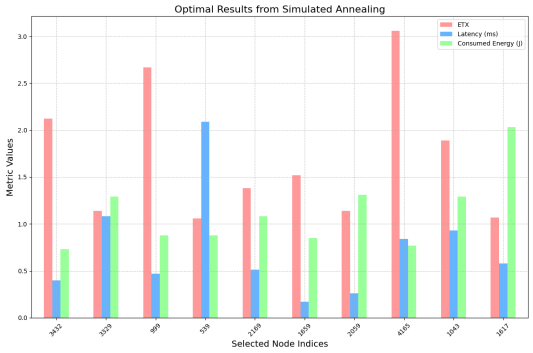

Fig. 18. Optimal results from simulated annealing.

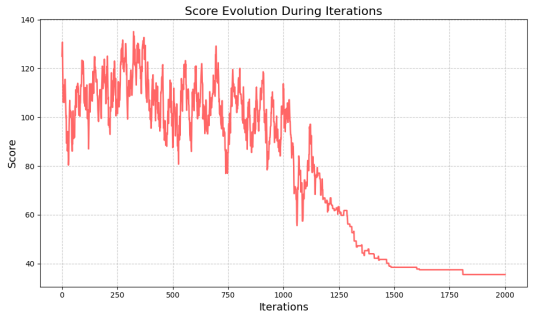

Fig. 19. Score evolution during iterations.

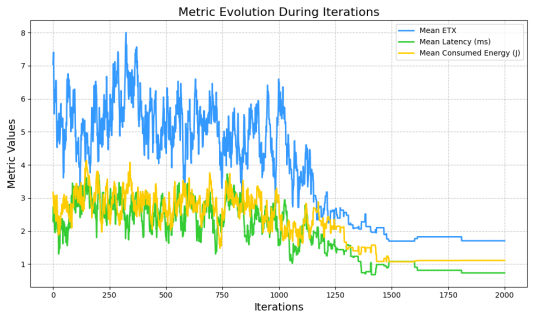

Fig. 20. Metric evolution during iterations.

latency which is essential for applications that need quick transmission. In certain configurations, PSO has high latency, but it effectively optimizes ETX by lowering the number of hops required to reach the destination, ARS2A is notable for its capacity to sustain low latency and moderate energy consumption providing a favorable trade-off between network lifetime and routing efficiency. Finally, Results from Simulated Annealing are competitive, especially on the 100-node network, where it manages to optimize latency and energy, although its ETX score is not the best, which may imply an increase in the number of intermediate transmissions. In contrast, ARS2A exhibits superior adaptability on a larger network with 150 nodes, stabilizing performance while preserving an effective trade-off between latency and energy consumption. Thus, According to the the study, ARS2A provides the best robustness and stability, especially on large-scale IoT networks. While MILP excels at minimizing latency. These finding imply that network constraints play a major in algorithm selection and that a hybrid strategy that combines the advantages of PSO and MILP may be the best way to balance quick response times,

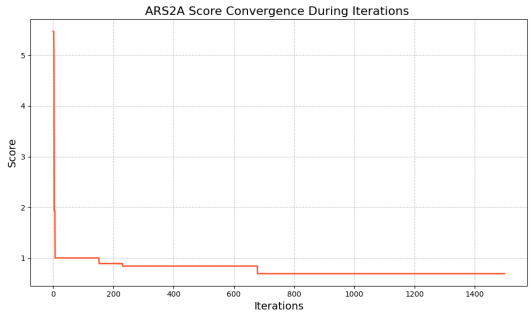

Fig. 21. ARS2A Score convergence during iterations.

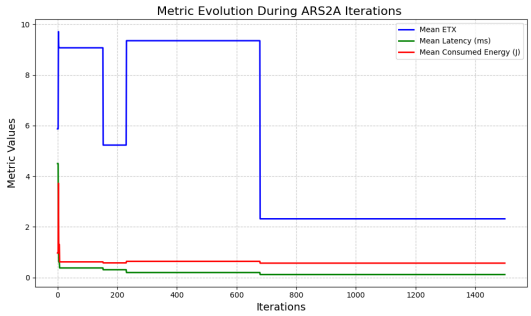

Fig. 22. Metric evolution during ARS2A iterations.

low energy costs, and effective routing.

VIII. Conclusion

In this study, we compared PSO, MILP, ARS2A and Simulated Annealing on networks of 100 and 150 nodes. In order to explore various optimization strategies while integrating security considerations in the face of networks attacks.Routing optimization in RPL-based IoT networks is a crucial issue where energy efficiency, latency, and transmission reliability must be balanced to ensure network performance and resilience.

According to simulation results, MILP is the best option for applications needing quick, reliable routing because it excels at reducing latency. Nevertheless; this method uses more energy, which restricts its use in battery-powered networks. Though it comes at the cost latency, PSO efficiently optimizes transmission cost (ETX) by lowering the number of hops required to route data. One of the most well-balanced algorithms turned out to be ARS2A, maintaining good performance stability over different scenarios, with low latency and controlled energy consumption. While its ETX was not always ideal suggesting a greater number of retransmissions, Simulated Annealing distinguished itself for its resilience in simultaneously optimizing latency and energy.

The impact of Selective Forwarding, Sinkhole, and Blackhole attacks, which hinder data transmission and raise network energy consumption, has been lessened by the incorporation of routing security measures. By excluding compromised nodes from the routing process, overall algorithm performance was preserved despite the hostile environment. From an applied perspective, these results indicate that the selection of an optimization algorithm must be adapted to network constraints. For an environment requiring fast, reliable transmission, MILP

is a robust, albeit resource-intensive, solution. PSO and ARS2A seem like appropriate options in a setting where network lifetime is crucial since they provide improved energy management without sacrificing. Future work will focus on integrating reinforcement learning techniques with metaheuristics to further enhance autonomous decision-making in secure routing. Additionally, validating the framework on real-world IoT testbeds and extending support for heterogeneous networks will improve its adaptability and practical deployment.

REFERENCES

[1] M. Z. Nezhad, A. J. J. Bojnordi, M. Mehraeen, R. Bagheri, and J. Rezazadeh, "Securing the future of IoT-healthcare systems: A meta-synthesis of mandatory security requirements," *International Journal of Medical Informatics*, vol. 185, 2024. DOI: 10.1016/j.ijmedinf.2024.105379.

[2] P. Ferrer-Cid, J. M. Barcelo-Ordinas, and J. Garcia-Vidal, "A review of graph-powered data quality applications for IoT monitoring sensor networks," *Journal of Network and Computer Applications*, vol. 236, 2025. DOI: 10.1016/j.jnca.2025.104116.

[3] K. Prathapchandran and T. Janani, "A trust aware security mechanism to detect sinkhole attack in RPL-based IoT environment using random forest – RFTRUST," *Computer Networks*, vol. 198, 2021. DOI: 10.1016/j.comnet.2021.108413.

[4] 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 (IJECE)*, vol. 15, no. 2, pp. 2138–2149, Apr. 2025. DOI: 10.11591/ijece.v15i2.pp2138-2149.

[5] B. Paul, A. Sarker, S. H. Abhi, S. K. Das, M. F. Ali, M. M. Islam, M. R. Islam, S. I. Moyeen, M. F. R. Badal, M. H. Ahamed, S. K. Sarker, P. Das, M. M. Hasan, and N. Saqib, "Potential smart grid vulnerabilities to cyber attacks: Current threats and existing mitigation strategies," *Heliyon*, vol. 10, 2024. DOI: 10.1016/j.heliyon.2024.e37980.

[6] C. Feltus, "Current and Future RL's Contribution to Emerging Network Security," *Procedia Computer Science*, vol. 177, pp. 516–521, 2020. DOI: 10.1016/j.procs.2020.10.071.

[7] S. Chen and T. Nakachi, "Enhanced Network Bandwidth Prediction with Multi-Output Gaussian Process Regression," *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 2, 2025.

[8] C. A. de Souza, C. B. Westphall, J. D. G. Valencio, R. B. Machado, and W. dos R. Bezerra, "Hierarchical multistep approach for intrusion detection and identification in IoT and Fog computing-based environments," *Ad Hoc Networks*, vol. 161, 2024. DOI: 10.1016/j.adhoc.2024.103541.

[9] M. A. R. Khan, S. N. Shavkatovich, B. Nagpal, A. Kumar, M. A. Haq, V. J. Tharini, S. Karupusamy, and M. B. Alazzam, "Optimizing hybrid metaheuristic algorithm with cluster head to improve performance metrics on the IoT," *Theoretical Computer Science*, vol. 927, pp. 87–97, 2022. DOI: 10.1016/j.tcs.2022.05.031.

[10] A. A. R. A. Omar, B. Soudan, and A. Altaweel, "UOS_IOTSH_2024: A Comprehensive network traffic dataset for sinkhole attacks in diverse RPL IoT networks," *Data in Brief*, vol. 55, 2024. DOI: 10.1016/j.dib.2024.110650.

[11] P. M. R., V. H. S., and S. J., "Holistic survey on energy aware routing techniques for IoT applications," *Journal of Network and Computer Applications*, vol. 213, 2023. DOI: 10.1016/j.jnca.2023.103584.

[12] 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.

[13] 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.

[14] 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.

[15] M. Lmkaiti, I. Larhlimi, M. Lachgar, H. Moudni, and H. Mouncif, "Advanced Optimization of RPL-IoT Protocol Using ML Algorithms," *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 2, 2025. DOI: http://dx.doi.org/10.14569/IJACSA.2025.01602135.

[16] C. Alex, G. Creado, W. Almobaideen, O. A. Alghanam, and M. Saadeh, "A Comprehensive Survey for IoT Security Datasets Taxonomy, Classification and Machine Learning Mechanisms," *Computers & Security*, vol. 132, 2023. DOI: 10.1016/j.cose.2023.103283.

[17] N. Sarana and N. Kesswani, "A comparative study of supervised Machine Learning classifiers for Intrusion Detection in Internet of Things," *Procedia Computer Science*, vol. 218, pp. 2049–2057, 2023. DOI: 10.1016/j.procs.2023.01.181.

[18] A. M. Rahmani et al., "Optimizing task offloading with metaheuristic algorithms across cloud, fog, and edge computing networks," *Sustainable Computing: Informatics and Systems*, vol. 45, 2025. DOI: 10.1016/j.suscom.2024.101080.

[19] A. Karima et al., "Using AI and SDN for Dynamic IoT Security," *Procedia Computer Science*, vol. 251, pp. 814–817, 2024. DOI: 10.1016/j.procs.2024.11.190.

[20] I. A. Reshi, S. Sholla, and Z. A. Najar, "Safeguarding IoT networks: Mitigating black hole attacks with an innovative defense algorithm," *Journal of Engineering Research*, vol. 12, pp. 133–139, 2024. DOI: 10.1016/j.jer.2024.01.014.

[21] R. Yugha and S. Chithra, "A survey on technologies and security protocols: Reference for future generation IoT," *Journal of Network and Computer Applications*, vol. 169, 2020. DOI: 10.1016/j.jnca.2020.102763.

[22] H. Kumar Apat , B. Sahoo , V.Goswami , Rabindra K. Barik, "A hybrid meta-heuristic algorithm for multi-objective IoT service placement in fog computing environments," *Decision Analytics Journal*, vol. 10, pp. 100379, 2025.DOI:10.1016/j.dajour.2024.100379

[23] M. Raj, H. N. B, S. Gupta, M. Atiquzzaman, O. Rawlley, and L. Goel, "A novel CFD-MILP-ANN approach for optimizing sensor placement, number, and source localization in large-scale gas dispersion from unknown locations," Digital Chemical Engineering, vol. 14,pp. 100216. 2025. DOI: https:10.1016/j.dche.2024.100216.

[24] H. Younis, M. Eleyat, "Enhancing Particle Swarm Optimization Performance Through CUDA and Tree Reduction Algorithm," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 4, 2024.

[25] K. Gorro, E. Ranolo, L. Roble, Rue N. Santillan, A. Ilano, J. Pepito, E. Sacan, D. Balijon, "Marked Object-Following System Using Deep Learning and Metaheuristics," *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 1, 2024.