

Secure Wireless Communication Using BD-RIS in UAV Networks

S.S.V.S.S.R.S.Sarma Adithe^{1,*}, Adapa V D S Kalki Bhavani², Siragam Naga Sai Tulasi Devi³,
Sorapalli M G Namratha Sri⁴ and Kanchi Eswar Ram Kumar⁵

¹⁻⁵ Department of ECE, BVCITS, Amalapuram, AP-533221, India.

*Corresponding Author: S S V S S R S Sarma Adithe. Email: sarmaadithe@Zohomail.Com

Received: 10/02/2026; Revised: 28/02/2026; Accepted: 21/03/2026; Published: 31/03/2026.

DOI: <https://doi.org/10.69996/fmep.2026004>

Abstract: Non-terrestrial networks have recently gained significant attention as an effective solution for expanding wireless coverage using aerial platforms such as high-altitude platform stations (HAPS) and unmanned aerial vehicles (UAVs). Despite their advantages, the open nature of wireless transmission makes these networks vulnerable to security threats, particularly eavesdropping attacks. This paper investigates a secure communication framework for a UAV-based secondary network operating within a cognitive radio environment. To enhance communication security, a beyond-diagonal reconfigurable intelligent surface (BD-RIS) is integrated with the UAV to intelligently manipulate the wireless propagation environment. The BD-RIS improves the signal quality at the legitimate receiver while reducing information leakage toward a potential eavesdropper. In addition, an adaptive power control mechanism is employed to ensure that the interference introduced to the primary network remains within an acceptable threshold. The proposed framework is implemented using MATLAB and Simulink to evaluate the achievable secrecy rate under different system conditions. Simulation results indicate that the BD-RIS assisted system provides a notable improvement in secrecy performance compared to conventional communication schemes without intelligent surface support. Furthermore, increasing the UAV transmits power and the number of BD-RIS elements leads to further improvements in secure communication performance.

Keywords: Beyond-Diagonal Reconfigurable Intelligent Surface (BD-RIS), Physical Layer Security, Unmanned Aerial Vehicle (UAV) Communications, Cognitive Radio Networks, Secrecy Rate Maximization.

1.Introduction

Wireless communication technologies continue to evolve rapidly to meet the increasing demand for reliable connectivity, high data rates, and wide-area coverage. Traditional terrestrial communication infrastructures often face limitations in providing seamless connectivity in remote regions, disaster zones, and maritime or mountainous environments [1-3]. To address these challenges, non-terrestrial networks (NTNs) have emerged as an important extension of conventional wireless systems. NTNs employ aerial platforms such as high-altitude platform stations (HAPS) and unmanned aerial vehicles (UAVs) to extend communication coverage and support flexible network deployment [4-5].

Although UAV-enabled communication systems provide several advantages, including mobility, rapid deployment, and improved line-of-sight connectivity, the open and broadcast nature of wireless channels introduces significant security concerns. In particular, transmitted signals can easily be intercepted by unauthorized receivers, leading to potential eavesdropping and information leakage [6]. Ensuring secure communication in such environments has therefore become a critical research challenge.



Conventional communication systems typically rely on cryptographic techniques implemented at higher layers of the protocol stack to guarantee data confidentiality. While these approaches are effective, they may require complex key management procedures and significant computational resources [7-9]. As a result, physical layer security (PLS) has gained increasing attention as an alternative approach that exploits the randomness and characteristics of wireless channels to enhance communication security. The main objective of PLS techniques is to ensure that the legitimate receiver experiences a better channel condition than the eavesdropper, thereby enabling a positive secrecy rate.

Recently, reconfigurable intelligent surfaces (RIS) have attracted significant interest as a promising technology capable of improving wireless communication performance by intelligently controlling the propagation of electromagnetic waves [10]. RIS consists of a large number of programmable passive elements that can adjust the phase and amplitude of incident signals, allowing the wireless environment to be dynamically reconfigured. By carefully designing the reflection characteristics of these elements, RIS can enhance signal strength at desired receivers while suppressing interference and signal leakage toward unintended users [11-14].

An advanced extension of conventional RIS technology is the beyond-diagonal reconfigurable intelligent surface (BD-RIS). Unlike traditional RIS architectures that rely on diagonal reflection matrices, BD-RIS introduces additional degrees of freedom by enabling more flexible signal coupling among surface elements [15]. This capability allows BD-RIS to provide more powerful signal manipulation and improved beamforming performance, which can significantly enhance communication reliability and security [16].

In cognitive radio enabled non-terrestrial networks, multiple communication systems share the same spectrum resources. In such scenarios, a secondary communication system must operate without causing harmful interference to the primary network. Therefore, the secondary transmitter must carefully regulate its transmission power according to an interference temperature constraint imposed by the primary receiver [17]. This requirement introduces an additional challenge in designing secure communication frameworks for UAV-assisted networks [18-19].

Motivated by these challenges, this work investigates a secure communication framework for a cognitive radio enabled UAV network assisted by a BD-RIS. In the considered system, a HAPS acts as the primary transmitter, while a UAV functions as the secondary transmitter that communicates with a legitimate secondary user in the presence of a potential eavesdropper [20-21]. The BD-RIS mounted on the UAV is utilized to manipulate the propagation environment in order to enhance the effective channel quality toward the legitimate receiver while limiting signal leakage toward the eavesdropper.

To further improve system performance, an adaptive power control mechanism is incorporated to ensure that the interference generated by the secondary transmission remains within the acceptable threshold of the primary network. The proposed framework is implemented using MATLAB and Simulink in order to evaluate the achievable secrecy rate under different system parameters such as UAV transmit power and the number of BD-RIS elements.

The simulation results demonstrate that integrating BD-RIS with UAV communication significantly improves the secrecy performance of the system compared with conventional communication schemes without intelligent surface support. These results highlight the potential of BD-RIS technology in enabling secure and efficient communication in future cognitive radio enabled non-terrestrial networks.

Contributions of This Work

The main contributions of this paper are summarized as follows:

- A secure communication framework is developed for a cognitive radio enabled UAV communication system operating in a non-terrestrial network environment. The framework considers the coexistence of a primary HAPS network and a secondary UAV network while addressing potential eavesdropping threats.
- A beyond-diagonal reconfigurable intelligent surface (BD-RIS) assisted transmission model is introduced to improve the propagation conditions between the UAV and the legitimate secondary user. The BD-RIS enables intelligent manipulation of electromagnetic waves to enhance the desired signal while limiting signal leakage toward the eavesdropper.
- An adaptive power control mechanism is incorporated to regulate the transmission power of the UAV while satisfying the interference temperature constraint imposed by the primary network. This ensures that the secondary communication operates without degrading the performance of the primary system.
- The proposed secure transmission framework is implemented using MATLAB and Simulink to evaluate system performance under realistic wireless channel conditions, including Rayleigh fading and additive white Gaussian noise.
- Extensive simulations are performed to analyze the impact of important system parameters such as UAV transmit power and the number of BD-RIS elements on the achievable secrecy rate. The results demonstrate that the integration of BD-RIS significantly enhances secure communication performance compared to systems without intelligent surface support.

2. Literature Review

Secure wireless communication has become an important research topic due to the increasing openness and vulnerability of modern wireless networks. Traditional approaches mainly rely on cryptographic techniques implemented at higher layers of the communication protocol stack. Although these methods provide strong protection, they require complex key management and computational resources, which may not always be suitable for resource-constrained wireless environments. As a result, physical layer security (PLS) has gained significant attention as a complementary technique that utilizes the inherent properties of wireless channels to improve communication confidentiality.

With the rapid development of intelligent wireless technologies, reconfigurable intelligent surfaces (RIS) have emerged as a promising solution for improving both communication performance and security. RIS consists of a large number of programmable passive elements that can adjust the phase and amplitude of reflected signals. By appropriately configuring these elements, RIS can control the propagation of electromagnetic waves in the wireless environment. Several studies have demonstrated that RIS can effectively enhance signal strength at desired receivers while suppressing interference and reducing information leakage toward unintended users.

Recent research has also explored the application of RIS in secure communication systems. In these works, RIS is used to improve the secrecy rate by enhancing the channel quality of the legitimate receiver relative to that of the eavesdropper. Various optimization techniques have been proposed to adjust the reflection coefficients of RIS elements in order to maximize secure transmission performance. These approaches show that RIS-assisted systems

can significantly outperform conventional communication systems without intelligent surface support.

An advanced extension of conventional RIS technology is the beyond-diagonal reconfigurable intelligent surface (BD-RIS). Unlike traditional RIS architectures that rely on simple diagonal reflection matrices, BD-RIS introduces additional flexibility by allowing more complex signal coupling among surface elements. This additional degree of freedom enables improved beamforming capability and more effective manipulation of the wireless propagation environment.

At the same time, unmanned aerial vehicles (UAVs) have become an important component of next-generation wireless networks. UAVs can act as mobile base stations or relay nodes, providing flexible coverage and rapid deployment in dynamic communication scenarios. When integrated into non-terrestrial networks (NTNs), UAVs can significantly extend communication coverage in areas where terrestrial infrastructure is limited or unavailable. However, UAV-based communication systems are also highly susceptible to eavesdropping due to their wide coverage and broadcast transmission characteristics.

Although several studies have investigated RIS-assisted secure communication and UAV-enabled wireless networks independently, limited research has addressed the joint integration of BD-RIS technology with UAV-assisted cognitive radio systems for improving secrecy performance. Therefore, this work focuses on developing a BD-RIS assisted secure transmission framework for cognitive radio enabled UAV communication systems operating in non-terrestrial network environments.

3. System Model

This section describes the communication model considered for the proposed BD-RIS assisted secure transmission framework. The system operates within a cognitive radio enabled non-terrestrial network environment where aerial communication platforms are utilized to extend wireless coverage.

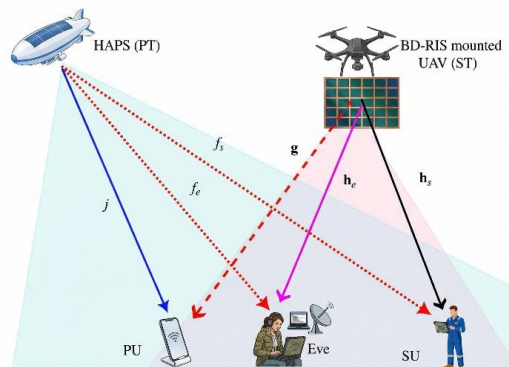


Figure 1: System model of BD-RIS assisted cognitive radio enabled non-terrestrial network.

As illustrated in Fig. 1, the network consists of a high-altitude platform station (HAPS) acting as the primary transmitter, a primary user (PU), and a secondary communication link established by an unmanned aerial vehicle (UAV). The UAV serves as the secondary transmitter and communicates with a legitimate secondary user (SU). In addition, a passive eavesdropper (Eve) is assumed to exist in the communication environment and attempts to intercept the transmitted signal.

To improve communication security, a beyond-diagonal reconfigurable intelligent surface (BD-RIS) is deployed near the UAV. The BD-RIS contains multiple programmable reflecting elements capable of adjusting the phase and amplitude of incident signals. By intelligently

controlling the reflection characteristics, the BD-RIS enhances the propagation conditions of the legitimate communication link while limiting signal leakage toward the eavesdropper.

Since the UAV operates as a secondary transmitter sharing spectrum resources with the primary network, its transmission must satisfy the interference constraint imposed by the primary receiver.

A. Signal Transmission Model

Let $\mathbf{x}$ denote the baseband signal transmitted by the UAV with transmit power P_s . In the proposed system, the information symbols are generated randomly and modulated using quadrature phase shift keying (QPSK).

The BD-RIS modifies the transmitted signal through its programmable reflection response. The effective reflected signal after BD-RIS processing can be expressed as

$$\mathbf{y} = \alpha \mathbf{x} \quad (1)$$

where α represents the effective reflection gain introduced by the BD-RIS and $\mathbf{x}$ denotes the transmitted signal.

B. Channel Model

The wireless links between the UAV and the receivers are modeled using independent Rayleigh fading channels to represent practical wireless propagation conditions. Additive white Gaussian noise (AWGN) is considered at all receivers.

The received signal at the legitimate secondary user is given by

$$\mathbf{y}_s = \mathbf{h}_s \mathbf{y} + \mathbf{n}_s \quad (2)$$

Similarly, the received signal at the eavesdropper is expressed as

$$\mathbf{y}_e = \mathbf{h}_e \mathbf{y} + \mathbf{n}_e \quad (3)$$

where $\mathbf{h}_s$ and $\mathbf{h}_e$ represent the channel coefficients corresponding to the UAV-to-SU link and UAV-to-Eve link, respectively. The terms $\mathbf{n}_s$ and $\mathbf{n}_e$ denote the additive white Gaussian noise components at the legitimate receiver and the eavesdropper, with variance σ^2 .

C. SINR Formulation

Based on the received signal expressions, the signal-to-interference-plus-noise ratio (SINR) at the legitimate receiver can be written as

$$\gamma_s = |\mathbf{h}_s \alpha \mathbf{x}|^2 / \sigma^2 \quad (4)$$

Similarly, the SINR at the eavesdropper is given by

$$\gamma_e = |\mathbf{h}_e \alpha \mathbf{x}|^2 / \sigma^2 \quad (5)$$

These SINR values determine the achievable communication rates of the legitimate receiver and the eavesdropper.

D. Secrecy Rate

The achievable secrecy rate is defined as the difference between the achievable data rates of the legitimate receiver and the eavesdropper. It is expressed as

$$R_{sec} = \max(0, \log_2(1 + \gamma_s) - \log_2(1 + \gamma_e)) \quad (6)$$

A positive secrecy rate indicates that the legitimate receiver experiences better channel conditions than the eavesdropper, ensuring secure communication.

E. Interference Constraint

Since the UAV operates as a secondary transmitter in a cognitive radio environment, its transmission must not cause harmful interference to the primary network. Therefore, the transmit power of the UAV must satisfy the following constraint

$$P_s \leq \min(P_{max}, I_{th} / |g|^2) \quad (7)$$

where $P_{\max}$ represents the maximum allowable transmit power of the UAV, I_{th} denotes the interference threshold tolerated by the primary receiver, and g represents the interference channel coefficient between the UAV and the primary user.

The objective of the proposed system is to maximize the achievable secrecy rate while satisfying the interference constraint imposed by the primary network.

4. Proposed BD-RIS Assisted Secure Transmission Scheme

This section presents the proposed BD-RIS assisted secure transmission scheme designed to improve the secrecy performance of the UAV communication system. Unlike the system model described in the previous section, this section focuses on the operational procedure used to enhance the legitimate communication link while reducing the probability of successful eavesdropping.

The proposed framework integrates three main components: adaptive power allocation at the UAV transmitter, intelligent signal reflection using BD-RIS, and secrecy rate evaluation based on the received signal quality.

A. Secure Transmission Strategy

The main objective of the proposed scheme is to maximize the achievable secrecy rate while satisfying the interference constraint imposed by the primary network. In order to achieve this objective, the UAV transmission is controlled based on the instantaneous channel conditions.

The UAV is allowed to transmit only when the channel condition of the legitimate user is stronger than that of the eavesdropper. This condition ensures that the legitimate receiver experiences a higher signal quality compared to the eavesdropper, which directly improves the secrecy rate of the system.

B. BD-RIS Assisted Signal Enhancement

The BD-RIS plays a key role in improving the quality of the legitimate communication link. By adjusting the reflection characteristics of its elements, the BD-RIS redirects the incident electromagnetic waves toward the legitimate receiver.

This intelligent reflection process effectively strengthens the received signal at the legitimate user while limiting the signal power received by the eavesdropper. As a result, the difference between the legitimate channel capacity and the eavesdropper channel capacity increases, leading to improved secrecy performance.

C. Adaptive Power Allocation

To ensure coexistence with the primary network, the transmit power of the UAV must satisfy the interference temperature constraint imposed by the primary receiver. Therefore, an adaptive power allocation strategy is implemented to determine the transmit power of the UAV.

The transmit power is dynamically adjusted according to the interference channel condition between the UAV and the primary user. If the interference level approaches the allowable threshold, the UAV transmission power is reduced to maintain acceptable interference levels.

This power control strategy allows the secondary communication system to operate efficiently without causing harmful interference to the primary network.

D. Operational Algorithm

The proposed secure transmission scheme follows the following operational steps:

1. Initialize system parameters including transmit power limits, noise variance, and channel coefficients.
2. Generate random data symbols and apply QPSK modulation at the UAV transmitter.

3. Estimate the channel conditions between the UAV, the legitimate user, the eavesdropper, and the primary receiver.
4. Apply the secure transmission condition by comparing the legitimate channel gain and the eavesdropper channel gain.
5. Determine the UAV transmit power using the interference constraint.
6. Apply BD-RIS reflection processing to enhance the propagation environment.
7. Propagate the signal through Rayleigh fading channels toward the receivers.
8. Compute the SINR values at the legitimate receiver and the eavesdropper.
9. Calculate the achievable secrecy rate based on the SINR values.
10. Repeat the process for multiple simulation iterations to obtain average performance results.

E. Implementation Framework

The proposed scheme is implemented using MATLAB and Simulink. The simulation framework consists of several functional modules including symbol generation, QPSK modulation, adaptive power control, BD-RIS processing, wireless channel modeling, SINR computation, and secrecy rate evaluation.

The performance of the system is analyzed using Monte Carlo simulations in order to evaluate the impact of key system parameters such as UAV transmit power and the number of BD-RIS reflecting elements on the achievable secrecy rate.

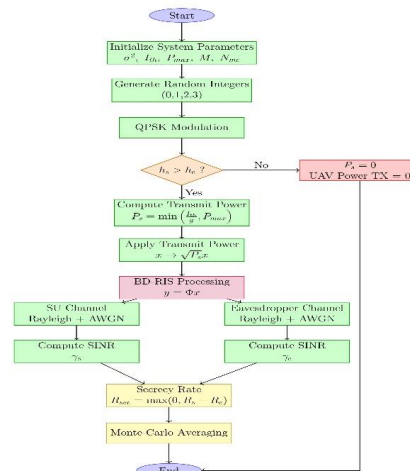


Figure 2: Flowchart of the proposed BD-RIS assisted secure transmission algorithm.

The simulation outputs the achievable secrecy rate under different system parameters such as UAV transmit power and number of BD-RIS elements.

5. Simulation Results and Discussion

This section presents the simulation results used to evaluate the performance of the proposed BD-RIS assisted secure communication framework. The system model and the proposed transmission scheme are implemented using MATLAB and Simulink in order to analyze the achievable secrecy performance under different system conditions.

The simulations consider a UAV acting as a secondary transmitter communicating with a legitimate secondary user in the presence of a passive eavesdropper. The wireless channels between the UAV and the receivers are modeled using Rayleigh fading in order to represent practical non-line-of-sight propagation environments. In addition, additive white Gaussian noise (AWGN) is considered at all receivers.

The main performance metric used in the simulations is the **achievable secrecy rate**, which represents the difference between the achievable communication rates of the legitimate receiver and the eavesdropper.

A. Simulation Parameters

The key simulation parameters used in the performance evaluation are summarized as follows.

- Noise variance : $\sigma^2 = 10^{-4}$
- Maximum UAV transmit power : $P_{max} = 25 \text{ dBm}$
- Interference threshold : $I_{th} = 10^{-5}$
- Primary transmitter power: $Q_p = 40 \text{ dBm}$
- Number of BD-RIS elements : $M = 8 - 64$
- Channel model : Rayleigh fading
- Modulation scheme : QPSK

Monte Carlo simulations are performed to obtain statistically reliable results by averaging the secrecy rate over multiple channel realizations.

B. Convergence of Secrecy Rate

Fig. 3 illustrates the convergence behavior of the achievable secrecy rate over several simulation iterations. The results compare the performance of the communication system with and without BD-RIS assistance.

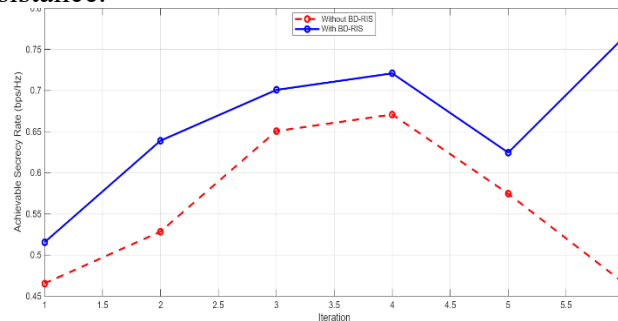


Figure 3: Convergence behavior of the achievable secrecy rate for different numbers of BD-RIS elements.

It can be observed that the secrecy rate gradually converges as the number of iterations increases. The system assisted by BD-RIS achieves a significantly higher secrecy rate compared to the conventional system without intelligent surface support. This improvement is mainly due to the ability of BD-RIS to enhance the signal strength at the legitimate receiver while reducing the effective signal power received by the eavesdropper.

C. Impact of UAV Transmit Power

Fig 4 presents the impact of UAV transmit power on the achievable secrecy rate. The transmit power of the UAV is varied from 20 dBm to 30 dBm to evaluate its effect on system performance.

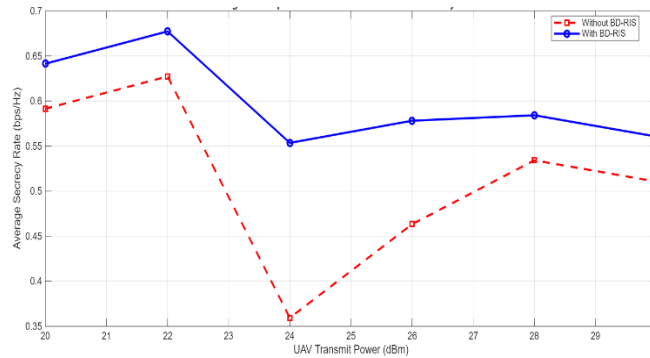


Figure 4: Impact of UAV transmit power on achievable secrecy rate.

The results indicate that the secrecy rate increases as the transmit power increases because the received signal strength at the legitimate receiver becomes stronger. However, the BD-RIS assisted system consistently outperforms the conventional system across all transmit power levels. This demonstrates that BD-RIS can effectively improve secure communication even when the transmit power is limited.

D. Impact of BD-RIS Elements

Fig. 5 shows the effect of the number of BD-RIS reflecting elements on the achievable secrecy rate. Increasing the number of RIS elements provides additional degrees of freedom for manipulating the wireless propagation environment.

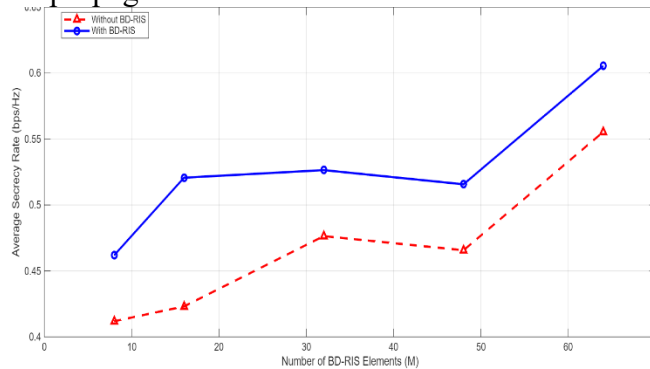


Figure 5: Achievable secrecy rate versus number of BD-RIS elements.

The results show that the secrecy rate improves as the number of BD-RIS elements increases. This occurs because a larger BD-RIS can more effectively enhance the signal propagation toward the legitimate receiver while suppressing the signal strength toward the eavesdropper.

Overall, the simulation results demonstrate that the proposed BD-RIS assisted secure transmission scheme significantly improves the secrecy performance of UAV communication systems operating in cognitive radio enabled non-terrestrial networks.

6. Conclusion

This paper investigated a BD-RIS assisted secure communication framework for UAV-enabled cognitive radio networks operating in non-terrestrial communication environments. The proposed system considers a UAV acting as a secondary transmitter communicating with a legitimate secondary user in the presence of a potential eavesdropper while sharing spectrum resources with a primary HAPS-based network.

To enhance communication security, a beyond-diagonal reconfigurable intelligent surface (BD-RIS) was integrated with the UAV communication system in order to intelligently

manipulate the wireless propagation environment. In addition, an adaptive power control mechanism was introduced to regulate the transmit power of the UAV while satisfying the interference constraint imposed by the primary network.

The proposed secure transmission scheme was implemented using MATLAB and Simulink, and the system performance was evaluated in terms of achievable secrecy rate. Simulation results demonstrated that the BD-RIS assisted system significantly improves secrecy performance compared with conventional communication systems without intelligent surface support. Furthermore, the results showed that increasing the UAV transmit power and the number of BD-RIS elements leads to further improvements in the achievable secrecy rate.

The findings of this work highlight the potential of BD-RIS technology in enhancing secure communication for UAV-assisted cognitive radio networks. Future work may investigate advanced BD-RIS optimization techniques, multi-user communication scenarios, and machine learning-based control strategies for dynamically adapting RIS configurations in complex wireless environments.

Acknowledgment: Not Applicable.

Funding Statement: The author(s) received no specific funding for this study.

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

References

- [1] W. U. Khan and A. Mahmood, "Beyond diagonal RIS for 6G nonterrestrial networks: Potentials and challenges," *IEEE Network*, vol. 39, no. 1, pp. 80–89, 2025.
- [2] M. M. Azari and S. Solanki, "Evolution of non-terrestrial networks from 5G to 6G: A survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2633–2672, 2022.
- [3] W. U. Khan and Z. Ali, "Rate splitting multiple access for next generation cognitive radio enabled LEO satellite networks," *IEEE Transactions on Wireless Communications*, vol. 22, no. 11, pp. 8423–8435, 2023.
- [4] M. Deng and M. Ahmed, "Reconfigurable intelligent surfaces enabled vehicular communications: A comprehensive survey of recent advances and future challenges," *IEEE Transactions on Intelligent Vehicles*, pp. 1–28, 2024.
- [5] Z. Ali and W. U. Khan, "Enhanced learning-based hybrid optimization framework for RSMA-aided underlay LEO communication with non-collaborative terrestrial primary network," *IEEE Transactions on Communications*, pp. 1–1, 2024.
- [6] W. U. Khan and E. Lagunas, "Opportunities for physical layer security in UAV communication enhanced with intelligent reflective surfaces," *IEEE Wireless Communications*, vol. 29, no. 6, pp. 22–28, 2022.
- [7] P. He and H. Lei, "Non-terrestrial network technologies: Applications and future prospects," *IEEE Internet of Things Journal*, pp. 1–1, 2024.
- [8] S. Shen, B. Clerckx, and R. Murch, "Modeling and architecture design of reconfigurable intelligent surfaces using scattering parameter network analysis," *IEEE Transactions on Wireless Communications*, vol. 21, no. 2, pp. 1229–1243, 2022.
- [9] C. Zhang, "Sum rate maximization for 6g beyond diagonal RIS-assisted multi-cell transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–11, 2025.
- [10] R. Allu and O. Taghizadeh, "Robust beamformer design in active RIS-assisted multiuser MIMO cognitive radio networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 9, no. 2, pp. 398–413, 2023.
- [11] H. Li, S. Shen and B. Clerckx, "Beyond diagonal reconfigurable intelligent surfaces: From

- transmitting and reflecting modes to single-, group-, and fully-connected architectures,” *IEEE Transactions on Wireless Communications*, vol. 22, no. 4, pp. 2311–2324, 2023.
- [12] W. U. Khan, E. Lagunas, A. Mahmood, M. Asif, M. Ahmed and S. Chatzinotas, “Integration of beyond diagonal RIS and UAVs in 6G NTN: Enhancing aerial connectivity,” *arXiv preprint arXiv:2409.06073*, 2024.
- [13] Sk Jagadeesh Babu and J.Madhuri, “Multi-Band Miniaturized Composite Normalized Transmission Line (CNTL) ZOR Antenna for Machine Learning-Enabled Microwave Communication,” *Journal of Microwaves and Antenna Applications*, vol. 1, no. 2, 2025.
- [14] X. Wu, J. Ma and X. Xue, “Joint beamforming for secure communication in RIS-assisted cognitive radio networks,” *Journal of Communications and Networks*, vol. 24, no. 5, pp. 518–529, 2022.
- [15] Z. Huang, C. He, Z. Gu, and M. Xiao, “Physical layer security for IRS-assisted cognitive radio networks,” *2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall)*, pp. 1–5, 2023.
- [16] K. S. Venkateswara Rao and A. Singh, “Security of RIS-aided energy harvesting based D2D communications in cognitive cellular network,” *2024 IEEE 99th Vehicular Technology Conference (VTC2024-Spring)*, pp. 1–6, 2024.
- [17] Nagaraju Panaganti, “Model-Based and LLM-Driven Meta-Ai Framework for Intelligent Permanent Magnet Synchronous Motor Drive Control,” *JEPE*, vol. 2, no. 3, pp. 41–55, 2025
- [18] L. Dong, Y. Huo, W. Yan, X. Tang, Y. Li and W. Cheng, “Joint secure transmission enhancement of primary and secondary users in RIS aided spectrum sharing cognitive radio networks,” *IEEE Transactions on Cognitive Communications and Networking*, pp. 1–1, 2025.
- [19] Z. Wang, W. Wu, F. Zhou, B. Wang, Q. Wu, T. Q. S. Quek and C.-B. Chae, “IRS-enhanced spectrum sensing and secure transmission in cognitive radio networks,” *IEEE Transactions on Wireless Communications*, vol. 23, no. 8, pp. 10 271–10 286, 2024.
- [20] C. Ding, J.-B. Wang et al., “Joint optimization of transmission and computation resources for satellite and high altitude platform assisted edge computing,” *IEEE Transactions on Wireless Communications*, vol. 21, no. 2, pp. 1362–1377, 2022.
- [21] Z. Ali, M. Asif, “Hybrid optimization for NOMA-based transmissive-RIS mounted UAV networks,” *IEEE Transactions on Consumer Electronics*, pp. 1–1, 2025.