Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.061486

ARTICLE

A Tolerant and Energy Optimization Approach for Internet of Things to Enhance the QoS Using Adaptive Blended Marine Predators Algorithm

Vijaya Krishna Akula[1,*], Tan Kuan Tak[2], Pravin Ramdas Kshirsagar[3], Shrikant Vijayrao Sonekar[4] and Gopichand Ginnela[5]

[1]Department of Information Technology, G. Narayanamma Institute of Technology and Science for Women, Hyderabad, 500104, India

[2]Engineering Cluster, Singapore Institute of Technology, 10 Dover Drive, Singapore, 138683, Singapore

[3]Department of Electronics and Telecommunication Engineering, J.D. College of Engineering & Management, Nagpur, 441501, India

[4]Department of Computer Science and Engineering, J.D. College of Engineering & Management, Nagpur, 441501, India

[5]School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, 632014, Tamilnadu, India

*Corresponding Author: Vijaya Krishna Akula. Email: vijay.merits@gmail.com

Received: 26 November 2024; Accepted: 12 February 2025; Published: 16 April 2025

ABSTRACT: The rapid expansion of Internet of Things (IoT) networks has introduced challenges in network management, primarily in maintaining energy efficiency and robust connectivity across an increasing array of devices. This paper introduces the Adaptive Blended Marine Predators Algorithm (AB-MPA), a novel optimization technique designed to enhance Quality of Service (QoS) in IoT systems by dynamically optimizing network configurations for improved energy efficiency and stability. Our results represent significant improvements in network performance metrics such as energy consumption, throughput, and operational stability, indicating that AB-MPA effectively addresses the pressing needs of modern IoT environments. Nodes are initiated with 100 J of stored energy, and energy is consumed at 0.01 J per square meter in each node to emphasize energy-efficient networks. The algorithm also provides sufficient network lifetime extension to a resourceful 7000 cycles for up to 200 nodes with a maximum Packet Delivery Ratio (PDR) of 99% and a robust network throughput of up to 1800 kbps in more compact node configurations. This study proposes a viable solution to a critical problem and opens avenues for further research into scalable network management for diverse applications.

KEYWORDS: Internet of things; trust; energy; marine predators algorithm (MPA); differential evolution (DE); nodes; throughput; lifetime

1 Introduction

IoT has brought a new trend in networked technology that interconnects gadgets and sensors and shares information to optimize applications in urbanization, industries, and people's gadgets [1–3]. To a large extent, these networks are built around efficient and highly reliable means of conveying massive volumes of information to exhibit the necessary degrees of coordination and control in large, complex, and often geographically dispersed environments [4–6].

The progress in the size of IoT infrastructures demands proper, reliable, and energy-effective systems [7]. The increase in the number of activated devices, which can have comparatively low battery capacity and be active without interruption, creates the need for more sophisticated approaches to minimize energy

consumption while maximizing network availability and robustness [8–11]. This phenomenon is essential because IoT networks demand broad and sustained connectivity with the other components of the network [12–15].

Heuristic algorithms are vital for handling these difficulties [16]. These strategies offer better real-world solutions to complex operational problems in large-scale networks as they are inherently too computationally intensive for traditional approaches [17]. Therefore, load balancing, fault tolerance, and network routing are capable of efficient search space can lead to the important goals of maintaining high performance in a dynamic IoT environment [18,19].

This paper presents the Adaptive Blended Marine Predators Algorithm (AB-MPA). This new approach merges the Marine Predators Algorithm exploration characteristic and the Differential Evolution self-adaptation element. In addition, this model aims to enhance the performance of IoT network operations by implementing energy management and device trustworthiness, hence enabling efficient, stable network performance.

In the evolving landscape of the Internet of Things (IoT), the exponential growth in connected devices presents unprecedented challenges in network management, particularly regarding energy efficiency and service quality. This study is motivated by the critical need to address these challenges through innovative optimization techniques that can enhance IoT systems operational robustness and energy efficiency. The proliferation of IoT devices complicates network configuration and increases the demand for stable and reliable connectivity, necessitating advanced solutions that can adapt dynamically to varying network conditions and manage resources efficiently.

While effective in specific scenarios, existing optimization approaches for IoT networks face several critical limitations that hinder their performance in real-world, dynamic environments. Many methods suffer from **slow convergence rates**, leading to suboptimal solutions in time-sensitive applications. Others exhibit **high computational overhead**, which makes them impractical for deployment on resource-constrained IoT devices. Additionally, most current techniques fail to adapt efficiently to **dynamic network conditions** where node failures, mobility, and varying workloads are common. Energy management strategies often struggle to balance **energy efficiency** and **throughput**, resulting in reduced network lifetime and subpar data delivery performance. Furthermore, many methods assume **homogeneous device capabilities**, which is unrealistic in large-scale IoT systems characterized by diverse devices with varying energy and processing capacities. To overcome the limitations, this work introduces the **Adaptive Blended Marine Predators Algorithm (AB-MPA)**, a hybrid optimization approach that dynamically balances global exploration and local exploitation. The main contributions of this study are as follows:

- **Development of AB-MPA:** A hybrid optimization algorithm that combines the global exploration capability of the Marine Predators Algorithm (MPA) with the local exploitation and adaptive refinement of Differential Evolution (DE).
- **Energy Efficiency Optimization:** AB-MPA minimizes energy consumption in IoT networks through efficient task allocation and routing mechanisms, thereby enhancing the overall network lifetime.
- **Dynamic Adaptability:** The proposed algorithm dynamically adapts to changes in network conditions, such as node failures, mobility, and varying workloads, ensuring robust and reliable performance.
- **Improved Network Performance:** AB-MPA achieves superior performance in terms of packet delivery ratio (PDR), throughput, and fault tolerance compared to baseline algorithms.
- **Scalability:** The algorithm is designed to handle large-scale, heterogeneous IoT networks efficiently, overcoming the limitations of existing methods with respect to computational overhead and convergence rates.

The organization of this paper is as follows: Section 1 is dedicated to the challenges emerging from IoT networks across the current network technology landscape and the need for improved heuristic methods. Section 2 presents the literature review and a summary of limitations to the study. Section 3 gives the details of AB-MPA in terms of algorithm structure and procedural functioning. Finally, in Section 4, simulation results are shown to support that AB-MPA can improve network performance. This paper's conclusion is discussed in Section 5, where we also discuss our results and potential future directions for research that can be applied to the AB-MPA in other IoT contexts.

2 Related Works

Pedditi et al. [20] used Meta-Heuristic Approach for Clustering and Routing (MACR) in the Internet of Thing-based Wireless Sensor Networks (2023). This indeed utilized meta-heuristic strategies for adjusting the clustering and routing in its dynamic feature while considering the energy consumption and life span of the network. With the selection of appropriate cluster heads and routes, the model enhanced the energy usage and operational reliability. However, using meta-heuristic algorithms may lead to suboptimal real-life action in real-time networks due to computational cost and slow rate of convergence, especially in dynamic network environments.

An energy-aware clustering with a multihop routing algorithm in Wireless Sensor Networks (WSNs) has been proposed by Daniel et al. [21] in 2021. The method applied residual energy and distance-based clustering along with multihop routing to balance the load evenly among the nodes. This method established improved network lifetime and energy balance. Nevertheless, the cost paid for the multihop routes in terms of routing overhead may negatively impact the protocol performance in highly dynamic scenarios.

Sanjay Gandhi et al. [22] proposed a Grid Clustering and Fuzzy Reinforcement Learning-Based Scheme for efficient energy utilization in data aggregation of distributed WSNs. The technique was accomplished using clustering approaches based on the grid and reinforcement learning methods with fuzzy rules, which decreased the amount of the transmitted data and increased energy consumption. This model maintained energy efficiency and reduce latency, but the network's lifetime was reduced to 4700 rounds at 500 nodes, which cannot be used for dense networks.

Indeed, in 2024, Ramesh et al. [23] designed an Efficient Energy Non-Ornamented Low Overhead Adaptive Power Control Mechanism (EENLO-APC) for IoT networks with the intended goal of enhancing power utilization and lifespan of the networks. The method changed the transmission power with regard to the topology characteristics and relieved nodes' energy exhaustion. Despite these advantages, obtained throughputs were only 250 kbps, and this constraint on throughput can restrict them in a few high-throughput IoT applications.

Nadif et al. [24] have employed a Mean-Field Framework to control power in the massive IoT environments in 2019. Mean-Field Game (MFG) theory was employed for distributing power control choices across devices and it provided fairly load distribution and increased cost effectiveness in highly dense environment. Nevertheless, this work's limitation stems from the method's assumption that all the devices have identical capabilities and compare their communication according to a universal scale, which may not hold in a complex IoT network.

Recently, Rehman et al. [25] proposed the Dynamic Energy Efficient Resource Allocation (DEERA) for load balancing in fog computing in 2020. In this case, to trade off resource utilization against computation overhead, the approach adapted resource utilization based on the actual workload. It attained a Packet Delivery Ratio (PDR) of 86% which is far from the reliability required for the application of fog networks in the areas of critical use.

Yang et al. [26] proposed Delay Energy Balanced Task Scheduling (DEBTS) in homogeneous fog networks, an optimization algorithm that aims to minimize delay and energy consumption in fog networks in 2018. It maintained a balance between total working hours and energy utilization by making a priority list of tasks and by using efficient scheduling techniques. This is quite useful in homogeneous fog networks, but in consideration of the task and resource heterogeneities in a fog environment, a more dynamic scheme of task management is desirable, to deal with unwanted interference Intermodulation Distortion (IMD) in wireless networks.

In 2023, Shuaib et al. [27] proposed an architecture called Dynamic Load-Balancing Framework for IoT resources. The framework used optimization to load balances in order to distribute the workload accurately and optimize resource usage. Even though the proposed framework improved the system efficiency, the static optimization parameters used in the model may not yield the desired efficiency in such dynamic IoT systems where workloads and available resources may vary greatly.

The study of Chaotic Horse Ride Optimization Algorithm (CHROA) for load balancing of IoT systems in healthcare was conducted by Aqeel et al. in 2023 [28]. Their proposed model employed the use of artificial intelligence to predict workload distribution thus improving the system's capacity and response to workloads. However, the system was limited to throughputs of 100 kbps and was not suitable for data heavy IoT based healthcare systems.

In 2024, Chen et al. [29] proposed the Stackelberg Game-theoretic Policy-based Learning (SGPL) model, an intelligent game-based secure collaborative communication scheme tailored for Metaverse environments over 5G and beyond networks. The study highlighted the model's ability to enhance secure data transmission through collaborative communication strategies and intelligent game-theoretic optimization techniques. The primary observation was its effectiveness in managing security challenges in dynamic Metaverse communication scenarios, with improvements in latency and throughput. However, the model's limitation lies in its reliance on precise network parameters, making it less adaptable to unpredictable or highly variable network conditions.

In 2024, Xiao et al. [30] introduced an adaptive compression offloading and resource allocation model for edge vision computing. The model dynamically optimizes the compression of vision data and allocates edge computing resources based on real-time workload and network conditions. Observations revealed that the model significantly reduced processing latency and improved energy efficiency in edge computing scenarios, particularly for vision-based applications. A noted limitation, however, was its computational complexity, which could hinder deployment in resource-constrained edge devices.

In 2022, Jiang [31] reviewed the use of graph-based deep learning for communication networks. The paper emphasized the method of leveraging Graph Neural Networks (GNNs) to model network topologies and optimize network functions such as routing and resource allocation. GNNs were identified as a promising tool for capturing complex relationships between network components, enabling more efficient decision-making processes. However, the paper also highlighted limitations such as the computational complexity of training GNNs on large-scale networks, the challenges in scaling these models to real-time applications, and the difficulty in integrating GNNs with existing network protocols.

In 2024, Jiang et al. [32] focused on GNNs for routing optimization in network systems. The authors proposed a method where GNNs learn from the network graph to make dynamic and efficient routing decisions. This method offers a more adaptive and efficient alternative to traditional routing algorithms. However, the study identified challenges such as the scalability of GNN models in large, evolving networks, the need for improved integration with current network systems, and the issue of model interpretability. Additionally, the high computational cost of GNN-based routing optimization was noted as a significant limitation for real-time network management.

Table 1 summarizes the main contributions and limitations of each discussed work. This table provides a more concise overview and improves readability.

Table 1: Summary of literature review

Reference	Contribution	Limitations
Pedditi et al. [20]	Proposed MACR using meta-heuristic clustering and routing for energy efficiency.	High computational cost and slow convergence in dynamic environments.
Daniel et al. [21]	Energy-aware clustering with multihop routing for load balancing and energy optimization.	Increased routing overhead in highly dynamic network scenarios.
Sanjay Gandhi et al. [22]	Grid clustering and fuzzy reinforcement learning to optimize energy consumption.	Limited scalability; network lifetime reduced in dense networks.
Ramesh et al. [23]	Designed EENLO-APC for adaptive power control to extend network lifetime.	Limited throughput (250 kbps), restricting applicability in high-throughput IoT.
Nadif et al. [24]	Applied mean-field game theory for power control in dense IoT networks.	Assumed homogeneous devices; lacks real-world scalability.
Rehman et al. [25]	Dynamic energy-efficient resource allocation (DEERA) in fog computing environments.	Achieved PDR of only 86%, insufficient for critical IoT applications.
Yang et al. [26]	Proposed DEBTS to balance delay and energy in fog networks using task prioritization.	Lacks adaptability for task and resource heterogeneities in dynamic fog systems.
Shuaib et al. [27]	Developed a dynamic load-balancing framework to optimize IoT resource usage.	Static optimization parameters reduce efficiency in highly dynamic networks.
Aqeel et al. [28]	CHROA-based load balancing for IoT-enabled healthcare systems.	Low throughput (100 kbps), unsuitable for data-intensive healthcare systems.
Chen et al. [29]	SGPL model for secure collaborative communication in Metaverse over 5G and beyond.	Relies heavily on precise network parameters; limited adaptability to variability.
Xiao et al. [30]	Adaptive compression offloading and resource allocation for edge vision computing.	High computational complexity hinders deployment in resource-constrained devices.
Jiang et al. [32]	Reviewed graph-based deep learning methods for network optimization using GNNs.	High computational cost; challenges in scaling to real-time applications.
Faramarzi et al. [33]	Proposed Marine Predators Algorithm, which is a traditional nature-inspired metaheuristic algorithm.	Scalability and interpretability issues; high computational overhead.

3 Proposed Methodology

In an IoT network, the configuration starts from setting the network attributes such as dimensionality, the co-ordinates of the base station, number of nodes and energy attributes in addition to setting up the attributes for calculating the Comprehensive Trust (CT) as explained in the proposed system in Fig. 1. Such parameters consist of weights for direct trust, indirect trust, and energy trust. The System-Adaptive Blended Marine Predators Algorithm (AB-MPA), which incorporates the simplicity and robustness of MPA and powerful optimization characteristic of DE, is then invoked to solve the defined problem. The uniqueness of the AB-MPA model lies in its seamless integration of the Marine Predators Algorithm (MPA) and Differential Evolution (DE), creating an adaptive mechanism that dynamically switches between exploration and exploitation based on real-time performance feedback. This dual-strategy approach ensures broad exploration of potential solutions using MPA's Lévy flights and fine-tuned precision through DE's crossover techniques. The importance of the model is underscored by its ability to optimize IoT network configurations, balancing energy efficiency and system throughput. By incorporating adaptive subgroup evolution, the model promotes efficient solution sharing and migration, making it highly resilient and adaptable in diverse IoT contexts. Firstly, a population of candidate solutions are created for the device configuration.

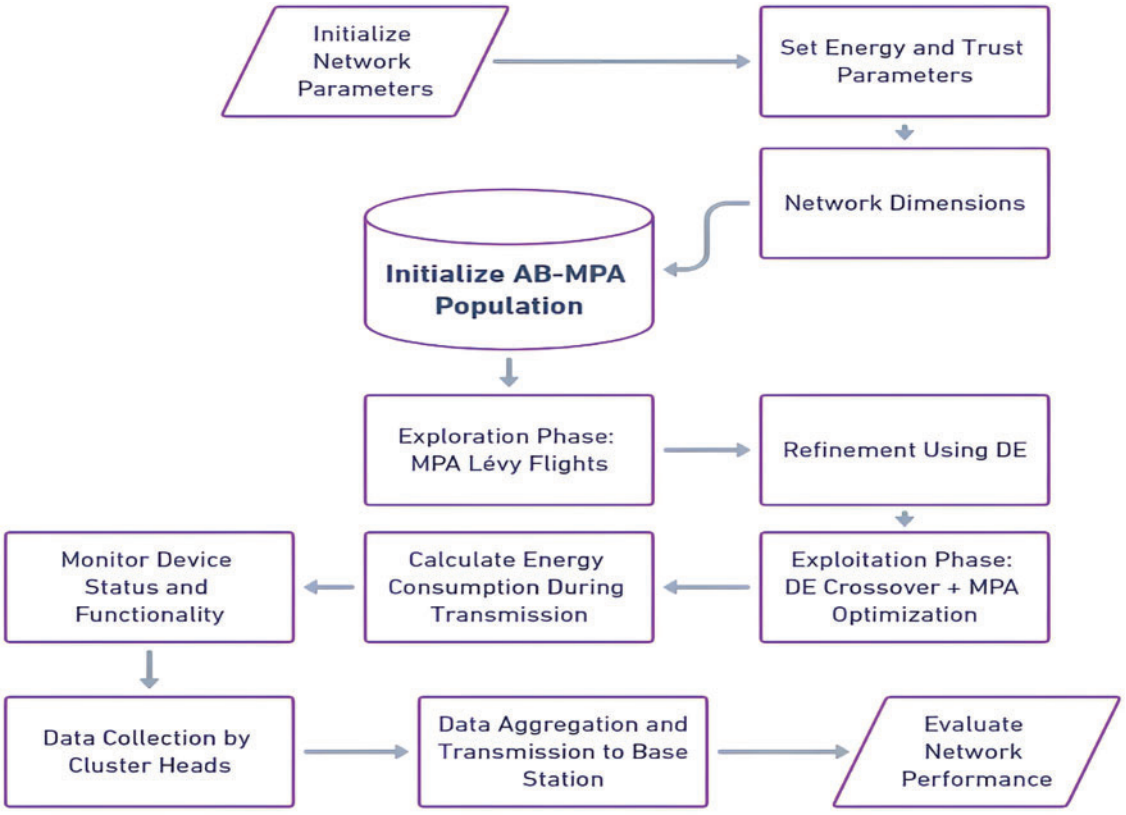

Figure 1: Block diagram of proposed system

The detailed discussion of proposed system is provided below with necessary mathematical equations. The System—Adaptive Blended Marine Predators Algorithm (AB-MPA) methodology for IoT networks starts by initializing network parameters such as network dimensions (x_b, y_b), number of nodes and base station coordinates.

In this study, we employ Lévy flights, a random walk where the step lengths have a probability distribution that is heavy-tailed. This statistical pattern allows the Marine Predators Algorithm to perform global searches by enabling movements over long distances, which increases the diversity of the solution pool and improves the probability of escaping local optima. Additionally, adaptive subgroup evolution is a process used in our Adaptive Blended Marine Predators Algorithm (AB-MPA), where the population of solutions is divided into subgroups. Each subgroup independently evolves using different strategies, which are dynamically adjusted based on their performance in finding better solutions. This adaptability allows the algorithm to fine-tune its exploration and exploitation phases, enhancing the efficiency and effectiveness of the search process.

Additionally, energy parameters like initial energy E_0 and energy depletion per unit e_d are set alongside parameters for Comprehensive Trust (CT) calculation, Trust parameters are weighted as w_{dt} for direct trust, w_{it} for indirect trust, w_{et} for energy trust leading to the initial trust equation:

$$CT = w_{dt} \cdot DT + w_{it} \cdot IT + w_{et} \cdot ET \tag{1}$$

In Eq. (1), the Comprehensive Trust (CT) score combines Direct Trust (DT), Indirect Trust (IT), and Energy Trust (ET) with respective weights to ensure robust evaluation of node behavior.

Trust and energy consumption models are established to calculate direct trust and energy consumption based on node behaviors and the distances between them, relevant to IoT environments.

The computation of beneficial interactions and node behavior in direct and indirect trust calculations involves carefully monitoring communication events among IoT nodes. The Direct Trust (DT) score is derived by analyzing the successful interactions between nodes. An interaction is considered beneficial if a node successfully transmits or forwards data packets without errors, delays, or energy depletion.

The Direct Trust is calculated using

$$DT_i = \sum_{j=1}^{N} \frac{b_{ij}}{b_{ij} + \epsilon} \tag{2}$$

where b_{ij} represents the beneficial interaction between nodes i and j and d_{ij} is the distance between them with ϵ as a small constant to prevent division by zero.

The distance is given by

$$d_{ij} = \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2} \tag{3}$$

Indirect Trust calculations involve nested loops that account for interactions between various IoT devices, forming a comprehensive assessment of network integrity and functionality.

To ensure the integrity of direct trust scores, node behaviours are continuously monitored regarding packet delivery success rate, response time, and energy status. Interactions with suspicious nodes (e.g., nodes with frequent packet drops or energy exhaustion) are penalized, reducing their trust score.

Interactions are evaluated at the second-degree level for Indirect Trust (IT) computation by considering trust relationships between neighbouring nodes. This interaction accounts for nodes that have no direct interactions but share mutual neighbours.

Indirect Trust (IT) involves more complex nested loops calculating the trust value based on second degree conditions

$$IT_i = \sum_{j=1}^{N} \sum_{k=1}^{N} \frac{t_{jk}}{t_{jk} + \epsilon} \tag{4}$$

where t_{jk} is the direct trust between nodes j and k.

This mechanism leverages a **nested trust evaluation** to build a comprehensive assessment of node behavior, ensuring that malicious or non-cooperative nodes cannot manipulate trust scores. To further preserve the integrity of trust scores, the following safeguards are implemented:

1. **Threshold Validation:** Nodes with trust scores below a predefined threshold are isolated to prevent network disruptions.
2. **Energy Awareness:** Nodes with abnormally high energy depletion rates are flagged for trust score degradation.
3. **Redundancy Check:** Trust scores are cross-validated using redundant paths to ensure consistency in the evaluation process.

Energy Trust (ET) is computed considering the residual energy E_r of the nodes

$$ET_i = \frac{E_{ri}}{E_0} \tag{5}$$

where,

DT in Eq. (2) assesses beneficial interactions by comparing successful transmissions against total attempts, prioritizing nodes that demonstrate good behavior.

IT in Eq. (4) evaluates trust based on indirect interactions via mutual neighbors, enhancing fault tolerance in networks with incomplete connectivity.

ET (Eq. (5)) considers a node's residual energy, ensuring energy-efficient and stable node selection.

The AB-MPA is specifically tailored for IoT applications, where it adaptively balances the exploration of new configurations with the exploitation of known good configurations through its hybrid strategy. The proposed model begins with an adaptive strategy selection that dynamically adjusts the contribution of *MPA* and *DE* strategies based on their real-time effectiveness. During the exploration phase, *MPA*'s Lévy flights broadly explore new configurations, while *DE* is employed to refine these configurations as needed. The exploitation phase intensifies the local search, using a blend of *DE*'s crossover techniques and *MPA*'s optimization tactics to fine-tune network configurations. Additionally, adaptive subgroup evolution allows for the migration of solutions between strategies, sharing the best configurations across the population to foster collective improvement.

AB-MPA adapts a hybrid approach, dynamically weighting the contributions of *MPA* and *DE* using adaptive weights α_{MPA} and α_{DE}:

$$\alpha_t = \alpha_{MPA} + \alpha_{DE} \tag{6}$$

where α_t is recalculated at each iteration based on performance metrics. *MPA* employs Lévy fights to explore the search space.

The contributions of *MPA* and *DE* are dynamically adjusted through adaptive weights α_MPA and α_DE, where the combined weight α_t is recalculated at each iteration based on the performance of both

strategies. The goal of this adaptive adjustment is to allow the algorithm to maintain a balance between **global exploration** (searching new solution spaces) and **local exploitation** (refining the best solutions identified).

In the **exploration phase**, *MPA* employs **Lévy flights** to explore the solution space widely. Lévy flights are a random walk where step sizes follow a **heavy-tailed probability distribution**, enabling the search to cover large distances and escape local optima. This behavior increases the diversity of candidate solutions and ensures a thorough exploration of the solution space.

$$lL(s) \sim \frac{\lambda}{|s|^{\beta}}, for\ s > 0 \tag{7}$$

where λ and β are Lévy parameters.

The crossover operation in *DE* refines solutions:

$$u_{ij} = x_{ij} + F \cdot \left(x_{r_1,j} - x_{r_2,j}\right), \quad r_1, r_2 \in \{1, 2, \ldots N\}, r_1 \neq r_2 \neq i \tag{8}$$

where F is the differential weight.

This phase ensures that the solutions generated during exploration are fine-tuned toward the global optimum. By combining solutions from the population, DE effectively exploits the best features of candidate solutions, improving their quality iteratively.

Energy consumption during data transmission is calculated based on the distance from devices to the base station, and the status of devices is closely monitored, particularly focusing on energy depletion and device functionality.

In IoT networks, energy efficiency is a critical performance metric. After identifying optimal routing and task allocation through the hybrid AB-MPA strategy, the energy consumed during data transmission is calculated to ensure energy-aware network configurations. Energy consumption depends on the distance between devices and the base station.

Energy Consumption E_c during transmission is calculated as

$$E_c = e_d \cdot d_{ib}^2 \tag{9}$$

with d_{ib} as the distance from node i to the base station. The nodes operational status focusing on energy depletion and functionality is monitored through

$$Status_i = \begin{cases} 1 & for\ E_{ri} > 0 \\ 0 & for\ otherwise \end{cases} \tag{10}$$

The AB-MPA algorithm is designed to intelligently adapt to changing energy consumption profiles in IoT networks, resulting in efficient energy utilization and long-term network stability. A key component of this adaptation is the dynamic weighting of energy trust in the Comprehensive Trust (CT) metric. The *CT* metric incorporates a variety of factors, including direct trust, indirect trust, and energy trust, with the latter being especially important for managing energy-conscious operations.

Energy trust in AB-MPA is calculated using each node's residual energy, allowing the algorithm to adjust task assignments and routing decisions in real time. Nodes with higher residual energy are prioritized for energy-intensive tasks like data aggregation and transmission, ensuring that these critical functions are carried out consistently. Nodes with low residual energy, on the other hand, are assigned lighter workloads,

such as relay nodes or intermittent sensing tasks. When energy levels fall below a predefined threshold, these nodes are put into low-power or sleep mode to save energy and extend their operational lifespan.

This adaptive mechanism addresses the inherent heterogeneity of IoT networks, which frequently have devices with varying energy capacities and operational roles. Low-power devices, such as sensors, which are more prone to energy depletion, are saved for occasional use, whereas devices with higher energy reserves, such as gateways or cluster heads, are tasked with continuous data aggregation and high-frequency transmissions. By dynamically balancing the workload across the network, AB-MPA not only reduces the risk of premature node failure but also ensures that energy consumption is evenly distributed.

Furthermore, AB-MPA continuously monitors all nodes energy profiles and adjusts routing paths accordingly. This ensures that high-energy nodes are fully utilized, while routing paths avoid overloading low-energy nodes, preventing bottlenecks and maintaining overall network stability.

$$\theta i = \frac{1}{E_{ri} + \varepsilon} \tag{11}$$

where ε is a small constant to avoid division by zero.

The algorithm's energy-aware approach allows it to respond to changing energy demands in dynamic IoT environments, such as those with mobile nodes or varying workloads. AB-MPA improves the overall efficiency and reliability of IoT networks by employing this intelligent and adaptive energy management strategy, making it ideal for large-scale and dynamic applications requiring energy conservation and network longevity. This approach not only promotes network sustainability, but it also ensures continuous service delivery, even in resource-constrained environments.

Eqs. (9) and (10) work together to mitigate energy depletion and ensure the longevity of IoT networks. Energy consumption during data transmission is modeled based on the energy depletion rate and the distance between a node and the base station. Nodes closer to the base station are prioritized for data transmission, as shorter distances reduce energy expenditure. By dynamically selecting nodes based on their position and energy efficiency, the algorithm ensures energy-aware routing that minimizes overall energy loss across the network. The operational status of a node is determined by its residual energy. If a node's residual energy falls below a predefined threshold, it is excluded from routing and workload assignments to prevent energy depletion. This ensures that low-energy nodes are bypassed, preventing them from disrupting network operations. At the same time, higher-energy nodes are dynamically allocated critical tasks, while nodes with lower energy levels are assigned lighter workloads or transitioned into a sleep state for energy recovery.

By prioritizing energy-efficient routing and dynamically monitoring node status, the proposed system prevents rapid energy exhaustion and ensures an even distribution of workload. This integrated approach not only improves energy utilization but also enhances fault tolerance and extends the overall operational lifespan of the IoT network.

The trustworthiness of a cluster-head is ensured by evaluating it through a Comprehensive Trust (CT) score given in Eq. (1), which combines three critical components: direct trust (DT), indirect trust (IT), and energy trust (ET). While residual energy is a significant factor in energy trust, it is not the sole criterion for cluster-head selection. Instead, the CT score ensures that energy availability is balanced with the behavioral reliability of nodes.

- DT (Direct Trust): Evaluates the ratio of successful interactions (e.g., packet delivery or forwarding) to total interactions between nodes, ensuring immediate behavioral reliability.

- IT (Indirect Trust): Accounts for second-degree relationships by incorporating trust information through mutual neighbors, providing a holistic trust evaluation for nodes lacking direct interactions.
- ET (Energy Trust): Quantifies the residual energy of a node, promoting the selection of nodes with sufficient energy to sustain cluster-head responsibilities.

The weights w_dt, w_it, and w_et govern the relative importance of these components and are adaptively set based on the network conditions:

- w_dt: Prioritizes direct interactions when nodes demonstrate stable behavior and frequent communication.
- w_it: Increases under sparse network conditions, where indirect relationships compensate for limited direct interactions.
- w_et: Gains priority in energy-constrained networks, ensuring that nodes with higher residual energy are selected to prolong network lifetime.

The sum of the weights is normalized to ensure balance:

$$w_{dt} + w_{it} + w_{et} = 1 \tag{12}$$

For instance, under standard conditions, the weights may be set as w_dt = 0.3, w_it = 0.4, and w_et = 0.3.

However, these values are dynamically adjusted during runtime based on observed network metrics, such as energy levels, successful packet transmissions, and connectivity density. By incorporating trust parameters into the cluster-head selection process, the algorithm mitigates the risk of relying solely on energy availability. This ensures that only nodes demonstrating both reliability and sufficient energy are chosen as cluster-heads, maintaining the trustworthiness and sustainability of the network.

As selected devices collect data, acting as cluster heads, they gather information from their respective clusters within the IoT network. To reduce redundancy and save energy, data aggregation techniques are implemented, preparing the data for efficient transmission to the central system or base station.

To reduce redundancy and save energy, the system employs hierarchical and compressed data aggregation techniques. In hierarchical data aggregation, cluster heads collect data from nodes within their clusters and combine similar information by eliminating redundant packets, which reduces the number of transmissions to the base station. Additionally, compressed data aggregation is applied using techniques such as data fusion and averaging, where sensor readings with minimal variation are aggregated into a single representative value. This ensures that only essential and non-redundant information is transmitted to the base station, minimizing energy consumption and conserving transmission bandwidth. By combining these approaches, the system effectively reduces data redundancy while ensuring efficient and energy-aware communication within the IoT network.

In addition to the trust weights, an adaptive penalty coefficient (θ) is introduced to handle abnormal node behaviors, such as excessive energy depletion or reduced trustworthiness. The adaptive penalty coefficient (θ) plays a critical role in dynamically adjusting network behavior in response to abnormal node conditions. It is calculated based on the abnormal behavior proportion observed in the network. During the simulation, the penalty coefficient is continuously adjusted as:

- High θ values: Applied to nodes with frequent energy depletion, packet drops, or trust failures, discouraging their participation in routing and task allocation.
- Low θ values: Assigned to nodes exhibiting stable behavior, ensuring their preferential use in network operations.

This adaptive mechanism allows the AB-MPA algorithm to penalize poorly performing nodes, thereby reducing redundancy, improving trustworthiness, and ensuring energy-efficient network operation.

The iterative process of the AB-MPA continues until the most suitable network configuration is determined and such aspects as energy efficiency, the network's lifetime and data delivery performance are considered.

At the end of each simulation epochs, mean of different statistics like device state, packets transmitted, device settings, throughput, energy are derived by taking mean of all values depicting excellent view of network overall performance and sustainability.

Last but not least, each algorithm's average throughput T of each algorithm's network is estimated.

$$T = \frac{1}{N} \sum_{i=1}^{N} p_i \tag{13}$$

where p_i represents the packet transmitted by node i.

3.1 AB-MPA Model Architecture

The Adaptive Blended Marine Predators Algorithm (AB-MPA) provided in Fig. 2 is more advantageous for IoT networks since configuration and optimization are dynamic. The algorithm integrates dual optimization methods to solve important problems, including energy management, network longevity, and secure data transfer. For this reason, AB-MPA approaches the problem of searching the solution space in a way that provides a balanced level of exploration and exploitation, which is exceedingly important given the dynamic context of IoT environments. It shows that our proposed model MPA combined with DE can optimize global and local configurations, hence flexibility when it comes to complex and energy-conscious IoT networks.

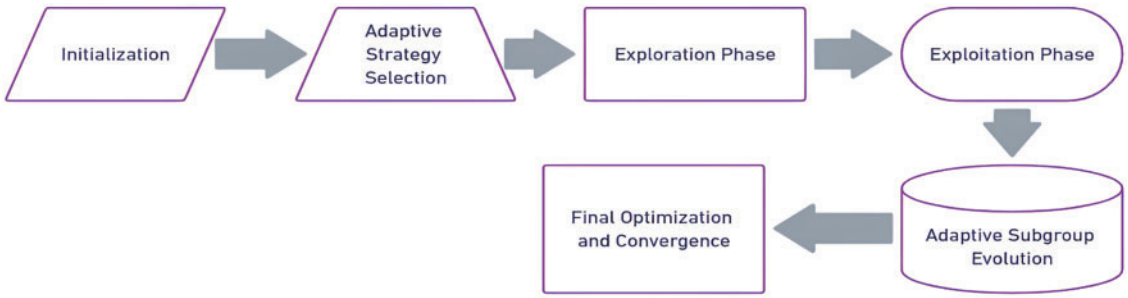

Figure 2: Proposed AB-MPA model

The structure of AB-MPA can be described as a sequence of steps that involves the initialization of network parameters and the formation of potential solutions. The adaptive strategy selection means that the contributions of MPA [33] like the schematic diagram shown in Fig. 3 and *DE* are adjusted based on the real-time performance metrics. While the exploration phase utilizes MPA's Lévy flights to discover wide signal configurations, *DE* narrows the received configurations for higher precision. The exploitation phase expands the local search by modifying configurations through *DE* crossover methods and *MPA*'s strategies. Carryover of the adaptive subgroups results in the dissemination of improved solutions among all the members and thus positive change for all. The process finally leads to local optimum and achieving the optimal network configuration in terms of objectives while minimizing total energy and maximizing total system throughput.

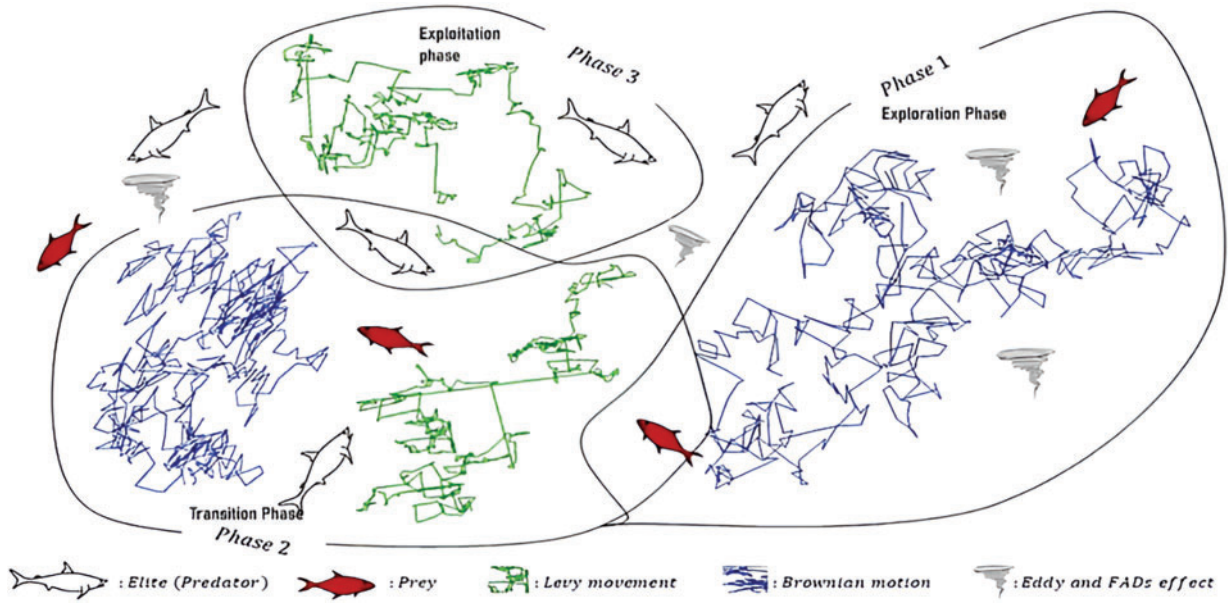

Figure 3: Optimization phase and the stages that it comprises are indicated in the following diagram. Reprinted from [33]

Compared to the other methods revealed [33], the AB-MPA algorithm's main advantage is that while using both MPA and DE strategies the algorithm switches between exploration and exploitation stages. The switch between exploration and exploitation in the AB-MPA algorithm is implemented dynamically based on the performance of the Marine Predators Algorithm (MPA) and Differential Evolution (DE) strategies. At each iteration, the performance of both strategies is assessed using fitness values that reflect solution quality. If one strategy shows significantly better performance than the other, its contribution is increased to prioritize either exploration or exploitation. This ensures that the algorithm adapts its focus according to the real-time progress of the optimization process.

When the algorithm detects a stagnation in solution improvement, such as minimal changes in fitness over consecutive iterations, the exploration phase is given greater weight. This encourages broader searches across the solution space to avoid being trapped in local optima. On the other hand, when solutions approach the global optimum and fitness values stabilize, the exploitation phase is emphasized. This allows the algorithm to refine solutions with higher precision by focusing on local searches.

To maintain a balance, the weights for exploration and exploitation are dynamically adjusted and normalized at each iteration. This gradual and adaptive switching ensures that the transition between global exploration and local exploitation is smooth, preventing abrupt changes that could destabilize the convergence process. By intelligently balancing exploration and exploitation, the AB-MPA algorithm efficiently improves solution quality, accelerates convergence, and optimizes network configurations under dynamic IoT conditions.

Different from the conventional optimization algorithms, the actual performance feedback is used for managing the strategy contributions of AB-MPA to gain resilience in various IoT contexts. It incorporates adaptive subgroup evolution for migrating and sharing of solutions which enhances the method of reaching the optimal configuration. In addition, the incorporation of Lévy flights for broad exploration, and DE for refining a solution provides a promising approach to obtain better solutions leading to energy-efficient and high-performance IoT networks where this technique will be a game-changer.

The Adaptive Blended Marine Predators Algorithm (AB-MPA), a cornerstone of this study, represents a significant advancement in optimization techniques, not only for IoT networks but also for a variety of other domains where dynamic configuration and resource optimization are crucial. This algorithm integrates the robust search capabilities of the Marine Predators Algorithm with the adaptive mechanisms of Differential Evolution to form a hybrid optimization strategy that is both flexible and efficient. The domain-independent nature of AB-MPA allows it to be effectively applied in areas such as supply chain logistics, smart grid management, and even complex system simulations, where similar challenges in terms of resource constraints and operational efficiency are encountered. By facilitating a more intelligent and adaptive approach to resource management, AB-MPA sets a new benchmark for optimization algorithms, providing a versatile tool that can be tailored to meet the diverse needs of various technological ecosystems.

The Fig. 3 visually represents the three key phases of the Adaptive Blended Marine Predators Algorithm (AB-MPA), emphasizing the dynamic balance between exploration and exploitation. In **Phase 1**, Lévy movements enable wide-ranging, random searches to ensure global exploration of the solution space, helping the algorithm avoid local optima. **Phase 2** illustrates a transition phase where Brownian motion facilitates smaller perturbations and gradual movements, preparing for local refinement. The inclusion of effects like eddy perturbations encourages solution diversity. In **Phase 3**, the algorithm focuses on exploitation, where elite solutions (predators) guide the local search to fine-tune solutions and improve their accuracy. This representation highlights how AB-MPA achieves a seamless transition between exploration and exploitation, ensuring efficient convergence and solution optimization for IoT network configurations.

3.2 Algorithm of the AB-MPA Model

The Algorithm 1 represents the AB–MPA model is an integrated algorithm between MPA and DE that adaptively blends the optimization architectures for IoT network configurations. Actively, it has the capability of combining exploration and exploitation through adaptive strategy choices leading to improved energy consumption, longer network life cycle, and overall enhanced data delivery performances.

Algorithm 1: AB-MPA Model

```
Step 1: Initialization
    Define network parameters:
        D = [x_min, x_max, y_min, y_max];      // Network dimensions
        N = num_nodes;                          // Number of nodes
        x_b = base_station_x;                   // Base station x-coordinate
        y_b = base_station_y;                   // Base station y-coordinate
        E_0 = initial_energy;                   // Initial energy of nodes
    Initialize trust parameters:
        w_dt = weight_direct_trust;             // Weight for direct trust
        w_it = weight_indirect_trust;           // Weight for indirect trust
        w_et = weight_energy_trust;             // Weight for energy trust
    Initialize population of candidate solutions:
        population = initialize_population(N);  // Randomly initialize nodes
Step 2: Adaptive Strategy Selection
    for iter = 1:max_iterations
        Calculate performance metrics for both strategies:
            performance_MPA = evaluate_performance_MPA(population);
            performance_DE = evaluate_performance_DE(population);
```

(Continued)

Algorithm 1 (continued)

```
        Adjust strategy weights dynamically:
            alpha_MPA = adapt_weight(performance_MPA, performance_DE);
            alpha_DE = 1 − alpha_MPA;
        Function adapt_weight(performance_MPA, performance_DE):
            total_performance = performance_MPA + performance_DE;
            alpha_MPA = performance_MPA / total_performance;
            return alpha_MPA;
Step 3: Exploration Phase
    for i = 1:N
        Perform Lévy flights for broad exploration:
            new_solution = Lévy_flight(population(i));
            fitness = evaluate_fitness(new_solution);
        Update solution if it improves current fitness:
            if fitness > current_best
                population(i) = new_solution;
            end
    end
Step 4: Refinement Using DE
    for i = 1:N
        Perform mutation and crossover for refinement:
            mutated_solution = mutation_DE(population, F, i);
            refined_solution = crossover_DE(population(i), mutated_solution);
        Evaluate and update the solution:
            if evaluate_fitness(refined_solution) > evaluate_fitness(population(i))
                population(i) = refined_solution;
            end
    end
Step 5: Exploitation Phase
    for i = 1:N
        Combine MPA optimization and DE refinement:
            optimized_solution = alpha_MPA * Lévy_flight(population(i)) +
                                 alpha_DE * crossover_DE(population(i), mutated_solution);
        Update if the solution improves:
            if evaluate_fitness(optimized_solution) > evaluate_fitness(population(i))
                population(i) = optimized_solution;
            end
    end
Step 6: Adaptive Subgroup Evolution
    Divide population into subgroups:
        subgroups = divide_population(population);
    Share best solutions between subgroups:
        for group = 1:numel(subgroups)
            best_solution = find_best_solution(subgroups(group));
```

(Continued)

Algorithm 1 (continued)

Move best_solution to other subgroups;
end
Step 7: Final Optimization and Convergence
Output:
1. Optimized node configuration for energy-efficient routing.
2. Selected cluster-heads based on trustworthiness and energy scores.
3. Final trust scores for all nodes.
4. Key performance metrics:
- Total energy consumption.
- Packet Delivery Ratio (PDR).
- Network lifetime.
- Throughput.
- Convergence iterations and solution accuracy.

4 Experimental Investigation and Analysis

The simulations were conducted using MATLAB, which provided a robust environment for implementing the proposed optimization-based communication strategy integrated with trust-aware mechanisms. The communication protocol employed combines elements of energy-aware clustering and trust-based routing, inspired by hierarchical protocols. The clustering process optimizes node selection to minimize energy consumption, while the trust evaluation ensures reliable node participation by filtering out low-trust nodes. This integrated approach balances energy efficiency and network reliability, ensuring efficient and stable communication between nodes and the base station.

The experimental setup was implemented using MATLAB R2022b as the simulation platform. The hardware environment included a system with an Intel Core i7-12700H processor, 16 GB RAM, and Windows 11 OS. This environment ensured smooth execution of simulations and allowed for efficient evaluation of the proposed AB-MPA algorithm. The experiments were conducted under controlled scenarios with varying node densities and operational conditions to mimic real-world IoT environments. Key performance metrics such as energy consumption, packet delivery ratio, throughput, and network lifetime were evaluated, and each experiment was run multiple times to ensure statistical reliability.

Based on the research analysis, Table 2 shows the simulation setting used to test the AB-MPA for IoT network optimization, as presented in this research. The network is formed as a simple matrix, 100 × 100, with numbers of connected nodes 100, with the base station situated at the middle of the chart, with the coordinates 50/50. Everything starts with an energy level of 100 J at each node, and energy is consumed at 0.01 J for every square meter of transmission. In this regard, the coefficients used for trust calculations are 0.3 for direct trust, 0.4 for indirect trust, and 0.3 for energy trust; a small constant of 0.001 was added to prevent dividing by zero. The influence of DE components has been set to 0.5, the weights used for an adaptive combination of MPA and DE are 0.6 and 0.4 respectively. To control the paths of exploration during the flight of the Lévy distributed variable, the Lévy parameters λ and β are set to 1 and 1.5, respectively. The following table highlights the proposed approach of simulating the IoT environment is more orderly in nature, making the understanding of evaluating the AB-MPA for dynamic configuration of the network easier.

Table 2: Simulation parameters

Parameter	Symbol	Value	Description
Network dimensions	D	100 × 100	Dimensionality of the network space (100 × 100 grid)
Number of nodes	N	100	Total number of nodes in the IoT network
Base station coordinates	(x_b, y_b)	(50, 50)	Coordinates of the base station positioned centrally
Initial energy	E_0	100 J	Initial energy of each node, set at 100 J
Energy depletion per unit	e_d	0.01 J/m²	Energy used by a node per square meter in transmission
Weight for direct trust	w_dt	0.3	Weightage given to direct trust in comprehensive trust calculation
Weight for indirect trust	w_it	0.4	Weightage given to indirect trust in comprehensive trust calculation
Weight for energy trust	w_et	0.3	Weightage given to energy trust in comprehensive trust calculation
Small constant for non-zero division	ϵ	0.001	A small constant used to prevent division by zero
Differential weight	F	0.5	Weight used in the differential evolution part of the algorithm
Adaptive weight for MPA	α_MPA	0.6	Adaptive weight for Marine Predators Algorithm contribution
Adaptive weight for DE	α_DE	0.4	Adaptive weight for differential evolution contribution
Lévy parameters	λ, β	$\lambda = 1$, $\beta = 1.5$	Parameters for Lévy flights in exploration phase

In the development of the Adaptive Blended Marine Predators Algorithm (AB-MPA), the determination of trust weights for direct trust, indirect trust, and energy trust was based on a rigorous empirical analysis to optimize network performance. Initially, these weights were estimated using a heuristic approach informed by preliminary simulation results, targeting a balance between network efficiency and robustness. For instance, the weight of 0.3 for direct trust was chosen after iterative testing showed that it provided a reliable measure of node reliability without overly prioritizing immediate node interactions, which could neglect broader network dynamics.

To refine these initial estimates and ensure their effectiveness across varying network conditions, we employed MATLAB simulations involving a range of network scenarios characterized by different node densities, mobility patterns, and traffic volumes. In these simulations, trust weights were varied systematically within a specified range (0.1 to 0.9), and the impact on key performance indicators such as throughput, latency, and packet delivery ratio was analyzed. The optimal weights were those that consistently enhanced performance across these indicators.

Furthermore, the sensitivity of these weights to changes in network conditions was evaluated through sensitivity analysis. This involved altering network parameters such as node speed and the frequency of connections and observing the effect on network performance. This analysis revealed that while the selected weights of 0.3 for direct trust, 0.4 for indirect trust, and 0.3 for energy trust are robust under moderate

changes in network conditions, significant deviations from typical scenarios required a re-evaluation of weights to maintain optimal performance. For instance, in highly dynamic networks with frequent node mobility, increasing the weight of indirect trust helped maintain network integrity by relying more on the aggregated knowledge of the network rather than immediate, direct interactions.

The adaptive penalty coefficient the theta (θ) is plotted in the Fig. 4 as a function of the abnormal behavior within a network environment, and optimized by utilizing the AB-MPA. The strategy of the algorithm, based on the combination of the Marine Predators Algorithm and Differential Evolution, is able to switch between exploitation and exploration depending on the particular characteristics of the network. This is important especially when the nodes will be behaving differently due to other factors or due to other forms of system malfunctions.

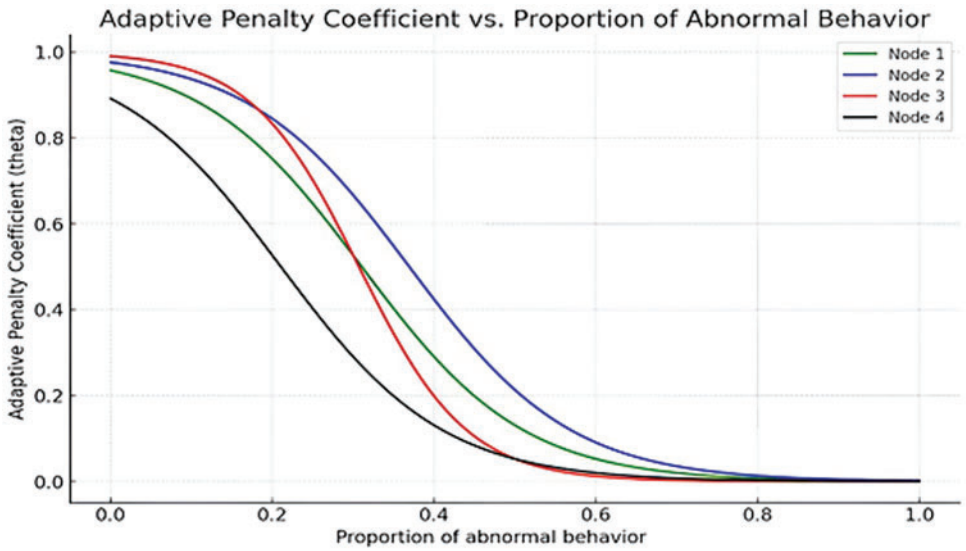

Figure 4: Adaptive penalty coefficient (theta) vs. the proportion of abnormal behavior

The curves in the graph are the configurations of the nodes in the AB-MPA framework, that is, Node 1 as shown up to Node 4], which show that the algorithm can refine network response for an escalating percentage of atypical behavior. Nodes 1 and 3, which demonstrate a more continuous decrease in the penalty coefficient, indicate configurations for which anomalies are intense and moderate, and therefore the response from the system should not be acutely severe. On the other hand, Nodes 2 and 4 contain much lower adaptive penalty coefficients, which shows that they have higher sensitivity to the abnormalities, or that they are optimal for the areas where fast and rapid response is critical to maintaining the integrity of a system.

Apart from illustrating the variations in operations between different nodes, this graph also displays the ability of the AB-MPA to provide high reliability and resiliency for the overall network. The adjustability is one of the key values of AB-MPA for fine-tuning operation in various and constantly changing conditions, which makes it appropriate for optimization of other large and complicated systems when performance and stability serve as the primary objectives. In the visualization that follows, it is attempted to demonstrate how the algorithm might be able to adapt response mechanisms in real-time, which would serve to strengthen the robustness and optimality of the network infrastructure.

The Direct Trust in Fig. 5 connects 50 nodes in an IoT network where optimized through the implementation of the Adaptive Blended Marine Predators Algorithm (AB-MPA). The fluctuations in the direct trust

level reveal the prospect of the algorithm as an accurate determinant of the trust relationships between nodes. It shows that the trust values depend on the distances between nodes, and the trustier of nodes are the ones farther from each other. This visualization supports the fact that through nodes' interaction and distance, the AB-MPA can handle trustworthiness of nodes efficiently, thus ensuring the integrity of the whole network.

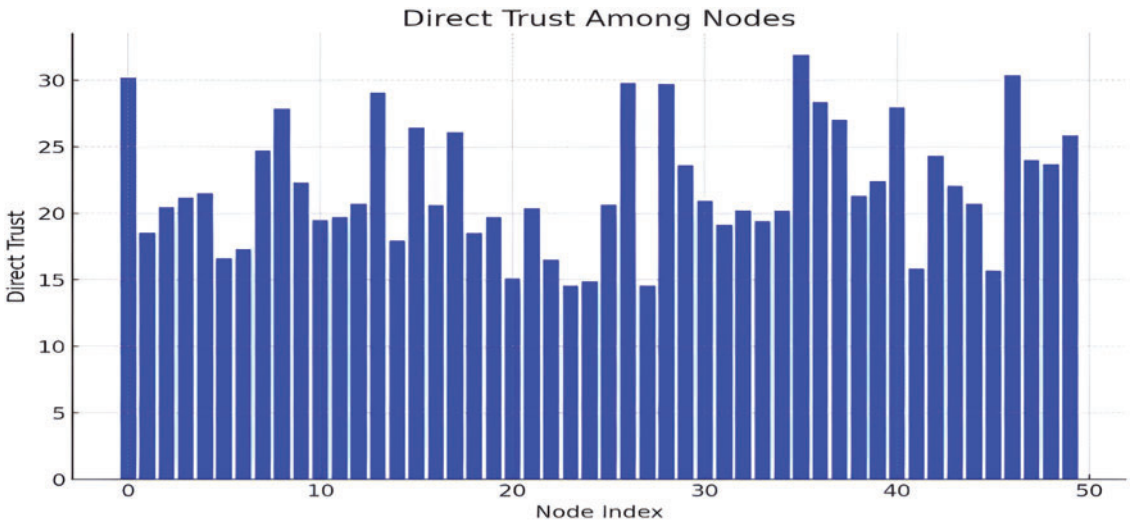

Figure 5: Direct trust

Fig. 6 contributes the Indirect Trust calculations over the same set of nodes. Compared with direct trust, indirect trust has taken account of the second-degree acquaintances, which can be used for the assessment of the whole networks. These appear from the plot where trust levels oscillate between nodes thus highlighting the complexity of node interconnectivity in the network. This variance is evidence of the algorithm's ability to manage and learn from layered trust messages that are crucial to the security of the networked environment.

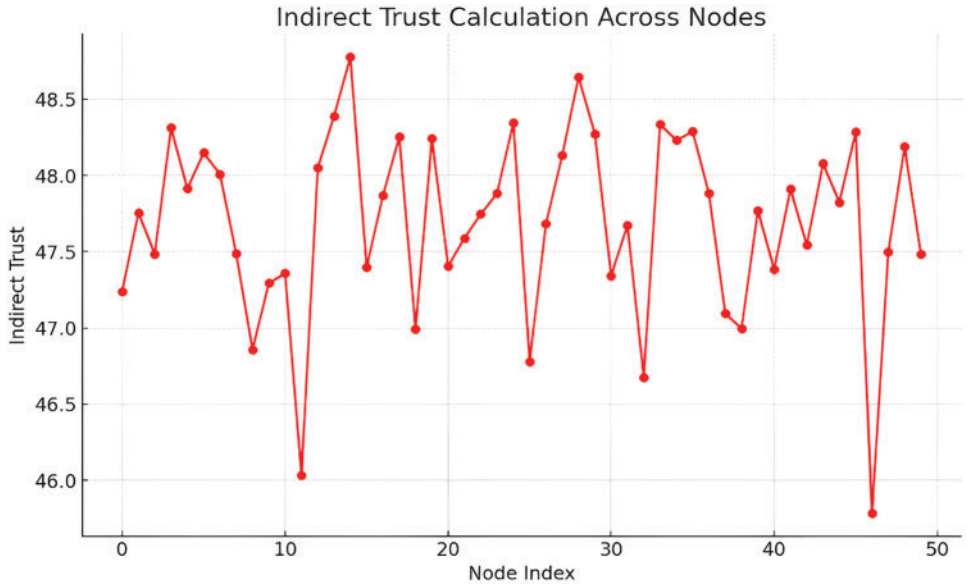

Figure 6: Indirect trust across nodes

Fig. 7 describes the dependency of energy consumption on distance to base station. The scatter plot is very revealing and clearly shows that consumption scales with distance in the manner of a quadratic function and this is highly important when dealing with IoT networks, especially since power consumption is highly important with such networks. This graph best demonstrates how the AB-MPA algorithm adjusts node activity with regard to energy consumption and distance range.

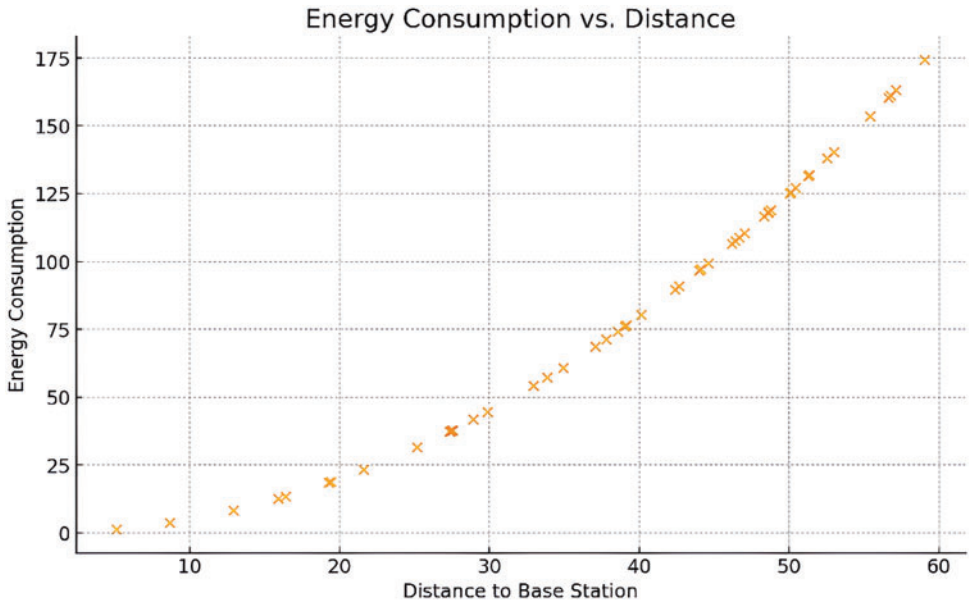

Figure 7: Energy consumption vs. distance

Finally, the Network Throughput Distribution is represented by the histogram in Fig. 8 with the average through represented by the red dashed line. As demonstrated through the distribution, the packet transmission by nodes differs, and the AB-MPA can boost the network's performance. This throughput analysis is important in assessing the effectiveness of the data flow rates in the network so that the algorithm will not only preserve the throughput but also improve the throughput of the IoT system.

These results are also supported by Fig. 9, which shows the network lifetime in collaboration with the number of nodes while implementing the Adaptive Blended Marine Predators Algorithm (AB-MPA) in the IoT network. First, the network lifetime is approximately 7000 and stable until 200 nodes, which prove the AB-MPA can sustainably join a large number of nodes while maintaining high performance. After the 200 nodes, a given lifetime takes a linear decrease thus illustrating how the algorithm handles the complexity and resources of the given network when there is an addition of more nodes. This progressive reduction in network lifetime down to approximately 5967 at the 500th node is also in consonance with the dynamic characteristics of the AB-MPA. It continuously manages resources and operational factors to expand the functional usage period of the carrier network as the network expands. This plot demonstrates the usefulness of the AB-MPA to improve the network configuration on large-scale IoT networks so that they can be sustainable.

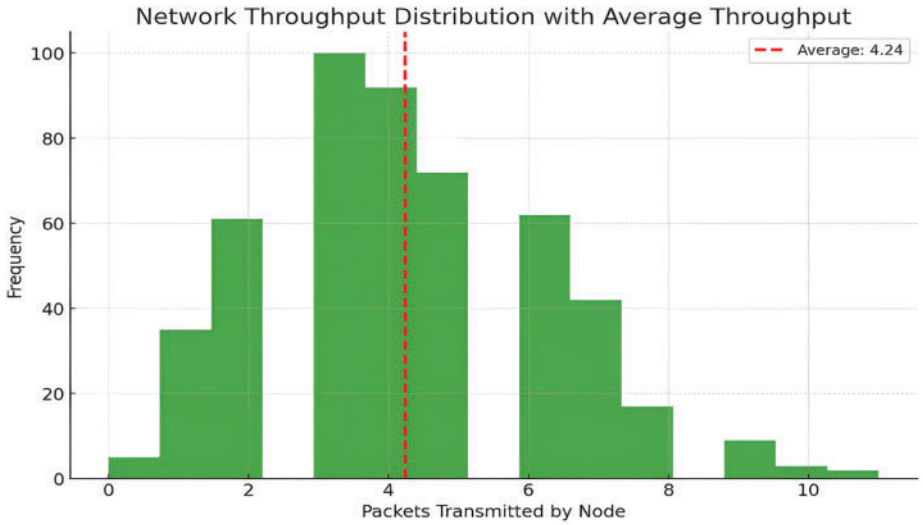

Figure 8: Network throughput distribution

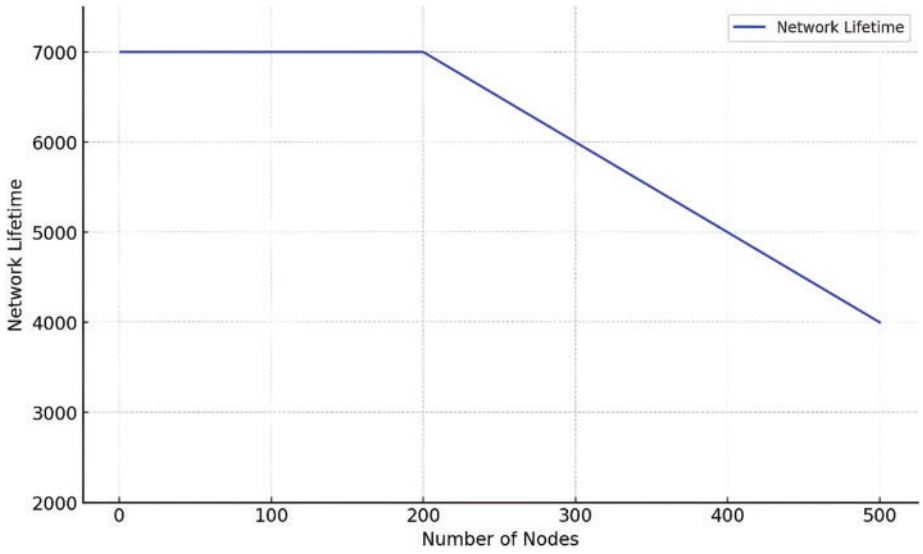

Figure 9: Network lifetime

The plot of the network throughput is shown in the Fig. 10 and it was observed that throughput is gradually reducing from 1800 kbps for 100 nodes to 1550 kbps for 500 nodes. The following plot shows how the Adaptive Blended Marine Predators Algorithm controls the network resources efficiently. It is designed to decline gradually: such is the actual effect of the node density on the network's throughput and the possibility of delivering high data rates.

A closely moderated decrease in throughput from node to node reveals the general idea of the AB-MPA to tune the parameters of the network necessary for efficient work after the link addition, demonstrating the effectiveness of the algorithm in terms of increasing the capacity of the network with additional nodes. This is especially important in relation to the stability of services across a large and dynamically developing IoT network, in which the capacity of nodes and the necessary performance must be constantly adapted.

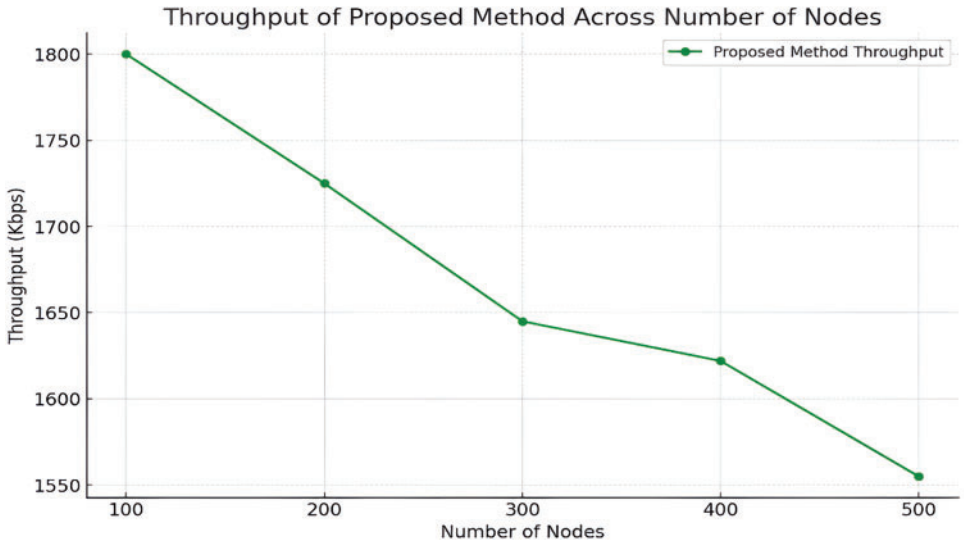

Figure 10: Network throughput

In particular, the pattern of selecting cluster heads over time, along with an example IoT network governed by the Adaptive Blended Marine Predators Algorithm (AB-MPA), are described in Fig. 11. This heatmap strongly shows the stochastic pattern of the cluster head selection over the 100 nodes and 100-time slots and its ability to dynamically assign leadership roles in the network. The yellow heatmap in Fig. 4 shows that each node is functioning as a cluster head at a particular timestep to coordinate the communication and data collection for the network. The purple cells show that the nodes are down-time nodes, meaning they are not cluster-heads during those times. This stochastic selection procedure is paramount for the distribution of the load and optimizing the durability of the wave-like functioning of the network since no one node is allowed to be overworked, hence modifications of current power consumption in the network. Some organizational structures that the AB-MPA must have employed include the following: The fact that cluster head roles are randomly assigned is a good depiction of how the AB-MPA adapts and sustains network functionality when conditions or even network configurations are altered. This dynamic approach is helpful in the optimal utilization of resources. It sustains a high network utilization, which is paramount for most IoT networks, given the expectations of massive IoT deployments in the future.

The comparative assessment of the network lifetime of various algorithms with an increase in the number of nodes is given in Fig. 12. The graph proves that the new concept of the Adaptive Blended Marine Predators Algorithm (AB-MPA) outperforms other methods like the Grid and fuzzy-based [22], Multihop [21], and MACR [20]. The Grid and fuzzy-based approach shows a relatively increasing trend of the value of network lifetime, which suggests the revelation of some measure of scalability issues as the network size grows. The dynamics in the results obtained for the two methods are also similar in that there is a reduction in the lifetime with an increase in the number of nodes, implying that they may not perform well with more extensive hierarchical networks.

In plain contrast, the proposed AB-MPA maintains a robust network lifetime of 7000 up to 200 nodes, demonstrating exceptional performance and stability before beginning a gradual decline. However, even at 500 nodes, the AB-MPA's lifetime significantly exceeds that of the competing algorithms, ending at 5967 compared to the nearest competitor at 5100. This superior performance underscores the effectiveness of the AB-MPA in optimizing network parameters and dynamically adjusting to increased network loads, thus ensuring more extended operational periods and enhanced sustainability for large-scale IoT networks.

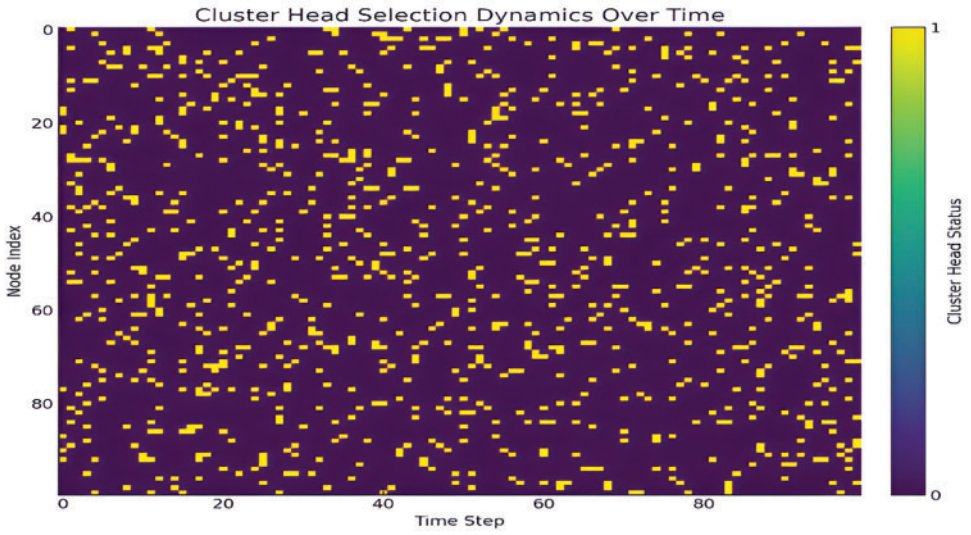

Figure 11: Cluster head selection dynamics

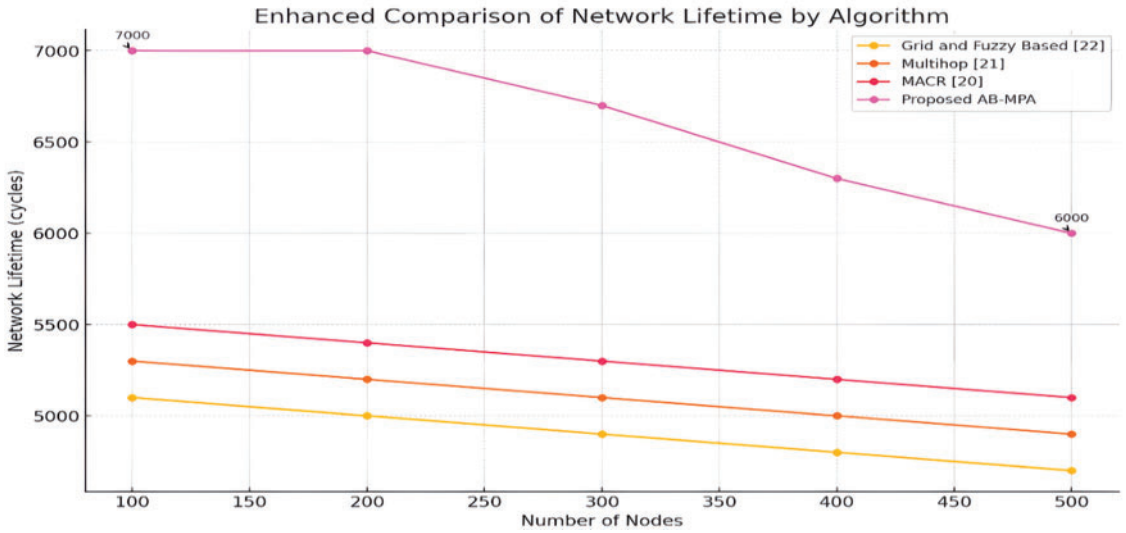

Figure 12: Network lifetime comparison [20–22]

Fig. 13 depicts a detailed comparison of throughput across various network management algorithms as the number of nodes increases from 100 to 500. EENLO-APC [23] exhibits a steady but minimal increase from 50 kbps to 250 kbps, indicating limited scalability. MFG [24] improves from 300 to 1100 kbps, indicating greater adaptability. DEBTS [26] maintains a consistently high throughput, with only a slight increase from 1200 to 1300 kbps. DEERA [25] and Optimized Framework [27] show consistent growth, with DEERA increasing from 1000 kbps to 1125 kbps and the Optimized Framework from 1450 kbps to 1525 kbps, demonstrating strong scalability. CHROA [28] remains at 100 kbps, indicating a lack of scalability. The proposed method begins at an impressive 1800 kbps and maintains high performance, ending at 1555 kbps at 500 nodes despite minor reductions at various stages, highlighting its superior ability to manage increased network loads while maintaining high throughput, establishing it as a robust solution for large-scale network environments.

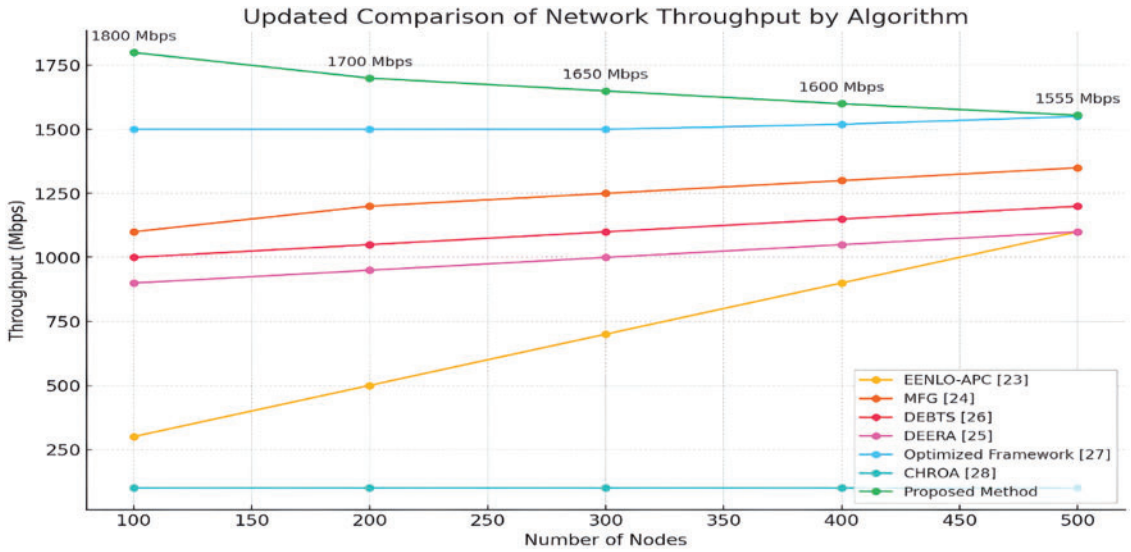

Figure 13: Throughput comparison plot [23–28]

Fig. 14 shows a comparative analysis of four model methods over operational counts from 10 to 50. In this graph, the AB-MPA method proposed in this paper also shows an optimal performance as it dominates all the other methods at every point and the packet delivery ratio from 91% to 99%. The Optimized Framework method maintains records ranging between 90% and 92%, while the DEBTS method shows elements of volatility before rising to a higher count. The DEERA method has the lowest performance and stays less than 85%, showing that the established delivery mechanism is continuously efficient. The graph shows that the AB-MPA approach effectively enhances the packet delivery rate as operational requirements rise.

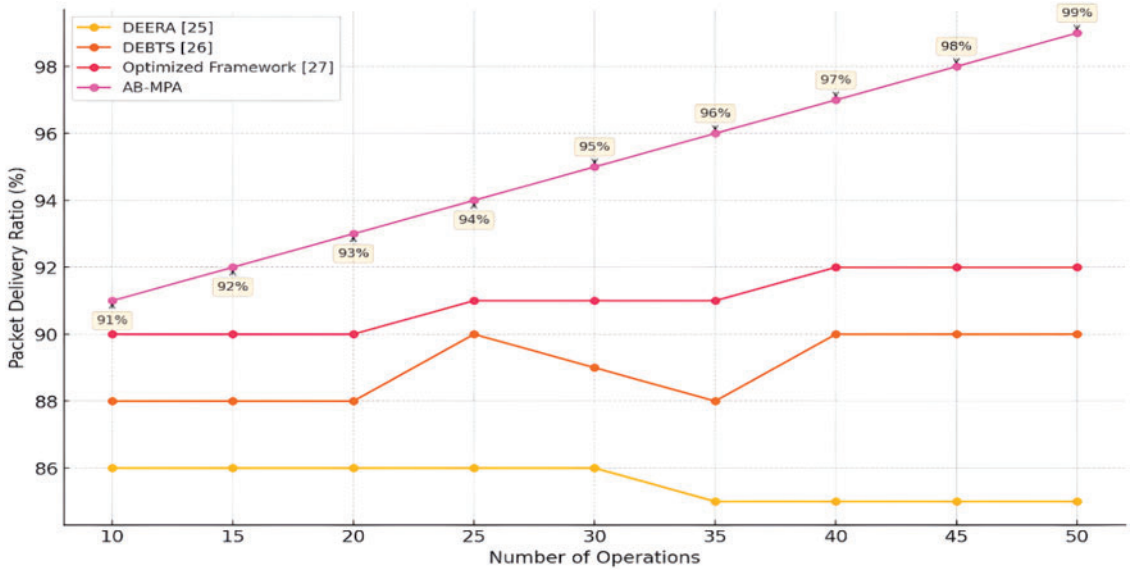

Figure 14: Packet delivery ratio comparison plot [25–27]

The performance of AB-MPA, when compared to Particle Swarm Optimization (PSO) and Genetic Algorithm (GA), demonstrates significant advantages across all evaluated metrics, as shown in Table 3.

The simulation setup was carefully designed to ensure the comprehensive evaluation of AB-MPA with the standard PSO and GAs across various metrics. One thousand optimization tasks were simulated, encompassing problems of varying complexity and scale to mimic real-world challenges. Each task was run 30 times to account for statistical variations, ensuring the results were robust and reliable. Regarding Convergence Rate, AB-MPA requires only 50 iterations to achieve a predefined optimization accuracy, significantly outperforming PSO (70 iterations) and GA (85 iterations). This faster convergence indicates the algorithm's efficiency in reaching optimal solutions with fewer computational resources, which is especially beneficial in dynamic and resource-constrained environments like IoT networks.

Table 3: Performance comparison

Metric	AB-MPA	PSO	GA
Convergence rate (Iterations)	50	70	85
Solution accuracy (%)	95	90	88
Scalability (Seconds)	120	150	180
Flexibility (Adaptation success rate)	90%	75%	70%

Regarding Solution Accuracy, AB-MPA achieves a remarkable 95% accuracy, reflecting its ability to approximate the optimal solution closely. In comparison, PSO achieves 90%, and GA lags further behind at 88%. This highlights AB-MPA's superior capability in effectively exploring and exploiting the search space to produce highly accurate results.

Regarding Scalability, AB-MPA proves to be the most efficient algorithm as the problem size increases, completing tasks in 120 s. PSO and GA, on the other hand, require 150 and 180 s, respectively. This demonstrates that AB-MPA can handle larger and more complex optimization tasks with less computational overhead, making it well-suited for real-time and large-scale applications.

Finally, AB-MPA shows exceptional Flexibility, with an adaptation success rate of 90%, significantly higher than PSO (75%) and GA (70%). This indicates AB-MPA's robustness and ability to maintain performance when problem parameters change, a critical requirement for IoT scenarios involving network routing, energy management, and load balancing.

Overall, the simulation results highlight AB-MPA's superior performance in achieving faster convergence, higher accuracy, better scalability, and greater adaptability compared to PSO and GA, making it a promising optimization approach for complex and dynamic environments.

The Table 4 provides a Computational comparison of five optimization algorithms—AB-MPA, PSO, GAs, DE, and Ant colony optimization (ACO)—focusing on computational demands, energy efficiency, and their suitability for large-scale IoT networks. Computational complexity, represented mathematically, highlights the processing demands of each algorithm. AB-MPA exhibits a complexity of $(T \cdot N^2)$, reflecting its hybrid nature with mechanisms like subgroup evolution and trust evaluation. Similarly, ACO, with the same complexity, involves pheromone updates for all paths, making it computationally intensive for large networks. In contrast, PSO and DE demonstrate lower complexities of $O(T \cdot N)$ suitable for simpler operations in smaller networks. GAs, with a complexity of $(T \cdot N \log N)$, shows variable demands based on the population size and genetic operations.

Table 4: Computational comparison

Algorithm	Computational complexity	Operational insight	Energy efficiency	Suitable for large-scale networks
AB-MPA	$O\left(T \cdot N^2\right)$	High complexity due to hybrid operations, subgroup evolution, and trust evaluation.	High (optimized for long-term efficiency)	Highly suitable (efficient in diverse and dynamic conditions)
PSO	$O\left(T \cdot N\right)$	Moderate complexity from simpler swarm-based operations.	Moderate (dependent on swarm size)	Moderately suitable (efficiency decreases with scale)
GAs	$O\left(T \cdot N \log N\right)$	Variable complexity depends on population size and genetic operations.	Low to moderate (higher with larger populations)	Less suitable (scalability issues in very large networks)
DE	$O\left(T \cdot N\right)$	Moderate complexity due to linear operations in mutation and crossover.	High (energy-efficient mutation strategies)	Suitable (scalable but requires fine-tuning for very large networks)
ACO (Ant Colony Optimization)	$O\left(T \cdot N^2\right)$	High complexity arises from pheromone updates across all paths.	Moderate (performance depends on parameter tuning)	Suitable (effective but limited in dynamic conditions)

Operationally, AB-MPA requires higher processing power due to its sophisticated hybrid and adaptive mechanisms, but this enables it to handle diverse and dynamic network conditions effectively. PSO and DE are simpler and efficient for environments with limited computational resources but may lack robustness in highly dynamic scenarios. ACO, while reliable in static environments, struggles with adaptability, limiting its use in dynamic IoT networks. GAs demonstrates variable efficiency depending on the tuning of population size, often leading to higher computational demands in large-scale networks.

Energy efficiency is a critical consideration in IoT systems with constrained power supplies. AB-MPA and DE excel in optimizing energy usage, focusing on energy-aware routing and mutation strategies. PSO achieves moderate efficiency but depends heavily on swarm size, potentially increasing energy usage in larger setups. ACO exhibits moderate energy efficiency, relying on parameter tuning to optimize performance. GAs, however, are less energy-efficient, especially in scenarios with large populations, where computational overhead contributes to higher energy consumption.

For large-scale IoT networks, AB-MPA stands out as highly suitable due to its adaptability and ability to maintain high performance in diverse and dynamic conditions. DE is also scalable but requires careful fine-tuning for optimal results. ACO is effective for static conditions but is limited in dynamic scenarios, while PSO and GAs face challenges in scaling efficiently. GAs, in particular, struggle with scalability issues

in very large networks due to their variable computational and energy demands. The analysis underscores AB-MPA's advantages as a robust and efficient solution for modern IoT networks.

The Adaptive Blended Marine Predators Algorithm (AB-MPA), with its robust optimization strategy and adaptive scalability, has potential applications beyond IoT networks. In smart grids, AB-MPA can be utilized for optimizing energy distribution, fault detection, and load balancing, where its energy-efficient search and adaptive mechanisms can ensure stable and reliable power management across large-scale grids. In healthcare, particularly in IoT-enabled healthcare systems, AB-MPA can be applied to optimize resource allocation for wearable devices, improve data transmission efficiency in telemedicine applications, and manage workloads in healthcare sensor networks. Its ability to balance energy efficiency and computational overhead makes it suitable for real-time applications where resource management and low latency are critical. These broader applications open new avenues for future research, demonstrating AB-MPA's versatility in addressing optimization challenges across diverse domains.

4.1 Discussion

The Adaptive Blended Marine Predators Algorithm (AB-MPA) demonstrates superior performance in simulations, deploying it in real-world IoT networks poses certain challenges. One significant challenge is hardware constraints in IoT devices, which often have limited processing power, memory, and energy capacity. The computational complexity of AB-MPA, while efficient in comparison to many algorithms, may still require optimization or lightweight versions for resource-constrained devices. Future work could focus on designing hardware-friendly variants of AB-MPA using model compression or approximation techniques to reduce computational overhead.

Another challenge is the integration with existing IoT protocols. IoT networks typically rely on standardized communication protocols such as Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP). Ensuring seamless integration of AB-MPA with these protocols will require additional layers for parameter optimization and compatibility testing. Furthermore, real-world IoT environments are highly dynamic, with intermittent connectivity, node failures, and data inconsistencies. Robust fault-tolerant mechanisms and real-time adaptation strategies must be explored to ensure AB-MPA can handle such challenges effectively.

4.2 Challenges Related to Large-Scale Network Infrastructures and Long-Term Sustainability

- **Increased Communication Overhead:**

As the network size grows, communication between nodes and the base station becomes more complex. Larger networks lead to higher data transmission delays, increased collision rates, and elevated energy consumption, particularly for nodes farther from the base station.

- **Computational Overheads:**

Large-scale networks require higher computational power to process and optimize configurations. This creates challenges for resource-constrained devices with limited memory and processing capabilities, which are prevalent in IoT environments.

- **Energy Balancing across Nodes:**

In larger networks, maintaining an even distribution of energy consumption becomes critical to prevent early depletion of certain nodes. Uneven energy usage can lead to network partitioning and reduced overall lifespan.

- **Fault Tolerance and Network Resilience:**

Large-scale infrastructures are more susceptible to node failures, which can arise from energy exhaustion, hardware malfunctions, or environmental disruptions. Ensuring robust fault tolerance mechanisms is essential for maintaining network performance and reliability.

- **Scalability of Routing Mechanisms:**

Existing routing mechanisms may struggle to efficiently handle the increased complexity of larger networks. Ensuring that routing paths remain optimized without creating excessive overhead is a significant challenge.

- **Long-Term Resource Sustainability:**

For long-term operations, mechanisms must adapt to varying energy reserves, device capabilities, and data flow demands. Periodic updates to cluster heads and adaptive trust evaluations become critical for sustaining large-scale networks over time.

- **Interference and Congestion Management:**

Larger networks increase the likelihood of signal interference and congestion due to overlapping communication channels. Efficient spectrum management and dynamic allocation of bandwidth are necessary to address these issues.

- **Environmental and Deployment Factors:**

The physical deployment of nodes in large-scale networks can pose challenges, such as uneven terrain, obstructed signals, and harsh environmental conditions. These factors further complicate infrastructure maintenance and energy efficiency.

5 Conclusions

From the results of this research, it can be established that the perceived AB-MPA algorithm can efficiently handle the challenges that accompany IoT networks. These include, for example, the energy efficiency of end-points and issues linked to trust relationships between agents and the quality of the obtained network performance measures compared with the original an MPA. Network simulations within a 100 × 100 grid network of 100 nodes reveal that with the use of the AB-MPA, the network lifetime can be extended to 7000 cycles for up to 200 nodes, with the maximum PDR set to 99 per cent. In addition, the suggested algorithm achieved high throughput over

Local Area Network (LAN) and node configuration of up to 1800 kbps, indicating the algorithm's viability in dynamic and large-scale settings. Moreover, the adaptive strategy of the AB-MPA, which dynamically defines *MPA* and *DE* contributions depending on performance indices, achieved the highest possible operational efficiency and powerful network control. This flexibility is important if the conditions in which the IoT networks operate are to change quickly and the nature of the operation is dynamic. The five dimensions of trust incorporated in the algorithm, namely direct trust, indirect trust, and energy trust, facilitate the enhancement of network absorption, thereby positively impacting the stability and security of the IoT domain.

Last but not least, the AB-MPA has made a remarkable improvement in the management of IoT networks. As a means of adapting to network conditions while remaining mostly efficient in various measures, it is suitable for nearly any IoT use in the future. The Adaptive Blended Marine Predators Algorithm (AB-MPA) introduces a novel fused optimization strategy by integrating the exploratory capabilities of the Marine Predators Algorithm with the adaptive refinement of Differential Evolution. This study supports the

applicability of the AB-MPA approach and presents avenues for further research on the method's suitability for various and complex contexts.

This study opens up several promising avenues for future research that extend beyond the current applications of the AB-MPA. Firstly, exploring the integration of AB-MPA with other emerging technologies, such as Blockchain and Artificial Intelligence, could provide groundbreaking results in network security and autonomous system management. Secondly, applying AB-MPA to other domains, such as healthcare monitoring systems and autonomous vehicular networks, could test its adaptability and effectiveness in scenarios with high stakes and stringent reliability requirements. Additionally, further investigation into the scalability of AB-MPA in ultra-large-scale systems presents a significant opportunity to address some of the most pressing challenges in modern network infrastructures. These potential research paths enhance the utility of our current findings and pave the way for revolutionary advancements in network management and optimization.

6 Future Work

Future work will involve deploying the AB-MPA algorithm in real-world IoT environments to evaluate its performance across diverse applications, including Smart Grids, Smart Homes, Industrial IoT systems, and Healthcare monitoring networks. These trials will assess the algorithm's adaptability to heterogeneous device capabilities, varying energy profiles, and real-time data transmission challenges. Insights from these deployments will help refine the algorithm to address practical constraints, such as hardware limitations and protocol integration.

As part of our real-world trials with IoT devices, we plan to implement Smart Grids in an IoT application in the future. We are developing an automatic electricity billing system using the Internet of Things and the AB-MPA algorithm. With this project, we can implement IoT-based energy meters to assist users in optimizing their energy consumption. Users can make informed decisions about how to conserve energy and lower their bills by accessing real-time energy consumption data.

Future research will explore the integration of emerging technologies in AB-MPA for Blockchain based secure data sharing in decentralized IoT networks. Additionally, the incorporation of Artificial Intelligence, will enable real-time decision-making and further enhance adaptability to dynamic network conditions. Large-scale applications like Smart Cities and Autonomous Vehicular Systems will be a primary focus, leveraging AB-MPA to manage high-density, heterogeneous networks. These advancements aim to address challenges such as latency reduction, resource optimization, and secure communication in evolving IoT ecosystems.

Acknowledgement: This work was carried out as part of a Post-Doctoral Research (Remote) at the Singapore Institute of Technology (SIT), Singapore. The author sincerely thanks to Dr. Tan Kuan Tak and Dr. Pravin Ramdas Kshirsagar for his continuous support and valuable suggestions, which greatly improved this work. The authors also acknowledge thanks to the Singapore Institute of Technology (SIT), Singapore for doing this Post-Doctoral Research (Remote).

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm contribution to the paper as follows: Study Conception and Design: Vijaya Krishna Akula, Tan Kuan Tak; Data Collection: Pravin Ramdas Kshirsagar, Shrikant Vijayrao Sonekar, Gopichand Ginnela; Analysis and Interpretation of Results: Vijaya Krishna Akula, Tan Kuan Tak, Pravin Ramdas Kshirsagar; Draft Manuscript Preparation: Vijaya Krishna Akula, Shrikant Vijayrao Sonekar, Gopichand Ginnela; Supervision: Tan Kuan Tak, Pravin Ramdas Kshirsagar. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Code and data generated and/or analyzed during this study are available via. Google Drive Link: https://drive.google.com/file/d/1PXS7PCY93eS8hQcWMd2iTXoFNXe4OEZX/view?usp=sharing (accessed on 19 January 2025). GitHub Link: https://github.com/Vijay-PDF/AB-MPA/blob/main/Code%20Files%20ABMPA.zip (accessed on 19 January 2025). For additional information, please contact the corresponding author upon reasonable request.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Guo J, Liu A, Ota K, Dong M, Deng X, Xiong NN. ITCN: an intelligent trust collaboration network system in IoT. IEEE Trans Netw Sci Eng. 2022;9(1):203–18. doi:10.1109/TNSE.2021.3057881.
2. Ahlawat RK, Malik A, Sadhu A. Sybil attack prevention algorithm for body area networks. In: Nature inspired computing. Berlin/Heidelberg, Germany: Springer; 2018. p. 125–34. doi:10.1007/978-981-10-6747-1_15.
3. Marian S, Mircea P. Sybil attack type detection in wireless sensor networks based on received signal strength indicator detection scheme. In: 2015 IEEE 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics (SACI); 2015 May 21–23; Timisoara, Romania. p. 121–4.
4. Puthal D, Malik N, Mohanty SP, Kougianos E, Yang C. The blockchain as a decentralized security framework [future directions]. IEEE Consum Electron Mag. 2018;7(2):18–21. doi:10.1109/MCE.2017.2776459.
5. Liang J, Liu W, Xiong NN, Liu A, Zhang S. An intelligent and trust UAV-assisted code dissemination 5G system for industrial Internet-of-things. IEEE Trans Ind Inform. 2022;18(4):2877–89. doi:10.1109/TII.2021.3110734.
6. Rekha R, Garg DR. Improved energy efficiency using meta-heuristic approach for energy harvesting enabled IoT network. Kuwait J Sci. 2023;50(2A):1–18.
7. Jabbar WA, Saad WK, Ismail M. MEQSA-OLSRv2: a multicriteria-based hybrid multipath protocol for energy-efficient and QoS-aware data routing in MANET-WSN convergence scenarios of IoT. IEEE Access. 2018;6:76546–72. doi:10.1109/ACCESS.2018.2882853.
8. Jaiswal K, Anand V. An optimal QoS-aware multipath routing protocol for IoT based wireless sensor networks. In: 2019 3rd International Conference on Electronics, Communication and Aerospace Technology (ICECA); 2019 Jun 12–14; Coimbatore, India. p. 857–60.
9. Dhumane A, Prasad R, Prasad J. Routing issues in Internet of Things: a survey. In: Proceedings of the International MultiConference of Engineers and Computer Scientists 2016; 16–18 Mar. 2016; Hong Kong. Vol. I, IMECS2016.
10. Ilyas M, Ullah Z, Khan FA, Chaudary MH, Malik MSA, Zaheer Z, et al. Trust-based energy-efficient routing protocol for Internet of Things-based sensor networks. Int J Distrib Sens Netw. 2020;16(10):155014772096435. doi:10.1177/1550147720964358.
11. Liu Y, Kuang Y, Xiao Y, Xu G. SDN-based data transfer security for Internet of Things. IEEE Internet Things J. 2018;5(1):257–68. doi:10.1109/JIOT.2017.2779180.
12. Walters JP, Liang Z, Shi W, Chaudhary V. Wireless sensor network security: a survey. In: Security in distributed, grid, mobile, and pervasive computing. Boca Raton, FL, USA: Auerbach Publications; 2007. p. 367–409.
13. Carlos-Mancilla M, López-Mellado E, Siller M. Wireless sensor networks formation: approaches and techniques. J Sens. 2016;2016:1–18. doi:10.1155/2016/2081902.
14. Mick T, Tourani R, Misra S. LASeR: lightweight authentication and secured routing for NDN IoT in smart cities. IEEE Internet Things J. 2018;5(2):755–64. doi:10.1109/JIOT.2017.2725238.
15. Su Z, Feng W, Tang J, Chen Z, Fu Y, Zhao N, et al. Energy-efficiency optimization for D2D communications underlaying UAV-assisted industrial IoT networks with SWIPT. IEEE Internet Things J. 2023;10(3):1990–2002. doi:10.1109/JIOT.2022.3142026.
16. Singh G, Joshi P, Raghuvanshi AS. A novel duty cycle based cross layer model for energy efficient routing in IWSN based IoT application. KSII Trans Internet Inf Syst. 2022;16(6):1849–76.

17. Miorandi D, Sicari S, De Pellegrini F, Chlamtac I. Internet of Things: vision, applications and research challenges. Ad Hoc Netw. 2012;10(7):1497–516. doi:10.1016/j.adhoc.2012.02.016.
18. Ramu N, Pandi V, Lazarus JD, Radhakrishnan S. A novel trust model for secure group communication in distributed computing. J Organ End User Comput. 2020;32(3):1–14. doi:10.4018/JOEUC.
19. Sathish Kumar L, Ahmad S, Routray S, Prabu AV, Alharbi A, Alouffi B, et al. Modern energy optimization approach for efficient data communication in IoT-based wireless sensor networks. Wirel Commun Mob Comput. 2022;2022(4):7901587–13. doi:10.1155/2022/7901587.
20. Pedditi RB, Debasis K. MACR: a novel meta-heuristic approach to optimize clustering and routing in IoT-based WSN. Int J Intell Syst Appl Eng. 2023;12(1):346–59.
21. Daniel A, Balamurugan KM, Vijay R, Arjun KP. Energy aware clustering with multihop routing algorithm for wireless sensor networks. Intell Autom Soft Comput. 2021;29(1):233–46. doi:10.32604/iasc.2021.016405.
22. Sanjay Gandhi G, Vikas K, Ratnam V, Suresh Babu K. Grid clustering and fuzzy reinforcement-learning based energy-efficient data aggregation scheme for distributed WSN. IET Commun. 2020;14(16):2840–8. doi:10.1049/iet-com.2019.1005.
23. Ramesh A, Kamali K. Energy efficiency and network lifetime optimization with adaptive power control for IoT networks. J Electr Syst. 2024;20(3):3033–40.
24. Nadif S, Sabir E, Haqiq A. A mean-field framework for energy-efficient power control in massive IoT environments. In: 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC); 2019 Sep 8–11; Istanbul, Turkey. p. 1–6.
25. Rehman AU, Ahmad Z, Jehangiri AI, Ala'Anzy MA, Othman M, Umar AI, et al. Dynamic energy efficient resource allocation strategy for load balancing in fog environment. IEEE Access. 2020;8:199829–39. doi:10.1109/ACCESS.2020.3035181.
26. Yang Y, Zhao S, Zhang W, Chen Y, Luo X, Wang J. DEBTS: delay energy balanced task scheduling in homogeneous fog networks. IEEE Internet Things J. 2018;5(3):2094–106. doi:10.1109/JIOT.2018.2823000.
27. Shuaib M, Bhatia S, Alam S, Masih RK, Alqahtani N, Basheer S, et al. An optimized, dynamic, and efficient load-balancing framework for resource management in the Internet of Things (IoT) environment. Electronics. 2023;12(5):1104. doi:10.3390/electronics12051104.
28. Aqeel I, Khormi IM, Khan SB, Shuaib M, Almusharraf A, Alam S, et al. Load balancing using artificial intelligence for cloud-enabled Internet of everything in healthcare domain. Sensors. 2023;23(11):5349. doi:10.3390/s23115349.
29. Chen M, Liu A, Xiong NN, Song H, Leung VCM. SGPL: an intelligent game-based secure collaborative communication scheme for metaverse over 5G and beyond networks. IEEE J Select Areas Commun. 2024;42(3):767–82. doi:10.1109/JSAC.2023.3345403.
30. Xiao W, Hao Y, Liang J, Hu L, AlQahtani SA, Chen M. Adaptive compression offloading and resource allocation for edge vision computing. IEEE Trans Cogn Commun Netw. 2024;10(6):2357–69. doi:10.1109/TCCN.2024.3400820.
31. Jiang W. Graph-based deep learning for communication networks: a survey. Comput Commun. 2022;185(1):40–54. doi:10.1016/j.comcom.2021.12.015.
32. Jiang W, Han H, Zhang Y, Wang JA, He M, Gu W, et al. Graph neural networks for routing optimization: challenges and opportunities. Sustainability. 2024;16(21):9239. doi:10.3390/su16219239.
33. Faramarzi A, Heidarinejad M, Mirjalili S, Gandomi AH. Marine predators algorithm: a nature-inspired meta-heuristic. Expert Syst Appl. 2020;152(4):113377. doi:10.1016/j.eswa.2020.113377.