

# Intelligent Beamforming and IRS Phase Optimization Model using Bidirectional Scaled Cosine Attention-based Causal Mamba-2 for Secure SWIPT Communications

Dr. Tagilapalli Shashi Kiran  
Neurosurgeon, Department of Neurosurgery,  
The Sixth Affiliated Hospital, Sun Yat-sen University,  
No. 26 Erheng Road, Tianhe District, Guangzhou 510655,  
Guangdong, P. R. China.  
jackyi77@hotmail.com

**Abstract:** Simultaneous Wireless Information and Power Transfer (SWIPT) has gained significant attention as an effective technology for enabling efficient and scalable wireless communication in large-scale networks. The integration of Intelligent Reflecting Surfaces (IRS) with SWIPT has further enhanced the potential to improve both energy and spectrum efficiency in next-generation wireless systems. However, challenges related to spectral efficiency and overall system performance remain, indicating the need for more advanced optimization techniques and enhanced communication frameworks. Additionally, as it ensures the security and integrity of data transferred within networks, secure information transmission is an essential component that cannot be disregarded. As a result, the communication system becomes susceptible to eavesdropping, which creates security risks. Therefore, an advanced approach is developed in order to address a number of concerns with the secret communication models. Here, a cutting-edge deep learning method is used to provide secure communication in an IRS connected to the SWIPT. The Bidirectional Scaled Cosine Attention-based Causal Mamba-2 Network (BSCA-CM2Net) is employed to learn the mapping between channel realizations and the corresponding beamforming vectors and IRS phase shifts, thereby eliminating the need for iterative optimization updates. The designed BSCA-CM2Net effectively addresses different problems caused by IRS phase-shift vectors and transmit beamforming at incomplete Channel State Information (CSI) under multi-eavesdropper conditions. Additionally, some experiments are carried out in the designed system to assess their effectiveness while taking other energy restrictions and secrecy performance into account.

**Keywords:** Secure SWIPT communications; Intelligent Beamforming; IRS Phase Optimization; Bidirectional Scaled Cosine Attention; Causal Mamba-2 Network

Received: May 15, 2026 Revised: May 28, 2026 Accepted: June 3, 2026

## Nomenclature

| Abbreviation | Description                                                        |
|--------------|--------------------------------------------------------------------|
| AI           | Artificial Intelligence                                            |
| AN           | Artificial Noise                                                   |
| B5G          | Beyond Fifth Generation                                            |
| BCD          | Block Coordinate Descent                                           |
| BSCA         | Bidirectional Scaled Cosine Attention                              |
| BSCA-CM2Net  | Bidirectional Scaled Cosine Attention-based Causal Mamba-2 Network |
| CCP          | Convex-Concave Procedure                                           |
| CM2Net       | Causal Mamba-2 Network                                             |
| CNN          | Convolutional Neural Network                                       |
| CSI          | Channel State Information                                          |
| GSM          | Generalized Spatial Modulation                                     |
| IoT          | Internet of Things                                                 |
| IoV          | Internet of Vehicles                                               |
| IRS          | Intelligent Reflecting Surface                                     |
| MIMO         | Multiple-Input Multiple-Output                                     |
| MMSE         | Minimum Mean Square Error                                          |
| SCA          | Successive Convex Approximation                                    |
| SINR         | Signal-to-Interference-plus-Noise Ratio                            |
| STB          | Space-Time Block Coding                                            |
| SWIPT        | Simultaneous Wireless Information and Power Transfer               |

## 1. Introduction

### 1.1 Background

The rapid advancement of beyond fifth-generation (B5G) and sixth-generation (6G) wireless networks has intensified the demand for communication systems that are energy-efficient, secure, and capable of delivering high performance [6]. Furthermore, the widespread adoption

of the Internet of Things (IoT), the Internet of Vehicles (IoV), and other intelligent applications has led to a substantial increase in the number of connected wireless devices. This has resulted in increasing energy consumption and security problems [7]. In large-scale networks, SWIPT is a useful technology for facilitating effective and long-lasting wireless communication. Beyond B5G and 6G communication systems, it enables wireless devices to gather energy and receive information from the same radio frequency waves, making it ideal for next-generation IoT [8]. IRSs have emerged as a promising technology for enhancing the performance of SWIPT networks by improving signal quality, increasing energy efficiency, and maximizing spectrum utilization [9]. An IRS is made up of many passive reflecting components that may intelligently regulate wireless signal propagation, increasing communication coverage and consuming less energy [10]. Even while IRS-assisted SWIPT systems have many benefits, they still have a number of issues with energy efficiency, spectrum efficiency, and overall communication performance, especially in large-scale, dynamic wireless environments [11].

Recent advances in Artificial Intelligence (AI), machine learning, and deep learning have significantly improved the performance of IRS-assisted SWIPT systems by enabling intelligent resource allocation, optimized beamforming, accurate channel prediction, adaptive phase shift design, and enhanced secure communication [12]. Deep learning models can enable adaptive optimization in dynamic communication contexts and learn intricate wireless channel properties from vast volumes of data [13]. These methods lessen the requirement for repeated iterative optimization while enhancing spectrum efficiency, energy harvesting performance, and secure transmission. Deep learning techniques still have some difficulties, though. To perform well, they often need a lot of training data, a lot of processing power, and a lot of training time [14]. Rapid changes in wireless channel circumstances may reduce their forecast accuracy, and many models need to be retrained frequently in order to adjust to changing network conditions. Furthermore, it is still challenging to choose the best model parameters and guarantee strong generalization across various communication circumstances [15]. These drawbacks underscore the need for more intelligent, lightweight, and effective deep learning frameworks that can offer precise optimization, safe communication, and increased energy efficiency in IRS-assisted SWIPT networks.

## 1.2 Contributions

The contributions of the proposed study are given below:

- ✚ To design a cohesive intelligent framework for safe communication in SWIPT networks supported by IRS. The suggested framework combines secure information transmission, IRS phase shift optimization, and transmit beamforming optimization into a single deep learning pipeline. It combines energy harvesting and communication security into a single architecture, allowing for dependable system performance and effective resource use. The framework lowers computational complexity while increasing communication dependability, energy efficiency, and secrecy performance. Furthermore, it offers a scalable system that can efficiently handle dynamic channel conditions in next-generation B5G and 6G wireless communication networks.
- ✚ To develop a BSCA-CM2Net mechanism for IRS phase shift optimization and safe beamforming. The suggested model efficiently learns the link between channel realizations, transmit beamforming vectors, and IRS phase shifts by combining the BSCA and CM2Net processes. More accurate feature representation is achieved by the BSCA mechanism, which emphasizes the most relevant channel features while capturing both forward and backward channel dependencies. Faster and more stable optimization is made possible by the CM2Net's effective modeling of long-range sequential dependencies with minimal computational complexity. Consequently, under imperfect CSI and multi-eavesdropper scenarios, the suggested model improves the secrecy rate and energy harvesting performance, eliminates repeated iterative optimization, and speeds up convergence.

## 1.3 Organization

The remainder of this paper is organized as follows:

Section 2 explains the baseline literature on secure communication, optimization techniques, and IRS-assisted SWIPT systems. Section 3 introduces the overall architecture of the proposed secure communication framework for IRS-assisted SWIPT networks. Section 4 details the proposed BSCA-CM2Net for transmit beamforming and IRS phase shift optimization. Section 5 presents the experimental configuration, performance evaluation, and comparative analysis.

Finally, Section 6 summarizes the key findings and outlines potential directions for future research.

## **2. Existing Works**

### **2.1 Related Works**

In 2026, Nguyen-Duy-Nhat and Pham [1] designed a framework for safe communication in IRS-assisted SWIPT systems using deep learning. The proposed system employed a multi-head attention-based Convolutional Neural Network (CNN) to jointly optimize the IRS phase shifts and transmit beamforming vectors under both perfect and imperfect CSI conditions. Experimental evaluations demonstrated that the proposed approach achieved superior performance compared with existing optimization methods in terms of secrecy rate, energy efficiency, and system robustness.

In 2024, Shi et al. [2] suggested an SWIPT model with active IRS assistance to optimize energy harvesting at the energy harvesting receiver. The proposed approach jointly optimized the base station transmit beamforming and active IRS phase shifts while satisfying the signal-to-interference-plus-noise ratio (SINR) and power constraints under both perfect and imperfect CSI scenarios. The suggested active IRS-assisted SWIPT system outperformed traditional passive IRS-assisted systems in terms of energy harvesting performance and communication efficiency, according to simulation results.

In 2026, Zhu et al. [3] suggested a SWIPT system that used mobile antennas and IRS to enhance energy collection and information transfer. To maximize the weighted sum rate while satisfying energy harvesting requirements, the proposed method jointly optimized the beamforming vectors, IRS phase shifts, and antenna deployment positions. Simulation results demonstrated that the proposed strategy achieved superior performance compared with existing techniques in terms of both communication efficiency and energy harvesting capability.

In 2025, Liong et al. [4] formulated a multi-user MIMO SWIPT system with IRS assistance that maximized the system sum-rate while taking secrecy into account. The proposed framework integrated MMSE, Block Coordinate Descent (BCD), Successive Convex Approximation (SCA), and penalized Convex-Concave Procedure (CCP) algorithms to jointly optimize the transmit precoding variables and IRS phase shift matrices. The simulation outcomes confirmed that the developed method provided better system performance and achieved higher sum-rate gains compared with conventional approaches.

In 2025, Xu and Shang [5] developed a Generalized Spatial Modulation (GSM) approach to enhance secure communication for SWIPT systems aided by IRS. The proposed technique combined Space-Time Block Coding (STBC) and an Artificial Noise (AN) generation strategy to boost secrecy and energy harvesting performance. Simulation findings revealed that the proposed method produced greater communication reliability, security, and efficiency than existing approaches.

### **2.2 Motivation**

The increasing demand for secure and energy-efficient wireless communication solutions in beyond 5G and 6G networks has positioned secure communication in IRS-assisted SWIPT systems as an important and emerging research area. Nevertheless, there are still several issues with traditional optimization and secure transmission techniques. The following lists some of the main research issues with the existing methods.

- The optimization procedure in traditional beamforming and IRS phase shift optimization methods relies on numerous iterative calculations. Real-time implementation becomes challenging as a result of the increased computing complexity and execution time. In order to lower computing costs and increase convergence time, an intelligent deep learning-based optimization technique is presented. It enhances overall communication performance and allows for quicker beamforming and IRS phase shift optimization.
- Traditional IRS-assisted SWIPT models are designed assuming perfect CSI. However, dynamic channel changes and channel estimate errors are common in real-world wireless situations, which lower communication performance and secrecy rate. Consequently, a strong learning-based strategy is created to manage poor CSI and enhance secure communication. Under dynamic wireless channel situations, it ensures dependable communication performance while increasing the secrecy rate.

- Existing secure communication frameworks face significant challenges in jointly optimizing transmit beamforming and IRS phase shifts, particularly in scenarios involving multiple eavesdroppers. These limitations hinder the ability of IRS-assisted SWIPT systems to simultaneously maximize spectral efficiency, energy harvesting efficiency, and secrecy rate. To address these challenges and enhance the overall performance of IRS-assisted SWIPT networks, an advanced deep learning-based framework is proposed for intelligent optimization of communication parameters.

### 3. Overview of SWIPT Communication Systems

#### 3.1 System Model

The considered downlink SWIPT-enabled IoT communication framework comprises an Access Point (AP) equipped with a Uniform Linear Array (ULA) of  $N$  antennas, an IRS consisting of passive reflecting elements arranged in a Uniform Rectangular Array (URA) containing  $O = O_x O_z$  passive reflecting elements, and two single-antenna users: a Legitimate Information User (IU) and an Energy User (EU) [1]. While the IRS cleverly modifies the phase shifts of its reflecting elements to regulate the wireless propagation environment and enhance communication performance, the AP concurrently delivers wireless information and energy to the authorized user. The energy consumer is regarded as an active eavesdropper with two roles in this system. In order to fuel its own operations, it first collects energy from the radio frequency signals that the AP transmits. Second, it uses the same received signal to try to intercept and decode the private information meant for the authorized information user. This illustrates a real-world security scenario in SWIPT-enabled IoT networks, where attackers can support continuous eavesdropping without the need for an external power source by using gathered energy. Therefore, even in the presence of such self-powered eavesdroppers, the primary goal is to increase the genuine user's secrecy rate while guaranteeing effective energy harvesting. This work examines a basic system with one information user and one energy user in order to clearly illustrate the suggested architecture and its performance. The main trade-off between energy harvesting and secure communication can be more thoroughly examined using this simple model. Even though the suggested architecture can be expanded to networks with several users and eavesdroppers, these situations present further difficulties, such as managing interference, scheduling users, and more intricate optimization restrictions. The system model's pictorial view is depicted in Fig. 1.

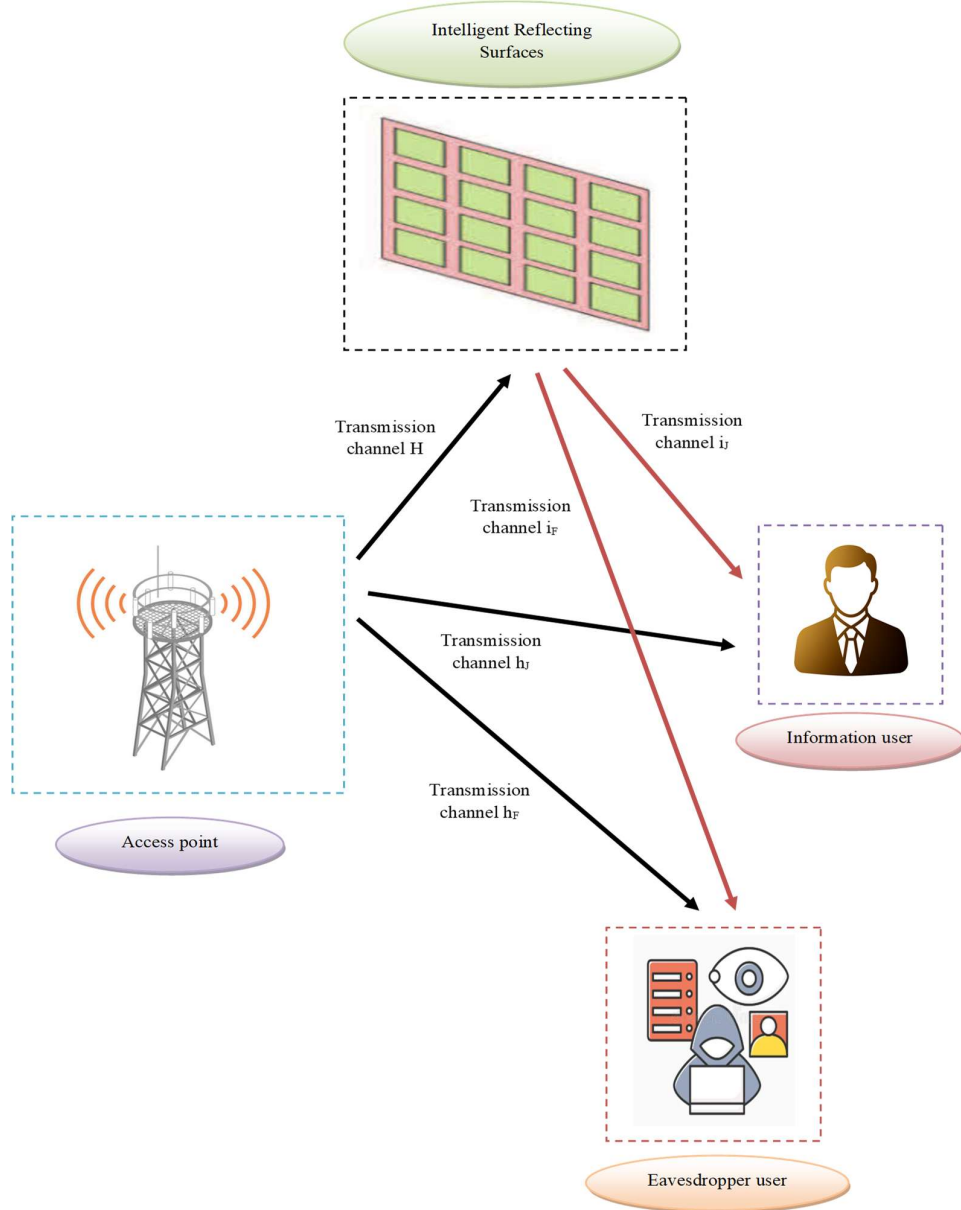


Fig. 1. Pictorial view of the system model

### 3.2 Channel Model

The channel corresponding to the links within the IRS and other network entities is represented as small-scale Rician fading channels. Let  $i_j^I, i_F^I \in \mathbb{Q}^{1 \times O}$  and  $h_j^I, h_F^I \in \mathbb{Q}^{1 \times N}$  represent the channel vectors for the IRS-to-IU, IRS-to-EU, AP-to-IU, AP-to-EU links, and the AP-to-IRS channel matrix, respectively. Specifically, the term  $H \in \mathbb{Q}^{O \times N}$  represents the IRS-associated channel matrix between the AP and the IRS. Both Line-of-Sight (LoS) and Non-Line-of-Sight (NLoS) propagation components are taken into account for all wireless links in the considered system. Accordingly, the corresponding channel models are formulated as given in the following equations.

$$i_j = \sqrt{i_0 e^{-\beta_i}} \left( \sqrt{\frac{L}{1+L}} i_{j,LoS} + \sqrt{\frac{1}{1+L}} i_{j,NLoS} \right) \quad (1)$$

$$h_j = \sqrt{h_0 e^{-\beta_h}} \left( \sqrt{\frac{L}{1+L}} h_{j,LoS} + \sqrt{\frac{1}{1+L}} h_{j,NLoS} \right) \quad (2)$$

$$H_j = \sqrt{H_0 e^{-\beta_H}} \left( \sqrt{\frac{L}{1+L}} H_{j,LoS} + \sqrt{\frac{1}{1+L}} H_{j,NLoS} \right) \quad (3)$$

Here,  $j \in \{J, F\}$  and the Rician K-factor are specified using the variable  $L$ . The parameters of the channels are characterized by three triplets  $(i_0, e_i, \beta_i)$ ,  $(h_0, e_h, \beta_h)$ , and  $(H_0, e_H, \beta_H)$ , corresponding to the IRS-ser links, AP-user links, and AP-IRS user links. The path loss coefficient, transmission distance, and path loss exponent are represented using each triplet. The NLoS components  $i_{j,NLoS}$ ,  $h_{j,NLoS}$ , and  $H_{j,NLoS}$  consist of independent and identically distributed complex Gaussian random variables. The LoS components are determined based on the corresponding channel geometry in Eq. (4), Eq. (5), and Eq. (6).

$$i_{j,NLoS} = \begin{bmatrix} 1, e^{-k \frac{2\pi}{\lambda_d} c_{IRS} \sin \psi_j \cos \phi_j}, \dots, e^{-k \frac{2\pi}{\lambda_d} c_{IRS} (O_I - 1) \sin \psi_j \cos \phi_j} \end{bmatrix}^U \otimes \begin{bmatrix} 1, e^{-k \frac{2\pi}{\lambda_d} c_{IRS} \sin \psi_j \sin \phi_j}, \dots, e^{-k \frac{2\pi}{\lambda_d} c_{IRS} (O_I - 1) \sin \psi_j \sin \phi_j} \end{bmatrix}^U, \quad (4)$$

$$\in \mathbb{Q}^{O \times 1}$$

$$h_{j,NLoS} = \begin{bmatrix} 1, e^{-k \frac{2\pi}{\lambda_d} c_{AP} \sin \psi_j \cos \phi_j}, \dots, e^{-k \frac{2\pi}{\lambda_d} (N-1) c_{AP} \sin \psi_j \cos \phi_j} \end{bmatrix}^U, \quad (5)$$

$$\in \mathbb{Q}^{N \times 1}$$

$$H_{NLoS} = \begin{bmatrix} 1, e^{-k \frac{2\pi}{\lambda_d} c_{IRS} \sin \psi_{AP} \cos \phi_{AP}}, \dots, e^{-k \frac{2\pi}{\lambda_d} c_{IRS} (N_y - 1) \sin \psi_{AP} \cos \phi_{AP}} \end{bmatrix}^U \otimes \begin{bmatrix} 1, e^{-k \frac{2\pi}{\lambda_d} c_{IRS} \sin \psi_{AP} \sin \phi_{AP}}, \dots, e^{-k \frac{2\pi}{\lambda_d} c_{IRS} (N_y - 1) \sin \psi_{AP} \sin \phi_{AP}} \end{bmatrix}^U \otimes \begin{bmatrix} 1, e^{-k \frac{2\pi}{\lambda_d} c_{AP} \sin \psi_{IRS} \cos \phi_{IRS}}, \dots, e^{-k \frac{2\pi}{\lambda_d} (N-1) c_{AP} \sin \psi_{IRS} \cos \phi_{IRS}} \end{bmatrix}^U \quad (6)$$

$$\in \mathbb{Q}^{O \times M}$$

Here, the Kronecker product is specified as  $\otimes$ , the wavelength of the middle frequency is specified as  $\lambda_d$ , the element distance is specified as  $c_{IRS}$ , and the antenna spacing is specified as  $c_{AP}$ . The Azimuth angle Of Arrival (AOA) of the way within the IRS and the device  $j$  is indicated as  $\psi_j$  and  $\phi_j$ .

### 3.3 Information and Energy Transfer Approach

The received signals at the IU and the EU, the achievable communication rates, harvested energy, secrecy rate, and optimization problem are described below.

Eq. (7) shows the received signal at the IU.

$$z_j = (i_j^t \eta H + h_j^t) x t + o_j \quad (7)$$

Here, the term  $\eta \in \mathbb{Q}^{O \times O}$  represents the IRS phase-shift diagonal matrix,  $y \in \mathbb{Q}^{N \times 1}$  represents the transmit beamforming vector,  $t$  is the transmitted information symbol, and  $o_j$  is the Additive White Gaussian Noise (AWGN) at the IU. The IRS intelligently adjusts its reflecting elements to strengthen the desired signal received by the legitimate user. Similarly, the received signal at the EU, which also acts as an eavesdropper, is given in Eq. (8).

$$z_F = (i_F^t \eta H + h_F^t) x t + o_F \quad (8)$$

In Eq. (8), the term  $o_j$  denotes the additive white Gaussian noise at the EU. The EU harvests energy from the received signal while simultaneously attempting to decode the confidential information transmitted to the legitimate user. During each transmission interval, the AP transmits a unit-power information symbol satisfying  $\mathbb{E}[|t|^2] = 1$ , using the beamforming vector  $x$ . At the same time, the IRS adjusts its phase-shift matrix to enhance the received signal at the IU while reducing signal leakage toward the EU.

The equivalent cascaded channels of the IU and EU are defined as  $\tilde{h}_j \triangleq i_j' \eta H + h_j^I$  and  $\tilde{h}_e \triangleq i_e' \eta H + h_e^I$ . These equivalent channels simplify the beamforming optimization process. The information transmission rate achievable by the IU is formulated according to Eq. (9).

$$S_j = \nu \log_2 \left( 1 + \frac{|\tilde{h}_j x|^2}{\zeta_j^2} \right) \quad (9)$$

In Eq. (9), the term  $\nu$  specifies the time allocated for information decoding, and the term  $\zeta$  represents the noise power at the IU. A higher received signal power leads to a larger achievable information rate.

Similarly, the achievable information rate of the EU is expressed in Eq. (10)

$$S_j = \nu \log_2 \left( 1 + \frac{|\tilde{h}_j x|^2}{\zeta_j^2} \right) \quad (10)$$

Eq. (10) represents the maximum information that the eavesdropper can decode from the received signal. The harvested energy at the IU is expressed in Eq. (11).

$$F_T = (1 - \nu) \rho |\tilde{h}_j x|^2 \quad (11)$$

In Eq. (11), the term  $\rho$  is the energy conversion efficiency of the harvesting circuit. The remaining transmission time is used for harvesting energy from the received RF signal. The achievable secrecy rate is obtained through Eq. (12).

$$S_T = \max(0, S_j - S_e) \quad (12)$$

Here, the term  $S_T$  denotes the secrecy rate,  $S_j$  specifies the achievable rate of the legitimate user, and  $S_e$  represents the achievable rate of the eavesdropper. A positive secrecy rate is achieved only when the information decoding rate of the legitimate user exceeds that of the eavesdropper. Therefore, the primary objective is to maximize the secrecy rate through the joint optimization of the transmit beamforming vector and the IRS phase-shift matrix. The optimization problem is formulated as given below.

$$(Q1): \max_{x, \eta} S_T \quad (13a)$$

$$t.u. \quad |x|^2 \leq Q_{\max}, \quad (13b)$$

$$F_j \geq F_{\min}, \quad (13c)$$

$$S_j \geq S_{th} \quad (13d)$$

$$|\eta_{o,o}| = 1, \quad o = 1, \dots, O \quad (13e)$$

Here, the term  $Q_{\max}$  specifies the maximum transmit power,  $F_{\min}$  specifies the minimum harvested energy requirement, and  $S_{th}$  denotes the minimum Quality of Service (QoS) threshold for the IU. The last constraint ensures that each IRS reflecting element maintains unit reflection amplitude. Due to the non-convex nature of both the objective function and the associated constraints, obtaining an optimal solution to this optimization problem directly is computationally challenging.

## 4. Proposed Methodology

### 4.1 Causal Mamba 2 Network

The CM2Net [16] is efficiently used for processing sequential data in an advanced State Space Model (SSM) architecture. By maintaining the causal attribute, this enhanced version of Mamba improves long-sequence modeling, computational efficiency, and inference speed. The following describes how CM2Net operates.

**Input Representation:** Let the input sequence be specified in Eq. (14).

$$Yx = \{yX_1, yX_2, \dots, yX_U\} \quad (14)$$

This equation gives the input feature vector at time step and indicates the length of the sequence. Eq. (15) uses a linear embedding layer to project the input into a higher-dimensional feature space.

$$a_u = X_d y_t + c_e \quad (15)$$

Here, the embedding weight matrix and bias vector are specified as  $X_d$  and  $c_e$ .

**Causal Convolution Layer:** A causal one-dimensional convolution ensures that future information is not utilized during prediction when extracting local temporal features.

$$d_u = \sum_{l=0}^{L-1} x_l a_{u-l} \quad (16)$$

In Eq. (16), the kernel size is represented as  $L$  and the convolution weights are represented as  $x_l$ . The causal structure ensures that the current output is solely influenced by previous observations.

**Selective State Space Modeling:** A selected SSM that captures long-range temporal dependencies is used to process the extracted features. The hidden state is updated according to the formulation provided in Eq. (17).

$$i_u = B i_{u-1} + C_u y_u \quad (17)$$

Here, the hidden state and state transition matrix are illustrated as  $i_u$  and  $B$ . The input-dependent projection matrix is specified as  $C_u$ . CM2Net dynamically adjusts its parameters according to the input sequence, enabling adaptive feature extraction.

**Selective Gating Mechanism:** The information that should be kept during state updates is decided by a gating mechanism.

$$\hat{y}_u = \sigma(X_h y_u) \odot y_u \quad (18)$$

Here, the term  $\sigma(\cdot)$  represents the sigmoid activation,  $X_h$  is the gating weight matrix, and  $\odot$  denotes element-wise multiplication. This mechanism suppresses irrelevant features while emphasizing informative patterns.

**State Update:** The gated input is used to iteratively update the concealed state using Eq. (19).

$$i_u = B i_{u-1} + C \hat{y}_u \quad (19)$$

Compared to attention-based architectures, this recursive formulation allows for the effective modeling of long-term dependencies with far less computational complexity.

**Output Layer:** The final output is obtained through a linear projection:

$$z_u = D i_u \quad (20)$$

Here,  $D$  is the output projection matrix,  $i_u$  and represents the predicted output. Hence, the model processes long sequences with linear time complexity, reducing computational cost and memory usage. This enables faster training and inference than traditional attention-based models.

#### 4. 2 Proposed BSCA-CM2Net for Multi-user Scenarios

The suggested BSCA-CM2Net is developed to provide secure communication in multi-user IRS-assisted SWIPT networks. This model directly predicts the optimal transmission through a single forward propagation. The input parameters from the wireless communication system's channel are initialized and passed to the proposed approach. The framework combines the BSCA mechanism with the CS2Net to provide secure communication in SWIPT networks with IRS assistance. The BSCA [17] approach is an attention mechanism that replaces the standard dot-product similarity with scaled cosine similarity. It computes the attention in both directions between two sets of representations. The performance of the attention mechanism is the feature interaction between shallow channel representations and high-level semantic channel features. This can be computed in Eq. (21) and Eq. (22).

$$Z_1 = \text{soft max} \left( \frac{yQ_1 yK_2^t}{\|yQ_1\| \|yK_2\|} \right) eV_1 \quad (21)$$

$$Z_2 = \text{soft max} \left( \frac{yQ_1 yK_2^t}{\|yQ_1\| \|yK_2\|} \right) eV_2 \quad (22)$$

Here, the obtained shallow features query, key, and value metrics are specified as  $yQ$ ,  $yK$ , and  $eV$ .

Similarly, the reverse attention can be expressed in Eq. (23) and Eq. (24).

$$Z_3 = \text{soft max} \left( \frac{yQ_2 yK_1^t}{\|yQ_2\| \|yK_1\|} \right) eV_1 \quad (23)$$

$$Z_4 = \text{soft max} \left( \frac{yQ_2 yK_1^t}{\|yQ_2\| \|yK_1\|} \right) eV_2 \quad (24)$$

Here, the first attention path refines high-level channel representations using detailed propagation information, and the second path suppresses redundant channel responses by

incorporating semantic guidance. Consequently, BSCA improves channel feature discrimination, strengthens inter-user feature correlation, and enhances the accuracy of beamforming optimization in multi-user environments. As this model computes the attention in both directions, it requires two attention operations instead of one. This may increase the computation and memory cost. It also causes loss of magnitude information because of the cosine similarity normalization of vectors. So, the CM2Net mechanism is incorporated with the BSCA module. This network captures long-range channel dependencies among multiple users and eavesdroppers through an efficient state-space learning mechanism. The CM2Net module uses an SSM strategy to efficiently capture both local and long-range dependencies in wireless channel features. The network selectively retains informative channel states while suppressing redundant and noisy feature responses, which results in more robust feature representations. Furthermore, CM2Net improves the extraction of spatial and temporal channel characteristics by enabling accurate beamforming and power allocation under dynamic multi-user communication scenarios. It also helps to mitigate the computational complexity while maintaining effective temporal modeling capability.

**Power-constrained output projection:** The features learned are projected into the beamforming matrix and IRS phase-shift vector. The beamforming matrix can be defined in Eq. (25).

$$X = \bar{X} \sqrt{\frac{Q_+}{\|\bar{X}\|_G^2}} \quad (25)$$

Here, the maximum allowable transmit power is indicated as  $Q_+$ . Likewise, the IRS phase-shift matrix is generated in Eq. (26).

$$\phi = \text{diag}(d^{k\bar{\theta}_1}, d^{k\bar{\theta}_2}, \dots, d^{k\bar{\theta}_N}) \quad (26)$$

This ensures that every IRS reflecting element satisfies the unit-modulus constraint.

**Multi-user optimization loss:** The proposed model BSCA-CM2Net is trained by maximizing the secrecy rate of all the authorized users through the satisfaction of lower harvested energy and QoS requirements. Thus, the overall loss function can be formulated as Eq. (27).

$$ssoL_{NV} = -\sum_{l=1}^L S_{T,l} + \sum_{l=1}^L \left[ \chi_f (F_{\min,l} - F_{J,l})_+^2 + \chi_s (S_{th,l} - S_{J,l})_+^2 \right] \quad (27)$$

In Eq. (27), the  $l^{th}$  IU secrecy rate is indicated as  $S_{T,l}$  and the penalty coefficients are indicated as  $\chi_f$  and  $\chi_s$ . Through the joint optimization of BSCA and CM2Net, the suggested framework efficiently generates the optimal beamforming vectors and IRS phase shifts for multiple users.

**Working:** In this framework, the suggested BSCA-CM2Net is developed to provide secure communication in multi-user IRS-assisted SWIPT networks. The initialized channel state parameters are used as the input to the framework. By integrating the BSCA module and CM2Net, the proposed framework can accurately estimate the optimal beamforming vectors and IRS phase-shift configurations through a single-pass forward propagation. BSCA enhances the channel feature interaction, strengthens inter-user correlations, and improves beamforming optimization. To mitigate the computational overhead of BSCA, CM2Net utilizes an efficient SSM strategy to capture local and long-range channel dependencies by suppressing redundant channel features. It increases the secrecy performance, energy efficiency, spectrum utilization, and computational scalability in wireless communication systems.

Thus, the proposed BSCA-CM2Net framework combines BSCA for effective channel feature learning and CM2Net for efficient dependency modelling. As a result, the model produces secure and computationally efficient communication in multi-user IRS-assisted SWIPT networks. The architectural view of the suggested BSCA-CM2Net for multi-user scenarios is shown in Fig. 2.

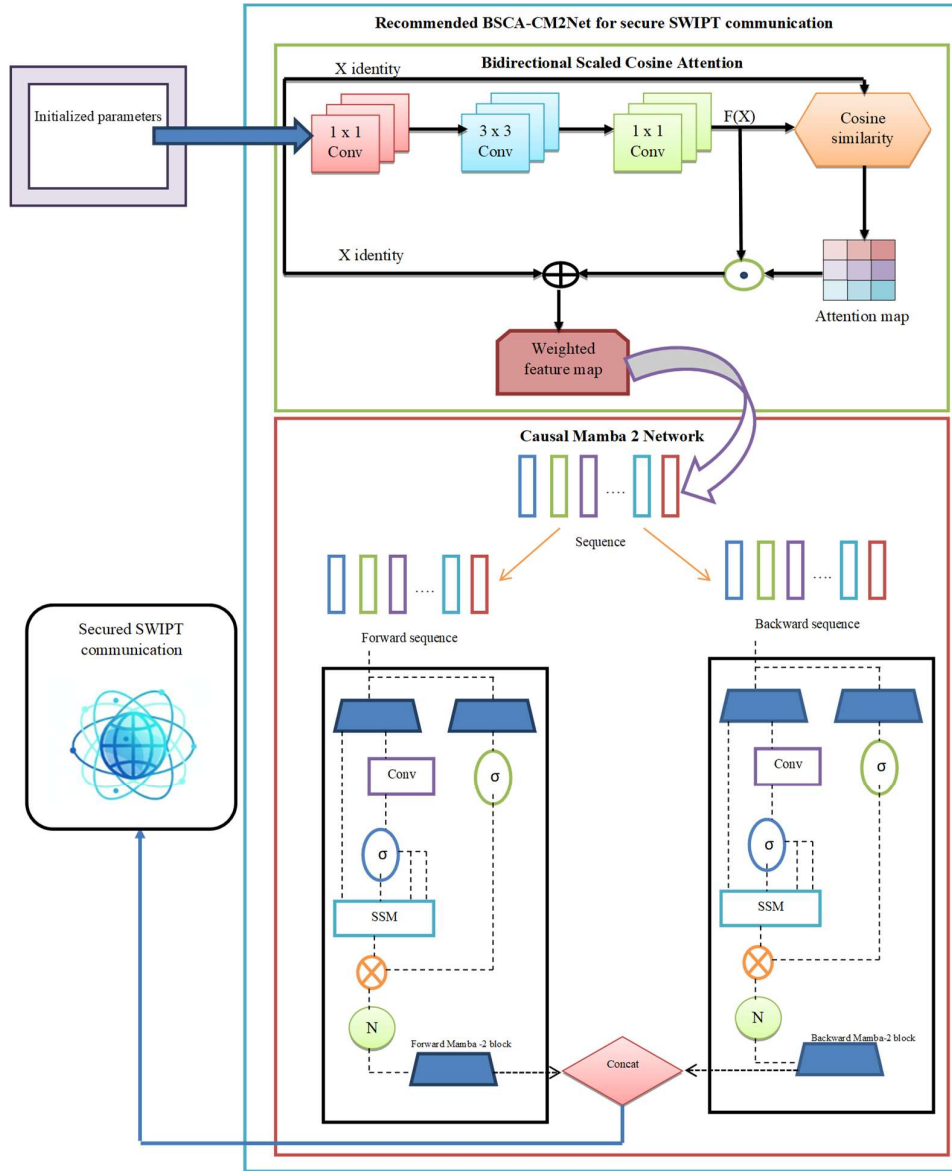


Fig. 2. Architectural view of suggested BSCA-CM2Net for multi-user scenarios

#### 4.3 Elucidation of Proposed Work

With the rising requirements for reliable and energy-conscious wireless communication systems, secure communication has become a crucial aspect of IRS-assisted SWIPT networks. Thus, for next-generation B5G and 6G networks, it is crucial to simultaneously improve secrecy performance, energy harvesting, and spectrum efficiency. Iterative algorithms, which are sensitive to poor CSI and demand a high computational cost, are the foundation of conventional optimization techniques. While communication performance has been enhanced by modern deep learning techniques, issues including high training complexity, decreased optimization accuracy under poor CSI, and limited adaptation to multi-eavesdropper situations still need to be addressed. In addition, achieving simultaneous optimization of transmit beamforming and IRS phase-shift configurations while satisfying both energy harvesting and physical-layer security constraints continues to be a complex challenge. Reliable communication in changing network situations also requires effective learning of complex wireless channel properties. Furthermore, practical real-time deployment depends on minimizing computing cost without sacrificing optimization precision. Addressing these limitations requires the development of an intelligent deep learning framework capable of performing secure beamforming and optimizing

IRS phase shifts. Accordingly, this work introduces a unified secure communication framework utilizing BSCA-CM2Net, as depicted in Fig. 3.

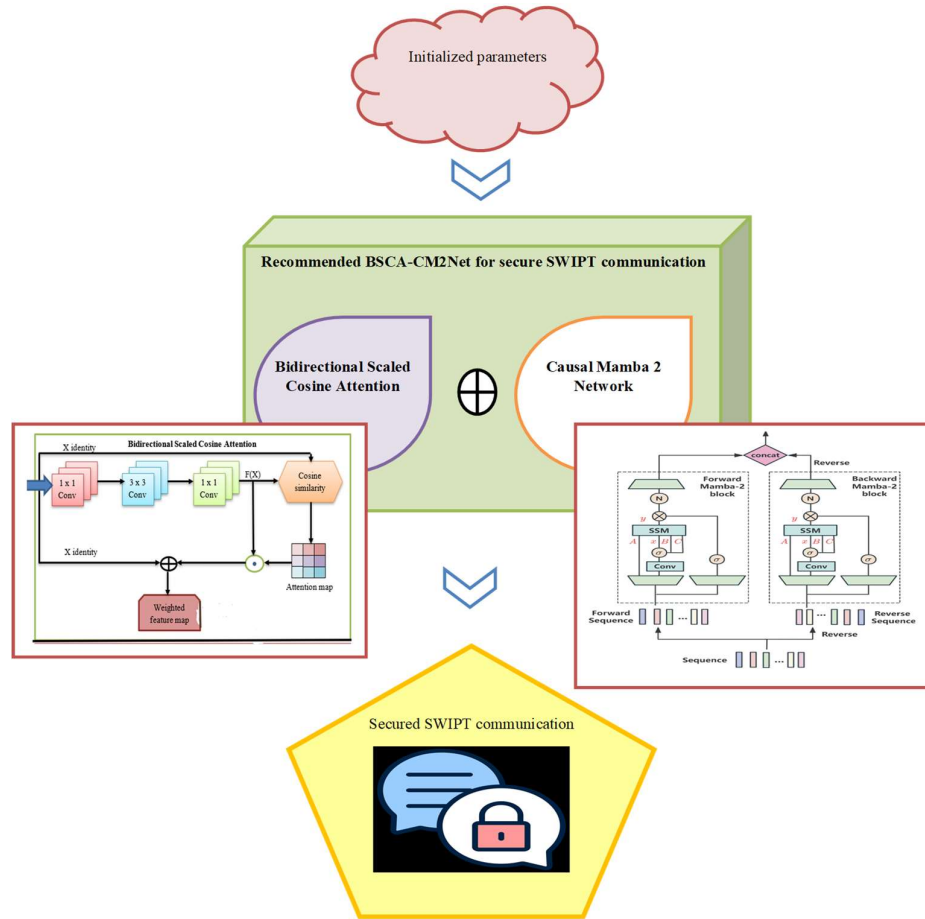


Fig. 3. Graphical illustration of recommended BSCA-CM2Net for secure wireless communication

The proposed framework is intended to provide secure communication in SWIPT networks with IRS assistance. First, the wireless communication system's channel input parameters are initialized. Subsequently, the BSCA-CM2Net framework processes the extracted channel information to determine the optimal transmit beamforming vectors and IRS phase shifts in a joint optimization manner. In order to accomplish precise channel feature learning and effective optimization within a single deep learning architecture, the framework integrates the BSCA method with the CM2Net. In order to enhance feature representation, the BSCA method suppresses redundant channel information and learns both forward and backward channel dependencies. Its attention mechanism to emphasize the most informative channel characteristics. Through an effective state-space architecture, the CM2Net efficiently captures long-range channel dependencies, lowers computing cost, and offers faster convergence with better optimization stability in dynamic wireless situations. The integration of these two approaches eliminates the requirement for repetitive iterative optimization while achieving accurate optimization of the transmit beamforming vectors and IRS phase-shift configurations. Consequently, the suggested framework satisfies the necessary transmit power and energy harvesting restrictions while increasing the secrecy rate and energy harvesting spectrum efficiency. Additionally, it successfully manages multi-eavesdropper scenarios and improper CSI, guaranteeing dependable and secure communication. In order to show the efficacy, robustness, and computing efficiency of the suggested framework, its performance is assessed using a number of performance indicators and contrasted with conventional approaches. Thus, the model provides secure SWIPT communication as an outcome of intelligent beamforming and IRS phase optimization.

## 5. Experimental Analysis

### 5.1 Simulation Setup

The suggested BSCA-CM2Net approach was implemented using Python for secure SWIPT communication. Under various parameter settings and network conditions, the performance of the suggested framework was estimated. This model was contrasted with prior conventional methods like CNN [18], Alternating Optimization (AO) [2], Successive Convex Approximation (SCA) [4], and Penalty Duality Decomposition (PDD) [3]. The simulation evaluations revealed that BSCA-CM2Net achieved better performance than conventional approaches, highlighting its effectiveness in intelligent beamforming optimization and IRS phase-shift optimization for secure SWIPT communication networks. Table 1 shows the system configuration details of the suggested work.

Table 1. System configuration of the suggested work

| Simulation parameters                    |                     |
|------------------------------------------|---------------------|
| Parameter                                | Values              |
| Fraction of time to information decoding | 0.5                 |
| Number of AP antennas                    | 32                  |
| IRS array configuration                  | 5 x 10              |
| Rician K-factor                          | 3 dB                |
| Noise power spectral density             | -1110 dBm           |
| Transmit power                           | 18-43 dBm           |
| Bandwidth                                | 1 MHz               |
| Path-loss for all channels               | 30+20 lg d          |
| Energy conversion efficiency             | 0.8                 |
| Path-loss exponent                       | 2.0                 |
| Software Requirement                     |                     |
| Software - PyCharm                       | version Python 3.11 |
| Hardware Requirement                     |                     |
| Machine                                  | Windows             |
| Version                                  | 11                  |
| Processor                                | i3                  |
| RAM                                      | 8GB                 |
| ROM                                      | 500GB               |

### 5.2 Comparison of Harvested Energy and Secrecy Rate vs. Transmit Power under Perfect-CSI Performance

Fig. 4(a) presents the variation of harvested energy with respect to transmit power when perfect CSI is assumed. The harvested energy increases almost linearly with increasing transmit power for all methods. The proposed model BSCA-CM2Net shows approximately 0.72 dB, while the existing models such as CNN, AO, SCA, and PDD show nearly identical harvested energy values around -5.94 dBm. This indicates stable energy harvesting performance over the estimated transmit power range.

Fig. 4(b) presents the secrecy rate performance as a function of transmit power assuming perfect CSI conditions. The secrecy rate enhances with increasing transmit power and gradually saturates at higher power levels. At 33 dBm, the proposed BSCA-CM2Net has a lower secrecy rate than the conventional methods by 9% for CNN, 6% for AO, 4% for SCA, and 3% for PDD. The obtained results verify that the proposed approach successfully maintains a balance between enhanced secrecy performance and improved robustness.

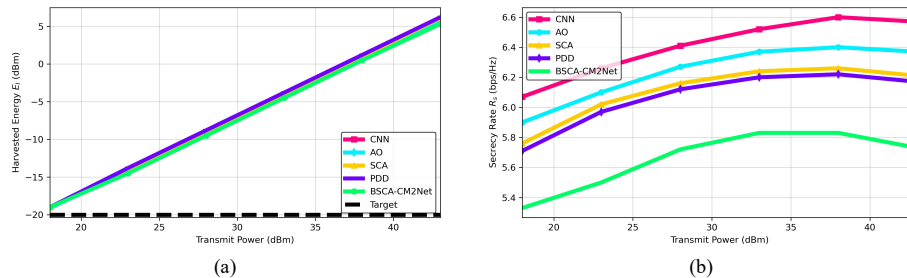


Fig. 4. Comparison of the proposed model in terms of (a) harvested energy vs transmit power and (b) Secrecy rate vs transmit power

### 5.3 Estimation of Imperfect-CSI performance

Fig. 5(a) depicts the variation in harvested energy of the suggested model compared with existing techniques. A gradual reduction in harvested energy is observed for all compared methods as channel estimation becomes less accurate. Nevertheless, the proposed work shows greater resilience to CSI uncertainty by preserving more stable energy harvesting performance than the existing approaches. The CSI error is lower for the suggested BSCA-CM2Net than for the existing methods by 17% for CNN, 2% for AO, 4% for SCA, and 6% for PDD.

Fig. 5(b) illustrates the impact of CSI error on the secrecy rate of the suggested model compared with existing techniques. An increase in channel estimation error leads to a reduction in secrecy performance for every method. Despite this, the proposed work consistently maintains the highest secrecy rate under imperfect CSI conditions. At 0.5 channel estimation error, it provides approximately 18.6% lower secrecy rate than the conventional method. Thus, the result demonstrates its strong robustness against channel estimation errors and its suitability for secure SWIPT communication.

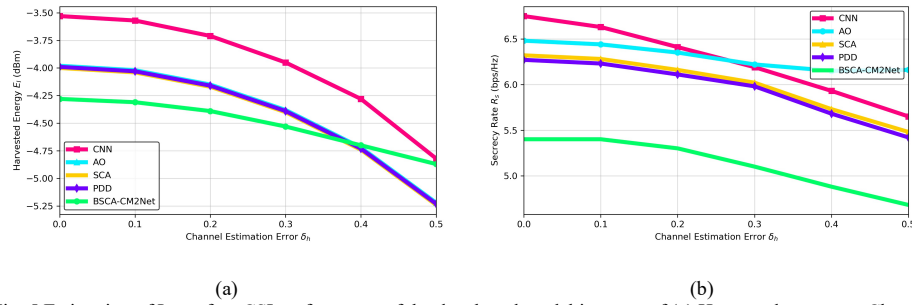


Fig. 5. Estimation of Imperfect-CSI performance of the developed model in terms of (a) Harvested energy vs Channel estimation error and (b) Secrecy rate vs Channel estimation error

### 5.4 Multi-user Fairness Performance Evaluation

Fig. 6 presents the multi-user performance evaluation for IUs and EUs. As the transmit power increases, the Sum Secrecy Rate (SSR) varies across all considered methods. The proposed BSCA-CM2Net consistently demonstrates improved performance over the entire power range. At the 25<sup>th</sup> transmit power level, the proposed approach reduces the SSR compared with CNN, AO, SCA, and PDD methods by 8%, 5%, 4%, and 4%, respectively. This performance variation is achieved through the joint optimization of transmit beamforming and IRS phase shifts, which facilitates efficient resource management and enhanced secrecy control in multi-user communication environments. The results demonstrate that the proposed work effectively supports secure communication in realistic multi-user SWIPT scenarios.

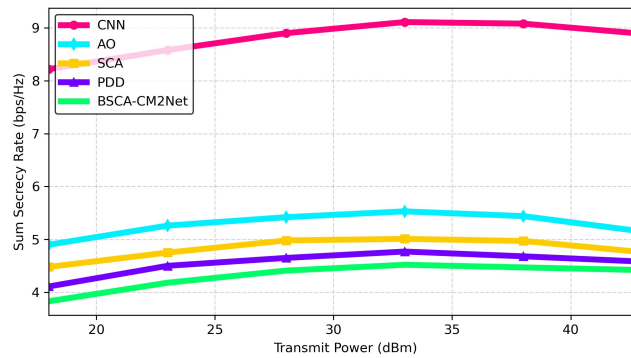


Fig. 6. Performance Evaluation of Multi-user Fairness

### 5.5 Secrecy Performance of Single-user vs. Multi-user

Fig. 7 illustrates a comparison between the secrecy performance of the original single-user scenario and the proposed multi-user framework. Although the secrecy rate of individual users is reduced because of resource sharing, the overall SSR improves considerably as the system simultaneously supports multiple users. The proposed multi-user approach achieves approximately 63% higher SSR than the single-user model. As a result, the proposed framework

demonstrates the spectral efficiency and effective support for secure multi-user SWIPT communication.

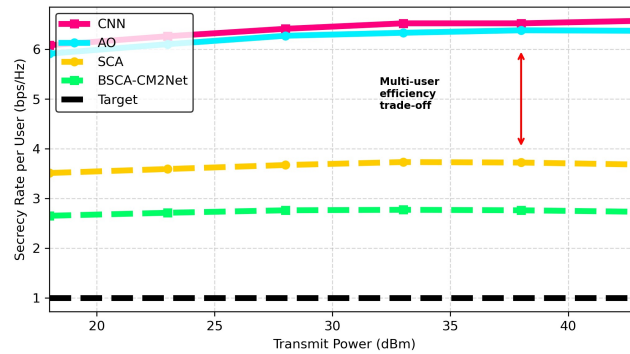


Fig. 7. Secrecy Performance of Single-user vs. Multi-user

### 5.6 Comparison of IRS Phase Shift Optimization

Fig. 8 depicts the comparison of IRS phase shift optimization for the suggested model BSCA-CM2Net over conventional methods. The proposed work provides the best robustness with strong secrecy performance, convergence, and scalability, making it suitable for practical deployments under imperfect CSI conditions. The BSCA-CM2Net offers low complexity and provides good convergence for real-time applications. It jointly improves secrecy rate, scalability, and convergence by effectively optimizing beamforming and IRS phase shifts. It provides effective optimization of communication and energy harvesting resources under varying network conditions. Overall, the proposed work achieves the best trade-off and makes it suitable for secure SWIPT systems under realistic channel conditions.

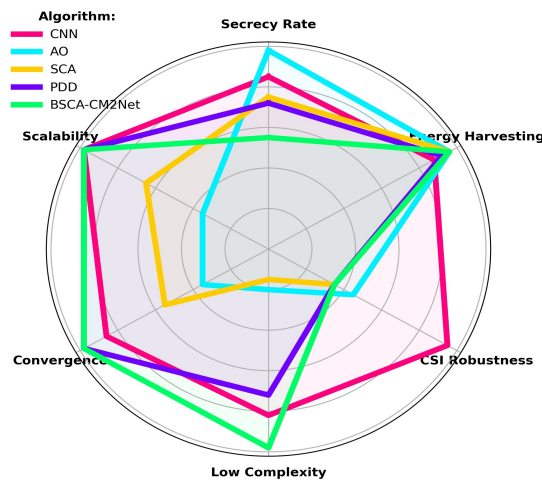


Fig. 8. Comparison of IRS Phase Shift Optimization

### 5.7 Total Harvested Energy vs. Number of Legitimate User Teams

Fig.9 represents the performance evaluation of the total harvested energy with respect to the number of legitimate user teams. As the number of legitimate user teams increases, the total harvested energy improves for all methods due to the increased opportunities for efficient energy transfer. The proposed BSCA-CM2Net consistently achieves the lowest harvested energy across all user configurations. At the 4<sup>th</sup> legitimate user, the proposed BSCA-CM2Net requires lower harvested energy than the conventional methods by approximately 50% and 40% compared with AO and CNN, respectively. The results indicate that the proposed BSCA-CM2Net achieves enhanced energy harvesting performance, improved scalability, and greater computational efficiency. Thus, it makes a promising solution for secure multi-user SWIPT systems and next-generation wireless communication networks.

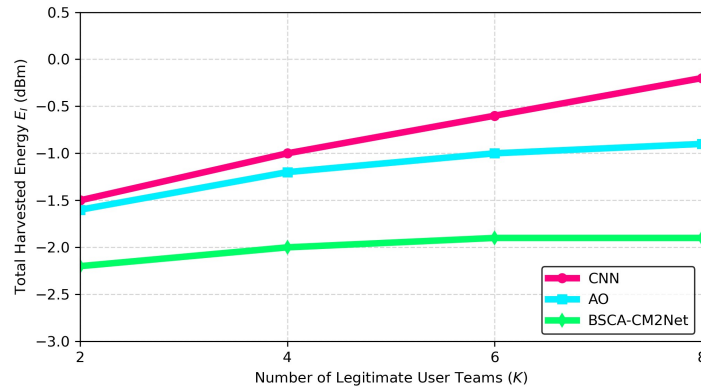


Fig. 9. Comparison of Total Harvested Energy vs. Number of Legitimate User Teams

### 5.8 Sum Secrecy Rate vs. Number of Eavesdropping Teams

Fig.10 indicates the performance evaluation of the SSR with respect to the number of eavesdropping teams. The proposed BSCA-CM2Net consistently achieves the highest secrecy performance across all eavesdropping scenarios. At the 4<sup>th</sup> eavesdropping team, the proposed BSCA-CM2Net achieves a lower SSR than the conventional methods by 98% of CNN, 64% of AO, and 20% of SCA. The results illustrate that the proposed BSCA-CM2Net provides improved robustness, scalability, and secrecy performance for secure multi-user SWIPT wireless communication systems.

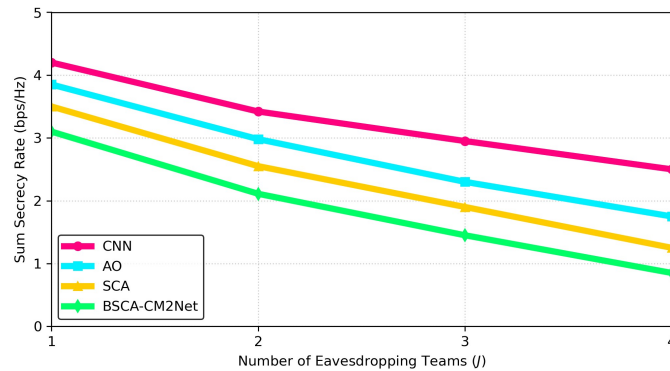


Fig. 10. Comparison of SSR vs. Number of Eavesdropping Teams

### 5.9 Comparison of Average Secrecy Rate for Different Spatial Degree-of-Freedom Array Configurations

Fig.11 shows the comparison of the average secrecy rate for different spatial degree-of-freedom array configurations using the proposed BSCA-CM2Net model and the conventional AO and CNN methods. The proposed BSCA-CM2Net approach consistently achieves the lowest secrecy rate across transmit antenna configurations. Compared with AO and CNN, the BSCA-CM2Net provides enhanced robustness, higher secrecy performance, and improved utilization of spatial resources. Thus, the proposed approach effectively strengthens secure communication by maximizing the secrecy rate under different antenna array sizes.

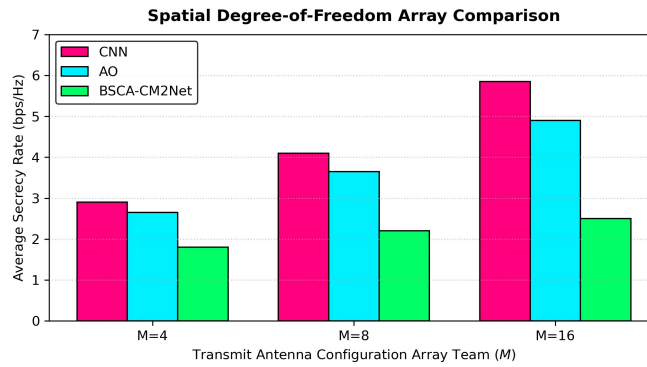


Fig. 11. Comparison of Average Secrecy Rate for Different Spatial Degree-of-Freedom Array Configurations

## 6. Conclusion

This study developed a deep learning-driven framework to enhance secure communication in IRS-assisted SWIPT networks. The wireless communication system's channel input parameters were initialized and sent into the suggested BSCA-CM2Net. The proposed model jointly optimized the transmit beamforming vectors and IRS phase shifts to maximize the secrecy rate, energy harvesting performance, and spectrum efficiency while minimizing computational complexity. The suggested BSCA-CM2Net has shown a better secrecy rate by reducing CNN by 22%, AO by 21%, SCA by 20%, and PDD by 17% at a 0.3 channel estimation error. The results of the experiments showed that the suggested framework fulfilled the requirements for energy harvesting and secrecy while outperforming current techniques in various communication circumstances.

**Limitations and future work:** The suggested BSCA-CM2Net framework has certain drawbacks despite greatly enhancing energy efficiency and secrecy performance. The accuracy of the predicted CSI determines its performance, and inaccuracies in channel estimation could lower optimization performance. Furthermore, the computational complexity during model training is increased when BSCA and CM2Net are combined. In order to lower computational costs without sacrificing optimization accuracy, future research will concentrate on developing lightweight deep learning models. The proposed framework will be further expanded to support wireless communication environments involving multiple users, multiple eavesdroppers, and rapidly changing network conditions.

## References

- [1] Nguyen-Duy-Nhat, V., and Pham, T. V., "Deep learning-driven joint beamforming and phase shift optimization for secrecy communication of IRS-aided SWIPT systems", *Computer Networks*, vol. 282, no. 112280, 2026.
- [2] Shi, W., Wu, Q., Wu, D., Shu, F., and Wang, J., "Joint Transmit and Reflective Beamforming Design for Active IRS-Aided SWIPT Systems", *Chinese Journal of Electronics*, vol. 33, no. 2, pp. 536–548, 2024.
- [3] Zhu, Y., Wu, Q., Guan, X., Zheng, Z., Wang, H., and Chen, W., "Joint Beamforming and Position Optimization for IRS-Aided SWIPT With Movable Antennas", *IEEE Journal on Selected Areas in Communications*, vol. 44, pp. 4982–4996, 2026.
- [4] Liong, H. J., Chiong, C. W., Gopal, L., and Juwono, F. H., "Optimal transmit precoding and phase shift design for intelligent reflecting surface-assisted MIMO SWIPT systems with secrecy consideration", *Digital Signal Processing*, vol. 165, no. 105338, 2025.
- [5] Xu, J., and Shang, P., "Spectral efficiency and secrecy enhancing scheme for IRS-aided SWIPT systems", *Discover Applied Sciences*, vol. 7, no. 79, 2025.
- [6] Huang, C., Chen, W., Wu, Q., Zhu, X., Li, Z., Wang, Y., and Yuan, J., "Dual-IRS aided near-/hybrid-field SWIPT: Passive beamforming and independent antenna power splitting design", *IEEE Transactions on Communications*, vol. 74, pp. 2841–2856, 2025.
- [7] Agarwal, A., "Fairness driven TDMA with joint phase and beamforming optimization for ND-IRS assisted MU-MISO communication systems", *Physical Communication*, vol. 69, no. 102587, 2025.
- [8] Vishwakarma, P., Dhar, S., Bhattacharjee, D., and Sur, S. N., "Energy harvesting efficiency optimization for IRS-assisted MIMO SWIPT system", *Physical Communication*, no. 102904, 2025.

- [9] Cui, W., Zhao, L., Cheng, J., and Gao, H., "Multi-objective joint resource allocation for IRS-assisted SWIPT System with Quantum Sand Cat Swarm Optimization", *AEU-International Journal of Electronics and Communications*, no. 155986, 2025.
- [10] Ma, W., Song, X., Zhao, Y., Yin, Z., Zheng, B., Tang, J., and Yang, Z., "Self-Sustainable IRS-Aided SWIPT: Beamforming Design and Resource Allocation", *IEEE Transactions on Communications*, vol. 74, pp. 2391–2404, 2025.
- [11] Pham-Viet, T., Van-Quang-Binh, N., Do, Q. V., and Koo, I., "Optimizing Energy Harvesting Efficiency for IRS-aided TS-SWIPT System with Continuous and Discrete Phase Shifts", *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, vol. 12, 2025.
- [12] Zhang, C., Qu, S., Zhao, L., Wei, Z., Tang, Q., and Wu, F., "Sustainable IRS-aided integrated sensing and communication system with SWIPT", *Arabian Journal for Science and Engineering*, vol. 50, pp. 12097–12105, 2025.
- [13] Sadia, H., Hassan, A. K., Abbas, Z. H., Abbas, G., Baker, T., and Saeed, N., "Maximizing Energy Efficiency in IRS-Assisted Phase Cooperative PS-SWIPT based Self-Sustainable IoT Network", *IEEE Open Journal of the Communications Society*, 2025.
- [14] Chhea, K., and Lee, J. R., "Enhancing Secure Energy Efficiency of SWIPT IoT Network Considering IRS and Artificial-Noise: A Deep Learning Approach", *IEEE Access*, vol. 13, pp. 63942–63951, 2025.
- [15] Cao, F., Zhang, Q., Han, Z., and Wang, E., "Robust Beamforming Design for RIS-Assisted SWIPT Systems over NOMA Networks", *Engineering Research Express*, 2026.
- [16] Wang, R., Chen, Y., Tay, F. E., and Ang, M. H., "Human-Inspired Compliance Manipulation for Multi-Stiffness Assembly via a Mamba-2-Enhanced Transformer Framework", *IEEE Robotics and Automation Letters*, vol. 10, no. 12, pp. 12349–12356, 2025.
- [17] Xu, X., and Xu, C., "Fusing Geometric and Semantic Features via Cosine Similarity Cross-Attention for Remote Sensing Scene Classification", *Sensors*, vol. 26, no. 1613, 2026.
- [18] Gong, L. H., Chen, Y. Q., Zhou, S., and Zeng, Q. W., "Dual discriminators quantum generation adversarial network based on quantum convolutional neural network", *Advanced Quantum Technologies*, vol. 8, 2025.