Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.047875

ARTICLE

Secrecy Outage Probability Minimization in Wireless-Powered Communications Using an Improved Biogeography-Based Optimization-Inspired Recurrent Neural Network

Mohammad Mehdi Sharifi Nevisi[1], Elnaz Bashir[2], Diego Martín[3,*], Seyedkian Rezvanjou[4], Farzaneh Shoushtari[5] and Ehsan Ghafourian[2]

[1]Department of Industrial Engineering, Iran University of Science and Technology, Narmak, Tehran, 16846-13114, Iran

[2]Department of Computer Science, Iowa State University, Ames, Iowa, IA, 50011, USA

[3]ETSI de Telecomunicación, Universidad Politécnica de Madrid, Madrid, 28040, Spain

[4]Department of Engineering, California State University East Bay, Hayward, California, 94542, USA

[5]Department of Industrial Engineering, Bu-Ali Sina University, Hamedan, 65178-38695, Iran

*Corresponding Author: Diego Martín. Email: diego.martin.de.andres@upm.es

Received: 20 November 2023 Accepted: 28 January 2024 Published: 26 March 2024

ABSTRACT

This paper focuses on wireless-powered communication systems, which are increasingly relevant in the Internet of Things (IoT) due to their ability to extend the operational lifetime of devices with limited energy. The main contribution of the paper is a novel approach to minimize the secrecy outage probability (SOP) in these systems. Minimizing SOP is crucial for maintaining the confidentiality and integrity of data, especially in situations where the transmission of sensitive data is critical. Our proposed method harnesses the power of an improved biogeography-based optimization (IBBO) to effectively train a recurrent neural network (RNN). The proposed IBBO introduces an innovative migration model. The core advantage of IBBO lies in its adeptness at maintaining equilibrium between exploration and exploitation. This is accomplished by integrating tactics such as advancing towards a random habitat, adopting the crossover operator from genetic algorithms (GA), and utilizing the global best (Gbest) operator from particle swarm optimization (PSO) into the IBBO framework. The IBBO demonstrates its efficacy by enabling the RNN to optimize the system parameters, resulting in significant outage probability reduction. Through comprehensive simulations, we showcase the superiority of the IBBO-RNN over existing approaches, highlighting its capability to achieve remarkable gains in SOP minimization. This paper compares nine methods for predicting outage probability in wireless-powered communications. The IBBO-RNN achieved the highest accuracy rate of 98.92%, showing a significant performance improvement. In contrast, the standard RNN recorded lower accuracy rates of 91.27%. The IBBO-RNN maintains lower SOP values across the entire signal-to-noise ratio (SNR) spectrum tested, suggesting that the method is highly effective at optimizing system parameters for improved secrecy even at lower SNRs.

KEYWORDS

Wireless-powered communications; secrecy outage probability; improved biogeography-based optimization; recurrent neural network

1 Introduction

Wireless-powered communication (WPC), a transformative paradigm in wireless communications, encompasses technologies such as wireless power transfer (WPT) and simultaneous wireless information and power transfer (SWIPT) [1]. WPT enables the wireless transmission of electrical power from a source to electronic devices, removing the need for physical connectors. Notable applications include wireless charging for mobile devices, biomedical implants such as pacemakers, and self-sustained sensor networks for environmental monitoring. SWIPT, on the other hand, combines power transfer with data transmission [2]. It empowers devices to recharge while simultaneously receiving data, opening doors for applications like solar-powered sensor networks, enhanced IoT devices in remote areas, and energy-harvesting communications for scenarios where traditional power sources are impractical. These innovations promise to revolutionize the Internet of Things (IoT) by increasing device autonomy and addressing some of the most pressing challenges in wireless communications [3–5].

While the concept of WPC opens the door to a vast array of opportunities, it is not devoid of challenges. A comprehensive understanding of these challenges is vital to harness the full potential of this paradigm [6]. These challenges include optimizing energy harvesting efficiency, improving data transmission rates, and ensuring system reliability under dynamic environmental conditions. In this context, security stands as a paramount concern. With the rapid adoption of WPC technologies, safeguarding the confidentiality and integrity of data transmission becomes imperative. This is precisely where the concept of secrecy outage probability (SOP) comes into play. SOP is a fundamental metric that quantifies the vulnerability of communication links to information leakage. It assesses the likelihood that the secrecy capacity of a wireless-powered communication system falls below a certain threshold, rendering it susceptible to security breaches [6–10]. The significance of minimizing SOP cannot be emphasized enough, as it is intricately linked to data security levels, particularly in situations where the transmission of sensitive information is a central concern. Attaining the utmost reduction in SOP plays a vital role in upholding the highest standards of data privacy and network robustness [11–15]. SOP minimization embodies a critical optimization problem. It demands the orchestration of numerous system parameters, such as the allocation of energy resources, the determination of transmission power, and the management of signal-to-noise ratios. This problem's intricacy is accentuated by the dynamic and often unpredictable nature of wireless channels, leading to variations in communication quality and potentially disruptive interferences. Achieving the lowest possible SOP is not solely a matter of security but a multifaceted challenge that involves the continuous balancing act of optimizing security while preserving operational efficiency [16–20].

1.1 Related Works

Wireless-powered communication networks have garnered significant attention due to their potential to enhance energy efficiency and extend network lifetime. One critical aspect of such networks is ensuring the security and confidentiality of communication, particularly in the presence of eavesdroppers. This section provides an overview of recent research related to secrecy outage probability minimization in wireless-powered communications. In their work, Cao et al. [1] introduced a joint artificial noise and power allocation (JAP) scheme for ensuring reliability and security in wireless-powered non-orthogonal multiple access (NOMA) systems. The study presents closed-form expressions for connection outage probability (COP), SOP, and effective secrecy throughput (EST). The proposed JAP scheme was found to outperform benchmark schemes, making it a notable contribution in the field of wireless-powered secure communications. Lee et al. [2] addressed secrecy

outage minimization in wireless-powered relay networks with destination-assisted cooperative jamming. Their work introduced power splitting-based relaying (PSR) and time switching-based relaying (TSR) protocols to control energy harvesting and minimize secrecy outages. The results demonstrated that these protocols could achieve near-optimal secrecy outage performance, even without precise knowledge of eavesdropper locations, under high signal-to-noise ratio (SNR) conditions. Chen et al. [3] focused on the secrecy communication of a wirelessly powered network, proposing protocols that combine maximum ratio transmission with zero-forcing (ZF) jamming to enhance physical layer security. They provided closed-form expressions for connection and secrecy outage probabilities, along with optimal time-switching ratio and power allocation for secrecy throughput maximization in high SNR regimes. Their proposed schemes effectively improved security in wireless-powered networks. Moon et al. [4] considered a wireless-powered communication network with an energy harvesting (EH) jammer, addressing secrecy performance optimization. Their work involved the transmission of energy signals and information in separate phases, effectively thwarting eavesdropping attempts. The research provided insights into maximizing secrecy rates under various channel state information scenarios, emphasizing the advantage of optimal power allocation for security in EH systems. Li et al. [5] explored the performance of friendly jammer selection-aided multiuser scheduling for wireless networks. They proposed random jammer selection-aided multiuser scheduling (RJS-MUS) and optimal jammer selection-aided multiuser scheduling (OJS-MUS) schemes, analyzing their impact on secrecy outage probability. Their research demonstrated that, under specific SNR conditions, the proposed schemes outperformed conventional non-jammer selection-aided multiuser scheduling (NJS-MUS), highlighting the potential of power allocation strategies to enhance security. Yan et al. [6] investigated transmit antenna selection in a multiple-input-multiple-output (MIMO) energy-harvesting system. Their work introduced optimal antenna selection (OAS) and suboptimal antenna selection (SAS) schemes, examining the secrecy performance of these schemes under various channel state information scenarios. Notably, their results showed that full knowledge of CSI led to better secrecy performance, emphasizing the importance of CSI in achieving security in MIMO systems.

Jiang et al. [7] contributed to the field by studying secrecy performance in wirelessly powered wiretap channels. Their work involved exploring multi-antenna transmission schemes and deriving closed-form expressions for achievable secrecy outage probability and average secrecy rate. It emphasized the role of channel state information in achieving substantial secrecy diversity gain, furthering our understanding of security in wireless-powered networks. Zen et al. [8] explored wirelessly powered backscatter communications in the context of smart sustainable cities. Their work addressed the secrecy performance of WP-BackComs using a stochastic geometry framework. They considered factors such as imperfect successive interference cancellation, non-linear energy harvesting, and energy-causality constraints in the analysis. The results emphasized the importance of optimizing reflection coefficients to minimize SOP and the potential benefits of optimal strategies in WP-BackComs. Xu et al. [9] studied resource allocation for secure communications in cooperative cognitive wireless-powered communication networks. Their research proposed a cooperative protocol for secondary users, focusing on maximization of the secondary user's ergodic rate while ensuring primary user security. Their algorithms considered perfect and imperfect channel state information and addressed both collusive and non-collusive eavesdroppers, highlighting the significance of secure resource allocation in cognitive wireless-powered networks. Tang et al. [10] addressed secrecy outage probability in wireless-powered cognitive radio networks. Their work focused on secure information transmission for secondary systems sharing the spectrum with primary networks and considered the presence of eavesdroppers. The closed-form analytical expressions revealed the trade-offs between primary outage

probability, secondary secrecy outage probability, and the probability of non-zero secrecy capacity. Their research also discussed optimal time-switching and power-splitting strategies to maximize secondary secrecy outage probability under primary constraints, highlighting the importance of securing cognitive radio networks. The work by Lee et al. [11] delved into deep-learning-assisted wireless-powered secure communications with imperfect channel state information. They aimed to find robust transmit power control strategies to maximize secrecy rates while accounting for imperfect channel state information (CSI). Their research included iterative methods and a deep learning (DL)-assisted approach to tackle the no convexity of the problem, demonstrating the robustness of DL-assisted strategies against channel errors. Liu et al. [12] proposed a tag selection scheme to enhance security in passive backscatter communication systems with multiple tags and eavesdroppers. They analyzed SOP while considering a non-linear energy harvesting model. Their research introduced dynamic reflection coefficient optimization and tag selection to maximize the instantaneous secrecy capacity.

Moon et al.'s research [13] delved into the intricacies of enhancing security in wireless-powered communication networks by introducing an energy harvesting (EH) jammer, where an eavesdropper seeks to intercept communication between a user and a hybrid access point (H-AP). Their study presents a novel approach to this challenge, dividing the communication process into two key phases: energy transfer (ET) and information transfer (IT). During the ET phase, the H-AP transmits an energy signal to replenish the batteries of both the EH user and the EH jammer. In the subsequent IT phase, the user sends its information signal to the H-AP, while the EH jammer leverages the harvested energy to generate jamming signals aimed at interfering with the eavesdropper. This innovative approach assumes only knowledge of the channel distribution information (CDI) of the eavesdropper, and it focuses on minimizing the secrecy outage probability through an optimized time allocation between the two phases. To manage complexity, Moon et al. offered a simplified closed-form solution, demonstrating through simulations that their method closely approaches the optimum performance. Their research provides insights into secure wireless-powered communication networks, particularly in scenarios with energy-harvesting jammers and partial channel information. Chen et al. [18] researched a unique hierarchical game model for enhancing physical layer security (PLS) through dynamic three-party collaborations. This system focuses on legitimate users (LUs) who strive to securely send confidential data to their respective base stations (BSs) via uplink channels, contending with potential eavesdroppers (EVs). Additionally, jammers (JAs) exist, which can opt to align with either LUs to boost their secure data transmission or with EVs to enhance eavesdropping capabilities, in return for possible rewards. They introduced a deep reinforcement learning (DRL) strategy for achieving equilibrium with long-term performance assurances in this hierarchical game. Through simulations, they demonstrated the effectiveness of their method, highlighting its advantages over similar approaches.

1.2 Paper Motivations and Contributions

The challenges involved in SOP minimization span the realms of both cyber security and system optimization. It requires the development of efficient algorithms [21–25]. That can adapt to evolving network conditions, effectively allocate power and resources, and dynamically adjust to potential security threats [5–8]. Furthermore, the integration of machine learning (ML) techniques introduces a new layer of complexity, but also the potential for groundbreaking advancements [26–28]. In the literature of wireless-powered communication, there have been notable efforts aimed at minimizing SOP as we investigated in Subsection 1.1. However, it is evident that while significant progress has been made, particularly in enhancing security against eavesdroppers, most existing research tends to focus on scenarios with specific conditions, such as high or perfect CSI. These studies often

present strategies optimized for idealized conditions and may not fully encapsulate the challenges encountered in more variable and realistic wireless network environments. Additionally, many of these approaches concentrate on theoretical models and may not sufficiently address the practical challenges of deployment in real-world scenarios. Moreover, proposing an efficient optimization scheme to tackle this challenge has proven to be a formidable task. The primary motivation of this work lies in advancing the state-of-the-art in wireless-powered communications. By minimizing SOP and, in turn, enhancing the secrecy performance, this paper not only contributes to the evolution of wireless-powered communication but also exemplifies the potential of combining nature-inspired optimization methods with advanced ML methods to address complex communication challenges [3–5]. ML techniques are now extensively and effectively utilized across various sectors [29–31]. Specifically, recurrent neural networks (RNNs) are increasingly used to reduce outage probabilities in wireless-powered communication, offering a smart solution to key challenges in today's wireless networks [25]. Their role is crucial for improving the dependability and effectiveness of these systems, particularly in managing the fluctuating and hard-to-predict nature of wireless channels. RNNs become essential in such scenarios because wireless communication faces various uncertainties like constantly changing channel conditions, variable energy harvesting rates, and unpredictable movements of users. They excel in fine-tuning power distribution and managing resources to lower the chances of outages, thereby boosting system reliability. Consequently, RNNs play a pivotal role in enhancing the performance of wireless-powered communication systems by continuously fine-tuning energy and resource allocation [26].

While DL algorithms can play a crucial role in reducing SOP, the primary difficulty is in adjusting the DL's hyper-parameters. Currently, meta-heuristic algorithms are used for fine-tuning network parameters. Training RNNs poses significant challenges, particularly with traditional gradient-based techniques, which often encounter limitations such as getting trapped in local minima and struggling with non-differentiable objectives [32–34]. These issues highlight the need for alternative optimization strategies to enhance RNN training. Biogeography-based optimization (BBO) emerges as a promising approach, illustrating the effectiveness of meta-heuristic methods in addressing these challenges. BBO offers a unique way of balancing exploration and exploitation, potentially avoiding local minima and improving training results. However, standard BBO has its drawbacks, including a propensity to get stuck in local optima and inefficient exploration of the search space, leading to suboptimal outcomes [35]. Improving BBO could lead to more powerful and versatile optimization algorithms, better equipped to address the complex problems encountered in real-world optimization scenarios. In light of these challenges and the pressing need for heightened security, this paper introduces a novel approach aimed at the minimization of SOP in wireless-powered communications. Our proposed method harnesses the power of an improved BBO (IBBO) to effectively train an RNN. This unique synergy between the IBBO and the RNN's capacity for learning complex relationships within wireless-powered communication scenarios promises to enhance system performance significantly. The main contributions of this paper can be summarized as follows:

- Our work introduces a novel approach to address the pressing challenge of minimizing SOP in the context of WPC. SOP, a pivotal metric, quantifies the vulnerability of communication links to information leakage, and our scheme offers a fresh perspective on how to effectively reduce it.
- In the proposed approach, this paper introduces an innovative IBBO algorithm, tailored to boost the weights and biases in RNN models (named IBBO-RNN). The proposed IBBO introduces an innovative migration model, detailed in Eqs. (11)–(13). This new approach aims to create a more intelligent migration structure, thus hastening the algorithm's progression towards

the optimal solution. The core advantage of IBBO lies in its adeptness at maintaining equilibrium between exploration and exploitation. This is accomplished by integrating tactics such as advancing towards a random habitat, adopting the crossover operator from genetic algorithms (GA), and utilizing the global best (Gbest) operator from particle swarm optimization (PSO) into the IBBO framework.

- The performance of the proposed IBBO-RNN is compared against eight ML models, namely capuchin search algorithm (CapSA), chimp optimization algorithm (ChOA), linear BBO, logarithmic BBO, backpropagation RNN (BP-RNN), long short-term memory (LSTM), support vector machine (SVM), and k-nearest neighbors (KNN).
- To validate our contributions, we conduct comprehensive simulations. The results unequivocally illustrate the effectiveness of our approach. By significantly reducing SOP, our method not only advances the state-of-the-art in WPC but also exemplifies the potential of integrating nature-inspired optimization techniques with advanced neural networks. This synergy addresses intricate communication challenges, ensuring higher data confidentiality and network integrity.

1.3 Paper Organization

The structure of the paper is organized as follows: Section 2 delves into the research model, encompassing the system model, SOP problem formulation, the proposed IBBO, and the evolutionary RNN. Section 3 presents the experimental findings and discussions, providing crucial insights. The paper concludes in Section 4 with a summary of the key contributions and the broader implications of the research.

2 Research Model and Methodology

This section explores the research model, which includes the system model, the formulation of the SOP problem, the proposed IBBO approach, and the evolutionary RNN.

2.1 System Model

The considered system model, as illustrated in Fig. 1, consists of a wireless-powered communication network. Within this setup, a legitimate user we refer to as Alice receives her power wirelessly from a distant power beacon (PB). The objective for Alice is to securely send a private message to Bob, another authorized receiver, across a wireless channel subject to fading. Concurrently, an eavesdropper, whom we call Eve, is attempting to capture and decipher the message from the signals that reach her.

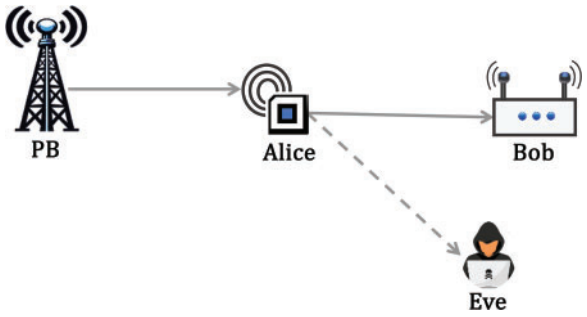

Figure 1: System model depicting the secure wireless power communication

For ease of analysis while maintaining the system's generality, it is assumed that each node in the network is equipped with only one antenna. Consequently, the power that Alice receives at any specific instant can be quantified by the Eq. (1):

$$P_R = P_T L_T d_T^{\alpha} g_T \tag{1}$$

Here, P_T represents the power transmitted by the power beacon (PB), L_T combines the effects of antenna gains and frequency-dependent propagation losses, d_T is the distance between the power beacon and Alice, $\alpha > 2$ is the path-loss exponent, and $g_T = |\mathrm{h_T}|^2$ signifies the normalized fading power channel coefficient between the power beacon and Alice, where $E[g_T] = 1$ (indicating an average value of 1). With these assumptions, the instantaneous SNR at user K, where K can be either Bob (B) or Eve (E), can be defined as Eq. (2):

$$\gamma_K = \frac{P_T L_T}{\sigma_K^2 d_T^{\alpha} d_K^{\alpha}} |h_T|^2 |h_K|^2 = \overline{\gamma}_K g_T g_K \tag{2}$$

Here, σ_K^2 represents the noise power at Bon/Eve, $\overline{\gamma}_K$ is the average SNR, and $g_K = |h_K|^2$ is the corresponding fading coefficient with an average value of 1. Furthermore, we assume that all channels in the system are quasi-static fading channels, meaning they remain constant during the transmission of an entire code word and change randomly from one transmission block to another. These channels are modeled using the independent Rayleigh distribution. The goal of this paper is to minimize the SOP, which is the probability that the instantaneous secrecy capacity falls below a threshold target secrecy rate; R_S. The secrecy capacity C_S is given by the difference between the capacities of the main channel (Alice to Bob) and the eavesdropper's channel (Alice to Eve):

$$C_S = [C_B - C_E]^+ \tag{3}$$

where $C_B = \log_2(1 + \gamma_B)$ and $C_E = \log_2(1 + \gamma_E)$, and $[X]^+$ denotes the positive part of X as $max\{C_B - C_E, 0\}$. Therefore, the SOP can be given by Eq. (4):

$$P_{SOP} = Pr\,(C_S \leq R_S) \tag{4}$$

Using the definition of C_S, we can deduce a mathematical representation for SOP:

$$P_{SOP} = Pr\left(\log_2 \frac{1 + \gamma_B}{1 + \gamma_E} \leq R_S\right) \tag{5}$$

Thus, according to Eq. (2), the cost function can be formulated as Eq. (6):

$$f(P_T, L_T, d_T, \alpha, \sigma_B^2, \sigma_E^2, d_B, d_E, h_T, h_B, h_E) = Pr\left(\log_2 \frac{1 + \gamma_B}{1 + \gamma_E} \leq R_S\right) \tag{6}$$

Under the following constraints:

$$0 \leq P_T \leq P_{max}$$

$\alpha > 2$ is a constant value.

h_T, h_B, and h_E follow independent Rayleigh distributions with the mean value of a_T, a_B, and a_E, respectively.

2.2 Standard BBO

The BBO algorithm, introduced by Dan Simon in 2008, is inspired by biogeography, a field that examines species distribution and their migration and adaptation processes in different geographic areas [35]. BBO utilizes the concepts of immigration, emigration, and speciation from biogeography to find optimal solutions in multi-objective optimization problems. In BBO, potential solutions are conceptualized as "habitats," each with a habitat suitability index (HSI) indicating its fitness. The algorithm operates through migration, mutation, and elitism. Habitats with higher fitness values are more likely to share their features with others, facilitating the spread of advantageous features. Conversely, habitats with lower fitness levels are prone to receiving features from others, potentially enhancing their quality. The emigration rate of a habitat depends on its fitness relative to the population's average fitness, with higher fitness habitats having higher emigration rates. Similarly, the likelihood of a habitat receiving immigrants correlates with the emigration rates of other habitats. The mathematical foundation of linear BBO is encapsulated in Eqs. (7), (8) that detail its operational mechanisms [35].

$$\mu_j\,(\mathrm{k}) = E \times \left(\frac{\mathrm{k\,(j)}}{N}\right) \tag{7}$$

$$\lambda_j\,(\mathrm{k}) = I \times \left(1 - \frac{\mathrm{k\,(j)}}{N}\right) \tag{8}$$

where $\mu_{k(j)}$ signifies the emigration rate, $\lambda_{k(j)}$ denotes the immigration rate, k_j refers to the species' rank, N represents the total population size, E and I are the maximum rates of emigration and immigration, respectively. Within BBO, the information exchange between habitats is facilitated probabilistically through the emigration and immigration rates of each solution [35]. The migration process in standard BBO is described by Eq. (9):

$$H_j\,(\mathrm{SIVs}) \leftarrow H_j\,(\mathrm{SIVs}) + H_i\,(\mathrm{SIVs}) \tag{9}$$

where H_j is the host habitat and H_i is the guest habitat. According to the Eq. (9), the host habitat receives information from the guest habitat and itself. Also, the mutation operator defines as Eq. (10):

$$m_j = m_{\max} \times \left(1 - \frac{p_j}{p_{\max}}\right) \tag{10}$$

where m_{max} is chosen by user, p_j reveals the probability of species count and p_{max} is the highest value of p_j.

2.3 Improved BBO

The linear BBO algorithm, like other optimization methods, faces several challenges that affect its applicability and efficiency. Its performance is sensitive to the precise tuning of various parameters, such as migration and immigration rates, which need careful adjustment for different problem domains. This sensitivity can make BBO challenging to apply broadly without specific tuning. Additionally, BBO tends to converge slowly, particularly in complex and high-dimensional problems, often requiring numerous iterations due to its probabilistic migration and immigration rules. The algorithm also struggles with effectively exploring the entire search space, especially in rugged, multi-modal landscapes, as it tends to focus on regions with higher fitness values, potentially overlooking other viable areas. Scalability is another issue, particularly with very high-dimensional problems or those with numerous constraints, as maintaining and updating habitat populations can be computationally

intensive. Furthermore, like many evolutionary algorithms, BBO faces difficulties in striking the right balance between exploration and exploitation, a critical aspect of its overall effectiveness [35].

To address these limitations, researchers have proposed various enhancements and modifications, such as hybridizing BBO with other techniques, introducing diversity-preserving mechanisms, or addressing parameter tuning issues. Recent research, particularly studies on Markov theory-based models, has explored the impact of different migration models on BBO's efficiency. Various models like linear BBO, quadratic BBO, sinusoidal BBO, generalized sinusoidal BBO, and exponential-logarithmic BBO have been introduced. The paper under discussion introduces a novel migration model for BBO, described in Eqs. (11)–(13), which proposes unique migration rates for each habitat. This new approach aims to create a smarter migration structure to accelerate convergence to the best solution, differing from previous models that used a single function for migration rates and treated all habitats uniformly.

$$\begin{cases} \mu_{k(j)} = \dfrac{2E}{3} \times \left(-cos\left(\dfrac{k\,(j)\,\pi}{N} \right) + 1 \right) \\ \lambda_{k(j)} = \dfrac{2I}{3} \times \left(cos\left(\dfrac{k\,(j)\,\pi}{N} \right) + 1 \right) \end{cases} \quad k(j) < \frac{N}{5} \tag{11}$$

$$\begin{cases} \mu_{k(j)} = \dfrac{E}{2} \times Ln\left(\dfrac{k\,(j)}{N} + 1 \right) \\ \lambda_{k(j)} = \dfrac{I}{2} \times exp\left(-\dfrac{k\,(j)}{N} \right) \end{cases} \quad \frac{N}{5} \le k(j) \le \frac{2N}{5} \tag{12}$$

$$\begin{cases} \mu_{k(j)} = \dfrac{2E}{3} \times \left(tan\,h\left(\dfrac{k\,(j)\,\pi}{N} - \dfrac{2\pi}{7} \right) + 1 \right) \\ \lambda_{k(j)} = \dfrac{2I}{3} \times \left(-tan\,h\left(\dfrac{k\,(j)\,\pi}{N} - \dfrac{2\pi}{7} \right) + 1 \right) \end{cases} \quad k(j) > \frac{2N}{5} \tag{13}$$

Selecting the six specified mathematical functions for migration rates, the IBBO employs a range of functions suited to combining habitats with diverse HSI, which enhances its overall effectiveness. In this paper, the GA's crossover operator is employed to enhance the exploitation capabilities of the BBO. During the optimization process, in addition to the regular migration of BBO, the crossover operator can be applied to selected pairs of habitats. This operation allows for a more diversified exchange of features between habitats, potentially leading to more effective exploration and exploitation of the search space. It can help in overcoming local optima issues by providing a mechanism to escape and explore new areas of the solution space. Additionally, the mechanism of moving towards the Gbest from the PSO algorithm has been utilized to improve the performance of the BBO. This concept can be applied to BBO by allowing habitats to be influenced not just by their features but also by the best solutions found in their neighborhood. This mimics the way particles in PSO are influenced by their neighbors. By moving habitats towards the best experiences of their neighbors, the BBO algorithm can more effectively explore the solution space and exploit the best-known solutions. This approach encourages convergence towards optimal or near-optimal solutions by leveraging collective knowledge.

Fig. 2 presents an example of the operators in the IBBO. Moving towards a random habitat involves occasionally directing a habitat towards a completely random position in the solution space. Such random movements can prevent the algorithm from getting stuck in local optima. It introduces an element of randomness that helps to explore potentially unvisited regions of the search space. While the PSO-inspired mechanism focuses on exploiting known good solutions, the random habitat movement

ensures that the algorithm does not overly focus on certain areas, thus maintaining a balance between exploration and exploitation. The key to effective optimization is balancing exploration and exploitation. Integrating moving towards a random habitat, the crossover operator from GA, and global best (Gbest) operator from PSO into BBO can help in maintaining this balance, as it introduces a new layer of complexity and adaptability to the search process. By incorporating these techniques, the BBO algorithm becomes more adaptable and robust, capable of handling a wider range of optimization problems.

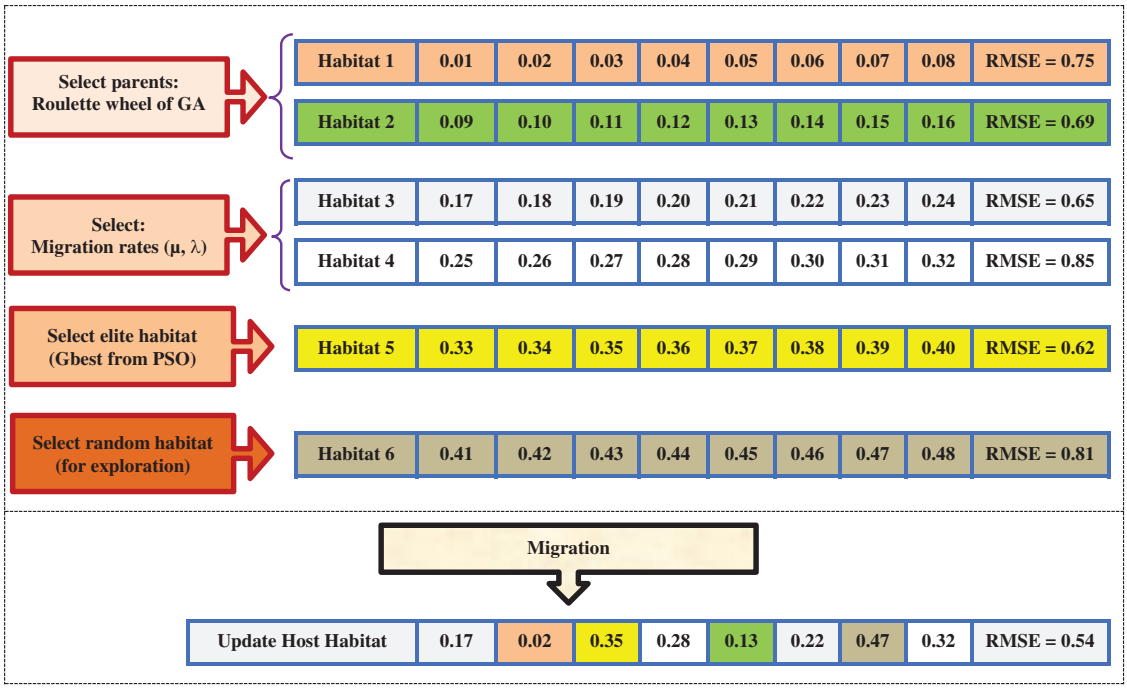

Figure 2: Illustration of IBBO operators utilized for weights and biases training

2.4 Evolutionary RNN

RNNs are a unique subset of artificial neural networks tailored for processing sequential data, setting them apart from traditional feed-forward neural networks. Their defining feature is a feedback loop that maintains a 'memory' of previous inputs, enabling the handling of variable input lengths and the integration of past information into current input processing [25]. Comprising multiple layers, including an input layer for sequence data, a recurrent layer that refeeds outputs into the network, and an output layer for final outcomes, RNNs utilize activation functions such as sigmoid, tanh, and ReLU to learn complex patterns. These networks are highly effective in tasks like language modeling, sentiment analysis, machine translation, text generation, and speech recognition, as well as in predicting time series data and, in combination with CNNs, generating images and videos [26].

However, RNNs encounter significant challenges, notably in capturing long-term dependencies and grappling with vanishing or exploding gradients during training. Their primary training method, gradient-based optimization techniques, has inherent limitations, including the risk of getting trapped in local optima, leading to less than optimal training outcomes. Moreover, these methods are computationally complex and time-consuming, especially in large networks or with long sequences, due to the

extensive computation of gradients across many layers and time steps. The vanishing gradient problem, where gradients become too small to effect meaningful learning, particularly hampers standard RNNs in handling long sequences and capturing long-term data dependencies. Conversely, the exploding gradient issue causes overly large updates to network weights, destabilizing training. These challenges collectively constrain the efficiency and applicability of RNNs in certain real-world applications.

Meta-heuristic algorithms [36–39], including BBO, are gaining recognition as effective tools for training the weights and biases of RNNs, offering several advantages over traditional gradient-based methods. One of their primary benefits is the ability to avoid getting trapped in local optima, a common issue with gradient-based techniques that follow the steepest descent. Meta-heuristics, in contrast, employ mechanisms to explore the search space more broadly and escape local minima, thus increasing the likelihood of identifying the global minimum. These algorithms are not dependent on the gradient of the error function, making them well-suited for optimizing functions that are non-differentiable, discontinuous, or highly nonlinear, which often poses challenges for gradient-based methods. This attribute is particularly beneficial in complex RNN architectures with a non-smooth error surface.

In this paper, the IBBO is utilized for training the RNN due to its ability to effectively balance exploration and exploitation. This equilibrium is key in training RNNs, as it allows the algorithm to investigate various weight and bias configurations without prematurely converging on a solution. The adaptive nature of the BBO, characterized by migration rates that change based on the quality of the habitats, enables the algorithm to modify its search strategy to suit the specific needs of the problem at hand. Such adaptability is particularly beneficial in training RNNs within dynamic environments, where data patterns may evolve over time. Fig. 3 shows the structure of the IBBO-RNN, and Fig. 4 shows the structure of a habitat in IBBO. Additionally, the cost function used in the IBBO is detailed in Eq. (14).

$$Mean\ Square\ Error(MSE) = \frac{1}{k}\sum_{i=1}^{k}(O_i - D_i)^2 \tag{14}$$

where k = the total number of samples, O_i = System output, D_i = Desire.

3 Results

This section evaluates the efficiency of the IBBO-RNN approach. Its performance are measured using eight well-known and advanced ML algorithms: CapSA, ChOA, linear BBO, logarithmic BBO, BP-RNN, LSTM, SVM, and KNN. The execution of various algorithms is carried out in the R Studio software environment. Detailed information regarding the calibration parameters linked to these algorithms can be found in Table 1. Calibrating meta-heuristic algorithm parameters is essential for optimal performance and requires meticulous attention. It involves determining the most effective parameter value combinations for efficient algorithm functioning. Before evaluating the algorithm's performance, it is vital to establish these optimal settings.

In this paper, we use a trial-and-error method for parameter calibration, systematically altering each parameter and observing the effects while maintaining all other variables constant. For example, in an algorithm with various parameters like learning rates, convergence thresholds, or population sizes, we individually test each to see how they influence the algorithm's behavior. A fitness function is used to evaluate the effectiveness of these parameter settings. This function provides a standard to assess the algorithm's performance with different parameter combinations. The possible range for each parameter is wide, but practical limitations necessitate selecting and presenting a manageable subset

of varied parameter instances. Table 1 displays this selection, offering a glimpse into the trial-and-error process by highlighting the parameter values that improved or reduced algorithm performance in certain cases.

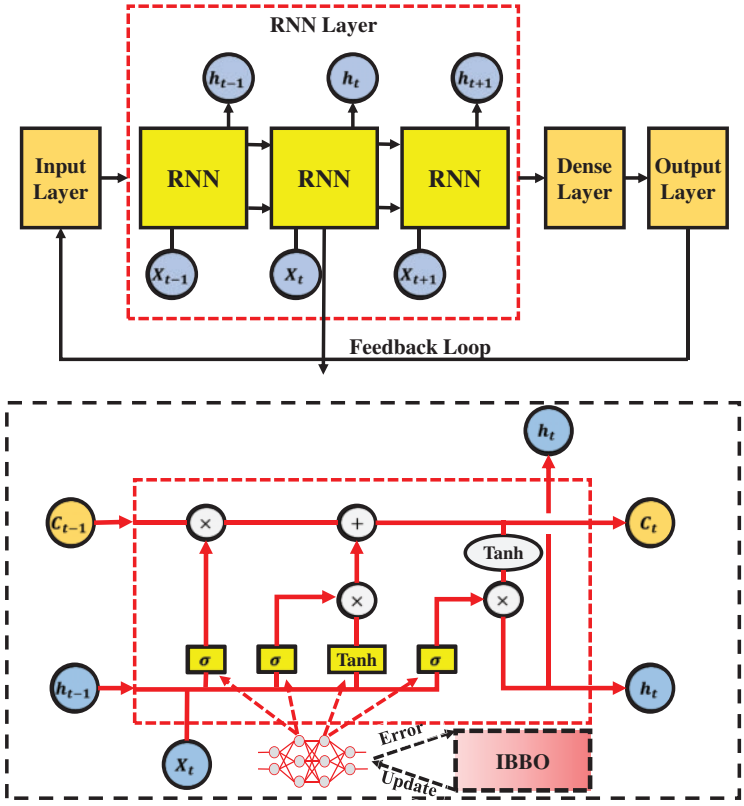

Figure 3: The structure of the proposed IBBO-RNN

Figure 4: The structure of a habitat in IBBO

Table 1: Parameter setting of algorithms through the trial and error method

Algorithm	Parameter	Value
IBBO and other BBO	The probability range for migrating into for each gene	[0, 1]
	Maximum emigration (I) and immigration (E) coefficient	1
	Elitism percent	11%
	Mutation rate	0.09
	Population size	120

(Continued)

Table 1 (continued)

Algorithm	Parameter	Value
	Iteration	300
CapSA	Velocity control constants	1.00
	Inertia parameter	0.65
	Balance and elasticity factors	0.72, 9
	Population size	120
	Iteration	300
ChOA	a	[−1, 1]
	f	Linearly decreased from 2 to 0
	Population size	120
	Iteration	300
RNN	Number of hidden layers	{10, 15, 20}
	Number of neurons in hidden layers	{50, 70, 100}
	Learning rate	0.08
	Dropout rate	0.2
	Activation	Tanh and sigmoid
	Optimizer	IBBO and SGD
LSTM	Number of hidden layers	{8, 10, 12}
	Number of neurons in hidden layers	{40, 70, 110}
	Learning rate	0.10
	Recurrent dropout Rate	0.3
	Activation	ReLU and Tanh
	Optimizer	Adam
SVM	C (regularization parameter)	10
	Kernel type	Linear
	Gamma	0.002
	Iteration	300
KNN	Number of neighbors (k)	7
	Distance metric	Euclidean distance
	Weights	Uniform
	Algorithm	Kd-tree
	Leaf size	30

Fig. 5 illustrates the performance of the SOP of the proposed scheme *vs.* the different values of the average SNR at Bob. In this figure, the SOP is inversely related to the SNR at Bob–as the SNR increases, the SOP decreases, indicating enhanced secrecy performance. The proposed IBBO-inspired RNN scheme demonstrates superior performance compared to other benchmark algorithms like KNN, SVM, and BP-based RNN. This can be observed from the steeper slope of the IBBO-based RNN curve, which indicates a faster reduction in SOP with increasing SNR. Notably, the IBBO-based RNN maintains lower SOP values across the entire SNR spectrum tested, suggesting that the method is highly effective at optimizing system parameters for improved secrecy even at lower SNRs.

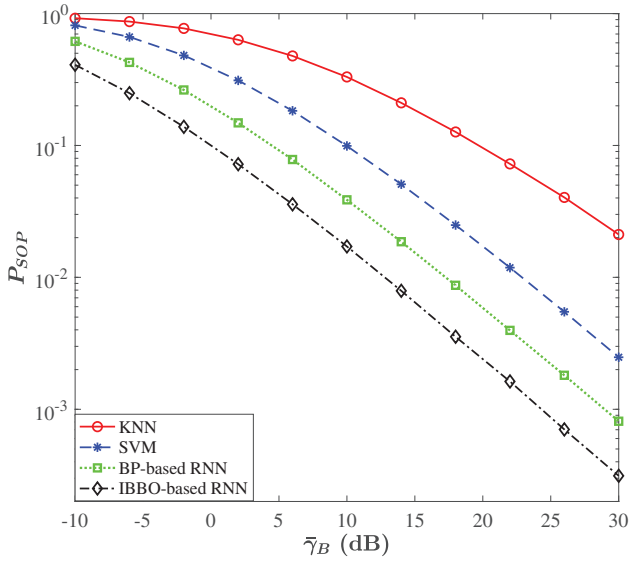

Figure 5: SOP performance of the proposed scheme *vs.* different average SNR at Bob

Fig. 6 presents the SOP performance against various values of R_S, which can be interpreted as the target secrecy rate or the rate of confidential information transmission. The SOP increases with higher R_S, which aligns with the expectation that higher data rates pose a greater challenge for maintaining secrecy due to increased vulnerability to interception. The IBBO-based RNN again outperforms the benchmark algorithms across all R_S values. However, the rate at which SOP increases with R_S is less steep for the IBBO-based RNN, indicating its robustness in maintaining secrecy even as demands on the system's secrecy capacity rise. This demonstrates the efficiency of the proposed method in managing energy harvesting and data transmission processes under various operational constraints.

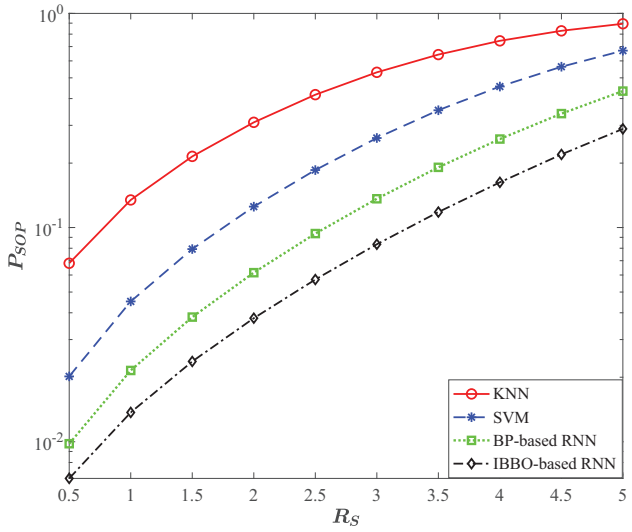

Figure 6: SOP performance of the proposed scheme for different values of R_S

The rest of this section evaluates the effectiveness of the IBBO-RNN and various other methods in reducing outage probability in wireless-powered communications. This assessment includes performing tests for sensitivity, accuracy, and specificity and utilizes Eqs. (15)–(17) for calculation.

$$Sensitivity = \frac{TP}{TP + FN} \tag{15}$$

$$Specificity = \frac{TN}{TN + FP} \tag{16}$$

$$Accuracy = \frac{TP + TN}{TP + FN + FP + TN} \tag{17}$$

where, TP = True positive, TN = True negative, FN = False negative, FP = False positive.

Table 2 presents the results from different algorithms designed for outage probability in wireless-powered communications. The table clearly demonstrates that the IBBO-RNN surpasses others in terms of sensitivity, specificity, and accuracy across training and validation sets. Specifically, the IBBO-RNN achieved accuracies of 98.92% and 99.45% in the testing and training datasets, respectively. Furthermore, it attained sensitivities of 99.14% and 99.65% in the test and train datasets, respectively. According to Table 2, the IBBO-RNN, CapSA-RNN, and ChOA-RNN algorithms recorded the top accuracy rates of 98.92%, 96.52%, and 95.62%, respectively, demonstrating a significantly improved capability in predicting outage probability in wireless-powered communications. In contrast, the BP-RNN, SVM, and KNN algorithms reported lower accuracy levels, with respective values of 91.27%, 88.81%, and 87.11%. The high sensitivity scores reflect superior algorithmic efficiency. The IBBO-RNN algorithm achieved the highest sensitivity of 99.14%, marking its exceptional performance over other models. On the other hand, the BP-RNN, SVM, and KNN algorithms showed lesser effectiveness.

Table 2: The results of architectures in the test and train datasets

Architectures	Training (%)			Validation (%)		
	Sensitivity	Specificity	Accuracy	Sensitivity	Specificity	Accuracy
IBBO-RNN	99.65	96.81	99.45	99.14	96.12	98.92
Linear BBO-RNN	95.32	92.47	94.02	94.68	92.09	93.29
Logarithmic BBO-RNN	95.96	93.27	94.71	95.17	92.58	94.05
CapSA-RNN	98.21	95.29	97.25	97.71	94.68	96.52
ChOA-RNN	97.26	94.53	96.24	96.85	94.03	95.62
BP-RNN	93.12	90.98	92.45	92.41	89.34	91.27
LSTM	93.49	91.15	92.86	92.85	89.69	91.74
SVM	90.18	87.75	89.66	89.49	86.65	88.81
KNN	89.63	86.05	88.77	88.29	85.91	87.11

Figs. 7 and 8 offer a graphical comparison among different architectural models. These models are ranked according to their performance, with the IBBO-RNN leading, followed by CapSA-RNN, ChOA-RNN, Logarithmic BBO-RNN, Linear BBO-RNN, LSTM, BP-RNN, SVM, and KNN.

The rankings reflect the effective training of these architectures using meta-heuristic algorithms, which have successfully maximized their operational efficiency. Additionally, the accuracy of these architectures is consistently high across various hybrid DL structures in both the testing and training datasets. This uniformity in performance indicates that the meta-heuristic algorithms incorporated into the training regimen have yielded reliable and consistent results across multiple models and datasets.

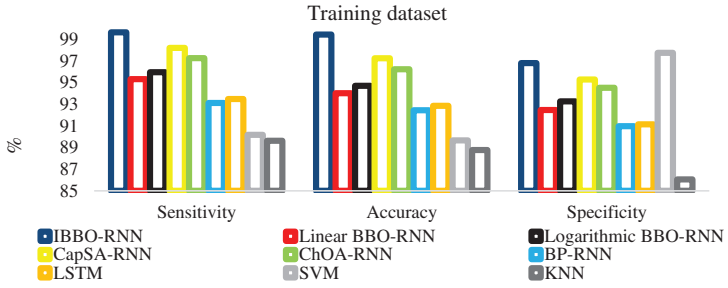

Figure 7: A visual representation showcasing the comparison of algorithms using training datasets

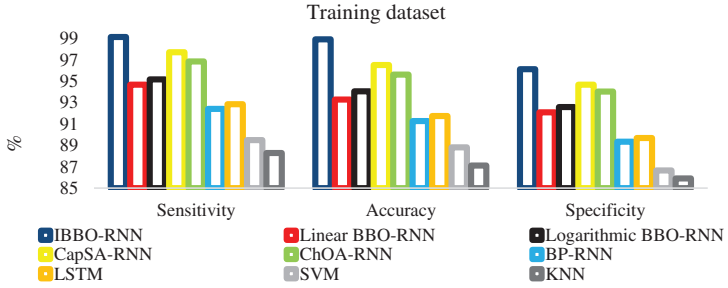

Figure 8: A visual representation showcasing the comparison of algorithms using validation datasets

Fig. 9 depicts a graphical comparison of the receiver operating characteristic (ROC) curves for different architectures. The ROC curve visually shows how well a binary classifier, like one that differentiates between two categories, performs as its discrimination threshold changes. It highlights the balance between the true positive rate (sensitivity) and the false positive rate (1-specificity) at various threshold levels. Sensitivity indicates the percentage of true positive cases accurately identified, whereas specificity denotes the percentage of true negative cases correctly classified. An analysis of the graph in Fig. 9 reveals that the area under the curve (AUC) for the IBBO-RNN surpasses that of the other architectures. The AUC is a measure of a classifier's overall effectiveness, reflecting the likelihood that a randomly selected positive instance is ranked above a randomly selected negative one. The greater AUC of the IBBO-RNN indicates its superior accuracy and discrimination capability relative to the others.

MSE criteria in Table 3 are utilized for evaluating the proposed models. Among these, the IBBO-RNN architecture shows a lower MSE compared to its counterparts, signifying the effectiveness of the proposed method in addressing the problem. The IBBO's key strength lies in its ability to balance exploration and exploitation. This balance is achieved by incorporating strategies such as moving towards a random habitat, integrating the crossover operator from GA, and employing the global best operator from PSO into the IBBO. The IBBO algorithm enhances the parameter optimization for the RNN, enabling it to more accurately represent and understand the patterns and relationships

in the data. Fig. 10 illustrates that the IBBO-RNN architecture converges faster than other models. At epoch 100, the IBBO-RNN nearly reaches the lowest MSE, while other models continue to show higher MSE values.

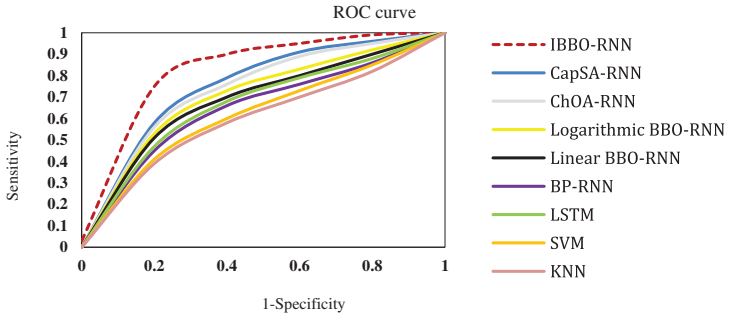

Figure 9: A visual comparison of the ROC curves for different architectures

Table 3: The MSE values of the different models

Architecture	MSE	
	Training datasets	Validation datasets
IBBO-RNN	0.00017	0.00082
Linear BBO-RNN	0.18965	0.32584
Logarithmic BBO-RNN	0.10563	0.25185
CapSA-RNN	0.00484	0.01941
ChOA-RNN	0.03974	0.04856
BP-RNN	0.54853	0.61056
LSTM	0.49652	0.58541
SVM	0.61423	0.89854
KNN	0.68452	0.94125

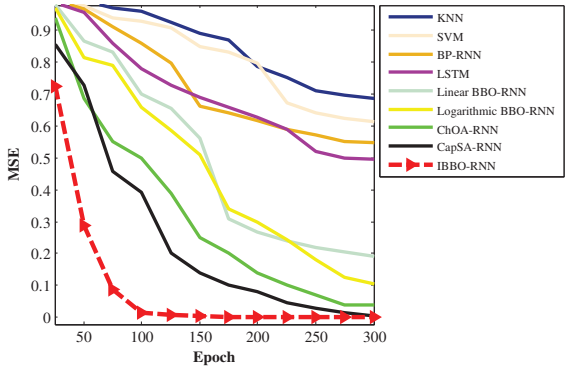

Figure 10: The convergence trend of architectures

4 Conclusion

This paper has presented a novel approach to addressing one of the key challenges in the field of wireless-powered communications, particularly within the context of the IoT: the minimization of SOP. Our work introduces an IBBO-inspired RNN, a method that blends the strengths of BBO with the capabilities of RNNs. The core of our approach is the innovative migration model within the IBBO, which adeptly balances exploration and exploitation through advanced techniques borrowed from GA and PSO. This balance is critical in optimizing the parameters of the RNN to reduce the SOP effectively. The IBBO-RNN achieved a remarkable accuracy rate of 98.92%, outperforming the BP-RNN and other algorithms, and demonstrated a lower MSE alongside a higher AUC. These metrics underscore not only the method's efficacy in SOP minimization but also its superiority over existing approaches. However, this research is not without its limitations and challenges. As with any advanced computational method, the complexity and computational requirements of the IBBO-RNN can be considerable. The effectiveness of RNNs heavily relies on extensive labeled data for training, which may not always be available. Furthermore, while our approach has shown excellent results in simulations, real-world deployment may present additional challenges, including varying environmental conditions and hardware limitations.

In conclusion, our work represents a significant advance in the field of wireless-powered communications, particularly in enhancing the security of IoT systems. It opens up new possibilities for the integration of nature-inspired optimization algorithms with DL architectures. For future work, we aim to refine the IBBO-RNN to be more computationally efficient and to test its robustness in real-world scenarios. Additionally, exploring the adaptability of our approach to other types of wireless communication challenges could further demonstrate its versatility and effectiveness. In our current paper, we focus on the innovative application and benefits of the IBBO-RNN. For future research, we plan to extend our comparisons to include deep reinforcement learning (DRL), federated transfer learning, and game theory-based methods. We believe such an expansion will significantly enhance the wireless communication field, especially in IoT and security contexts.

Acknowledgement: The work described in this paper has been developed within the Project PRESECREL. We would like to acknowledge the financial support of the Ministerio de Ciencia e Investigación (Spain), in relation to the Plan Estatal de Investigación Científica y Técnica y de Innovación 2017–2020.

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: M. M. Sharifi Nevisi, E. Bashir, S. Rezvanjou; data collection: M. M. Sharifi Nevisi, E. Ghafourian, F. Shoushtari; analysis and interpretation of results: E. Bashir, D. Martín, S. Rezvanjou, E. Ghafourian, F. Shoushtari; draft manuscript preparation: M. M. Sharifi Nevisi, E. Bashir, D. Martín. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

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

References

[1] K. Cao *et al.*, "Achieving reliable and secure communications in wireless-powered NOMA systems," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1978–1983, 2021. doi: 10.1109/TVT.2021.3053093.

[2] K. Lee, J. Bang, and H. H. Choi, "Secrecy outage minimization for wireless-powered relay networks with destination-assisted cooperative jamming," *IEEE Internet. Things.*, vol. 8, no. 3, pp. 1467–1476, 2020. doi: 10.1109/JIOT.2020.3013573.

[3] Z. Chen, L. Hadley, Z. Ding, and X. Dai, "Improving secrecy performance of a wirelessly powered network," *IEEE Trans. Commun.*, vol. 65, no. 11, pp. 4996–5008, 2017. doi: 10.1109/TCOMM.2017.2732449.

[4] J. Moon, H. Lee, C. Song, and I. Lee, "Secrecy performance optimization for wireless powered communication networks with an energy harvesting jammer," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 764–774, 2016. doi: 10.1109/TCOMM.2016.2623627.

[5] B. Li, Y. Zou, J. Zhou, F. Wang, W. Cao and Y. D. Yao, "Secrecy outage probability analysis of friendly jammer selection aided multiuser scheduling for wireless networks," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3482–3495, 2019. doi: 10.1109/TCOMM.2019.2894824.

[6] P. Yan, J. Yang, M. Liu, J. Sun, and G. Gui, "Secrecy outage analysis of transmit antenna selection assisted with wireless power beacon," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7473–7482, 2020. doi: 10.1109/TVT.2020.2992766.

[7] X. Jiang, C. Zhong, X. Chen, T. Q. Duong, A. T. Tsiftsis and Z. Zhang, "Secrecy performance of wirelessly powered wiretap channels," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3858–3871, 2016. doi: 10.1109/TCOMM.2016.2592529.

[8] J. Zan, L. Shi, G. Lu, and Y. Ye, "Wireless-powered backscatter communications for smart sustainable cities: A secrecy analysis," *Sustain. Energy Technol. Assess.*, vol. 56, pp. 103036, 2023. doi: 10.1016/j.seta.2023.103036.

[9] D. Xu and Q. Li, "Resource allocation for secure communications in cooperative cognitive wireless powered communication networks," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2431–2442, 2018. doi: 10.1109/JSYST.2018.2883491.

[10] K. Tang, S. Liao, M. Z. A. Bhuiyan, and W. Shi, "Secrecy outage probability of secondary system for wireless-powered cognitive radio networks," in *Proc. 5th Int. Conf. Dependability Sens., Cloud, Big Data Syst. Appl.*, DependSys, Guangzhou, China, 2019, pp. 3–17.

[11] W. Lee, K. Lee, and T. Q. Quek, "Deep-learning-assisted wireless-powered secure communications with imperfect channel state information," *IEEE Internet. Things J.*, vol. 9, no. 13, pp. 11464–11476, 2021. doi: 10.1109/JIOT.2021.3128936.

[12] Y. Liu, Y. Ye, and R. Q. Hu, "Secrecy outage probability in backscatter communication systems with tag selection," *IEEE Wirel. Commun. Lett.*, vol. 10, no. 10, pp. 2190–2194, 2021. doi: 10.1109/LWC.2021.3095969.

[13] J. Moon, H. Lee, C. Song, and I. Lee, "Secrecy outage minimization for wireless powered communication networks with an energy harvesting jammer," in *IEEE Global Commun. Conf. (GLOBECOM)*, Washington DC, USA, IEEE, 2016, pp. 1–5.

[14] H. Rabiei, M. Kaveh, M. R. Mosavi, and D. Martín, "MCRO-PUF: A novel modified crossover RO-PUF with an ultra-expanded CRP space," *Comput. Mater. Contin.*, vol. 74, no. 3, pp. 4831–4845, 2023. doi: 10.32604/cmc.2023.034981.

[15] M. Kaveh, Z. Yan, and R. Jantti, "Secrecy performance analysis of RIS-aided smart grid communications," *IEEE Trans. Ind. Inform.*, pp. 1–13, 2023. doi: 10.1109/TII.2023.333384.

[16] M. Kaveh, F. R. Ghadi, R. Jäntti, and Z. Yan, "Secrecy performance analysis of backscatter communications with side information," *Sens.*, vol. 23, no. 20, pp. 8358, 2023. doi: 10.3390/s23208358.

[17] A. Venkatesh and S. Asha, "DERNNet: Dual encoding recurrent neural network based secure optimal routing in WSN," *Comput. Syst. Sci. & Eng.*, vol. 45, no. 2, pp. 1375–1392, 2023. doi: 10.32604/csse.2023.030944.

[18] R. Chen, C. Yi, K. Zhu, J. Cai, and B. Chen, "A DRL-Based hierarchical game for physical layer security with dynamic trilateral coalitions," in *ICC 2023–IEEE Int. Conf. Commun.*, Rome, Italy, IEEE, 2023, pp. 4495–4500.

[19] M. Waqas, S. Bano, F. Hassan, S. Tu, G. Abbas and Z. H. Abbas, "Physical layer authentication using ensemble learning technique in wireless communications," *Comput. Mater. Contin.*, vol. 73, no. 3, pp. 4489–4499, 2022. doi: 10.32604/cmc.2022.029539.

[20] H. M. Wang and X. G. Xia, "Enhancing wireless secrecy via cooperation: Signal design and optimization," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 47–53, 2015. doi: 10.1109/MCOM.2015.7355565.

[21] M. Kaveh, M. R. Mosavi, D. Martin, and S. Aghapour, "An efficient authentication protocol for smart grid communication based on on-chip-error-correcting physical unclonable function," *Sustain. Energy, Grids Netw.*, vol. 36, pp. 101228, 2023.

[22] S. Miri, M. Kaveh, H. S. Shahhoseini, M. R. Mosavi, and S. Aghapour, "On the security of 'an ultra-lightweight and secure scheme for communications of smart metres and neighbourhood gateways by utilisation of an ARM Cortex-M microcontroller'," *IET Inform. Secur.*, vol. 17, no. 3, pp. 544–551, 2023. doi: 10.1049/ise2.12108.

[23] S. S. Fard, M. Kaveh, M. R. Mosavi, and S. B. Ko, "An efficient modeling attack for breaking the security of XOR-Arbiter PUFs by using the fully connected and long-short term memory," *Microprocess. Microsyst.*, vol. 94, pp. 104667, 2022. doi: 10.1016/j.micpro.2022.104667.

[24] F. R. Gahdi and D. Martin, "Performance analysis of RIS/STAR-IOS-aided V2V NOMA/OMA communications over composite fading channels," *IEEE Trans. Intell. Vehi.*, pp. 1–9, 2023. doi: 10.1109/TIV.2023.3337898.

[25] R. Khanduzi and A. K. Sangaiah, "An efficient recurrent neural network for defensive Stackelberg game," *J. Comput. Sci.*, vol. 67, pp. 101970, 2023. doi: 10.1016/j.jocs.2023.101970.

[26] S. Zhang *et al.*, "Differentiating brain states via multi-clip random fragment strategy-based interactive bidirectional recurrent neural network," *Neural. Netw.*, vol. 165, no. 1, pp. 1035–1049, 2023. doi: 10.1016/j.neunet.2023.06.040.

[27] U. Kaya, A. Yılmaz, and S. Aşar, "Sepsis prediction by using a hybrid metaheuristic algorithm: A novel approach for optimizing deep neural networks," *Diagnostics*, vol. 13, no. 12, pp. 1–15, 2023. doi: 10.3390/diagnostics13122023.

[28] E. Ghandourah, S. Khatir, E. M. Banoqitah, A. M. Alhawsawi, B. Benaissa and M. A. Wahab, "Enhanced ANN predictive model for composite pipes subjected to low-velocity impact loads," *Build.*, vol. 13, no. 4, pp. 973, 2023. doi: 10.3390/buildings13040973.

[29] J. Parmar, S. Chouhan, V. Raychoudhury, and S. Rathore, "Open-world machine learning: Applications, challenges, and opportunities," *ACM Comput. Surv.*, vol. 55, no. 10, pp. 1–37, 2023. doi: 10.1145/3561381.

[30] M. Gheisari *et al.*, "Deep learning: Applications, architectures, models, tools, and frameworks: A comprehensive survey," *CAAI Trans. Intell. Technol.*, vol. 8, no. 3, pp. 581–606, 2023. doi: 10.1049/cit2.12180.

[31] S. Dargan, M. Kumar, M. R. Ayyagari, and G. Kumar, "A survey of deep learning and its applications: A new paradigm to machine learning," *Arch. Comput. Method. Eng.*, vol. 27, pp. 1071–1092, 2020. doi: 10.1007/s11831-019-09344-w.

[32] M. Kaveh, S. Aghapour, D. Martin, and M. R. Mosavi, "A secure lightweight signcryption scheme for smart grid communications using reliable physically unclonable function," in *IEEE Int. Conf. Environ. Electr. Eng.*, Madrid, Spain, IEEE, 2020, pp. 1–6.

[33] A. H. Ribeiro, K. Tiels, L. A. Aguirre, and T. Schön, "Beyond exploding and vanishing gradients: Analyzing RNN training using attractors and smoothness," in *Int. Conf. Artif. Intell. Stat.*, 2020, pp. 2370–2380.

[34] Z. Allen-Zhu, Y. Li, and Z. Song, "On the convergence rate of training recurrent neural networks," *Adv. Neural Inf. Process. Syst.*, vol. 32, 2019.

[35] M. Kaveh, M. S. Mesgari, D. Martín, and M. Kaveh, "TDMBBO: A novel three-dimensional migration model of biogeography-based optimization (case study: Facility planning and benchmark problems)," *J. Supercomput.*, vol. 79, pp. 1–56, 2023. doi: 10.1007/s11227-023-05047-z.

[36] M. Kaveh, M. S. Mesgari, and B. Saeidian, "Orchard algorithm (OA): A new meta-heuristic algorithm for solving discrete and continuous optimization problems," *Math. Comput. Simulat.*, vol. 208, pp. 95–135, 2023. doi: 10.1016/j.matcom.2022.12.027.

[37] Y. Tian, S. Peng, X. Zhang, T. Rodemann, K. C. Tan and Y. Jin, "A recommender system for metaheuristic algorithms for continuous optimization based on deep recurrent neural networks," *IEEE Trans. Artif. Intell.*, vol. 1, no. 1, pp. 5–18, 2020. doi: 10.1109/TAI.2020.3022339.

[38] M. Kaveh and M. S. Mesgari, "Application of meta-heuristic algorithms for training neural networks and deep learning architectures: A comprehensive review," *Neural. Process. Lett.*, vol. 55, no. 4, pp. 4519–4622, 2023. doi: 10.1007/s11063-022-11055-6.

[39] H. Ma, D. Simon, P. Siarry, Z. Yang, and M. Fei, "Biogeography-based optimization: A 10-year review," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 1, no. 5, pp. 391–407, 2017. doi: 10.1109/TETCI.2017.2739124.