2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT) | 979-8-3503-6908-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICEEICT61591.2024.10718409

Intelligent Beamforming for Enhanced Secrecy and Performance in Reconfigurable Intelligent Surfaces

Sivasankar S, Markkandan S
School of Electronics Engineering, Vellore Institute of Technology, Chennai, India
markkandan.s@vit.ac.in

***Abstract*—Intelligent Reflecting Surfaces (IRS) are pivotal in enhancing wireless communication systems by shaping the propagation environment. This study introduces a customized beamforming algorithm for Reconfigurable Intelligent Surface (RIS) setups, aiming to enhance wireless communication security by refining beamforming and IRS configurations. The process involves initializing system parameters, optimizing beamforming vector w and IRS reflection matrix Θ to maximize secrecy rate R_s, while adhering to power and phase shift constraints. Through gradient ascent, the optimization boosts signal strength at the user equipment (UE) while minimizing eavesdropping risks. Simulations demonstrate significant secrecy rate improvements with more reflecting elements, surpassing traditional Physical Layer Security (PLS) and backscatter methods. The proposed scheme effectively counters eavesdropping threats and optimizes resource allocation in multi-user scenarios, providing a robust solution for secure wireless communications.**

***Index Terms*—Intelligent reflecting surfaces, Reflecting Elements, eavesdroppers, Secrecy Rate, beamforming.**

I. Introduction

The emergence of Intelligent Reflecting Surfaces (IRS) is revolutionizing wireless communication systems by optimizing signal propagation through tunable elements managed by a control circuit board. As shown in Figure 1, signals from the base station are reflected by the IRS towards devices, enhancing signal quality and coverage. However, the passive nature of IRS introduces security concerns, potentially enabling eavesdropping attacks.

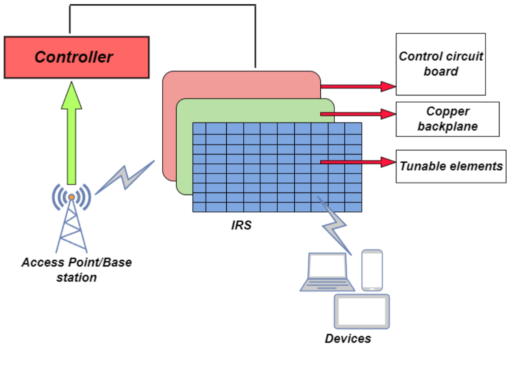

Fig. 1. Architecture of IRS

This research investigates IRS vulnerabilities, proposes mitigation strategies for eavesdropping risks, and evaluates their impact on system performance, aiming to secure wireless networks empowered by IRS[5].

The paper is structured as follows: Section II provides an overview of IRS-based communication systems and eavesdropping attacks, while Section III outlines the problem formulation for secure beamforming. Section IV compares benchmark schemes, and Section V introduces the proposed intelligent beamforming scheme. Section VI presents simulation results and performance analysis, and Section VII concludes the paper.

II. Classification Of Eavesdropping Attacks On IRS

A. Passive and Active Eavesdropping

Passive eavesdropping exploits signal reflections to capture sensitive data using strategically placed devices to intercept unintended signal leakage[1]. Figure 2 illustrates a model where an eavesdropper (Eve) can intercept signals intended for legitimate users.

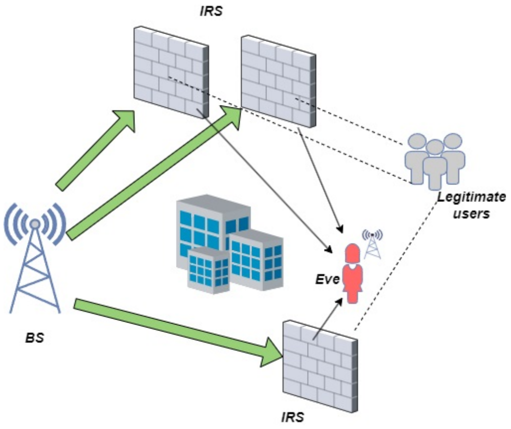

Fig. 2. Eavesdropping attack on IRS

To mitigate this, an AN-aided capacity-threshold on-off transmission scheme is proposed, maintaining communication quality for authorized users and reducing side-lobe leakage. Active eavesdropping uses IRS to intercept or obstruct signals by altering the positions of elements like reflectors or antennas[14]. An active uplink relay station (RS) aided by IRS is suggested to secure transmissions, optimizing power allocation and IRS phase shift to maximize secrecy rates and prevent eavesdropping.

B. Physical layer Authentication using Machine Learning

Legitimate users can authenticate themselves to establish secure communication channels. Encryption techniques can be used to protect the transmitted data, ensuring that even if intercepted, it remains unintelligible to the eavesdropper.The article [4] examines physical layer authentication, where an authenticator distinguishes between a legitimate user and an attacker based on characteristics of parallel wireless channels affected by time-varying fading.Machine learning-based classification methods, like one-class classifiers and binary classifiers, are evaluated.

C. Jamming and Interference

Artificial interference signals are created within the system to hinder eavesdroppers from intercepting and decoding communication. These interference techniques, also known as jamming, pose challenges to wireless communication, as discussed in [7]. The paper explores strategies for secure communication in the presence of jammers and eavesdroppers, focusing on an intelligent reflecting surface (IRS) assisted system. In this system, a base station (BS) endeavors to transmit information reliably to users despite uncertainties about the transmissions of jammers and eavesdroppers.

D. Beamforming and Directional Transmission

Directional beamforming techniques are utilized to concentrate transmitted signals towards intended users, reducing the risk of eavesdropping [11]. This ensures signals reach only authorized recipients, as suggested by [8], who propose using intelligent reflecting surfaces (IRSs) to bolster wireless communication security. Their focus lies on an IRS-assisted setup, where a multi-antenna transmitter communicates with a single-antenna receiver in the presence of potential eavesdroppers. However, the proposed BCD algorithm faces a drawback: IRSs, being passive, are vulnerable to physical attacks like tampering or signal interception.

E. Signal Power Control

Decreasing signal strength beyond a certain threshold can help lower the chance of eavesdropping since intercepted signals become too weak for extracting useful data. Research conducted by scholars in [9] tackles the non-convex aspect of this issue using block coordinate descent (BCD) and minorization maximization (MM) algorithms. Their study indicates that employing these algorithms in IRS-aided NOMA surpasses orthogonal multiple access methods in terms of secrecy rates.

F. Intrusion Detection Systems

Implementing intrusion detection systems (IDS) within the IRS system aids in identifying and tracking potential eavesdroppers by continuously monitoring the network for suspicious activities or unauthorized access attempts.However, the presence of eavesdroppers raises security concerns within the IRS system. Pilot Spoofing Attacks (PSA), discussed by the authors in [15], manipulate channel estimation during the pilot training phase, exploiting the reliance on pilot-assisted channel estimation methods to obtain Channel State Information (CSI). PSA can be seen as a form of intrusion where attackers manipulate the channel estimation process to deceive the system. IDS plays a vital role in detecting and preventing such intrusions; however, detecting PSA in IRS-assisted systems presents significant challenges.Table 1 presents a summary of optimization approaches for secured communications in intelligent surface-aided communications.

III. Problem Formulation and System Model

Consider a wireless communication system with a base station (BS) equipped with N antennas, an Intelligent Reflecting Surface (IRS) composed of $M = M_h \times M_v$ reflecting elements, a legitimate receiver (User Equipment, UE), and one or more eavesdroppers.The received signal at the UE can be expressed as

$$y_{\text{UE}} = \left(\alpha_c \mathbf{h}_{iu}^H \Theta \mathbf{H}_{bi} + \alpha_d \mathbf{h}_{bu}^H\right) \mathbf{w} s + n \tag{1}$$

where

- α_d and α_c denote the path losses for the direct BS-UE link and the BS-IRS-UE cascaded link, respectively.
- $\mathbf{h}_{iu} \in \mathbb{C}^{1\times M}$ is the IRS-UE channel vector.
- $\mathbf{H}_{bi} \in \mathbb{C}^{M\times N}$ represents the BS-IRS channel matrix.
- $\mathbf{h}_{bu} \in \mathbb{C}^{1\times N}$ denotes the BS-UE channel vector.
- $\mathbf{w} \in \mathbb{C}^{N\times 1}$ is the beamforming vector at the BS.
- s is the transmitted data with zero mean and unit variance.
- $n \sim \mathcal{CN}(0, \sigma^2)$ is the additive white Gaussian noise.
- $\Theta = \text{diag}(\xi) e^{j\theta}$ is the diagonal matrix of the IRS reflection coefficients.

The received signal at an eavesdropper (Eve) is given by

$$y_{\text{Eve}} = \left(\alpha_{ce} \mathbf{h}_{ie}^H \Theta \mathbf{H}_{bi} + \alpha_{de} \mathbf{h}_{be}^H\right) \mathbf{w} s + n_e \tag{2}$$

where the subscript e refers to parameters associated with the eavesdropper. The objective is to maximize the secrecy rate by optimizing the beamforming vector $\mathbf{w}$ and the IRS reflection matrix Θ. The secrecy rate R_s is defined as

$$R_s = \max\{R_{\text{UE}} - R_{\text{Eve}}, 0\} \tag{3}$$

where R_{UE} and R_{Eve} are the achievable rates at the UE and the eavesdropper, respectively.

IV. Comparison Strategies

This section compares two benchmark strategies: the Conventional IRS-Based Physical Layer Security (PLS) strategy and the IRS Backscatter-Aided Anti-Eavesdropping strategy.

A. Conventional IRS-Based PLS Strategy

This strategy utilizes an IRS to passively reflect signals, enhancing security by maximizing the legitimate user's signal-to-noise ratio (SNR) while minimizing the eavesdropper's SNR. The received signal at the user y_u and eavesdropper y_e are modeled as

$$y_u = (H_{su} + H_{ru}H_{sr})w_s + H_{ju} + H_{ru}H_{jr}v_z + n_u \tag{4}$$

$$y_e = (H_{se} + H_{re}H_{sr})w_s + n_e \tag{5}$$

TABLE I
OPTIMIZATION APPROACHES SUMMARY

Approach	Challenges	Algorithm	Ref.
Joint optimization of active transmit beamforming at AP and passive reflect beamforming at IRS	Limited secrecy in correlated channels, weaker legit communication compared to eavesdropping.	Alternating optimization with semidefinite relaxation.	[2]
ML-based channel estimation	Managing device influx, MIMO, beamforming in 5G, dynamic channel traits.	Backpropagation Neural Network for supervised channel estimation.	[3]
IRS-based Non-Orthogonal Multiple Access	Ensuring security, overcoming obstacles.	AF relay technique, cooperative jamming.	[5],[9]
Uplink Rate Splitting (RS)	Eavesdropping threat mitigation.	Alternating Optimization for power, receiver filter, IRS precoding.	[12]
Three-Step Training (TST) Scheme	Handling uncertain channel info for spoofing attack detection.	TST with two-way and additive pilot training stages.	[13]

B. IRS Backscatter-Aided Anti-Eavesdropping Strategy

This strategy incorporates active backscattering and artificial noise (AN) to impair the eavesdropper's channel. The received signals for the user y_u and eavesdropper y_e are described as

$$y_u = H_{su}w_s + H_{ru}H_{sr}w + H_{jr}v_a + H_{ju}v_z + n_u \tag{6}$$

$$y_e = H_{se}w_s + H_{re}H_{sr}w + H_{jr}v_a + n_e \tag{7}$$

Both strategies have their limitations. The Conventional IRS-Based PLS strategy relies on passive reflection, limiting its ability to actively interfere with the eavesdropper's channel. The non-convex optimization problem involving joint optimization of beamforming vectors and IRS phase shifts is computationally intensive and complex. The IRS Backscatter-Aided Anti-Eavesdropping strategy uses active backscattering and AN, which adds complexity and potential interference management issues. The inclusion of AN requires careful design to avoid affecting the legitimate user's signal, increasing overall system complexity[6]. Active components lead to higher power consumption and hardware complexity compared to passive IRS. Both strategies face challenges in adapting to varying channel conditions and ensuring robust security in dynamic environments.

V. PROPOSED ALGORITHM: INTELLIGENT BEAMFORMING SCHEME (IB SCHEME)

A. Initialization

Set initial system parameters, including the number of iterations, locations of BS, IRS, UE, and eavesdropper(s), and the path loss values.

B. Optimization of Beamforming Weights

Algorithm 1 Optimization of Beamforming Weights

```
    Initialize $\mathbf{w}$ and $\Theta$. Iteratively optimize $\mathbf{w}$ and $\Theta$ to maximize the secrecy rate $R_s$:
        $\max_{\mathbf{w},\Theta} R_s$                                                  (8)
    subject to:
        $\|\mathbf{w}\|^2 \leq P_{\text{max}},$                                        (9)
        $0 \leq \xi_m \leq 1,$                                                      (10)
        $\theta_m \in \left\{0, \frac{2\pi}{K}, \ldots, \frac{2\pi(K-1)}{K}\right\}, \quad \forall m.$   (11)
    convergence
```

here, P_{max} is the maximum transmission power, and $K = 2^B$ where B is the number of bits for phase shifts.

1) Step-by-Step Optimization Process:

- **Initialization Parameters:** Initialize system parameters such as the number of antennas at the BS (N), the number of reflecting elements at the IRS (M), and the path loss values for the different links (α_d, α_c, etc.).
- **Initial Values:** Start with initial values for the beamforming vector $\mathbf{w}$ and the IRS reflection matrix Θ.

2) Objective Function: The goal is to maximize the secrecy rate R_s, which is defined as

$$R_s = \max\{R_{UE} - R_{Eve}, 0\} \tag{12}$$

where R_{UE} and R_{Eve} are the achievable rates at the UE and the eavesdropper, respectively.

3) Achievable Rates: The channel gains and SNR calculations for the eavesdropper scenario are given by the following expressions

$$H = \alpha_{ch} H_{iu} \Theta H_{bi} + \alpha_{dh} H_{bu} \tag{13}$$

$$H_{\text{Eve}} = \alpha_{ce} H_{ie} \Theta H_{bi} + \alpha_{de} H_{be} \tag{14}$$

$$\text{SNR}_{\text{UE}} = \frac{|H\mathbf{w}|^2}{\sigma^2} \tag{15}$$

$$\text{SNR}_{\text{Eve}} = \frac{|H_{\text{Eve}}\mathbf{w}|^2}{\sigma^2} \tag{16}$$

Detailed Derivation

Step 1: Reformulating the Problem

Given the problem

$$\begin{aligned} \text{minimize} \quad & \sigma_u^2 \text{Tr}(X_u U^H H_u H_u^H U) \\ & - \sigma_u \text{Tr}(X_u H_u H_u^H U) \\ & - \sigma_u \text{Tr}(X_u U^H H_u U) \\ & + \sigma_e^2 \text{Tr}(X_e H_e H_e^H) = 0 \end{aligned}$$

$$\text{Subject to:} \quad \|w\|^2 \le P_t$$

Step 2: Lagrangian Formulation

Introducing the Lagrange multiplier β, the Lagrangian function for the problem is

$$\begin{aligned} f(\mathbf{w}, \beta) = \; & \sigma_u^2 \, \text{Tr}(X_u U^H H_u^H H_u U) - \sigma_u \, \text{Tr}(X_u H_u^H U) \\ & - \sigma_u \, \text{Tr}(X_u U^H H_u) + \sigma_e^2 \, \text{Tr}(X_e H_e^H H_e) \\ & + \beta(\mathbf{w}^H \mathbf{w} - P_t) \end{aligned} \tag{17}$$

Step 3: Deriving the Optimal Beamforming Vector

To find the optimal $\mathbf{w}$, we take the derivative of $f(\mathbf{w}, \beta)$ with respect to $\mathbf{w}$ and set it to zero

$$\frac{\partial f(\mathbf{w}, \beta)}{\partial \mathbf{w}} = 0 \tag{18}$$

Solving this yields

$$\begin{aligned} w^\circ = & \left(\beta I + A_u^H U X_u U^H A_u + A_e^H X_e A_e\right)^{-1} \\ & \times \left(A_u^H U X_u - A_u^H U X_u U^H B_u\right) \end{aligned} \tag{19}$$

where:

$$A_u = \sigma_u (H_{su} + H_{ru} H_{sr}), \quad B_u = \sigma_u (H_{ru} H_{jrv}) \tag{20}$$

$$A_e = \sigma_e (H_{se} + H_{re} H_{sr}), \quad B_e = \sigma_e (H_{re} H_{jrv}) \tag{21}$$

Step 4: Optimization Using Bisection Method for β

The optimal β can be found using a bisection search method to satisfy the power constraint

$$\text{Tr}(\mathbf{w}\mathbf{w}^H) = P_t \tag{22}$$

Step 5: Iterative Optimization Using Gradient Ascent

We now use the closed-form solution $\mathbf{w}^\circ$ as the initial beamforming vector and iteratively optimize $\mathbf{w}$ using gradient ascent to maximize the secrecy rate R_s.

Objective Function: The secrecy rate R_s is given by

$$R_s = \max\{R_{UE} - R_{Eve}, 0\} \tag{23}$$

where:

$$R_{UE} = \log_2 \left(1 + \frac{|H\mathbf{w}|^2}{\sigma^2}\right) \tag{24}$$

$$R_{Eve} = \log_2 \left(1 + \frac{|H_{\text{Eve}}\mathbf{w}|^2}{\sigma^2}\right) \tag{25}$$

Gradient Calculation: The gradient of R_s with respect to $\mathbf{w}$ is

$$\nabla_{\mathbf{w}} R_s = \frac{\partial R_s}{\partial \mathbf{w}} \tag{26}$$

Update Rule: The beamforming vector $\mathbf{w}$ is updated iteratively using

$$\mathbf{w}(t+1) = \mathbf{w}(t) + \eta \nabla_{\mathbf{w}} R_s \tag{27}$$

where η is the step size.

Step 6: Iterative Optimization Algorithm

Combine the closed-form solution $\mathbf{w}^\circ$ with the iterative optimization steps. The algorithm is as follows

1) Initialize $\mathbf{w}$ with $\mathbf{w}^\circ$ and set the system parameters.
2) Compute the closed-form solution $\mathbf{w}^\circ$.
3) Iteratively update $\mathbf{w}$ using gradient ascent:
   a) Calculate R_{UE} and R_{Eve}.
   b) Compute the gradient $\nabla_{\mathbf{w}} R_s$.
   c) Update $\mathbf{w}$ using the gradient ascent rule: $\mathbf{w}(t+1) = \mathbf{w}(t) + \eta \nabla_{\mathbf{w}} R_s$
4) Check for convergence:
   a) If the change in R_s is below a predefined threshold, stop.
   b) Otherwise, repeat step 3.

Detailed Derivation of Gradient $\nabla_{\mathbf{w}} R_s$

To explicitly compute the gradient $\nabla_{\mathbf{w}} R_s$, we need to consider the derivatives of the secrecy rate components For R_{UE}

$$\nabla_{\mathbf{w}} R_{UE} = \frac{1}{\ln(2)} \cdot \frac{H^H H \mathbf{w}}{\sigma^2 + |H\mathbf{w}|^2} \tag{28}$$

For R_{Eve}

$$\nabla_{\mathbf{w}} R_{Eve} = \frac{1}{\ln(2)} \cdot \frac{H_{\text{Eve}}^H H_{\text{Eve}} \mathbf{w}}{\sigma^2 + |H_{\text{Eve}}\mathbf{w}|^2} \tag{29}$$

Thus, the gradient $\nabla_{\mathbf{w}} R_s$ is

$$\nabla_{\mathbf{w}} R_s = \nabla_{\mathbf{w}} R_{UE} - \nabla_{\mathbf{w}} R_{Eve} \tag{30}$$

Substituting the gradients

$$\nabla_{\mathbf{w}} R_s = \frac{1}{\ln(2)} \left(\frac{H^H H \mathbf{w}}{\sigma^2 + |H\mathbf{w}|^2} - \frac{H_{\text{Eve}}^H H_{\text{Eve}} \mathbf{w}}{\sigma^2 + |H_{\text{Eve}} \mathbf{w}|^2} \right) \tag{31}$$

Iterative Update Using Gradient Ascent: With $\nabla_{\mathbf{w}} R_s$ computed, the update rule becomes

$$\begin{aligned} w(t+1) = w(t) + \eta \cdot \frac{1}{\ln(2)} \Bigg(& HH^H H_w(t) \frac{\sigma^2}{\sigma^2 + |Hw(t)|^2} \\ & - HH_{\text{Eve}}^H H_{\text{Eve}} w(t) \frac{\sigma^2}{\sigma^2 + |H_{\text{Eve}} w(t)|^2} \Bigg) \end{aligned} \tag{32}$$

By combining the closed-form solution $\mathbf{w}^\circ$ derived from the Lagrangian method with the iterative gradient ascent optimization, we effectively optimize the beamforming vector $\mathbf{w}$ to maximize the secrecy rate R_s. This approach ensures that the initial solution is refined iteratively, leveraging both analytical and numerical optimization techniques.

TABLE II
EVALUATION STEPS

Parameters	Range
Number of reflecting elements	10 to 100
Number of eavesdroppers	1 to 10
Number of legitimate users	1 to 10
Carrier frequency	800 MHz
Path loss at 1 meter	-30 db
Base station location	(10,0,10)
IRS location	(5,67,2)
Eavesdropper location	(10,60,5)

C. Novelty

The proposed IB Scheme optimizes beamforming and IRS reflection coefficients together to maximize secrecy rate, unlike conventional methods. It actively combines techniques and employs intelligent iterative optimization for dynamic adjustments, improving security against eavesdroppers. Leveraging gradient ascent for beamforming and discrete optimization for IRS coefficients ensures strong signals at the legitimate receiver while minimizing leakage to eavesdroppers, offering a robust solution to wireless security challenges.Table II outlines the parameters and their ranges for the evaluation steps. Reflecting elements range from 10 to 100, eavesdroppers from 1 to 10, and legitimate users from 1 to 10. The carrier frequency is set at 800 MHz, and the path loss at 1 meter is -30 dB. The base station is located at (10,0,10), the IRS at (5,67,2), and the eavesdropper at (10,60,5)[10]. These parameters define the evaluation setup.

VI. Simulated Results

The impact of the number of reflecting elements on secrecy rates in a wireless communication system is assessed. The setup includes a transmitter, a legitimate receiver, and an eavesdropper, with an IRS positioned between the transmitter and receiver to enhance secrecy.

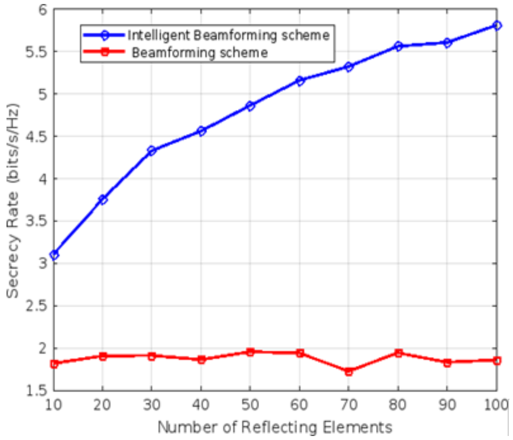

Fig. 3. *Secrecy rate vs Number of reflecting elements*

Simulations in Fig. 3 adjust the number of reflecting elements from 10 to 100, keeping other factors constant. Secrecy rates are calculated based on the difference between data rates received by the legitimate receiver and the eavesdropper.

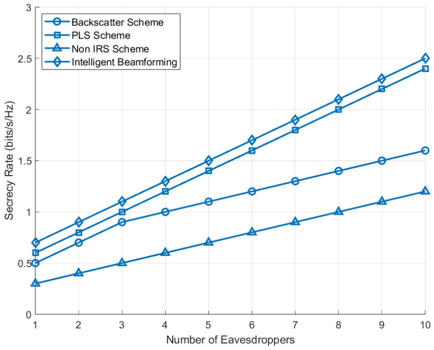

Fig. 4. *Secrecy rate vs Number of eavesdroppers*

The simulation reveals that secrecy rates notably improve with an increased number of reflecting elements. Our proposed intelligent beamforming (IB) scheme outperforms other techniques like PLS and backscatter, owing to boosted signal strength at the receiver and controlled signal degradation at the eavesdropper via IRS-based intelligent beamforming.Simulations are conducted with varying numbers of reflecting elements and eavesdroppers (1 to 10) as illustrated in Figure 4.This study explores the impact of eavesdropper quantity on the secrecy rate in a wireless communication system.Figure 5 illustrates the impact of the number of base station antennas (ranging from 1 to 16) on secrecy rates. As the number of antennas increases, secrecy rates improve significantly across various schemes, with intelligent beamforming reaching 5.8 bits/s/Hz at 14 antennas. In comparison, Backscatter, PLS, and non-IRS schemes achieve lower rates of 4, 2.8, and 2 bits/s/Hz respectively.

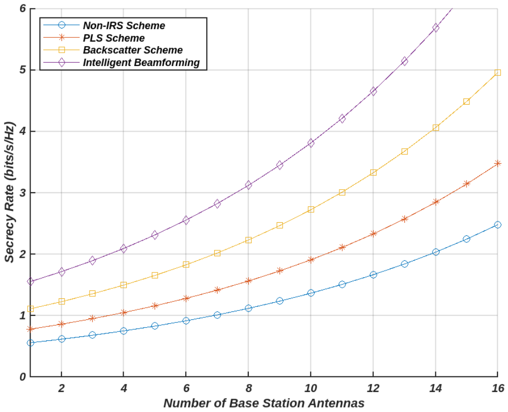

Fig. 5. *Secrecy rate vs Number of base station antennas*

Secrecy rates are measured at the legitimate receiver across various SNR values. Expectedly, secrecy rates rise with more eavesdroppers due to increased interference and interception risks.The impact of the number of legitimate users on the signal-to-noise ratio (SNR) in wireless communication systems, with multiple reflecting elements and a fixed number of eavesdroppers, is examined.Figure 6 shows simulation results for 1 to 10 legitimate users. As more users join, the total transmitted power is divided, decreasing SNR and increasing bit error rates due to resource limitations and heightened interference. Effective resource allocation and interference management are essential to maintain satisfactory SNR levels in multi-user environments.

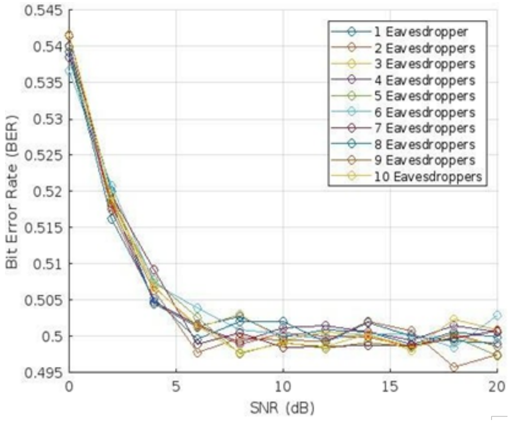

Fig. 6. *BER vs SNR for different eavesdropper scenarios*

VII. Conclusion

Simulations demonstrate the effectiveness of the proposed Intelligent Beamforming (IB) scheme in boosting the secrecy rate of IRS-assisted wireless communication systems. Increasing the number of reflecting elements significantly enhances signal strength at the legitimate receiver while degrading it at the eavesdropper. The scheme remains robust against multiple eavesdroppers and underscores the importance of efficient resource allocation with more legitimate users. Outperforming conventional strategies, the IB scheme dynamically adjusts beamforming vectors and IRS reflection coefficients to maximize the secrecy rate. Future research should integrate larger antenna arrays and adapt to diverse conditions and attack scenarios to ensure robust physical layer security.

References

[1] H. Wang et al., ”Resisting Malicious Eavesdropping: Physical Layer Security of mmWave MIMO Communications in Presence of Random Blockage,” in IEEE Internet of Things Journal, vol. 9, no. 17, pp. 16372-16385, 1 Sept.1, 2022, doi: 10.1109/JIOT.2022.3153054.

[2] M. Cui, G. Zhang, and R. Zhang, “Secure wireless communication via intelligent reflecting surface,” IEEE Wireless Commun. Lett., vol. 8, no. 5, pp. 1410–1414, Oct. 2019.

[3] R. Uma Mageswari, Gousebaigmohammad, Devee Siva Prasad Dulam, S. Shitharth, G. Surya Narayana, A. Suresh, Jaikumar R, Leena Bojaraj, S. Chandragandhi, Amsalu Gosu Adigo, ”Machine Learning Empowered Accurate CSI Prediction for Large-Scale 5G Networks”, Wireless Communications and Mobile Computing, vol. 2022.

[4] L. Senigagliesi, M. Baldi, E. Gambi, ”Comparison of Statistical and Machine Learning Techniques for Physical Layer Authentication”, IEEE Transactions on Information Forensics and Security, 2020.

[5] A. Souzani, M. A. Pourmina, P. Azmi and M. Naser-Moghadasi, ”Physical Layer Security Enhancement via IRS Based on PD-NOMA and Cooperative Jamming,” in IEEE Access, vol. 11, pp. 65956-65967, 2023, doi: 10.1109/ACCESS.2023.3290104.

[6] X. Guan, Q. Wu, and R. Zhang, “Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?” IEEE Wireless Commun. Lett., vol. 9, no. 6, pp. 778–782, Jun. 2020.

[7] Y. Sun, K. An, J. Luo, Y. Zhu, G. Zheng and S. Chatzinotas, ”Intelligent Reflecting Surface Enhanced Secure Transmission Against Both Jamming and Eavesdropping Attacks,” in IEEE Transactions on Vehicular Technology, vol. 70, no. 10, pp. 11017- 11022, Oct. 2021, doi: 10.1109/TVT.2021.3104580

[8] X. Yu, D. Xu and R. Schober, ”Enabling Secure Wireless Communications via Intelligent Reflecting Surfaces,” 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 2019, pp. 1-6, doi: 10.1109/GLOBECOM38437.2019.9014322.

[9] Y. Pei, X. Yue, Y. Yao, X. Li, H. Wang, and D.-T. Do. ”Secrecy communications of intelligent reflecting surfaces aided NOMA networks,” Phys. Commun., vol. 52, 2022.

[10] B. Ling, J. Lyu and L. Fu, “Placement Optimization and Power Control in Intelligent Reflecting Surface Aided Multiuser System,” 2021 IEEE Global Communications Conference (GLOBECOM), 2021.

[11] Y. Cao, S. Xu, J. Liu and N. Kato, ”IRS Backscatter Enhancing Against Jamming and Eavesdropping Attacks,” in IEEE Internet of Things Journal, vol. 10, no. 12, pp. 10740-10751, 2023, doi: 10.1109/JIOT.2023.3241839.

[12] J. Zhou, W. Hou, Y. Mao and C. Tellambura, ”Securing Medical Sensor Data: A Novel Uplink Scheme With Rate Splitting and Active Intelligent Reflecting Surface,” in IEEE Communications Letters, vol. 28, no. 3, pp. 493-497, March 2024, doi: 10.1109/LCOMM.2024.3359064.

[13] X. Liu, Y. Tao, C. Zhao and Z. Sun, ”Detect Pilot Spoofing Attack for Intelligent Reflecting Surface Assisted Systems,” in IEEE Access, vol. 9, pp. 19228-19237, 2021, doi: 10.1109/ACCESS.2021.3054821.