RSMA-Enhanced Secure Transmission Scheme for Active STAR-RIS-Aided Networks

Xinying Guo, Rui Yuan, Jiankang Zhang, *Senior Member, IEEE,* Yi Song, Sheng Chen, *Life Fellow, IEEE*

***Abstract*—In this letter, a secure transmission scheme is proposed for active simultaneously transmitting and reflecting reconfigurable intelligent surface (STAR-RIS)-aided networks based on rate-splitting multiple access (RSMA). Specifically, we formulate a joint optimization problem which maximizes the minimum secrecy rate by simultaneously designing the base station beamforming vectors and the active STAR-RIS coefficient matrices. To tackle this challenging non-convexity joint optimization, we design an efficient alternating optimization algorithm, which leverages the weighted minimum mean square error method to reformulate legitimate user rates and applies successive convex approximation to handle eavesdropper rates. Simulation study shows that our proposed active STAR-RIS achieves superior security performance compared to its passive counterpart, while our RSMA strategy provides higher secrecy rates than both space-division multiple access and non-orthogonal multiple access schemes under the considered system setting.**

***Index Terms*—Active simultaneously transmitting and reflecting reconfigurable intelligent surfaces, physical layer security, rate-splitting multiple access, alternating optimization.**

I. Introduction

Simultaneously transmitting and reflecting reconfigurable intelligent surface (STAR-RIS), capable of effectively reconfiguring the wireless environment on both sides [1], has attracted considerable attention from the wireless communication research community. However, owing to the massive "multiplicative fading" effect [2], traditional passive STAR-RIS only attains limited capacity gains. To address this inherent constraint, active STAR-RIS has been proposed, incorporating elements that simultaneously adjust and amplify signals to improve achievable performance [3].

The full space covered by STAR-RIS may render the information vulnerable to eavesdropping because of the inherent broadcast characteristics of wireless channels. As a countermeasure, physical layer security (PLS) leverages the randomness of wireless channels to prevent privacy leakage by designing secure beamforming [4]. However, when eavesdroppers are spatially close to legitimate users, beamforming alone cannot guarantee secure transmission. A powerful technique for enhancing confidentiality is to inject artificial noise (AN) to weaken the decoding capability of eavesdroppers [5]. Although this approach is effective, it introduces two primary limitations: 1) it consumes additional power that would otherwise be available for useful message transmission; 2) AN inevitably impairs the signal quality for legitimate users.

By inherently supporting interference exploitation, rate-splitting multiple access (RSMA) provides a powerful approach to address the aforementioned two limitations. By spliting each legitimate user's message into common and private parts, it allows the common message to serve a dual role without consuming extra power: delivering data to legitimate users and acting as AN to confuse potential eavesdroppers [6], [7]. Under specified quality of service constraints, the work [6] addressed the optimization problem for worst-case secrecy energy efficiency. The work [7] proposed a secure transmission scheme for multiple-input single-output RSMA systems. Attracted by the potential advantages of both STAR-RIS and RSMA, recent works [8], [9] considered their integration to enhance communication security. However, these contributions are primarily confined to passive STAR-RISs in idealized single-eavesdropper scenarios, which suffer from limited performance gains due to the "multiplicative fading" effect. To address this limitation, the study [10] investigated active RIS-aided anti-jamming communications from a security confrontation perspective, demonstrating significant gains over passive designs. Nevertheless, this work fails to exploit the advantages of RSMA technology, which serves as a more potent paradigm for security enhancement.

To bridge this gap, we propose a novel secure transmission scheme that systematically integrates RSMA with active STAR-RIS technology to combat the threats posed by multiple eavesdroppers. The primary objective is to ensure both fairness and confidentiality among legitimate users by maximizing the minimum secrecy rate, which is achieved through the joint optimization of the base station (BS) beamforming vectors and the active STAR-RIS coefficient matrices. To effectively solve this challenging non-convex joint optimization, an alternating optimization (AO) algorithm based on the weighted minimum mean square error (WMMSE) and successive convex approximation (SCA) techniques is designed. In our proposed algo-

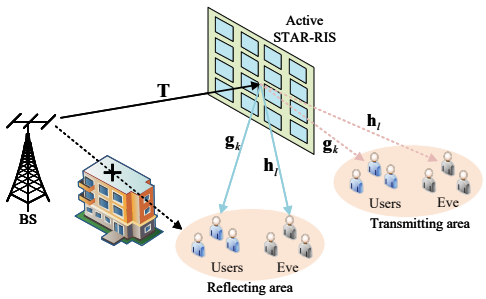


Fig. 1. RSMA-enhanced secure active STAR-RIS communication system.

This work was supported by the National Natural Science Foundation of China (Grants 61901159).

X. Guo, R. Yuan and Y. Song are with Key Laboratory of Grain Information Processing and Control (Henan University of Technology), Ministry of Education, and also with College of Information Science and Engineering, Henan University of Technology, Zhengzhou 450001, China (E-mails: guoxinying@haut.edu.cn, yuanrui@stu.haut.edu.cn and songyi@haut.edu.cn).

J. Zhang is with Department of Computing & Informatics, Bournemouth University, BH12 5BB, UK (E-mail: jzhang3@bournemouth.ac.uk).

S. Chen is with School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, UK (E-mail: sqc@ecs.soton.ac.uk).

rithm, WMMSE is employed to reformulate the legitimate user rates, while SCA is utilized to handle the eavesdropping rates. Simulation study confirms that active STAR-RIS effectively mitigates the multiplicative fading of passive designs, and the results obtained demonstrated that our proposed scheme achieves superior security performance over the space-division multiple access (SDMA) and non-orthogonal multiple access (NOMA)-based baselines.

II. Active STAR-RIS Network with RSMA

Fig. 1 depicts the secure communication system leveraging an active STAR-RIS, where RSMA is adopted to enhance transmission security. An M-antenna BS and an N-element active STAR-RIS are deployed in the network. The active STAR-RIS elements are indexed by the set $\mathcal{N}=\{1,\ldots,N\}$. K legitimate users indexed by the set $\mathcal{K}=\{1,\ldots,K\}$ and L eavesdroppers indexed by the set $\mathcal{L}=\{1,\ldots,L\}$ are present, all assumed with a single antenna. The legitimate users and eavesdroppers located in the reflecting area are indexed by $\mathcal{K}_{\rm r}=\{1,\ldots,k_0\}$ and $\mathcal{L}_{\rm r}=\{1,\ldots,l_0\}$, respectively, while those in the transmitting area are indexed by $\mathcal{K}_{\rm t}=\{k_0+1,\ldots,K\}$ and $\mathcal{L}_{\rm t}=\{l_0+1,\ldots,L\}$.

It is assumed that the direct links connecting the BS to all legitimate users and eavesdroppers are blocked by tall buildings. Let the channel linking the BS to the active STAR-RIS be $\mathbf{T}\in\mathbb{C}^{N\times M}$, and denote the channels linking the active STAR-RIS to legitimate user k and to eavesdropper l as $\mathbf{g}_k\in\mathbb{C}^{N\times 1}$, $\forall k\in\mathcal{K}$, and $\mathbf{h}_l\in\mathbb{C}^{N\times 1}$, $\forall l\in\mathcal{L}$, respectively. The active STAR-RIS employs energy-splitting protocol, with all its elements concurrently handling reflection and transmission. The corresponding reflection and transmission matrices are respectively $\mathbf{\Phi}_{\rm r}=\mathrm{diag}(\mathbf{v}_{\rm r})$ and $\mathbf{\Phi}_{\rm t}=\mathrm{diag}(\mathbf{v}_{\rm t})$, where $\mathbf{v}_i$ $(i\in\{\mathrm{r},\mathrm{t}\})$ are structured as $[\beta_{i,1}e^{j\theta_{i,1}},\ldots,\beta_{i,N}e^{j\theta_{i,N}}]$, with $\beta_{i,n}>0$ and $\theta_{i,n}\in[0,2\pi)$ being the nth element's amplification factor and phase shift.

A. Signal Model

RSMA divides each legitimate user's message into the two parts: common part and private part. The common parts from all legitimate users are jointly encoded into a common stream x_c, and the private part of legitimate user k is encoded into a dedicated private stream x_k, with the power of both x_c and x_k normalized to 1. Collectively denoted by $[x_c,x_1,\ldots,x_K]^{\rm T}$, these streams undergo linear precoding with beamforming vectors $\mathbf{w}_c\in\mathbb{C}^{M\times 1}$ for x_c and $\mathbf{w}_k\in\mathbb{C}^{M\times 1}$ for x_k. Therefore, the composite transmit signal is $\mathbf{x}=\mathbf{w}_c x_c+\sum_{k\in\mathcal{K}}\mathbf{w}_k x_k$. Accordingly, the signals received at the kth legitimate user and at the lth eavesdropper are expressed respectively as

$$y_k=\mathbf{g}_k^{\rm H}\mathbf{\Phi}_i\mathbf{T}\mathbf{x}+\mathbf{g}_k^{\rm H}\mathbf{\Phi}_i\mathbf{z}+n_k,\ \forall k\in\mathcal{K}_i,\ i\in\{\mathrm{r},\mathrm{t}\},\quad(1a)$$

$$y_l=\mathbf{h}_l^{\rm H}\mathbf{\Phi}_i\mathbf{T}\mathbf{x}+\mathbf{h}_l^{\rm H}\mathbf{\Phi}_i\mathbf{z}+n_l,\ \forall l\in\mathcal{L}_i,\ i\in\{\mathrm{r},\mathrm{t}\},\quad(1b)$$

where $\mathbf{z}\sim\mathcal{CN}(\mathbf{0}_N,\sigma_0^2\mathbf{I}_{N\times N})$ is the thermal noise introduced by the active STAR-RIS, while $n_k\sim\mathcal{CN}(0,\sigma_k^2)$ and $n_l\sim\mathcal{CN}(0,\sigma_l^2)$ are the additive white Gaussian noises at legitimate user k and eavesdropper l. Therefore the average received signal powers at legitimate user k and eavesdropper l can be calculated as in (2) at the bottom of this page.

According to RSMA decoding principle, each legitimate user decodes the common stream first by considering all private streams as interference and then uses successive interference cancellation (SIC) to remove this decoded common signal before recovering its own private stream [11]. Hence, the signal-to-interference-plus-noise ratios (SINRs) for decoding the common and private streams at the kth legitimate user can be expressed respectively as

$$\gamma_{c,k}=S_{c,k}I_{c,k}^{-1}\ \text{and}\ \gamma_{p,k}=S_{p,k}I_{p,k}^{-1}.\quad(3)$$

The corresponding achievable rates are expressed as

$$R_{c,k}=\log(1+\gamma_{c,k})\ \text{and}\ R_{p,k}=\log(1+\gamma_{p,k}).\quad(4)$$

To ensure that every legitimate user can successfully decode the common stream, the common rate is restricted to $R_c=\min_{k\in\mathcal{K}}\{R_{c,k}\}$.

Given that eavesdroppers may also employ SIC to intercept both common and private messages, the common message itself can act as AN to degrade their decoding performance. The corresponding SINRs for the lth eavesdropper to decode the common stream and the kth legitimate user's private stream are therefore expressed as

$$\gamma_{c,l}=S_{c,l}I_{c,l}^{-1}\ \text{and}\ \gamma_{k,l}=S_{k,l}(S_{c,l}+I_{k,l})^{-1}.\quad(5)$$

The corresponding achievable rates are given by

$$R_{c,l}=\log(1+\gamma_{c,l})\ \text{and}\ R_{k,l}=\log(1+\gamma_{k,l}).\quad(6)$$

For the common message to effectively serve as AN, the condition $R_c>\max_{l\in\mathcal{L}}\{R_{c,l}\}$ must hold. Moreover, the common secrecy rate must be shared by all legitimate users, which requires $\sum_{k\in\mathcal{K}}R_{c,k}^{\rm sec}\le R_c-\max_{l\in\mathcal{L}}\{R_{c,l}\}$, where $R_{c,k}^{\rm sec}$ is the common secrecy rate allocated to legitimate user k.

$$T_{c,k}=\overbrace{\left|\mathbf{g}_k^{\rm H}\mathbf{\Phi}_i\mathbf{T}\mathbf{w}_c\right|^2}^{S_{c,k}}+\underbrace{\overbrace{\left|\mathbf{g}_k^{\rm H}\mathbf{\Phi}_i\mathbf{T}\mathbf{w}_k\right|^2}^{S_{p,k}}+\overbrace{\sum_{j=1,j\neq k}^{K}\left|\mathbf{g}_k^{\rm H}\mathbf{\Phi}_i\mathbf{T}\mathbf{w}_j\right|^2+\sigma_0^2\left\|\mathbf{g}_k^{\rm H}\mathbf{\Phi}_i\right\|^2+\sigma_k^2}^{I_{p,k}}}_{I_{c,k}=T_{p,k}},\ \forall k\in\mathcal{K}_i,i\in\{\mathrm{r},\mathrm{t}\},\quad(2a)$$

$$T_{c,l}=\overbrace{\left|\mathbf{h}_l^{\rm H}\mathbf{\Phi}_i\mathbf{T}\mathbf{w}_c\right|^2}^{S_{c,l}}+\underbrace{\overbrace{\left|\mathbf{h}_l^{\rm H}\mathbf{\Phi}_i\mathbf{T}\mathbf{w}_k\right|^2}^{S_{k,l}}+\overbrace{\sum_{j=1,j\neq k}^{K}\left|\mathbf{h}_l^{\rm H}\mathbf{\Phi}_i\mathbf{T}\mathbf{w}_j\right|^2+\sigma_0^2\left\|\mathbf{h}_l^{\rm H}\mathbf{\Phi}_i\right\|^2+\sigma_l^2}^{I_{k,l}}}_{I_{c,l}=T_{k,l}},\ \forall l\in\mathcal{L}_i,i\in\{\mathrm{r},\mathrm{t}\}.\quad(2b)$$

Consequently, the total secrecy rate of legitimate user k can be expressed as

$$R_k^{\text{sec}} = R_{c,k}^{\text{sec}} + [R_{p,k} - \max_{l\in\mathcal{L}}\{R_{k,l}\}]^+, \tag{7}$$

where $[x]^+ = \max\{x, 0\}$.

B. Problem Formulation

Our objective is to maximize the minimum secrecy rate among all legitimate users by jointly optimizing the BS beamforming vectors and the active STAR-RIS coefficient matrices. This leads to the joint optimization problem

$$\max_{\mathbf{w}_c,\mathbf{w}_k,\mathbf{\Phi}_i,\{R_{c,k}^{\text{sec}}\}} \min_{k\in\mathcal{K}} R_k^{\text{sec}} \tag{8a}$$

$$\text{s.t.} \sum_{j\in\mathcal{K}_1} \|\mathbf{w}_j\|^2 \le P_{\text{BS}}, \tag{8b}$$

$$\sum_{i\in\{\text{r,t}\}} \left(\sum_{j\in\mathcal{K}_1} \|\mathbf{\Phi}_i\mathbf{T}\mathbf{w}_j\|^2 + \sigma_0^2\|\mathbf{\Phi}_i\|_{\text{F}}^2 \right) \le P_{\text{RIS}}, \tag{8c}$$

$$\sum_{k\in\mathcal{K}} R_{c,k}^{\text{sec}} \le R_c - \max_{l\in\mathcal{L}}\{R_{c,l}\}, \tag{8d}$$

$$R_{c,k}^{\text{sec}} \ge 0, \ \forall k, \tag{8e}$$

$$\beta_{\text{r},n}^2 + \beta_{\text{t},n}^2 \le \beta_{\max}, \ \forall n, \tag{8f}$$

where $\mathcal{K}_1 = \{c, 1, \ldots, K\}$, P_{BS} and P_{RIS} denote the power thresholds at the BS and active STAR-RIS, respectively, with the corresponding constraints given in (8b) and (8c), while (8d) and (8e) represent the constraints on the common secrecy rate allocation, and (8f) models the hardware limitations on the elements of the active STAR-RIS. The optimization (8) is non-convex because the variables $\mathbf{w}_c$, $\mathbf{w}_k$ and $\mathbf{\Phi}_i$ are highly coupled. Thus it cannot be solved directly.

III. Algorithm Design

We develop an AO framework to solve the challenging optimization (8), incorporating both WMMSE and SCA techniques. Specifically, WMMSE is utilized to transform the legitimate rate expressions, while SCA is applied to approximate the eavesdropping rates. Finally, we analyze its computational complexity and convergence.

A. Problem Reformulation

To make the problem (8) more tractable, we define

$$\mathbf{g}_k^{\text{H}}\mathbf{\Phi}_i\mathbf{T} = \mathbf{v}_i\mathbf{G}_k \text{ and } \mathbf{h}_l^{\text{H}}\mathbf{\Phi}_i\mathbf{T} = \mathbf{v}_i\mathbf{H}_l, \tag{9}$$

where $\mathbf{G}_k = \text{diag}(\mathbf{g}_k^{\text{H}})\mathbf{T}$ and $\mathbf{H}_l = \text{diag}(\mathbf{h}_l^{\text{H}})\mathbf{T}$ for $k \in \mathcal{K}_i$, $l \in \mathcal{L}_i$ and $i \in \{\text{r,t}\}$. Based on (9), the received power in (2a) can be updated to (10), as shown at the bottom of this page, which is then used to recalculate the legitimate users' rates. Similarly, constraint (8c) can be updated to

$$\sum_{i\in\{\text{r,t}\}} \left(\sum_{j\in\mathcal{K}_1} \|\text{diag}(\mathbf{T}\mathbf{w}_j)\mathbf{v}_i\|^2 + \sigma_0^2\|\mathbf{v}_i\|^2 \right) \le P_{\text{RIS}}. \tag{11}$$

Then we introduce a non-negative auxiliary variable R^{sec} to tackle the non-smoothness in (8a). Therefore, the problem (8) can be transformed to

$$\max_{\mathbf{w}_c,\mathbf{w}_k,\mathbf{v}_i,\{R_{c,k}^{\text{sec}}\},R^{\text{sec}}} R^{\text{sec}} \tag{12a}$$

$$\text{s.t.} \sum_{k\in\mathcal{K}} R_{c,k}^{\text{sec}} \le R_{c,k} - R_{c,l}, \ \forall l \in \mathcal{L}, \tag{12b}$$

$$R_{c,k}^{\text{sec}} + R_{p,k} - R_{k,l} \ge R^{\text{sec}}, \ \forall k \in \mathcal{K}, \forall l \in \mathcal{L}, \tag{12c}$$

$$\text{(8b), (8e), (8f), (11).} \tag{12d}$$

B. Problem Solving

The strong coupling among the variables $\mathbf{w}_c$, $\mathbf{w}_k$ and $\mathbf{v}_i$ renders the problem (12) challenging to solve directly. We employ WMMSE to recast the legitimate rates. In particular, the kth legitimate user utilizes equalizer $g_{c,k}$ to recover the common stream x_c. Upon eliminating the common stream, the private stream is subsequently recovered using the equalizer $g_{p,k}$. Therefore, the estimated common and private signals at the kth legitimate user are expressed as $\hat{x}_{c,k} = g_{c,k}y_k$ and $\hat{x}_{p,k} = g_{p,k}(y_k - \mathbf{v}_i\mathbf{G}_k\mathbf{w}_c x_c)$, respectively. The mean square errors (MSEs) of these two estimates can be expressed as

$$\begin{aligned}\varepsilon_{c,k} &= \mathbb{E}\left\{|\hat{x}_{c,k} - x_{c,k}|^2\right\} \\ &= |g_{c,k}|^2 T_{c,k} - 2\Re\left(g_{c,k}\mathbf{v}_i\mathbf{G}_k\mathbf{w}_c\right) + 1,\end{aligned} \tag{13a}$$

$$\begin{aligned}\varepsilon_{p,k} &= \mathbb{E}\left\{|\hat{x}_{p,k} - x_{p,k}|^2\right\} \\ &= |g_{p,k}|^2 T_{p,k} - 2\Re\left(g_{p,k}\mathbf{v}_i\mathbf{G}_k\mathbf{w}_k\right) + 1.\end{aligned} \tag{13b}$$

By setting $\frac{\partial\varepsilon_{c,k}}{\partial g_{c,k}} = 0$ and $\frac{\partial\varepsilon_{p,k}}{\partial g_{p,k}} = 0$, the optimal equalizers are given by

$$g_{c,k}^{\text{MMSE}} = (\mathbf{v}_i\mathbf{G}_k\mathbf{w}_c)^{\text{H}} T_{c,k}^{-1} \text{ and } g_{p,k}^{\text{MMSE}} = (\mathbf{v}_i\mathbf{G}_k\mathbf{w}_k)^{\text{H}} T_{p,k}^{-1}. \tag{14}$$

Plugging the optimal equalizers into (13), the minimized MSE (MMSE) is given by

$$\varepsilon_{\delta,k}^{\text{MMSE}} = \min_{g_{\delta,k}} \varepsilon_{\delta,k} = T_{\delta,k}^{-1} I_{\delta,k}, \ \forall \delta \in \{c, p\}. \tag{15}$$

The corresponding SINR in (3) can be rewritten as $\gamma_{\delta,k} = \frac{1}{\varepsilon_{\delta,k}^{\text{MMSE}}} - 1$. The corresponding rate is $R_{\delta,k} = -\log\left(\varepsilon_{\delta,k}^{\text{MMSE}}\right)$ for $\forall \delta \in \{c, p\}$. The common and private augmented weighted MSEs at the kth legitimate user are defined by

$$\zeta_{\delta,k} = \eta_{\delta,k}\varepsilon_{\delta,k} - \log(\eta_{\delta,k}), \ \forall \delta \in \{c, p\}, \tag{16}$$

where $\eta_{\delta,k}$ denotes the positive weight of the MSE. Then, the optimal equalizers are obtained by solving $\frac{\partial\zeta_{\delta,k}}{\partial g_{\delta,k}} = 0$, which yields $g_{\delta,k}^* = g_{\delta,k}^{\text{MMSE}}$. Consequently, the optimal augmented weighted MSEs become

$$\zeta_{\delta,k}(g_{\delta,k}^{\text{MMSE}}) = \eta_{\delta,k}\varepsilon_{\delta,k}^{\text{MMSE}} - \log(\eta_{\delta,k}), \ \forall \delta \in \{c, p\}. \tag{17}$$

By further solving $\frac{\partial\zeta_{\delta,k}(g_{\delta,k}^{\text{MMSE}})}{\partial\eta_{\delta,k}} = 0$, the optimal weight is expressed as

$$\eta_{\delta,k}^* = \eta_{\delta,k}^{\text{MMSE}} = \left(\varepsilon_{\delta,k}^{\text{MMSE}}\right)^{-1}, \ \forall \delta \in \{c, p\}. \tag{18}$$

$$T_{c,k} = \overbrace{\left|\mathbf{v}_i\mathbf{G}_k\mathbf{w}_c\right|^2}^{S_{c,k}} + \underbrace{\overbrace{\left|\mathbf{v}_i\mathbf{G}_k\mathbf{w}_k\right|^2}^{S_{p,k}} + \overbrace{\sum_{j=1,j\neq k}^{K} \left|\mathbf{v}_i\mathbf{G}_k\mathbf{w}_j\right|^2 + \sigma_0^2\left\|\mathbf{v}_i\text{diag}\left(\mathbf{g}_k^{\text{H}}\right)\right\|^2 + \sigma_k^2}^{I_{p,k}}}_{I_{c,k}=T_{p,k}}, \ \forall k \in \mathcal{K}_i, i \in \{\text{r,t}\}. \tag{10}$$

Substituting (18) into (17), the relationship between the legitimate rate and WMMSE is established as

$$\zeta_{\delta,k}^{\mathrm{MMSE}} = 1 - R_{\delta,k},\ \forall \delta \in \{c,p\}. \tag{19}$$

However, eavesdropping rate is non-convex, making the problem (12) challenging to solve. To obtain a feasible solution, the eavesdropping rate should be approximated by its upper bounds. This requirement leads to the infeasibility of the WMMSE. To address this challenge, we introduce the non-negative auxiliary variables λ_l with $\forall l \in \mathcal{L}$. Then the negative rates of eavesdropper l can be divided into

$$-R_{j,l} \geq \log\left(1 - |\mathbf{v}_i\mathbf{H}_l\mathbf{w}_j|^2\lambda_l^{-1}\right), \forall j \in \mathcal{K}_1, \tag{20}$$

and

$$\lambda_l \leq \sum_{j\in\mathcal{K}_1} |\mathbf{v}_i\mathbf{H}_l\mathbf{w}_j|^2 + \sigma_0^2\left\|\mathbf{v}_i\mathrm{diag}\left(\mathbf{h}_l^{\mathrm{H}}\right)\right\|^2 + \sigma_l^2. \tag{21}$$

Although constraint (20) is convex, constraint (21) is non-convex. To address this difficulty, given the local points $\mathbf{w}_j^{(t)}$ and $\mathbf{v}_i^{(t)}$ at the tth iteration, we apply SCA to approximate (21) with the concave lower bound (22), as shown at the bottom of this page. Leveraging the aforementioned reformulations, we can rewrite the problem (12) as

$$\max_{\substack{\mathbf{w}_c,\mathbf{w}_k,\mathbf{v}_i,\\ g_{\delta,k},\eta_{\delta,k},\{R_{c,k}^{\mathrm{sec}}\},R^{\mathrm{sec}}}} \quad R^{\mathrm{sec}} \tag{23a}$$

$$\text{s.t.} \sum_{k\in\mathcal{K}} R_{c,k}^{\mathrm{sec}} \leq 1 - \min_{\eta_{c,k},g_{c,k}} \zeta_{c,k} + \log\left(1 - |\mathbf{v}_i\mathbf{H}_l\mathbf{w}_c|^2\lambda_l^{-1}\right),$$
$$\forall k \in \mathcal{K}_i, \forall l \in \mathcal{L}_i, i \in \{\mathrm{r},\mathrm{t}\}, \tag{23b}$$

$$R_{c,k}^{\mathrm{sec}} - \min_{\eta_{p,k},g_{p,k}} \zeta_{p,k} + \log\left(1 - |\mathbf{v}_i\mathbf{H}_l\mathbf{w}_k|^2\lambda_l^{-1}\right)$$
$$\geq R^{\mathrm{sec}} - 1,\ \forall k \in \mathcal{K}_i, \forall l \in \mathcal{L}_i, i \in \{\mathrm{r},\mathrm{t}\}, \tag{23c}$$

$$\text{(8b)},\ \text{(8e)},\ \text{(8f)},\ \text{(11)},\ \text{(22)}. \tag{23d}$$

The problem (23) remains non-convex, rendering its direct resolution intractable. However, by splitting the coupled variables into three blocks: $\{g_{\delta,k},\eta_{\delta,k}\}$, $\{\mathbf{w}_c,\mathbf{w}_k\}$ and $\{\mathbf{v}_i\}$, the problem exhibits convexity with respect to any individual block when the other two are fixed. Specifically, the block $\{g_{\delta,k},\eta_{\delta,k}\}$ can be updated in the closed form based on (14) and (18), while the blocks $\{\mathbf{w}_c,\mathbf{w}_k\}$ and $\{\mathbf{v}_i\}$ are optimized using standard convex solvers such as CVX. This observation prompts the application of the AO algorithm to address the problem. The detailed algorithmic procedure of this AO framework is summarized in Algorithm 1.

Algorithm 1 AO Algorithm Based on WMMSE and SCA

1: **Initialize** $\mathbf{w}_c^{(0)}$, $\mathbf{w}_k^{(0)}$ and $\mathbf{v}_i^{(0)}$, give the convergence threshold ω, and set the iteration index $t=0$.
2: **Repeat**
3: $t \leftarrow t+1$.
4: Update $g_{\delta,k}^{(t)}$ and $\eta_{\delta,k}^{(t)}$ based on (14) and (18);
5: Solving the problem (23) to update $\mathbf{w}_c^{(t)}$ and $\mathbf{w}_k^{(t)}$;
6: Solving the problem (23) to update $\mathbf{v}_i^{(t)}$;
7: **Until** the improvement in the objective value is smaller than a predefined threshold ω.

C. Complexity and Convergence Analysis

At each iteration of Algorithm 1, the computational complexity arises from three parts: 1) the estimation of power components conducted through WMMSE updates with a complexity of $\mathcal{O}(K(K+1)NM)$; 2) the construction of convex upper bounds achieved by SCA reformulation with a complexity of $\mathcal{O}\left(L(K+1)NM\right)$; and 3) the joint optimization of $\{\mathbf{w}_c,\mathbf{w}_k\}$ and $\{\mathbf{v}_i\}$ performed using the interior-point technique with a complexity of $\mathcal{O}\left((M(K+1))^{3.5}+(2N+2)^{3.5}\right)$. Consequently, the total computational complexity per iteration is on the order of $\mathcal{O}\left(K^2NM+(M(K+1))^{3.5}+(2N+2)^{3.5}\right)$.

Given a feasible initial point, the algorithm maintains feasibility across iterations. Let $R\left(\mathbf{w}_c^{(t)},\mathbf{w}_k^{(t)},\mathbf{v}_i^{(t)}\right)$ denote the objective function at the tth iteration. Following steps 5 and 6 of the proposed algorithm, we can obtain

$$R\left(\mathbf{w}_c^{(t+1)},\mathbf{w}_k^{(t+1)},\mathbf{v}_i^{(t+1)}\right) \geq R\left(\mathbf{w}_c^{(t+1)},\mathbf{w}_k^{(t+1)},\mathbf{v}_i^{(t)}\right)$$
$$\geq R\left(\mathbf{w}_c^{(t)},\mathbf{w}_k^{(t)},\mathbf{v}_i^{(t)}\right), \tag{24}$$

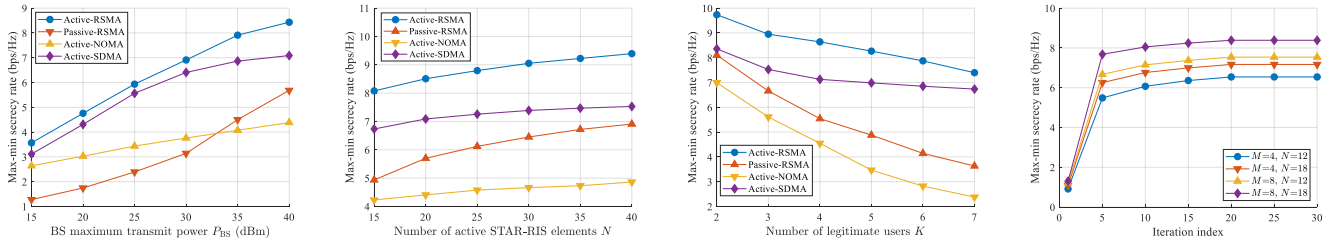
which shows that the objective function is monotonically non-decreasing. Moreover, the objective function possesses a finite upper bound imposed by the power constraints, and thus the convergence of Algorithm 1 is assured.

IV. Simulation Study and Results Analysis

We evaluate the secrecy performance of our proposed RSMA-enhanced active STAR-RIS scheme (Active-RSMA) through comprehensive numerical simulations. We benchmark our design against the RSMA-enhanced passive STAR-RIS (Passive-RSMA), which lacks signal amplification and introduces no thermal noise, with coefficients satisfying $\beta_{\mathrm{r},n}^2 + \beta_{\mathrm{t},n}^2 = 1, \forall n$. We further compare our design with the active STAR-RIS based on SDMA and NOMA schemes (Active-SDMA and Active-NOMA).

In the simulation setup, the BS is located at $(0,0)$ m, while the active STAR-RIS is deployed at $(10,20)$ m. The legitimate users and eavesdroppers are independently and uniformly distributed in a square region $(0,20)\times(0,20)$ m^2, where the area is split into a reflecting area for $x<10$ m and a transmitting area for $x>10$ m. This work adopts a Rician fading channel model with large-scale attenuation, following the setup in [8]. The model parameters include a reference path loss of -30 dB at 1 m, a path loss exponent of 2.2 and a Rician factor of 10 for all links. Other system parameters are set as: $M=8$, $N=20$, $K=4$, $L=2$, $\beta_{\max}=40$, $P_{\mathrm{BS}}=40$ dBm, $P_{\mathrm{RIS}}=30$ dBm and $\sigma_0^2=\sigma_k^2=\sigma_l^2=-84$ dBm, $\forall k,\forall l$. To investigate the performance upper bound of the proposed secrecy scheme, similar to [9], we assume that instantaneous channel state information (CSI) of all the channel links are available at the

$$\lambda_l \leq \sum_{j\in\mathcal{K}_1}\left(2\Re\left(\mathbf{v}_i^{(t)}\mathbf{H}_l\mathbf{w}_j^{(t)}\mathbf{w}_j^{\mathrm{H}}\mathbf{H}_l^{\mathrm{H}}\left(\mathbf{v}_i^{(t)}\right)^{\mathrm{H}}\right) - \left|\mathbf{v}_i^{(t)}\mathbf{H}_l\mathbf{w}_j^{(t)}\right|^2\right) + \sum_{j\in\mathcal{K}_1}\left(2\Re\left(\mathbf{v}_i^{(t)}\mathbf{H}_l\mathbf{w}_j^{(t)}\left(\mathbf{w}_j^{(t)}\right)^{\mathrm{H}}\mathbf{H}_l^{\mathrm{H}}\mathbf{v}_i^{\mathrm{H}}\right) - \left|\mathbf{v}_i^{(t)}\mathbf{H}_l\mathbf{w}_j^{(t)}\right|^2\right)$$
$$+ 2\Re\left(\mathbf{v}_i^{(t)}\mathrm{diag}\left(\mathbf{h}_l^{\mathrm{H}}\right)\left(\mathrm{diag}\left(\mathbf{h}_l^{\mathrm{H}}\right)\right)^{\mathrm{H}}\mathbf{v}_i^{\mathrm{H}}\right)\sigma_0^2 - \sigma_0^2\left\|\mathbf{v}_i^{(t)}\mathrm{diag}\left(\mathbf{h}_l^{\mathrm{H}}\right)\right\|^2 + \sigma_l^2. \tag{22}$$



(a) (b) (c) (d)

Fig. 2. Performance comparison of four schemes: (a) max-min secrecy rate versus BS maximum transmit power P_{BS}, (b) max-min secrecy rate versus the number of STAR-RIS elements N, and (c) max-min secrecy rate versus the number of legitimate users K, as well as convergence of Algorithm 1: (d).

BS. The case of imperfect CSI as noted in [11] is beyond the scope of this study and is reserved for future research.

Fig. 2 (a) depicts the max–min secrecy rate versus BS maximum transmit power P_{BS}. As expected, the max–min secrecy rates of all the four schemes increases with P_{BS}. Our proposed scheme significantly outperforms both the SDMA and NOMA schemes, and the performance gap with SDMA further widens at higher power levels. This is because interference becomes increasingly dominant in the SDMA scheme as P_{BS} increases, causing its secrecy rate to gradually saturate. Moreover, the NOMA-based scheme suffers from stringent successive decoding constraints, which degrade its secrecy performance. In contrast, the proposed scheme fully exploits the dual role of the common stream, thereby avoiding rate saturation and demonstrating its effectiveness. In addition, our proposed scheme achieves superior secrecy capacity over the passive STAR-RIS counterpart, proving its effectiveness in overcoming the "multiplicative fading" effect.

Fig. 2 (b) plots the max–min secrecy rate versus the number of STAR-RIS elements N. Clearly, the max-min secrecy rates of all the four schemes increase with N, since a larger N provides more spatial degrees of freedom to strengthen cascaded channels and enable more effective beamforming design, thus enhancing secrecy performance. Our proposed scheme consistently surpasses the three benchmark schemes across all considered values of N. Moreover, the performance margin of our proposed RSMA scheme over the second-best SDMA scheme expands with a larger N, confirming the effectiveness of our design. Furthermore, compared with its passive STAR-RIS counterpart, the active STAR-RIS achieves an average secrecy rate gain of about 2.3 bps/Hz over the considered range of N. The result fully indicates that the active STAR-RIS can produce greater performance benefits with fewer elements than its passive counterpart.

Fig. 2 (c) depicts the max–min secrecy rate performance of different schemes under different numbers of legitimate users K. Two interesting phenomena can be observed. First, the secrecy advantage of our proposed scheme over the second best SDMA scheme decreases as K increases. This is because the common rate in RSMA is constrained by the minimum decoding capability among the K users, and its secrecy rate must be allocated to the entire group. Second, the superiority of the proposed design over the passive STAR-RIS and NOMA benchmarks becomes more pronounced as K increases. The passive STAR-RIS suffers more severely from multi-user interference due to the lack of active amplification and interference control, while the NOMA scheme is constrained by strict decoding requirements, causing its secrecy performance to degrade more rapidly as K increases.

The convergence behavior of Algorithm 1 is assessed in Fig. 2 (d) for different numbers of BS antennas M and active STAR-RIS elements N. In all configurations, the curves demonstrate monotonic improvement before reaching stable plateaus, thereby verifying the convergence guarantee established in our analysis.

V. Conclusions

In this work, we have addressed the challenge of secure transmission in active STAR-RIS based networks. Our proposed solution synergistically integrates RSMA, where a joint beamforming and RIS configuration optimization is formulated to maximize the minimum secrecy rate. To solve this challenging joint optimization, we have devised an efficient algorithm based on AO, WMMSE and SCA. Numerical simulations demonstrate that this approach yields a considerable enhancement in secrecy performance compared to benchmarks employing passive STAR-RIS, SDMA or NOMA.

References

[1] Y. Liu, *et al.*, "STAR: Simultaneous transmission and reflection for 360° coverage by intelligent surfaces," *IEEE Wireless Commun.*, vol. 28, no. 6, pp. 102–109, Dec. 2021.

[2] Z. Zhang, *et al.*, "Active RIS vs. passive RIS: Which will prevail in 6G?," *IEEE Trans. Commun.*, vol. 71, no. 3, pp. 1707–1725, Mar. 2023.

[3] J. Xu, *et al.*, "Active simultaneously transmitting and reflecting (STAR)-RISs: Modeling and analysis," *IEEE Commun. Lett.*, vol. 27, no. 9, pp. 2466–2470, Sep. 2023.

[4] X. Dong, *et al.*, "STAR-RIS aided secure MIMO communication systems," *IEEE Trans. Veh. Technol.*, vol. 73, no. 10, pp. 15715–15720, Oct. 2024.

[5] Y. Han, *et al.*, "Artificial noise aided secure NOMA communications in STAR-RIS networks," *IEEE Wireless Commun. Lett.*, vol. 11, no. 6, pp. 1191–1195, Jun. 2022.

[6] Y. Liu, *et al.*, "Worst-case energy efficiency in secure SWIPT networks with rate-splitting ID and power-splitting EH receivers," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1870–1885, Mar. 2022.

[7] H. Fu, *et al.*, "Robust secure beamforming design for two-user downlink MISO rate-splitting systems," *IEEE Trans. Wireless Commun.*, vol. 19, no. 12, pp. 8351–8365, Dec. 2020.

[8] Z. Wang, *et al.*, "Maximizing the minimum secrecy rate for STAR-RIS-assisted systems With RSMA strategy," *IEEE Wireless Commun. Lett.*, vol. 14, no. 11, pp. 3625–3629, Nov. 2025.

[9] B. Wang, *et al.*, "Secure transmission design for rate-splitting empowered STAR-RIS-aided networks," *IEEE Wireless Commun. Lett.*, vol. 13, no. 9, pp. 2581–2585, Sep. 2024.

[10] X. Tang, *et al.*, "Active RIS-aided anti-jamming wireless communications: A Stackelberg game perspective," *IEEE Trans. Commun.*, vol. 74, pp. 2612–2625, 2026.

[11] T. Zhang, *et al.*, "Rate-splitting with hybrid messages: DoF analysis of the two-user MIMO broadcast channel with imperfect CSIT," *IEEE Trans. Wireless Commun.*, vol. 23, no. 9, pp. 10514–10529, 2024.