International Journal of Trendy Research in Engineering and Technology
Volume 10 Proceedings of RISET-26
ISSN No. 2582-0958

Proceedings of 3rd International Conference RISET-2026 held at Yogananda College of Engineering &Technology (YCET), Jammu held on 13th of May, 2026

ENHANCED PHYSICAL LAYER SECURITY IN IRS-ASSISTED MISO COMMUNICATION SYSTEM

Kritika Upadhyay, Shashi Ranjan Kumar, Manisha Bharti

Department of Electronics & Communication Engineering, National Institute of Technology Delhi, Delhi, India
Corresponding Author: Kritika Upadhyay. kritikaupadhyay@nitdelhi.ac.in

ABSTRACT

The focus of this research is the examination of how a large number of infrared transmitters (IRS), when used together with an oversized MISO transmit beamforming vector, can improve the overall capacity of wireless communications to provide them with more secure communication pathways by increasing the amount of secrecy available. The proposed process of creating the optimal amount of secrecy-rate maximization is achieved through a joint optimisation approach with realistic channel models, that conducts numerical analysis and simulation of the proposed processes. The results of the simulations conducted within this process have shown that IRS-Assisted Wireless Systems offer a greater level of secrecy capacity and have increased energy efficiency than conventional methods. The results demonstrate that IRS-Assisted Wireless Systems could be utilised in next generation secure wireless communication.

Keywords: Beamforming, Intelligent Reflecting Surface, MISO Systems, Physical Layer Security

I. INTRODUCTION

With the rapid advancement of Wireless Communication technologies toward Ultra-High Data Rate, Low Latency and Energy Efficient provides a challenge of having Secure and Reliable Transmission. The ability of Wireless Channels to be Broadcast means that they are vulnerable to Eavesdropping and thus creates serious Security Risks. Physical Layer Security (PLS) has received increasing interest as a viable method of stopping Information Theft because it takes advantage of the properties of Wireless Channels. Compared to conventional Encryption Techniques, PLS provides several advantages, including [1,2] a lower level of complexity, no requirement for Keys, and the potential to enhance existing Security Techniques [3,4]. The principles of PLS were first proposed by Shannon [5] and later formalized by Wyner [6] using the concept of Wiretap Channels. More recently, Intelligent Reflecting Surfaces (IRS) are considered a feasible solution for significantly increasing the Quality of Received Signal at the Destination Receiver [7].

Several methods, including traditional beamforming [8-10] and artificial noise (AN) generation [11-13], can be employed in physical layer security to guarantee secure communication, particularly in situations when there is a direct line of communication between the end users and the transmitter (Tx). Additionally, using Intelligent Reflecting Surface (IRS) technology can improve wireless systems' secrecy performance even more. By strategically deploying IRS within the signal propagation environment, it is possible to improve the overall system performance [14]. In recent years, several studies have explored the use of IRS to evaluate and improve the security aspects of wireless communication systems

Previous research has explored IRS applications in [15,16] secure transmission, such as a system for mm-Wave and THz bands. Some studies have investigated IRS-assisted transmission without requiring eavesdropper channel state information, proposing joint beamforming and jamming to minimize transmit power and improve receiver performance. Other work has focused on [17] IRS-aided MISO wireless systems in the presence of strong eavesdropper links and robust secure beamforming for [18] IRS-assisted mm-Wave systems with multiple eavesdroppers.[19] IRS has also been utilized to facilitate data transmission to multiple users while preventing information leakage, and to minimize transmit power for multi-user scenarios under SINR constraints. Additionally, IRS-assisted solutions have been developed to maximize secrecy in scenarios with a single legitimate user antenna and multiple eavesdropper antennas [20,21].

In this work, we propose an IRS-assisted approach to ensure secure communication for a legitimate user, especially in scenarios where the line-of-sight (LoS) path is blocked. The system setup includes a multi-antenna transmitter and single-antenna users, forming a MISO configuration. In order to maximize the signal intensity at the intended user and minimize it at the eavesdropper, we create a cooperative beamforming approach. This beamformer combines techniques like Maximal Ratio Transmission (MRT) [22] with traditional Zero-Forcing (ZF) beamforming [19].

By combining IRS with beamforming, the proposed method increases security by reducing exposure to potential eavesdroppers and more precisely directing the signal to the authorized user. We evaluate this method against standard approaches such as MRT and ZF, using performance metrics

like channel capacity and secrecy capacity under Rayleigh fading conditions. Simulation results are also provided to show how the number of transmit antennas and IRS elements influence the system's secrecy performance.

II. Communication Model and Confidentiality Metrics

Fig. 1 illustrates a secure wireless communication system enhanced by an Intelligent Reflecting Surface (IRS) in a Multiple-Input Single-Output (MISO) setup. A 5G base station attempts to transmit data to a legitimate receiver, but a direct path is blocked by an obstacle. The IRS, which has several reflecting elements (referred to as M elements), is used to reroute the signal in order to get around this. The IRS receives the signal through the channel denoted by H and, using the best phase shifts, smartly reflects it toward the approved receiver through the channel g^T to increase signal strength and security. The IRS is configured to weaken the signal in this direction, decreasing the likelihood of interception, even while an eavesdropper simultaneously receives a signal via channel k^T. This setup shows how IRS technology may deliberately reroute signals to improve secrecy performance, especially when direct communication is hindered by physical constraints.

In this configuration, the base station sends the information to an IRS, which reflects it towards the legitimate receiver. The path between the BS and IRS is modeled by the channel matrix H, while the path to the legitimate user and eavesdropper are modeled by the vectors gT and kT, respectively. The eavesdropper (also known as an attacker) has one antenna and attempts to listen to the communication between the BS and IRS. The IRS must help to increase the composite signal received by the legitimate receiver as well as reduce the amount of signal that goes directly to the eavesdropper.

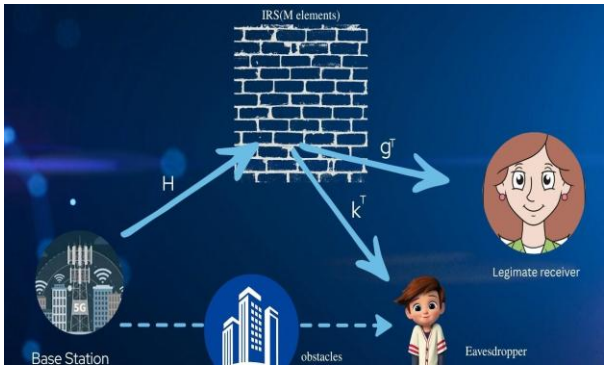

Figure 1: MISO System Setup

This model will provide insight into the potential for secure transmission of signals and the maximum secrecy capacity in the case where direct paths between receivers have been obstructed or are subject to interception.

The eavesdropper signal and the legitimate signal are expressed as follows:

1. Legitimate User's Received Signal (Y_L):

$$\boldsymbol{Y_L}^T = (g^T \Theta H) w \sqrt{P_{tx}} x + N_L \quad \textbf{(1)}$$

g^T : Channel vector (IRS → Bob).

H : Channel matrix (BS → IRS)

θ = diag($\beta 1 e^{j\theta 1}$,...,$\beta M e^{j\theta} M$): IRS reflection matrix.

w: Beamforming vector at BS

P_{tx}: Transmit power,

x: Transmitted signal, *NL*: Noise at Bob.

2. Eavesdropper's Received Signal (Y_E):

$$Y_E{}^T = (k^T \theta H) w \sqrt{P_{tx}}\, x + N_E \quad \textbf{(2)}$$

i) k^T : Channel vector (IRS → Eve).

ii) N_E : Noise at Eve.

Analysis of Beamforming Approaches for Secrecy Enhancement

The highest speed at which an authorized user can safely send data, even in the presence of an eavesdropper, is known as secrecy capacity. It guarantees the confidentiality of the data while it is being transmitted. The legal channel capacity is the highest data rate that the intended recipient can reliably achieve, whereas the eavesdropper channel capacity represents the highest rate at which the data could potentially be intercepted. With just one antenna, the eavesdropper tries to listen in on the conversation. In order to maximize signal intensity at the authorized recipient and reduce signal leakage toward the eavesdropper, the IRS is essential.

Maximum Ratio Transmission (MRT) is a beamforming technique employed by the transmitter to enhance the signal-to-noise ratio (SNR) for authorized users [23]

$$w_{MRT} = \frac{(C_L{}^T)^*}{||C_L{}^T||} \quad (3)$$

where $C_L{}^T = g^T \Theta H$

||.|| represents the Euclidean norm.

The secrecy capacity for MRT based scheme is thus given as:

Secrecy Capacity for MRT:

$$C_s = log_2(1 + \frac{P_{tx}|C_L{}^T w_{MRT}|^2}{\sigma_L{}^2}) - log_2(1 + \frac{P_{tx}|C^T{}_E w_{MRT}|^2}{\sigma^2{}_E}) \quad (4)$$

ZF Beamforming: A signal processing method called ZF ensures that no transmitted signal reaches the eavesdropper. It places the beamforming vector in the "null space" of the eavesdropper's channel so that the eavesdropper receives nearly nothing. This is achieved by making the transmitted signal orthogonal to the eavesdropper's channel. The formula for secrecy capacity in the ZF approach takes into account this design, ensuring maximum signal strength at the legitimate user while completely blocking it from the eavesdropper.

$$CE^T W_{ZF}[25]=0;$$

where $C_E{}^T = k^T \theta H$

Secrecy Capacity for ZF:

$$C_s = log_2(1 + \frac{P_{tx}|C_L{}^T w_{ZF}|^2}{\sigma_L{}^2}) - log_2(1 + \frac{P_{tx}|C^T{}_E w_{ZF}|^2}{\sigma^2{}_E}) \quad (5)$$

Limitation of ZF Beamforming:

The main drawback of this method is that it only tries to block the signal from reaching the eavesdropper, without paying attention to how strong the signal is for the legitimate user. As a result, the overall security performance can suffer—especially when the transmit power is low.

III. SYSTEM DESIGN AND IMPLEMENTATION

In this section, we focus on increasing the secrecy rate of the communication system, assuming that the transmitter has complete channel state information. Equation (3) illustrates that the secrecy capacity can be improved by incrementing the transmission rate to the authorized user and reducing the amount of information lost to any eavesdropper. This has already been studied using individual beamforming techniques like Maximum Ratio Transmission (MRT) and Zero-Forcing (ZF)[24]. ZF may weaken the intended signal while attempting to remove the eavesdropper's signal. In contrast, MRT primarily increases the authorized user's signal without taking the eavesdropper into account. We suggest a novel beamforming approach that combines the advantages of ZF and MRT in order to overcome this trade-off. In a scenario where the direct line-of-sight (LoS) path is obstructed, we incorporate an Intelligent Reflecting Surface (IRS) to assist communication in a non-line-of-sight (NLoS) environment. Our proposed solution—referred to as a joint beamforming scheme— simultaneously boosts the legitimate user's signal and suppresses potential information leakage to eavesdroppers, thus achieving more secure wireless transmission.

The joint beamformer combines the strengths of MRT and ZF:

$$W_{COM} = \alpha W_{MRT} + \beta \hat{W}_{ZF} \quad (6)$$

where the complex weighting coefficients that require optimization are denoted by α and β.

The beamforming parameter $\hat{W}_{ZF}$ is given as [25]:

$$\widehat{W_{ZF}} = \frac{S(:,1)}{||S(:,1||}$$

The optimization challenge is to maximize the secrecy capacity using the joint beamformer W_{COM} while optimizing the complex weights α and β.

$$\max \alpha,\beta \quad C_s(W_{COM}), \quad (7)$$

$$\text{Subject to } ||\alpha^2|| + ||\beta^2|| \leq 1$$

where

$$C_s(w_{COM}) = log_2(1 + \frac{P_{tx}|C_L{}^T w_{COM}|^2}{\sigma_L{}^2}) - log_2(1 + \frac{P_{tx}|C^T{}_E w_{COM}|^2}{\sigma^2{}_E})$$

The exhaustive search technique finds the optimal values of complex weights α and β.

IV. RESULTS AND DISCUSSION

In order to evaluate the performance of the suggested joint beamforming system using MATLAB, we offer the simulation results. The approach of simulation-based validation, similar to methodologies used in [25], ensures a detailed comparative analysis of beamforming strategies.

The secrecy capacity (measured as bits/second/Hertz) is assessed over a range of transmit power for three distinct techniques of signal transmission; namely, Joint Beamforming, ZF (Zero Forcing), and MRT (Maximum Ratio Transmission). The vertical axis depicts safe secret data transfer and the horizontal axis depicts transmit power, ranging from 0 to 50 dBm. Clearly illustrated by the red line, ZF beamforming continues to provide the greatest increase in secrecy capacity as power levels are increased. This suggests that ZF prevents eavesdroppers from receiving signals, and as such provides a very high level of security for those using it. By contrast, the blue line, representing MRT, shows minimal changes in secrecy capacity even though power increases dramatically.

In fact, the black line for Joint Beamforming hovers consistently between 2.5and 3 bits/s/Hz with very minor oscillations. Therefore, it is very clear from the above that the right choice of beamforming technique is extremely important, especially for solutions involving IRS or MISO; ZF provides

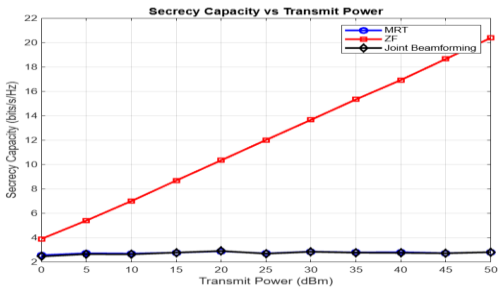

Figure 2: Secrecy Capacity vs. Transmit Power.

users of these solutions with greater security and is therefore, the most superior technique of the three. The benefits seen with the Joint Beamforming technique occur from the combination of both MRT and ZF techniques. However, the MRT technique's secrecy capacity remains largely unaltered since it just focuses on boosting the authorized user's signal while disregarding the eavesdropper's channel.

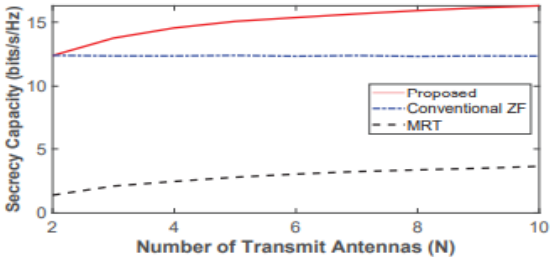

Figure 3**:** Secrecy capacity varying with transmit antenna

In order to further confirm the effectiveness of the proposed joint beamformer, we will observe how changing the number of transmit antennas (N) affects the secrecy capacity in bits/sec/Hz (for three different types of beamforming techniques) in the wireless system, using the data presented in Figure 3 on the secrecy capacity for Maximum Ratio Transmission (MRT), Conventional ZF (Zero Forcing), and the Proposed Beamforming Technique.. On the horizontal axis, the number of antennas increases from 2 to 10, and on the vertical axis, the secrecy capacity is plotted. The represented by the solid red line, clearly performs the best—it starts at a high secrecy capacity and gradually increases as the number of transmit antennas grows, reaching close to 16 bits/s/Hz when 10 antennas are used. The proposed method improves secrecy by directing signals toward the legitimate receiver and away from the eavesdroppers using multiple antennas more effectively than Conventional Zero-Forcing (ZF) methods, which provide sufficient secrecy capacity of around 12 bits/s/Hz regardless of numbers of antennas used. MRT method performs the worst, with relatively little improvement in terms of increasing number of antennas; thus, it is the least secure as it amplifies transmitted signals at each of the receivers without actively minimizing unintentional receivers' access to the signal. Therefore, the proposed beamforming technique offers the greatest advantage for increasing secrecy capacity for the larger number of antennas that a Multi-Antenna Wireless Systems provides.

Band-width (Hz) vs Capacity of Channel (bps) (See Figure 4). There are two separate plots for SNR Levels of 20 dB and 10 dB. Both plots indicate an increase in the channel capacity as band-width increases, however, at some point after the band-width reaches a certain level (due to an increase in band-width), channel capacity increases become less significant than before (less than the rate of growth).

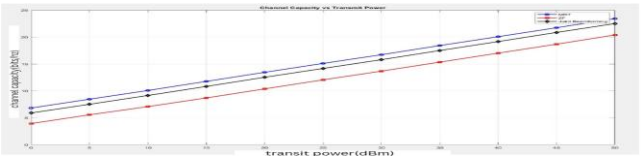

Figure 4**:** channel capacity vs transit power

For any given band-width value, at every value of SNR the channel capacity would be greater at an SNR of 20 dB than would be at SNR of 10 dB. Importantly, it is evident from this comparison that the higher the SNR (greater than 10 dB), the greater the data-carrying capacity of a digital transmission system or network.

V. CONCLUSION

In order to provide secure data transmission in a MISO wireless system, we presented a combined beamforming strategy in this study that incorporates ZF and MRT techniques. To handle non-line-of-sight (NLoS) scenarios, we utilized Intelligent Reflecting Surface (IRS) technology to establish an effective communication link between the transmitter and the user. The research study introduced a secure data transmission method for MISO wireless systems through a combined beamforming approach which uses ZF and MRT techniques. The communication link between transmitter, and user received an effective solution through our implementation of Intelligent Reflecting Surface (IRS) technology for non-line-of-sight (NLoS) scenarios. The results from the simulations clearly reveal that the integrated beamforming approach significantly improves secrecy performance. The proposed method has been verified to be effective and reliable, as it improves the signal quality for the intended recipient while reducing leakage to possible eavesdroppers. The result even further shows that secrecy capacity increases with an increased number of transmit antennas and IRS components. Such secure beamforming strategies can also be envisioned for extension toward other wireless domains, including optical f-OFDM systems, where novel transmission techniques are actively being developed [26].

REFERENCES

[1] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," IEEE J. Sel. Areas Commun., vol. 36, no. 4, pp. 679–695, 2018.

[2] S. Ji and W.-Q. Wang, "Physical-layer security for frequency diverse array communication system over nakagami-m fading channels," IEEE Syst. J., vol. 14, no. 2, pp. 2370–2381, 2020.

[3] J. Tang, H. Wen, K. Zeng, R.-F. Liao, F. Pan, and L. Hu, "Light-weight physical layer enhanced security schemes for 5G wireless networks," IEEE Netw., vol. 33, no. 5, pp. 126–133, 2019.

[4] J. Tang, M. Dabaghchian, K. Zeng, and H. Wen, "Impact of mobility on physical layer security over wireless fading channels," IEEE Trans. Wireless Commun., vol. 17, no. 12, pp. 7849–7864, 2018.

[5] C. E. Shannon, "Communication theory of secrecy systems," The Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, 1949.

[6] A. D. Wyner, "The wire-tap channel," The Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, 1975.

[7] S. Gong, X. Lu, D. T. Hoang, D. Niyato, L. Shu, D. I. Kim, and Y.-C. Liang, "Toward smart wireless communications via intelligent reflecting surfaces: A contemporary survey," IEEE Commun. Surveys Tuts., vol. 22, no. 4, pp. 2283–2314, 2020.

[8] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," IEEE Trans. Signal Process., vol. 60, no. 1, pp. 310–325, 2012.

[9] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—part II: The MIMOME wiretap channel," IEEE Trans. Inf. Theory, vol. 56, no. 11, pp. 5515–5532, 2010.

[10] A. Khisti A. and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," IEEE Trans. Inf. Theory, vol. 56, no. 7, pp. 3088–3104, 2010.

[11] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," IEEE Trans. Veh. Technol., vol. 59, no. 8, pp. 3831–3842, 2010.

[12] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multilevel secrecy rate maximization," IEEE Trans. Signal Process., vol. 61, no. 10, pp. 2704–2717, 2013

[13] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks," IEEE Trans. Signal Process., vol. 63, no. 1, pp. 206–220, 2015

[14] L. Yang, J. Yang, W. Xie, M. O. Hasna, T. Tsiftsis, and M. D. Renzo, "Secrecy performance analysis of RIS-aided wireless communication systems," IEEE Trans. Veh. Technol., vol. 69, no. 10, pp. 12 296–12 300, 2020.

[15] J. Qiao and M.-S. Alouini, "Secure transmission for intelligent reflecting surface-assisted mmWave and terahertz systems," IEEE Wireless Commun. Lett., vol. 9, no. 10, pp. 1743–1747, 2020.

[16] H. Wang, J. Bai, and L. Dong, "Intelligent reflecting surfaces assisted secure transmission without eavesdropper's CSI," IEEE Signal Process. Lett., vol. PP, pp. 1–1, 07 2020.

[17] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," IEEE Wireless Commun. Lett., 8(5)1410–1414, 2019.

[18] X. Lu, W. Yang, X. Guan, Q. Wu, and Y. Cai, "Robust and secure beamforming for intelligent reflecting surface aided mm-wave MISO systems," IEEE Wireless Commun. Lett., 9(12)2068–2072, 2020.

[19] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent reflecting surface: A programmable wireless environment for physical layer security," IEEE Access, vol. PP, pp. 1–1, 06 2019.

[20] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," IEEE Trans. Wireless Commun., vol. 18, no. 11, pp. 5394–5409, 2019.

[21] K. Feng, X. Li, Y. Han, S. Jin, and Y. Chen, "Physical layer security enhancement exploiting intelligent reflecting surface," IEEE Commun. Lett., vol. 25, no. 3, pp. 734–738, 2021.

[22] J. Myung, H. Heo, and J. Park, "Joint beamforming and jamming for physical layer security," ETRI Journal, vol. 37, no. 5, pp. 898–905, 2015

[23] M. A. B. Mohammad, A. A. Osman, and N. A. A. Elhag, "Performance comparison of MRT and ZF for single cell downlink massive MIMO system," in 2015 International Conference on Computing, Control, Networking, Electronics and Embedded Systems Engineering (ICCNEEE), 2015, pp. 52–56.

[24] T. Lo, "Maximum ratio transmission," IEEE Trans. Commun., vol. 47, no. 10, pp. 1458–1461, 1999.

[25] Upadhyay, K. and Bharti, M., 2025. Simulative Performance Investigation of OFDM & f-OFDM for Optical Wireless Communication System: SIMULATIVE PERFORMANCE INVESTIGATION OF OFDM & F-OFDM. Journal of Scientific & Industrial Research (JSIR), 84(02), pp.162-169.

[26] Upadhyay, K., Bharti, M. & Kumar, M. A novel technique Spanding for optical f-OFDM system. J Opt (2025).