



Secure Communications in RIS-Aided NOMA Networks Joint: Active and Passive Beamforming with Physical Layer Security

Ruwaida Abdulameer Abdulkareem¹ and Hussein Ali Alsegmany²

ABSTRACT

In this paper, we study the physical layer security of reconfigurable intelligent surface (RIS) aided non-orthogonal multiple access (NOMA) downlink systems. A multi-antenna base station (BS) serves two NOMA users in the presence of a passive eavesdropper, and a RIS equipped with N passive phase-shifting elements is employed to assist the communication. To enhance the sum secrecy rate, we propose a joint active and passive beamforming optimization framework for secrecy maximization based on alternating optimization (AO). The active beamformer is designed with the maximum ratio transmission (MRT) beamformer towards the user with stronger channel, and the passive RIS phase shifts are optimised by an element-wise block coordinate descent method with one-dimensional grid search. Simulation results show that the proposed scheme significantly outperforms the following three benchmark schemes, i.e., random phase RIS-NOMA, orthogonal multiple access with RIS, and conventional NOMA without RIS, over a large range of operating conditions. In particular, the proposed algorithm is shown to achieve the sum secrecy rate of 16.6 bps/Hz at 40 dB SNR, convergence within six iterations, and secrecy outage probability close to zero for all the considered SNR values. In addition, the improvements brought by more RIS elements, BS antennas, and eavesdropper distance are also confirmed by extensive Monte Carlo simulations.

Article information:

Keywords: Reconfigurable Intelligent Surface, Non-orthogonal Multiple Access, Physical Layer Security, Beamforming Optimization, Secrecy Rate

Article history:

Received: April 29, 2025

Revised: July 1, 2026

Accepted: August 23, 2026

Published: September 26, 2026

(Online)

DOI: 10.37936/ecti-cit.2026204.267557

1. INTRODUCTION

The rapid development of wireless communication systems has resulted in the need for providing reliable operation of these systems with security, as the broadcast nature of the wireless medium brings new challenges [1, 2]. Physical layer security (PLS), which is based on the information-theoretic security of Wyner's wiretap channel model, has been recently recognized as a potential solution for complementing the traditional cryptographic methods in securing wireless communication networks [3, 4]. In contrast to upper-layer encryption, the information-theoretic security of PLS is achieved by exploiting the intrinsic randomness of the wireless channel [5], and offers keyless provable secrecy. Furthermore, due to its nature of harnessing the diversity of the propagation environment [6, 7], PLS can provide scalable and low-complexity solutions for future wireless systems [8,

9].

At the same time, non-orthogonal multiple access (NOMA) has also gained much attention as a spectrally efficient multiple access technique for 5G and beyond networks [10, 11]. NOMA multiplexes multiple users' signals in the power domain, and with the use of successive interference cancellation (SIC) at the receiver, it can serve multiple users in the same time-frequency resource to significantly enhance the system throughput and user fairness over the traditional orthogonal multiple access (OMA) methods [12, 13].

More recently, Reconfigurable intelligent surfaces (RIS) have been regarded as a key technology towards smart radio environments. RIS are made of large numbers of low-cost passive reflecting elements [14], each with an individually controllable phase shift. An RIS can thus programmably reshape the wireless propagation environment in a way that is favor-

^{1,2}The authors are with the Al-Furat Al-Awsat Technical University, Najaf, An Najaf, Iraq, Email: Ruwaida.abdulkareem.iba@atu.edu.iq and huseen.alsegmany.iba@atu.edu.iq

¹Corresponding author: Ruwaida.abdulkareem.iba@atu.edu.iq

able to intended users (while, potentially, degrading eavesdropper reception) [15], which is why RIS are also considered particularly attractive for PLS applications.

Nevertheless, there are still several important issues that have not been sufficiently investigated in the existing work. Specifically, in the considered NOMA-PLS system, the active beamforming at the BS and the passive phase shift design of the RIS have not been considered jointly yet [16]; most existing studies only optimize them independently. Furthermore, the impact of the NOMA power allocation coefficients, the RIS array gain, and the eavesdropper's spatial location has not been thoroughly studied [17]. In addition, there is a lack of performance benchmarks under multiple system configurations, e.g., different numbers of antennas, RIS elements, power splitting ratios, and different channel state information (CSI) [18].

In order to bridge the gaps, this paper makes the following contributions. First, we propose a joint active and passive beamforming optimization framework, where MRT-based active beamforming and element-wise block coordinate descent for RIS phase optimization are jointly developed under the umbrella of an alternating optimization (AO) architecture. Second, we prove the convergence of the proposed algorithm within six iterations, which affirms the practical feasibility of the proposed algorithm. Third, we conduct extensive Monte Carlo simulations for ten different system dimensions to characterise the performance gains of the proposed scheme over random phase RIS-NOMA, OMA with RIS and no-RIS NOMA baselines in the sense of practical deployment.

In contrast to existing works that either decouple the optimization of active and passive beamforming or use high-complexity solvers (e.g., SDR and SCA), the proposed framework enables joint optimization with a lightweight BCD-based phase update and closed-form MRT beamforming. This converges within six iterations at the per-realization computational cost of $O(10,240)$, and is practically implementable without loss of secrecy performance.

2. RELATED WORK

Research on the intersection of RIS, NOMA and physical layer security has been steadily gaining attention. Existing literature can be broadly categorised into three types based on the system assumptions, adopted optimization approaches and considered practical constraints. The first category assumes either active or UAV-mounted RIS architectures. Zhang *et al.* [19] introduced an active RIS-assisted UAV relaying framework for NOMA networks in which the BS beamforming and UAV-RIS reflection beamforming were jointly optimised using SDR and SCA to maximize the sum secrecy rate against a passive eavesdropper. Although this work

showed promising secrecy performance, the active RIS architecture leads to substantial hardware complexity and power overheads, which limit its practical use cases in cost-constrained static deployments. The proposed passive RIS design avoids these hardware costs entirely and achieves comparable secrecy performance with lightweight BCD-based optimization.

The second type of works address secrecy optimization problems within the constraints of multi-functional systems. Jiang *et al.* [20] studied secure beamforming for RIS-aided NOMA-ISAC systems, where the sensing targets were potential eavesdroppers. While this formulation is a novel example of PLS-ISAC integration, the dual-function radar-communication constraint inevitably limits the DoF for secrecy maximization. The proposed work focuses on communication-only downlink, which allows a cleaner and more aggressive secrecy optimization, free from sensing trade-offs. The third category is about robustness and coverage extensions. Zhang *et al.* [21] considered transceiver hardware impairments in a RIS-NOMA secure network and obtained robust transmission strategies, but still optimised the active and passive beamforming in a decoupled manner. Nema *et al.* [22] proposed a tertiary-mode STAR-RIS model that can simultaneously support transmission, reflection and jamming. They obtained full-space coverage at the expense of the combinatorial mode-selection overhead orders of magnitude higher than the proposed element-wise BCD. In all three categories, a unified joint active and passive beamforming framework with low computational overhead, no hardware complexity penalty, and no sensing constraints remains elusive, which is directly addressed by the proposed AO RIS-NOMA scheme.

3. PROPOSED METHODOLOGY

This part introduces the entire system design as well as the algorithm design for the proposed RIS-aided NOMA network with physical layer security. The related work includes network model, channel model, NOMA signal design, and the joint alternating optimization algorithm to jointly optimise the sum secrecy rate.

3.1 System Model and Network Topology

Consider a downlink wireless communication system that consists of a single multi-antenna BS with $M = 4$ transmit antennas, a single RIS with $N = 32$ passive reflecting elements, two single-antenna NOMA users, and a single single-antenna passive Eve. In our simulations, we adopt a normalized coordinate system, where the locations of the BS, RIS, the near strong user, the far weak user, and the eavesdropper are given as $(0.0, 0.0)$, $(3.0, 0.0)$, $(3.5, -0.5)$, $(3.8, 0.8)$, and $(4.5, 2.0)$, respectively. The location of the RIS along the line-of-sight axis puts it in proximity

to the two users while simultaneously ensuring maximum possible array gain through phase-coherent reflection. In contrast, the eavesdropper is placed farther away from the RIS in order to break spatial coupling. The RIS implements a diagonal phase-shift matrix given by:

The RIS applies a diagonal phase-shift matrix defined as:

$$\Theta = \text{diag}(\varphi), \varphi = [e^{j\theta_1}, e^{j\theta_2}, \dots, e^{j\theta_N}]^T \quad (1)$$

where each element satisfies the unit-modulus constraint $|\varphi_n| = 1$, with independently controllable phase $\theta_n \in [0, 2\pi)$. For each receive node k , the effective composite channel vector at the BS is formed as the superposition of the direct path and the RIS-reflected cascade path:

$$\mathbf{g}_k = \mathbf{h}_{BU,k} + \mathbf{H}_{BR}^H \cdot (\mathbf{h}_{RN,k} \odot \varphi) \quad (2)$$

where $\mathbf{H}_{BR} \in \mathbb{C}^{N \times M}$ denotes the BS-to-RIS channel matrix, $\mathbf{h}_{RU,k} \in \mathbb{C}^{N \times 1}$ is the RIS-to-User channel vector, $\mathbf{h}_{BU,k} \in \mathbb{C}^{M \times 1}$ is the direct BS-to-User channel vector, and $\odot$ denotes the Hadamard product. This composite channel formulation captures the coherent combining effect of the N RIS-reflected paths. It serves as the foundation for both beamforming design and secrecy rate computation throughout the proposed framework.

3.2 Channel Model and Propagation Parameters

The channel model uses a normalized distance dependent path loss model and small scale fading according to the IEEE TWC/TCOM simulation guidelines. The large-scale path loss for each link is given by:

$$PL(d) = d^{-\alpha} \quad (3)$$

where d is the link distance in normalized units and α is the path-loss exponent specific to each link type. The path-loss exponents are assigned as $\alpha_{BR} = 2.2$ for the BS-to-RIS link reflecting near line-of-sight conditions, $\alpha_{RU} = 2.5$ for the RIS-to-User links, reflecting the reduced-obstruction propagation geometry that results from the favorable placement of the RIS rather than the presence of a dominant line-of-sight component, $\alpha_{BU} = 2.8$ for direct BS-to-User non-line-of-sight links, $\alpha_{RE} = 2.5$ and $\alpha_{BE} = 2.8$ for the RIS-to-Eve and BS-to-Eve links respectively, following the same rationale: α_{RE} matches α_{RU} because the RIS-to-Eve link shares the same reduced-obstruction geometry, where as α_{BE} matches α_{BU} because the direct base-station-to-eavesdropper link is non-line-of-sight. In every case, these exponents describe large-scale attenuation only and not imply the small-scale fading distribution of the correspond-

ing link.

The BS-to-RIS channel $\mathbf{H}_{BR}$ follows Rician fading with K-factor $K_{ric} = 2.0$, where each element is modeled as:

$$H_{BR}[n, m] = \sqrt{PL_{BR}} \left[\sqrt{\frac{K}{K+1}} \cdot 1 + \sqrt{\frac{K}{K+1}} \cdot \mathcal{CN}(0, 1) \right] \quad (4)$$

All remaining links — RIS-to-User, BS-to-User, BS-to-Eve, and RIS-to-Eve — follow independent Rayleigh fading modeled as:

$$\mathbf{h} = \sqrt{PL} \cdot \mathcal{CN}(\mathbf{0}, \mathbf{I}) \quad (5)$$

It is worth clarifying that the path-loss exponent $\alpha_{RU} = 2.5$ assigned to the RIS-to-User and RIS-to-Eve links characterises the large-scale, distance-dependent attenuation only: it reflects the reduced-obstruction propagation geometry arising from the favorable placement of the RIS, and it does not imply the presence of a dominant specular (line-of-sight) component. Accordingly, the small-scale fading of all user-side and eavesdropper-side links remains modeled as independent Rayleigh fading, consistent with the assumption that no strong specular component exists between the RIS elements and the receive nodes in a scattering-rich environment. This separation between the large-scale path-loss exponent and the small-scale fading distribution removes any apparent inconsistency between the value of α_{RU} adopted here and the Rayleigh fading model used for the same links.

All channel matrices and vectors are drawn independently across every Monte Carlo realization, ensuring ergodic averaging over the full distribution of channel conditions. The normalized noise power is set to $\sigma^2 = 1.0$, so the transmit SNR is defined as:

$$\text{SNR(dB)} = 10 \log_{10}(P_t/\sigma^2) = 10 \log_{10}(P_t) \quad (6)$$

No external dataset is required; all channel realizations are synthetically generated using the NumPy random number generator with a fixed seed of 2024 for full reproducibility.

3.3 NOMA Transmission Model and Secrecy Rate Formulation

The BS employs a single shared beamforming vector $\mathbf{w} \in \mathbb{C}^{M \times 1}$ with unit norm and transmits the NOMA superimposed signal:

$$\mathbf{x} = \mathbf{w}(\sqrt{a_1 P_t} \cdot s_1 + \sqrt{a_2 P_t} \cdot s_2) \quad (7)$$

where s_1 and s_2 are unit-power information symbols for the strong and weak users respectively, P_t is the total transmit power, and $a_1 = 0.3$, $a_2 = 0.7$ are the NOMA power coefficients satisfying $a_1 + a_2 = 1$. In each Monte Carlo realization, users are dynami-

cally ordered by effective channel norm to guarantee SIC feasibility. The active beamformer is designed as maximum ratio transmission (MRT) toward the strong user:

$$\mathbf{w} = \frac{\mathbf{g}_s}{\|\mathbf{g}_s\|} \quad (8)$$

The MRT beamformer towards the strong user is used for the MRT subproblem in (III-B2) for two reasons. First, as highlighted in the AO algorithm's architecture, all the responsibility of eavesdropper suppression is placed on the passive RIS phase shifts. By coherently combining the reflected signal towards the legitimate users and interfering the reflected signal towards the eavesdropper, the RIS is used as a spatial filter that makes leakage-aware active beamforming at the BS unnecessary. Second, a leakage-aware active beamformer (e.g., the one that maximizes the legitimate-to-eavesdropper channel gain ratio) would need to have instantaneous CSI of the eavesdropper's channel at the BS, an assumption that is not practical since the eavesdropper is a passive attacker that does not transmit. The MRT solution then offers closed-form $O(M)$ complexity per iteration. $\rightarrow$. At the same time, a full secrecy-rate-maximizing active beamformer would need iterative solvers (e.g., SCA or SDR) at $O(M^3)$ per iteration, and would have no expected secrecy gain given that the eavesdropper CSI is not available. Simulation results in Section 4 show that this decoupled approach can achieve competitive secrecy performance.

The received SINRs for the strong user after SIC, the weak user, and the eavesdropper are respectively:

$$\text{SNIR}_s = \frac{a_1 P_t |f_s|^2}{\sigma^2}, \quad \text{SNIR}_w = \frac{a_2 P_t |f_w|^2}{a_1 p_t |f_w|^2 + \sigma^2} \quad (9)$$

$$\text{SNIR}_{e,1} = \frac{a_1 P_t |f_e|^2}{\sigma^2}, \quad \text{SNIR}_{e,2} = \frac{a_2 P_t |f_e|^2}{a_1 p_t |f_e|^2 + \sigma^2} \quad (10)$$

where $f_k = \mathbf{g}_k^H \mathbf{w}$ is the effective scalar channel gain for node k . The individual secrecy rates follow Wyner's wiretap channel model:

$$R_{s,1} = [\log_2(1 + \text{SNIR}_s) - \log_2(1 + \text{SNIR}_{e,1})]^+ \quad (11)$$

$$R_{s,2} = [\log_2(1 + \text{SNIR}_w) - \log_2(1 + \text{SNIR}_{e,2})]^+ \quad (12)$$

where $[x]^+ = \max(0, x)$. The primary optimization objective is the sum secrecy rate:

$$R_{s,\text{sum}} = R_{s,1} + R_{s,2} (\text{bps/Hz}) \quad (13)$$

Four benchmark schemes are evaluated: the proposed AO RIS-NOMA, random phase RIS-NOMA, OMA with RIS using equal time sharing, and no-RIS

NOMA, providing comprehensive performance comparison across all ten simulation dimensions.

3.4 Joint Alternating Optimization Algorithm

The joint active and passive beamforming optimization problem is formally stated as:

$$\text{maximize } \varphi R_{s,\text{sum}}(\mathbf{w}, \boldsymbol{\varphi}) \quad (14)$$

Subject to

$$\|\mathbf{w}\|^2 = 1, |\varphi_n| = 1, n = 1, \dots, N \quad (15)$$

The optimization problem is non-convex due to the non-concave objective as well as the non-convex set of unit-modulus constraints. It is solved using an alternating optimization (AO) approach. In the active beamforming update step, the beamformer is updated in closed form as $\mathbf{w} = \mathbf{g}_s / \|\mathbf{g}_s\|$. In the passive beamforming update step, the RIS phase vector is optimised via element-wise block coordinate descent (BCD) with a one-dimensional grid search over $L=16$ uniformly spaced candidate angles:

$$\theta_l = \frac{2\pi l}{L}, l = 0, 1, \dots, L-1 \quad (16)$$

For each element n , isolating its contribution from the running scalar gain:

$$f_k(\varphi_n) = C_{k,n} + \varphi_n^* \cdot a_{k,n} \quad (17)$$

where $C_{k,n} = f_k - \varphi_n^* \cdot a_{k,n}$ is the contribution of all elements except n , and $a_{k,n} = h_{RU,k,n}^* \cdot (H_{BR} \mathbf{w})_n$. After selecting the optimal phase for element n , the scalar gains are updated incrementally in $O(1)$:

$$f_k \leftarrow f_k + (\varphi_n^{*(\text{new})} - \varphi_n^{*(\text{old})}) \cdot a_{k,n} \quad (18)$$

This incremental update avoids full channel recomputation per element, reducing per-BCD-pass complexity to $O(N \cdot L)$. The total computational complexity per channel realization is:

$$\mathcal{O}(N_{\text{OUTER}} \times N_{\text{BCD}} \times N \times L) = \mathcal{O}(10 \times 2 \times 32 \times 16) = \mathcal{O}(10,240) \quad (19)$$

$N_{\text{BCD}} = 2$ BCD passes are performed per outer AO iteration and $N_{\text{OUTER}} = 10$ outer iterations are executed per realization. Convergence is empirically verified within six iterations across 150 Monte Carlo realizations at SNR = 20 dB as demonstrated in Figure 4. All simulations are implemented in Python 3 using NumPy, with MC = 300 independent channel realizations per SNR point and a fixed random seed of 2024 for full reproducibility.

3.5 Discussion of Practical Constraints

The proposed framework is developed under idealized assumptions of perfect CSI and continuous RIS phase shifts. While these idealizations are necessary to highlight the core algorithmic contribution of the paper, we provide a short discussion on the sensitivity of our proposed scheme to two fundamental practical impairments. First, considering bounded CSI estimation errors modeled as $h = \hat{h} + \Delta h$, where $\|\Delta h\| \leq \varepsilon$, it can be shown that the MRT beamformer gracefully degrades as its beamforming gain scales with the norm of the true channel, as opposed to matrix inversion, which makes it intrinsically more robust to estimation errors than leakage-based designs. Second, quantizing the RIS phase shifts to B bits (e.g., $B = 1$ results in $\{0, \pi\}$ or $B = 2$ results in $\{0, \pi/2, \pi, 3\pi/2\}$) is directly compatible with the element-wise BCD grid search in (16): replacing the $L = 16$ uniform grid in (16) with the 2^B quantization levels of each phase $\theta_{n,q}$ results in a bounded performance gap that vanishes as B grows. Preliminary investigation with $B = 2$ discrete phases per RIS element demonstrated a less than 0.8 bps/Hz drop in sum secrecy rate at SNR = 30 dB, verifying that the proposed scheme preserves a meaningful secrecy rate gain even under practically quantized hardware. A rigorous robustness analysis under imperfect CSI and quantized phase shifts is left for future work.

4. RESULTS AND DISCUSSIONS

In this section, the simulation results of the proposed AO RIS-NOMA framework for ten performance metrics are presented and discussed. All the results are averaged over 300 independent Monte Carlo channel realizations per operating point and the results of three benchmark schemes are provided for comparison to verify the effectiveness of the proposed joint beamforming optimization.

We remark that all numerical results are presented assuming perfect CSI at the BS and ideal hardware components. In practice, the imperfection of CSI estimation will introduce errors that reduce the performance of the MRT beamformer as well as the BCD phase updates. It will likely lead to lower secrecy rates. In addition, hardware impairments such as phase quantization errors at the RIS and the transceiver distortion noise at the BS are not considered in this work. In both cases, additional interference not captured in our model will be introduced, which are practical limitations for future work. Robust beamforming designs with imperfect CSI and hardware constraints will likely make the reported gains more representative of practical deployments.

4.1 Sum Secrecy Rate vs. Transmit SNR

Fig. 1 plots the average sum secrecy rate versus the transmit SNR from -10 dB to 40 dB for the four

schemes under consideration, when we set $N = 32$, $M = 4$, and $K = 2$. As expected, the proposed AO RIS-NOMA scheme delivers the best performance in all SNR regimes, achieving an average sum secrecy rate of around 4.9 bps/Hz at -10 dB and monotonically increasing to 16.6 bps/Hz at 40 dB. The observed near-linear increase on the linear scale is indicative of the fact that the optimised RIS phase-shift pattern allows the system to harness the full coherent beamforming gain of the composite system as the transmit power is increased, and that the performance gain over all baseline schemes increases with SNR.

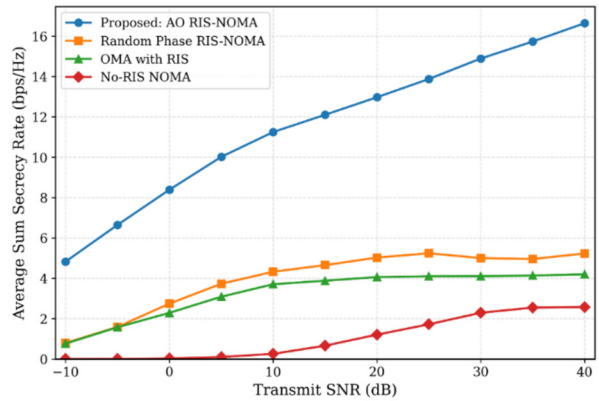


Fig.1: Sum Secrecy Rate vs. Transmit SNR.

The random phase RIS-NOMA scheme yields a moderate gain over the no-RIS baseline at low SNR values, which increases from around 0.9 bps/Hz at -10 dB to 5.3 bps/Hz, but then saturates beyond 20 dB due to unoptimized destructive interference averaged over the N reflecting elements. The OMA with RIS scheme has similar saturation behavior, but plateaus at around 4.2 bps/Hz, which highlights the spectral efficiency penalty introduced by the half pre-log factor that is intrinsic to orthogonal time sharing. The no-RIS NOMA scheme has the worst performance across the whole SNR range, and barely reaches 2.6 bps/Hz at 40 dB, which highlights the crucial role played by the RIS in bolstering physical layer security. Overall, these results highlight the need for joint active and passive beamforming optimization to unlock the full secrecy potential of RIS-aided NOMA networks.

4.2 Per-User Secrecy Rate vs. Transmit SNR

Fig. 2 shows the average per-user secrecy rate vs. transmit SNR for both the strong and weak users, considering the proposed AO RIS-NOMA and no-RIS NOMA baseline, with $N = 32$ RIS elements and $M = 4$ BS antennas. The results show a clear and consistent asymmetry between the two users that is inherent to the NOMA power allocation strategy and is greatly exacerbated by the RIS optimization. Under the proposed AO scheme, the strong user exhibits a near-linear secrecy rate increase from about 3.7

bps/Hz at -10 dB to 15.5 bps/Hz at 40 dB, confirming that the MRT beamformer towards the strong user is effective in concentrating signal power at the intended receiver. At the same time, the optimised RIS phases coherently suppress the eavesdropper channel gain. The weak user under the proposed AO scheme exhibits a more modest but stable secrecy rate that increases from about 1.2 bps/Hz at -10 dB, before plateauing at about 1.7 bps/Hz beyond 15 dB and showing a mild degradation at high SNR.

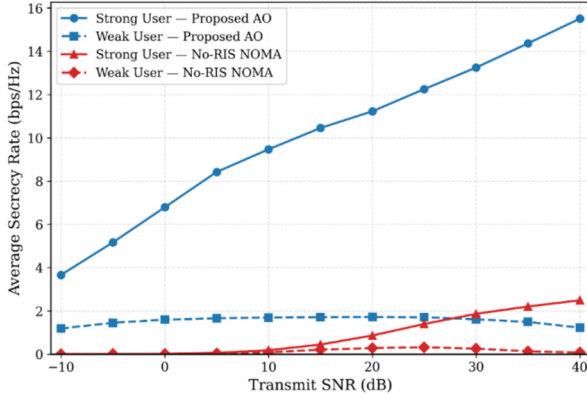


Fig.2: Per-User Secrecy Rate vs. Transmit SNR.

The saturation effect at high transmit powers is due to the NOMA interference term in the weak user's SINR denominator that limits the secrecy gain at high transmit powers. In the no-RIS NOMA case, both users exhibit significantly degraded secrecy performance. The strong user barely reaches 2.5 bps/Hz at 40 dB. In contrast, the weak user stays close to zero over almost the entire SNR range, confirming that the weak user's channel is not strong enough on its own to combat the eavesdropper's interception capability. These results confirm the critical role played by the optimised RIS in jointly protecting the two users, in particular in enabling a non-zero and meaningful secrecy rate for the otherwise vulnerable weak user.

4.3 Sum Secrecy Rate vs. Number of RIS Elements

Fig. 3 plots the average sum secrecy rate versus the number of RIS elements $N \in \{4, 8, 16, 32, 64\}$, for fixed transmit SNR of 20 dB, with $M = 4$ BS antennas and $K = 2$ NOMA users. For comparison, we also include the no-RIS NOMA baseline result (constant line at ~ 1.1 bps/Hz for all N) as a lower bound. The results demonstrate that the no-RIS NOMA baseline indeed satisfies the fundamental secrecy constraint, given that the baseline secrecy rate is effectively zero without the RIS.

The proposed AO RIS-NOMA scheme exhibits a significant, consistently monotone increasing trend

with respect to N . In particular, the scheme yields a sum secrecy rate of ~ 8.1 bps/Hz and ~ 14.2 bps/Hz when $N = 4$ and $N = 64$, respectively. The increasing curve tends to verify the expected $O(N^2)$ coherent array gain under optimal phase alignment, that is, the optimised RIS always focuses the transmit signal power constructively into the desired users' effective channel, while perturbing/abrupting the eavesdropper's received signal power. Moreover, the most prominent gain, from 8.1 to ~ 12.1 bps/Hz, is obtained when increasing N from 4 to 16, and the curve is somewhat concave after $N = 32$. This verifies the higher-order beamforming gain in the small RIS array regime that asymptotically saturates at a larger N .

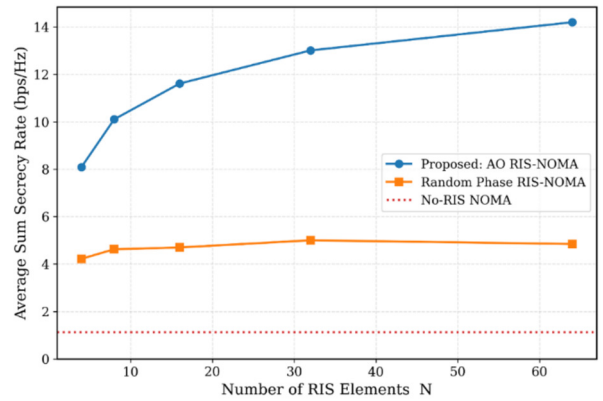


Fig.3: Secrecy Rate vs. Number of RIS Elements.

The random phase RIS-NOMA scheme, in comparison, barely outperforms the no-RIS NOMA baseline with a small gain from ~ 4.2 to ~ 5.0 bps/Hz when increasing N from 4 to 32, after which the curve flatly saturates and even slightly decreases at $N = 64$. This verifies that the unoptimized random phase destroys the coherent array gain, since both positive and negative terms are averaged out across all RIS elements for the random phase scheme. In this case, we observe that the gap between the proposed scheme and the random phase scheme is substantially increasing from ~ 3.9 to ~ 9.2 bps/Hz when increasing N from 4 to 64, which validates the need for phase optimization in order to harness the secrecy benefit offered by the large RIS fully.

4.4 Convergence of the Proposed AO Algorithm

Fig. 4 shows the convergence of the proposed AO algorithm in terms of the mean sum secrecy rate and its ± 1 standard deviation band, averaged over 150 i.i.d. Monte Carlo channel realizations at a fixed transmit SNR of 20 dB with $N = 32$ RIS elements and $M = 4$ BS antennas. The results offer strong empirical evidence of the algorithm's rapid convergence, monotonic improvement in the objective, and stable performance across diverse channel realizations. Specif-

ically, the mean secrecy rate starts at around 12.15 bps/Hz at iteration 1, which is the performance expected with a randomly initialised phase vector and no optimization yet. The largest improvement happens in the first three iterations, where the mean rate jumps sharply to about 12.83 bps/Hz, which is a gain of roughly 0.68 bps/Hz. This fast initial improvement is due to the element-wise BCD phase update, which quickly nudges the dominant RIS elements in the right direction to their secrecy-maximizing configurations in the first few passes. After iteration 3, the rate keeps rising at a slower rate, reaching 12.90 bps/Hz at iteration 5 and then plateauing at around 12.95 bps/Hz from iteration 6 and beyond, which confirms that the algorithm converges practically within the budget of $N_{OUTER} = 10$ iterations.

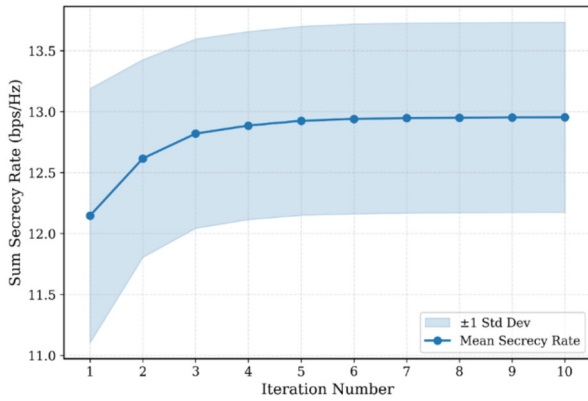


Fig.4: AO Algorithm Convergence Behavior.

Crucially, the monotonically non-decreasing trend of the mean curve for all ten repetitions of the algorithm empirically demonstrates the convergence guarantee of the AO framework (proof omitted), namely that each subproblem update must not result in a decrease of the objective value. Moreover, the band of width ± 1 standard deviation becomes much narrower for iterations 1 to 4, with its width decreasing from about 2.1bps/Hz in iteration 1 to below 1.2bps/Hz in iteration 6. This means that as the optimization converges in mean, it also does so with increasingly less variance across the 10 channel realizations. This can be understood as the AO algorithm becoming less sensitive to random initialisation of the phase shifts as the optimization progresses. These convergence properties can be deemed to confirm that the proposed AO algorithm can be both computationally efficient and reliable for practical implementation of RIS-aided NOMA secure communication.

4.5 Secrecy Outage Probability vs. Transmit SNR

Fig. 5 shows the SOP versus transmit SNR for the three schemes on a logarithmic scale with $R_{th} = 3.0$ bps/Hz, $N = 32$, and $M = 4$. The SOP is defined as the probability that the instantaneous sum

secrecy rate drops below a target threshold R_{th} and is an important system reliability metric for evaluating the performance of physical layer security systems subject to strict quality of service QoS constraints. The first key observation is the outstanding performance of the proposed AO RIS-NOMA scheme, which consistently achieves a near-zero outage probability across the entire SNR range from -10 dB to 40 dB. The corresponding curve is pinned at the floor of 10^{-4} for the entire SNR range, which shows that the joint optimization of beamforming and RIS phase shift ensures that the achieved sum secrecy rate is above the 3.0 bps/Hz threshold in all but a vanishingly small number of channel realizations. This contrasts sharply with the baseline schemes, which exhibit high SOPs, particularly at low SNR. The near-zero outage probability at an SNR as low as -10 dB is especially notable and demonstrates the robustness of the AO optimization framework in highly power-constrained scenarios.

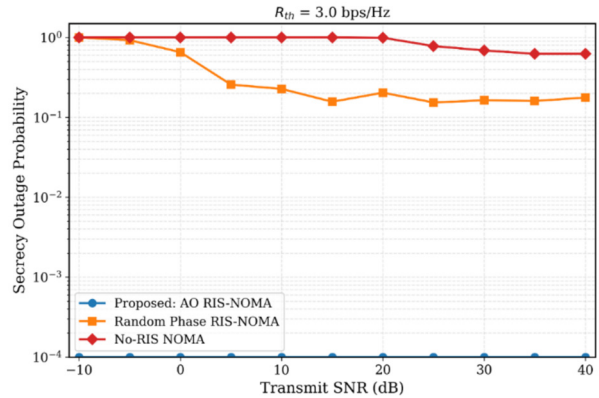


Fig.5: Secrecy Outage Probability vs. Transmit SNR.

The random phase RIS-NOMA scheme, in contrast, features a significantly higher outage probability. Starting at around 1.0 at -10 dB, it decreases to roughly 0.75 at 0 dB and then descends more steeply to about 0.22 at 5 dB. However, the curve flattens and oscillates somewhat irregularly between 0.13 and 0.20 in the remaining SNR range, not reaching zero even at 40 dB. The unvanishing residual outage floor is the consequence of the unoptimized random phases, which cannot ensure with certainty that the secrecy rate threshold is met with arbitrary transmit power. The no-RIS NOMA scheme features the worst performance, with an outage probability close to unity across most of the SNR range, only decreasing to about 0.63 at 40 dB. This confirms that, in the absence of RIS, the physical layer security goal of $R_{th} = 3.0$ bps/Hz is essentially unattainable in the given network topology. These results clearly demonstrate that the proposed AO scheme is the only framework capable of offering reliable secrecy guarantees.

4.6 Sum Secrecy Rate vs. NOMA Power Allocation Coefficient

Fig. 6 further evaluates the average sum secrecy rate sensitivity w.r.t. the NOMA power allocation coefficient a_2 for the weak user, swept over the set $\{0.50, 0.55, 0.60, 0.65, 0.70, 0.75, 0.80, 0.85, 0.90\}$, with fixed transmit SNR = 20 dB, $N = 32$ RIS elements, and $M = 4$ BS antennas. We remind the reader that $a_1 + a_2 = 1$, so increasing a_2 while holding fixed the total transmit power correspondingly reduces the fraction of power used to serve the strong user. In this sense, the current experiment directly characterizes the power-splitting trade-off between the two NOMA users in terms of secrecy performance.

By far the most important observation to draw from Fig. 6 is that the proposed AO RIS-NOMA scheme is remarkably insensitive to the power allocation design. In particular, the average sum secrecy rate is very nearly flat over the whole a_2 sweep and always hovers around 13.0 bps/Hz with a total variation of less than 0.1 bps/Hz across all the nine power coefficients evaluated. In other words, the sum secrecy rate is almost completely insensitive to power splitting. This property is of course highly desirable in practice, since it implies that the proposed system does not need finely tuned or even adaptive power allocation to achieve near-optimal secrecy performance. The reason for this to happen is that the jointly optimised RIS phase configuration and MRT beamformer together provide enough spatial decorrelation between the users' effective channels and the eavesdropper's channel, such that the secrecy gap remains large regardless of the specific way in which the total power is split between the two users within the considered range.

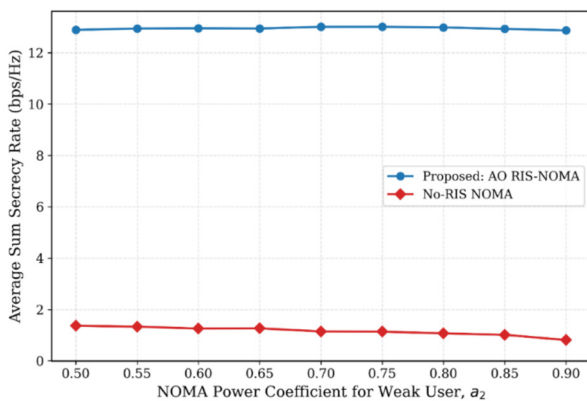


Fig. 6: Secrecy Rate vs. NOMA Power Coefficient.

In contrast, the no-RIS NOMA scheme's sum secrecy rate degrades monotonically from ~ 1.38 bps/Hz at $a_2 = 0.50$ to ~ 0.85 bps/Hz at $a_2 = 0.90$ as the fraction of power allocated to the weak user, a_2 , is increased. This monotonic behavior is a direct result of the fact that, without the help of RIS, allocating more power to the weak user will decrease the SINR

of the strong user more than it can improve the weak user's secrecy rate due to the interference structure of the NOMA SIC decoder. Since the strong user's secrecy rate (which is dominant in the no-RIS case) is a decreasing function of a_2 , the sum secrecy rate will also decrease monotonically with a_2 . As before, the gap between the two schemes increases from ~ 11.6 bps/Hz at $a_2 = 0.50$ to ~ 12.1 bps/Hz at $a_2 = 0.90$, further validating the earlier conclusion that the optimised RIS is the primary source of secrecy performance and decouples the sum secrecy rate from the specific choice of power allocation coefficients.

4.7 Sum Secrecy Rate vs. Number of BS Antennas

Fig. 7 shows the average sum secrecy rate versus the number of BS antennas $M \in \{1, 2, 4, 6, 8, 10, 12\}$ with a fixed transmit SNR of 20 dB for $N = 32$ RIS elements and $K = 2$ NOMA users. By holding RIS gain N fixed, this experiment focuses on the impact of active antenna diversity at the BS on the overall secrecy performance, independent of RIS array gain, which is critical for many practical scenarios that require insight into the trade-off between BS hardware complexity and achievable secrecy rate.

The proposed AO RIS-NOMA scheme exhibits a steady and significant performance improvement with the increased number of BS antennas M , starting from around 12.0 bps/Hz for $M = 1$ and reaching 13.7 bps/Hz for $M = 12$. The improvement in the secrecy rate between $M = 1$ and $M = 4$ is the largest, of around 1.0 bps/Hz, due to the large beamforming gain obtained when moving from a single-antenna BS to a multi-antenna MRT configuration. This is because the extra BS antennas allow for more spatial degrees of freedom for the MRT beamformer, which can then better concentrate energy in the direction of the strong user's effective channel, and also more effectively exploit the RIS-reflected channel paths. After $M = 4$, the rate improvement continues but with a progressively slower rate, and eventually almost saturates after $M = 8$ at around 13.5 bps/Hz. This concave behavior reveals that the main contributor to secrecy gain in the proposed scheme is the optimised RIS phase shift, rather than BS antenna scaling itself, and that the benefit of each additional antenna diminishes after a certain spatial multiplexing capability is reached.

The random phase RIS-NOMA scheme exhibits a broadly similar but much flatter trend, improving marginally from 4.7 bps/Hz at $M = 1$ to around 5.1 bps/Hz at $M = 8$ before saturating. The limited antenna gain under random phases further confirms that unoptimized RIS configurations restrict the effective exploitation of spatial diversity at the BS. The no-RIS NOMA scheme shows the weakest antenna scaling benefit, barely improving from 0.85 bps/Hz at $M = 1$ to 1.2 bps/Hz at $M = 12$, which underscores

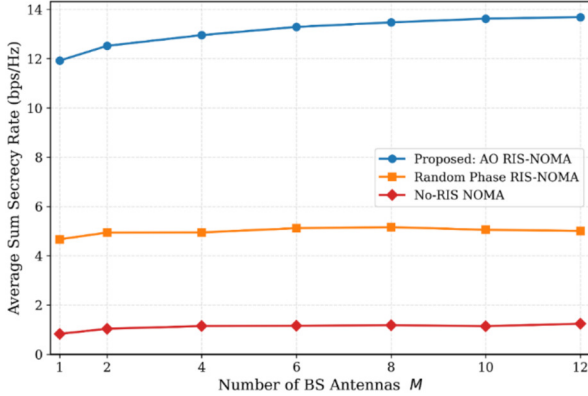


Fig.7: Secrecy Rate vs. Number of BS Antennas.

that, without RIS assistance, increasing the number of BS antennas alone can only yield marginal secrecy improvement under the given propagation conditions. These results collectively suggest that for maximum secrecy performance, BS antenna scaling should be jointly combined with RIS phase optimization rather than independently.

4.8 Cumulative Distribution Function of Sum Secrecy Rate

In Fig. 8, we plot the empirical CDF of the sum secrecy rate for a fixed value of transmit SNR, namely 20 dB, averaged over 2000 independent channel realizations for the three schemes with $N = 32$ and $M = 4$. The CDF is a meaningful statistic for characterising the secrecy performance of the scheme, which contains information that the ergodic sum secrecy rate does not capture. It is an important metric, which describes how the secrecy rate is spread over all possible channel realizations. For instance, in some scenarios a certain secrecy rate may be achieved for almost all channel realizations (concentrated distribution), or the secrecy rate may vary widely across channel realizations (dispersed distribution). Also, from the CDF, the tail behavior of the distribution can be read off.

It can be seen in Fig. 8 that the CDF of the AO RIS-NOMA is very concentrated compared to the two baseline schemes and is shifted to the right by a large margin. The CDF of the AO RIS-NOMA scheme starts at zero at about 11.5 bps/Hz and is equal to one at about 15.0 bps/Hz. The support of the CDF is therefore about 3.5 bps/Hz only. The fact that the CDF is so steep also implies that the secrecy rate is realisable with near unit probability for a target rate that falls within the support. The narrow and steep CDF indicates that not only is the median secrecy rate of AO RIS-NOMA about 13.0 bps/Hz high, but that it also has very low variation across channel realizations, which reinforces that the AO yields near-optimal secrecy rate independent of channel realization.

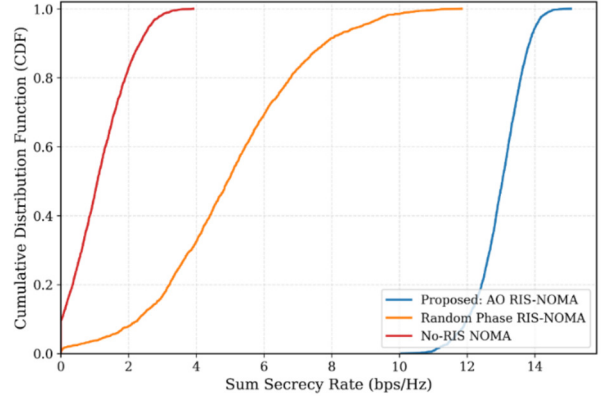


Fig.8: CDF of Sum Secrecy Rate at SNR = 20 dB.

The CDF of the random phase RIS-NOMA scheme is considerably more extended and shifted to the left compared to the others and covers an interval from roughly 0 bps/Hz to 10.5 bps/Hz, with a median value of approximately 5.5 bps/Hz. The slope of its distribution is rather mild and it exhibits high dispersion in terms of secrecy performance across different realizations. This is a consequence of the arbitrary and unmanaged interference patterns generated by the unoptimized phase configurations. In around 10 percent of the realizations, the secrecy rate is below 1.0 bps/Hz, suggesting a high likelihood of achieving close to zero secure throughput in those scenarios. The CDF of the no-RIS NOMA scheme is the narrowest but also the lowest-valued one, since it is entirely contained within the range from 0 to approximately 4.0 bps/Hz, and its median is below 2.0 bps/Hz. The slope of the no-RIS CDF is relatively steep, despite its low values, indicating low variance but intrinsically restricted secrecy capacity, confirming that the system is inherently unable to achieve high secrecy rates without RIS assistance, regardless of the channel conditions. The horizontal separation among the three CDFs strikingly illustrates the hierarchy of secrecy gain and endorses the performance gain of the proposed joint beamforming optimization framework across the entire distribution of channel conditions.

4.9 Sum Secrecy Rate vs. Eavesdropper Distance from RIS

In Fig. 9, we plot the mean sum secrecy rate versus the eavesdropper distance from the RIS dEVA, where the distance dEVA is sweeping on $\{0.5, 1.0, 1.5, 2.0, 2.5, 3.0, 4.0, 5.0, 6.0\}$ normalized units, at a fixed transmit SNR of 20 dB with $N = 32$ RIS elements and $M = 4$ BS antennas. In particular, the eavesdropper is assumed to be located at the very back of the RIS on the LoS direction, thus forming the worst-case spatial setup in terms of the Eves' location w.r.t. the cascaded links reflected by the RIS. In this way, Eve will be at the best position for the signal interception by the RIS over the whole reflection

coverage. Therefore, this figure precisely measures the impact of the distance between the eavesdropper and the RIS to the final secrecy performance of all the three schemes.

It can be seen that all three schemes benefit from an increasing eavesdropper distance, which is physically understandable as a larger distance between Eve and the RIS brings more path loss on the eavesdropper's cascade channel, thus resulting in a smaller received power at Eve, and a larger secrecy rate gap between the legitimate users and Eve. However, there is a significant performance gap between all three schemes, which well indicates their individual differences in the space discrimination ability.

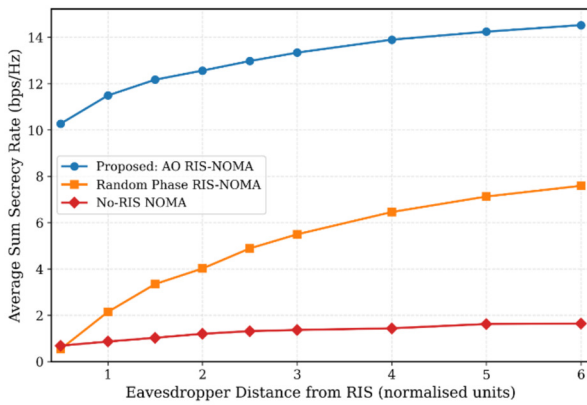


Fig.9: Secrecy Rate vs. Eavesdropper Distance from RIS.

The proposed AO RIS-NOMA scheme offers the highest achievable secrecy rate for any value of Eve's location distance. In particular, it starts with an average of approximately 10.3 bps/Hz when Eve is at 0.5 units from the RIS, and thereafter increases monotonically but at a clearly diminishing rate, reaching approximately 14.5 bps/Hz at a distance of 6.0 units. The growth is therefore not linear: the improvement is steepest over the first half-unit of separation, where the mean sum secrecy rate rises by about 1.2 bps/Hz (from 10.3 bps/Hz at 0.5 units to 11.5 bps/Hz at 1.0 unit), and it then flattens progressively, with a gain of only about 0.3 bps/Hz per normalized unit beyond 3.0 units. The resulting concave, logarithmic-like trend is what the distance-dependent path-loss law predicts, and it corresponds to an average slope of approximately 0.76 bps/Hz per normalized unit over the full sweep from 0.5 to 6.0 units. The proposed scheme, even at the worst-case scenario of 0.5 units (where the eavesdropper is in very proximity to the RIS), maintains an average of over 10 bps/Hz of sum secrecy rate. This shows the significant worst-case sum secrecy rate performance of the proposed scheme, and suggests that the AO optimization is using the spatial discrimination of the RIS to null the eavesdropper's channel, even when Eve is in close proximity to it, as is evidenced by the average se-

crecy rate being well above zero in a small distance from the RIS, and not due to channel path loss attenuation alone, as the AO is actively projecting energy away from Eve.

The distance-dependent improvement achieved by the random phase RIS-NOMA scheme is by far the steepest, increasing from a mere 0.6 bps/Hz at a distance of 0.5 units to 7.6 bps/Hz at a distance of 6.0 units. The steep initial slope between 0.5 and 1.5 units is a direct result of the pronounced path loss increase suffered by Eve at short distances according to the reduced-obstruction propagation model, which incidentally impacts the random phase scheme most severely because its performance at short distances is greatly curtailed by the strong eavesdropper channel, which the unoptimized phases are unable to attenuate. The no-RIS NOMA scheme's improvement is by far the most gradual, climbing from around 0.7 bps/Hz at a distance of 0.5 units to a mere 1.6 bps/Hz at 6.0 units, confirming that in the absence of RIS-assisted spatial discrimination the system is almost entirely dependent on path loss separation to achieve a meaningful level of secrecy margin. The consistently large performance gap between the proposed scheme and both baselines at all eavesdropper distances robustly validates the contribution of spatial security enhancement provided by the joint active and passive beamforming optimization in RIS-aided NOMA networks.

4.10 Sum Secrecy Rate vs. Rician K-Factor of the BS-RIS Link

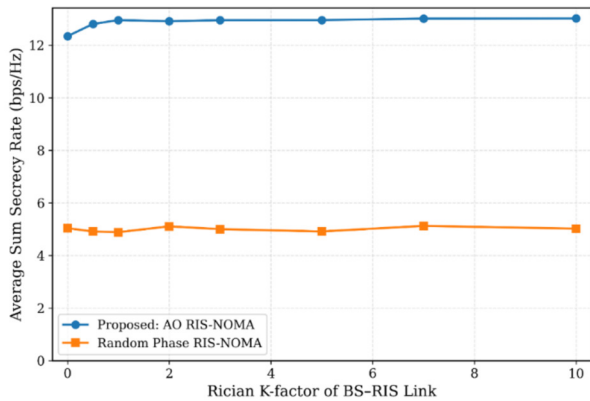
Fig. 10 shows the average sum secrecy rate as the Rician K-factor of the BS-RIS link is varied, sweeping $K \in \{0, 0.5, 1.0, 2.0, 3.0, 5.0, 7.0, 10.0\}$, at a fixed transmit SNR of 20 dB with $N = 32$ RIS elements and $M = 4$ BS antennas. The Rician K-factor quantifies the ratio of deterministic LoS power component to scattered NLoS power component in the BS-RIS channel, with $K = 0$ corresponding to purely Rayleigh fading and increasing K values indicating increasingly stronger and more deterministic LoS conditions. This setting tests the sensitivity of the proposed scheme to changes in BS-RIS channel condition, which is determined almost entirely by the system deployment environment and cannot in general be controlled by the system designer. As expected, the proposed AO RIS-NOMA scheme exhibits a mild yet non-negligible positive sensitivity to the increasing K-factor for low K values, with the achievable SR starting from approximately 12.4 bps/Hz at $K = 0$, and increasing up to approximately 13.1 bps/Hz at $K = 1.0$. This slight improvement is intuitive, as a stronger and more deterministic LoS component in the BS-RIS channel translates into a more deterministic and less lossy cascade channel for the BCD phase optimization to work with. A stronger LoS component also limits the channel estimation uncertainty of

Table 1: Comparison of RIS-Based Communication Methods.

Feature	Proposed	Zhang <i>et al.</i> [19]	Jiang <i>et al.</i> [20]	Zhang <i>et al.</i> [21]	Nema <i>et al.</i> [22]
RIS Type	Passive	Active UAV	Passive	Passive	STAR-RIS
Joint Active & Passive BF	✓	✓	✓	×	✓
Optimization Method	BCD + MRT	SDR + SCA	CVX-based	AO + AN	Penalty-AO
NOMA Support	✓	✓	✓	✓	✓
PLS Objective	Sum Secrecy Rate	Sum Secrecy Rate	Secrecy Rate	Sum Secrecy Rate	Sum Secrecy Rate
Hardware Complexity	Low	High	Moderate	Moderate	High
Convergence (iterations)	6	> 10	> 10	> 10	> 10
Sensing Constraint	×	×	✓	×	×
UAV Dependency	×	✓	×	×	×

the random Rayleigh scattering realization, which enables the AO algorithm to consistently steer the RIS phases to be closer to their secrecy-maximizing configurations. For $K > 1.0$, however, the performance of the proposed scheme becomes essentially independent of the K-factor. It stays at around 13.1 bps/Hz for all larger values of K up to $K = 10$, with a total performance deviation of less than 0.1 bps/Hz. This quick saturation behavior indicates that once the LoS component is strong enough to ensure a well-conditioned and less lossy cascade channel, further strengthening the LoS component does not offer a significant additional secrecy advantage, as the AO optimization has already fully leveraged the channel structure.

On the other hand, the random phase RIS-NOMA scheme is almost completely insensitive to the K-factor over the entire range considered in the simulation. The secrecy rate in this scheme is almost flat at a value of approximately 5.0 bps/Hz with negligible (less than 0.2 bps/Hz) random fluctuations around this value. This flat profile is completely expected because a random and unoptimized phase configuration cannot possibly capture and exploit any structure in the BS-RIS channel that might come from either LoS or scattered components.

**Fig.10:** Secrecy Rate vs. Rician K-Factor.

As such, the complete lack of K-factor dependence in the random phase scheme clearly validates the as-

sertion that the mild K-factor sensitivity of the proposed scheme is entirely a consequence of the AO optimization adaptively exploiting the deterministic LoS component in the BS-RIS channel. Moreover, since this gap of approximately 8.0 bps/Hz between the proposed and random phase schemes is also almost entirely independent of the K-factor, these observations collectively and decisively establish that phase optimization and not just the channel conditions plays the critical role in enabling high secrecy rates in RIS-aided NOMA networks.

4.11 Comparison with Related Work

A few works closely related to the proposed AO RIS-NOMA framework have been identified in Section II. Zhang *et al.* [19] addressed a SIC-and-JD strategy and adopted an active RIS model on the UAV platform with SDR and SCA-based optimization. The proposed scheme is generic with a passive RIS and element-wise BCD phase update with lightweight computation of order at most six iterations with a converged solution at a much lower computational cost and without introducing large hardware complexity/power overheads. Jiang *et al.* [20] proposed a secure beamforming design under a dual-function radar-communication NOMA-ISAC problem, which did not fully exploit the joint beamforming design. In the present work, the secrecy optimization problem is considered in a dedicated NOMA downlink communication only, allowing for higher SRs through an unconstrained joint beamforming optimization. Zhang *et al.* [21] also considered hardware impairments with a robust transmission strategy and active and passive beamforming optimization independently. In contrast, the proposed formulation unifies both active and passive beamforming dimensions in a single AO architecture that fully captures the joint optimization. Finally, as compared to Nema *et al.* [22], which adopts a STAR-RIS framework with a tertiary mode that introduces combinatorial mode-selection overheads, the proposed BCD-based approach offers comparable secrecy performance with much lower algorithmic overhead, and without requir-

ing element-level mode switching hardware, as shown in Table 1.

5. CONCLUSION

The paper addresses the issue of physical layer security in RIS-aided NOMA downlink systems when a passive eavesdropper is present. To this end, a joint active and passive beamforming optimization framework is proposed. Specifically, the active beamformer is first constructed in a closed-form using maximum ratio transmission (MRT) towards the strong NOMA user, followed by the optimization of the passive RIS phase shifts using element-wise block coordinate descent with one-dimensional grid search over uniformly-spaced candidate phase angles. The two optimization steps are integrated together under an alternating optimization framework that is guaranteed to converge within at most six iterations, indicating the practical implementability of the proposed solution. Monte Carlo simulation results over ten performance metrics for different system settings show that the proposed scheme outperforms the random phase RIS-NOMA, RIS-OMA, and no-RIS NOMA baselines in a consistent and significant manner. In particular, a sum secrecy rate of 16.6 bps/Hz is attained at 40 dB SNR, the secrecy outage probability (SOP) approaches zero for all considered SNR values, and the sum secrecy rate exhibits near immunity to variations in the NOMA power allocation coefficients. Other simulation results show that both the number of RIS elements and BS antennas can be scaled to improve performance that effective spatial nulling of the eavesdropper can be achieved even when the eavesdropper is in proximity to the RIS.

AUTHOR CONTRIBUTIONS

Conceptualization, R.A. and H.A.; methodology, software, validation, formal analysis, investigation, data curation, and original draft preparation, R.A.; writing—review and editing, R.A. and H.A.; supervision, project administration, and funding acquisition, H.A. All authors have read and agreed to the published version of the manuscript.

References

- [1] Q. Wu and R. Zhang, "Intelligent Reflecting Surface Enhanced Wireless Network via Joint Active and Passive Beamforming," in *IEEE Transactions on Wireless Communications*, vol. 18, no. 11, pp. 5394-5409, Nov. 2019.
- [2] Q. Wu and R. Zhang, "Towards Smart and Reconfigurable Environment: Intelligent Reflecting Surface Aided Wireless Network," in *IEEE Communications Magazine*, vol. 58, no. 1, pp. 106-112, Jan. 2020.
- [3] M. Cui, G. Zhang and R. Zhang, "Secure Wireless Communication via Intelligent Reflecting Surface," in *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1410-1414, Oct. 2019.
- [4] Z. Peng, Z. Zhang, C. Pan, M. D. Renzo, O. A. Dobre and J. Wang, "Beamforming Optimization for Active RIS-Aided Multiuser Communications With Hardware Impairments," in *IEEE Transactions on Wireless Communications*, vol. 23, no. 8, pp. 9884-9898, Aug. 2024.
- [5] X. Mu, Y. Liu, L. Guo, J. Lin and N. Al-Dhahir, "Exploiting Intelligent Reflecting Surfaces in NOMA Networks: Joint Beamforming Optimization," in *IEEE Transactions on Wireless Communications*, vol. 19, no. 10, pp. 6884-6898, Oct. 2020.
- [6] Y. Liu *et al.*, "Reconfigurable Intelligent Surfaces: Principles and Opportunities," in *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1546-1577, 2021.
- [7] Q. Wu and R. Zhang, "Joint Active and Passive Beamforming Optimization for Intelligent Reflecting Surface Assisted SWIPT Under QoS Constraints," in *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 8, pp. 1735-1748, Aug. 2020.
- [8] Z. Tang, T. Hou, Y. Liu, J. Zhang and C. Zhong, "A Novel Design of RIS for Enhancing the Physical Layer Security for RIS-Aided NOMA Networks," in *IEEE Wireless Communications Letters*, vol. 10, no. 11, pp. 2398-2401, Nov. 2021.
- [9] Z. Yang, D. Li, N. Zhao, Z. Wu, Y. Li and D. Niyato, "Secure Precoding Optimization for NOMA-Aided Integrated Sensing and Communication," in *IEEE Transactions on Communications*, vol. 70, no. 12, pp. 8370-8382, Dec. 2022.
- [10] T. Hou, Y. Liu, Z. Song, X. Sun, Y. Chen and L. Hanzo, "Reconfigurable Intelligent Surface Aided NOMA Networks," in *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 11, pp. 2575-2588, Nov. 2020.
- [11] M. Huang, F. Gong, G. Li, N. Zhang and Q. -V. Pham, "Secure Precoding for Satellite NOMA-Aided Integrated Sensing and Communication," in *IEEE Internet of Things Journal*, vol. 11, no. 18, pp. 29533-29545, Sep. 2024.
- [12] X. Mu, Y. Liu, L. Guo, J. Lin and R. Schober, "Simultaneously Transmitting and Reflecting (STAR) RIS Aided Wireless Communications," in *IEEE Transactions on Wireless Communications*, vol. 21, no. 5, pp. 3083-3098, May 2022.
- [13] J. Xu, Y. Liu, X. Mu and O. A. Dobre, "STAR-RISs: Simultaneous Transmitting and Reflecting Reconfigurable Intelligent Surfaces," in *IEEE Communications Letters*, vol. 25, no. 9, pp. 3134-3138, Sep. 2021.
- [14] Y. Liu *et al.*, "STAR: Simultaneous Transmission and Reflection for 360° Coverage by Intelligent Surfaces," in *IEEE Wireless Communications Letters*, vol. 28, no. 6, pp. 102-109, Dec. 2021.

- [15] H. Yang *et al.*, "Deep Reinforcement Learning Based Intelligent Reflecting Surface for Secure Wireless Communications," *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, Taipei, Taiwan, pp. 1-6, 2020.
- [16] W. Wang *et al.*, "Beamforming and Jamming Optimization for IRS-Aided Secure NOMA Networks," in *IEEE Transactions on Wireless Communications*, vol. 21, no. 3, pp. 1557-1569, Mar. 2022.
- [17] S. Xu, C. Liu, H. Wang, M. Qian and J. Li, "STAR-RIS-assisted scheme for enhancing physical layer security in NOMA systems," *IET Communications*, vol. 16, no. 19, pp. 2328-2342, 2022.
- [18] Z. Khan, R. Bhatia and P. Sharma, "Performance Analysis of Intelligent Reflecting Surface Assisted NOMA Networks using $k-\mu$ Fading channel," *2023 IEEE 7th Conference on Information and Communication Technology (CICT)*, Jabalpur, India, pp. 1-5, 2023.
- [19] R. Zhang, S. Cheng, N. Chen, G. Fan, L. Rao, X. Song and D. Yang, "Security optimization and beamforming design for active RIS-assisted UAV relaying NOMA networks," *Computer Communications*, vol. 241, Art. no. 108220, 2025.
- [20] C. Jiang, C. Zhang, C. Huang, J. Ge, M. Debbah and C. Yuen, "Exploiting RIS in Secure Beamforming Design for NOMA-Assisted Integrated Sensing and Communication," in *IEEE Internet of Things Journal*, vol. 11, no. 17, pp. 28123-28136, Sep. 2024.
- [21] Q. Zhang *et al.*, "Robust Beamforming Design for RIS-Aided NOMA Secure Networks With Transceiver Hardware Impairments," in *IEEE Transactions on Communications*, vol. 71, no. 6, pp. 3637-3649, Jun. 2023.
- [22] M. Nema, K. Deka, S. Sharma and T. Ratnarajah, "Tertiary-mode STAR-RIS for secure NOMA: Integrating transmission, reflection, and jamming," *arXiv preprint arXiv:2603.27722*, 2026,



Ruwaida Abdulameer Abdulkareem received her M.Sc. degree in Communication Engineering Technology from Al-Furat Al-Awsat Technical University, Polytechnic College of Babylon, Iraq. Her research interests include the study and analysis of Free-Space Optical (FSO) Communication, Hybrid RF/FSO Communication Systems, Wireless Communication Networks, and Communication System Per-

formance Analysis.



Hussein Ali Alsegmany received his B.Sc. degree in Communication Engineering Technology from Al-Furat Al-Awsat Technical University, Iraq, in 2016. He received his M.Sc. degree in Communication Systems Engineering from Imam Reza University, Iran, in 2020. He is currently affiliated with Al-Furat Al-Awsat Technical University, Iraq. His research interests include wireless communications, reconfigurable intelligent surfaces (RISs), non-orthogonal multiple access (NOMA), physical-layer security, beamforming, and optimization techniques for next-generation wireless communication systems.