Security Enhancement for STARS with An Untrusted User

Suyu Lv, Yuanwei Liu, Xiaodong Xu and Arumugam Nallanathan

***Abstract*—A secure transmission framework is proposed for simultaneously transmitting and reflecting surface (STARS) networks in presence of an untrusted user. The active and passive secure beamforming optimization problem is addressed. A double-loop alternating optimization (DLAO) algorithm is proposed for maximizing the achievable sum secure capacity (SC). More particularly, the *inner loop* is for beamforming optimization by utilizing successive convex approximation approaches, while the *outer loop* is for the rank-one constraint recovery by utilizing penalty-based optimization approaches. Numerical results demonstrate that: 1) the proposed DLAO algorithm converges within a few iterations; 2) the proposed framework is capable of achieving enhanced SC compared to conventional reflecting/transmitting-only reconfigurable intelligent surfaces.**

***Index Terms*—Beamforming, physical layer security (PLS), simultaneously transmitting and reflecting surface (STARS), untrusted user.**

I. Introduction

Recently, a new paradigm named simultaneously transmitting and reflecting surfaces (STARSs) has received intensive attention. As a remedy for reflecting-only reconfigurable intelligent surfaces (RISs), the incident signals on STARSs can be transmitted and reflected to both sides of the surface at the same time. *Full-space* smart radio environment can be achieved by intelligently adjusting the reflection and transmission coefficient of STARSs, while providing new degrees-of-freedom for manipulating signal propagation [1]–[3].

However, the distinctive capability of STARSs to reconfigure the full-space transmission environment will unavoidably lead to full-space eavesdropping, which means that eavesdroppers on either side can access confidential information passing through STARSs, posing a stringent security challenge. For enhancing security performance in STARS systems, the authors in [4]–[7] utilized physical layer security (PLS) approach to degrade the information leakage by exploiting the randomness of wireless fading channels. The secrecy performance in STARS-assisted non-orthogonal multiple access (NOMA) systems was investigated in [4], [5], where analytical and asymptotic expressions of the secrecy outage probabilities were derived in [4], and imperfect eavesdropping channel state information (CSI) was considered in [5]. To solve the problem that the eavesdroppers may enjoy similar performance gains as the legitimate users in STARS-aided NOMA system, an artificial noise assisted secure communication strategy was proposed by the authors of [6]. The potential of STARS in improving the security in multiple-input-single-output networks was studied in [7]. Considering the difficulty of obtaining CSI knowledge of eavesdroppers in RIS systems, the authors in [8]–[13] studied the robust and confidential transmission problems without perfect CSI of eavesdropping channels.

In addition to the possible full-space information leakage in STARS systems, what's worse is that some untrusted users can act as internal eavesdroppers, not only decoding their own intended signals, but also trying to intercept the confidential information of other users [14]. In this case, it is necessary not only to ensure that the required signals can be correctly received, but also to minimize the possibility of information leakage, which requires a novel secure beamforming design. To the best of our knowledge, the security enhancement design for STARS systems with untrusted users is still in its infancy, which motivates us to develop this work.

In this article, we propose a secure communication framework for STARS with an untrusted user, who tries to wiretap the other user's confidential information in addition to receiving its own intended signals. We propose a double-loop alternating optimization (DLAO) algorithm for maximizing the achievable sum secure capacity (SC) to achieve security enhancement. Numerical results verify the superiority of our proposed DLAO-STARS scheme compared to the benchmark schemes. The notations used in this paper are presented in **TABLE I**.

TABLE I
NOTATIONS

Notations	Meanings
$\boldsymbol{R}$	user on reflection space
$\boldsymbol{T}$	user on transmission space
M	number of BS antennas
K	number of STARS elements
$\boldsymbol{\Theta}_t/\boldsymbol{\Theta}_r$	transmission/reflection-coefficient matrix of STARS
$\boldsymbol{\omega}_t/\boldsymbol{\omega}_r$	active beamforming vector for $\boldsymbol{T}/\boldsymbol{R}$
β_k^r/β_k^t	amplitude response of k-th element
θ_k^r/θ_k^t	phase-shift coefficient of k-th element
$\|\mathbf{X}\|_*$	nuclear norm of matrix X
$\|\mathbf{X}\|_2$	spectral norm of matrix X
$\mathrm{diag}\,(\mathbf{x})$	diagonal matrix whose diagonal elements are $\mathbf{x}$
$[\cdot]^+$	$\max\{\cdot, 0\}$
$\mathbf{I}_n$	n-order identity matrix

II. System Model and Problem Formulation

A. System Model

We consider a downlink secure transmission framework for STARS, consisting of a multiple-antenna BS and two single-antenna users, as shown in Fig. 1. The STARS splits the whole communication network into two spaces, where the area on the

Suyu Lv is with the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China (e-mail: lvsuyu@bupt.edu.cn).

Xiaodong Xu is with the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China, and also with the Department of Broadband Communication, Peng Cheng Laboratory, Shenzhen 518066, Guangdong, China (e-mail: xuxiaodong@bupt.edu.cn).

Yuanwei Liu and Arumugam Nallanathan are with the School of Electronic Engineering and Computer Science, Queen Mary University of London, London E1 4NS, U.K. (e-mail: yuanwei.liu@qmul.ac.uk; a.nallanathan@qmul.ac.uk).

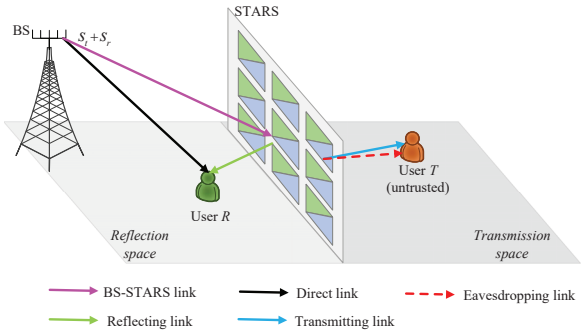

Fig. 1. Secure transmission framework for STARS with untrusted user.

same side as the BS is called the reflection space, and the area on the other side of the BS is called the transmission space. Accordingly, the user on the transmission space and the user on the reflection space are denoted as $\boldsymbol{T}$ and $\boldsymbol{R}$, respectively. The BS is equipped with M antennas and the STARS consists of K elements. Consider the case that $\boldsymbol{T}$ is the untrusted user, who tries to intercept the confidential information of $\boldsymbol{R}$ in addition to receiving its own signals. That is, these two users are both trusted to the network at the service level, but $\boldsymbol{T}$ is untrusted to $\boldsymbol{R}$ from the data perspective. In this condition, we consider that the perfect CSI can be obtained.

Energy splitting (ES) protocol is adopted by STARS [1], where the amplitude response satisfies the energy conservation constraint, and the phase-shift coefficients of transmission and reflection are independent of each other. Denote the reflection- and the transmission-coefficient matrix of STARS as $\boldsymbol{\Theta}_r \in \mathbb{C}^{K\times K}$ and $\boldsymbol{\Theta}_t \in \mathbb{C}^{K\times K}$ respectively, which are given by $\boldsymbol{\Theta}_z = \text{diag}\left(\sqrt{\beta_1^z}e^{j\theta_1^z}, \cdots, \sqrt{\beta_K^z}e^{j\theta_K^z}\right), z \in \{t, r\}$, with $\beta_k^r, \beta_k^t \in [0,1]$ representing the amplitude response of the k-th element, satisfying $\beta_k^r + \beta_k^t = 1$, and $\theta_k^r, \theta_k^t \in [0, 2\pi)$ denoting the phase-shift coefficient of the k-th element. In this paper, we consider that the STARS elements are passive and there is no energy loss. When considering energy consumption requirements of RISs or STARSs, simultaneous wireless information and power transfer (SWIPT) can be regarded as a promising solution [15].

We consider that the direct links only exist from BS to $\boldsymbol{R}$ but not from BS to $\boldsymbol{T}$. Therefore, signals intended for $\boldsymbol{R}$ can transmitted through the combined links while the signals intended for $\boldsymbol{T}$ can only be transmitted through the links established by STARS. The transmitted signals of the BS are given by

$$\mathbf{y} = \boldsymbol{\omega}_t s_t + \boldsymbol{\omega}_r s_r, \tag{1}$$

where $\boldsymbol{\omega}_t \in \mathbb{C}^{M\times 1}$ and $\boldsymbol{\omega}_r \in \mathbb{C}^{M\times 1}$ are the active beamforming vectors that BS allocates to $\boldsymbol{T}$ and $\boldsymbol{R}$, s_t and s_r $\left(\mathbb{E}\{|s_t|^2\} = 1, \mathbb{E}\{|s_r|^2\} = 1\right)$ are the intended information symbols for $\boldsymbol{T}$ and $\boldsymbol{R}$, respectively.

The channel from BS to STARS is model as Rician fading channels due to the favor positions for establishing line-of-sight (LoS) links [16], which can be generated by

$$\mathbf{G}_{b,s} = \sqrt{h_0 (d_{b,s})^{-\alpha}} \left(\sqrt{\tfrac{\kappa}{1+\kappa}}\mathbf{G}_{b,s}^{LoS} + \sqrt{\tfrac{1}{1+\kappa}}\mathbf{G}_{b,s}^{NLoS}\right), \tag{2}$$

where h_0 denotes the path loss at the reference distance $d = 1$m, $d_{b,s}$ is the distance between BS and STARS, $\alpha \geq 2$ is the path loss exponent, and κ is the Rician factor. $\mathbf{G}_{b,s}^{LoS} \in \mathbb{C}^{K\times M}$ is the deterministic LoS component, $\mathbf{G}_{b,s}^{NLoS} \in \mathbb{C}^{K\times M}$ is the Non-LoS component modeled by circularly symmetric complex Gaussian distribution with zero mean and unit variance. The channels from STARS to $\boldsymbol{T}$ and $\boldsymbol{R}$ are denoted by $\mathbf{g}_{s,t} \in \mathbb{C}^{K\times 1}$ and $\mathbf{g}_{s,r} \in \mathbb{C}^{K\times 1}$ respectively, which can be generated by Rayleigh fading mode due to the rich scattering [17], with the mathematical form as $\mathbf{g}_{s,t} = (d_{s,t})^{-\frac{\alpha}{2}}\mathbf{h}_{s,t}$ and $\mathbf{g}_{s,r} = (d_{s,r})^{-\frac{\alpha}{2}}\mathbf{h}_{s,r}$. $\mathbf{h}_{s,t} \sim \mathcal{CN}\left(0, \mu_{s,t}^2\mathbf{I}_K\right)$ and $\mathbf{h}_{s,r} \sim \mathcal{CN}\left(0, \mu_{s,r}^2\mathbf{I}_K\right)$ are the small-fading vectors, $d_{s,t}$ and $d_{s,r}$ respectively denote the distances from the STARS to $\boldsymbol{T}$ and $\boldsymbol{R}$. Similarly, the direct link from the BS to the $\boldsymbol{R}$ is denoted by $\mathbf{g}_{b,r} \in \mathbb{C}^{1\times M}$, generated by Rayleigh fading mode. Therefore, we can obtain the equivalent BS-RIS-$\boldsymbol{T}$ channel and BS-RIS-$\boldsymbol{R}$ channel as $\boldsymbol{c}_{b,t} = \mathbf{g}_{s,t}^H\boldsymbol{\Theta}_t\mathbf{G}_{b,s}$ and $\boldsymbol{c}_{b,r} = \mathbf{g}_{b,r} + \mathbf{g}_{s,r}^H\boldsymbol{\Theta}_r\mathbf{G}_{b,s}$ respectively.

Thus, the received superimposed signals at $\boldsymbol{T}$/$\boldsymbol{R}$ are respectively given by

$$\mathbf{y}_z = \boldsymbol{c}_{b,z}\left(\boldsymbol{\omega}_t s_t + \boldsymbol{\omega}_r s_r\right) + \mathbf{n}_z, z \in \{t, r\}, \tag{3}$$

where $\mathbf{n}_z \sim \mathcal{CN}\left(0, \sigma_z^2\right)$ is the independent identically distributed additive white Gaussian noise at $\boldsymbol{T}$/$\boldsymbol{R}$. The signal to interference plus noise ratio (SINR) of $\boldsymbol{T}$/$\boldsymbol{R}$ to decode its own intended signal $s_{t/r}$ can be expressed as

$$\gamma_{z\to z} = \frac{|\boldsymbol{c}_{b,z}\boldsymbol{\omega}_z|^2}{|\boldsymbol{c}_{b,z}\boldsymbol{\omega}_{\bar{z}}|^2 + \sigma_z^2}, z \in \{t, r\}, \tag{4}$$

which determines the maximum data rate of the two users. If $z = r$, then $\bar{z} = t$, else $\bar{z} = r$. In order to guarantee the data transmission requirements of users, we consider that the achievable rate should exceed a certain threshold, that is,

$$R_z = \log_2\left(1 + \gamma_{z\to z}\right) \geq \eta_z, z \in \{t, r\}. \tag{5}$$

The SINR for wiretapping s_r at $\boldsymbol{T}$ is

$$\gamma_{t\to r} = \frac{|\boldsymbol{c}_{b,t}\boldsymbol{\omega}_r|^2}{|\boldsymbol{c}_{b,t}\boldsymbol{\omega}_t|^2 + \sigma_t^2}, \tag{6}$$

which determines the maximum eavesdropping rate as follows

$$R_{t\to r,e} = \log_2\left(1 + \gamma_{t\to r}\right). \tag{7}$$

Accordingly, the achievable sum secure capacity of $\boldsymbol{T}$ and $\boldsymbol{R}$ can be given by

$$C_{\text{sum}} = \textstyle\sum_{z\in\{t,r\}}\left[R_z - R_{\bar{z}\to z,e}\right]^+, \tag{8}$$

where $[\cdot]^+ = \max\{\cdot, 0\}$. Particularly, $R_{r\to t,e} = 0$ since $\boldsymbol{R}$ is the trusted user and $\boldsymbol{T}$'s signals are not eavesdropped.

B. Problem Formulation

For improving the transmission performance while guaranteeing security, we consider to maximize the sum SC through jointly optimizing active and passive beamforming, whose mathematical form is given as follows

$$\max_{\{\boldsymbol{\omega}_z, \boldsymbol{\Theta}_z\}} C_{\text{sum}}, \tag{9a}$$
$$s.t. \left\|\boldsymbol{\omega}_t\right\|^2 + \left\|\boldsymbol{\omega}_r\right\|^2 \leq P_{\max}, \tag{9b}$$
$$\beta_k^r, \beta_k^t \in [0,1], \forall k \in \mathcal{K}, \tag{9c}$$
$$\beta_k^r + \beta_k^t = 1, \forall k \in \mathcal{K}, \tag{9d}$$
$$\theta_k^r, \theta_k^t \in [0, 2\pi), \forall k \in \mathcal{K}, \tag{9e}$$
$$R_z \geq \eta_z, \forall z \in \{t, r\}, \tag{9f}$$

where (9b) is the power budget at the BS, (9c) is the amplitude constraint of STARS because of its passivity, (9d) holds due to the law of energy conservation, (9e) is the phase-shift coefficient constraint of STARS, and (9f) is the data rate requirement of $\boldsymbol{T}$/$\boldsymbol{R}$.

III. Proposed Solutions

A. Problem Reformulation

It can be observed that problem (9) is a non-convex optimization problem due to the non-convexity of the objective function and constraints in (9). Furthermore, the highly-coupled optimization variables $\boldsymbol{\omega}_z$ and $\boldsymbol{\Theta}_z$ make it tricky to obtain global optimal solutions. In this section, we develop an alternate algorithm to find a high-quality suboptimal solution. At first, we recast (9) into a more tractable form.

Lemma 1: The received signal strength can be equivalently transformed as the following form

$$|\boldsymbol{c}_{b,r}\boldsymbol{\omega}_z|^2 = \mathbf{g}_{b,r}\boldsymbol{W}_z\mathbf{g}_{b,r}^H + \mathrm{Tr}\left(\mathbf{Q}_z\mathbf{U}_r\right), \tag{10a}$$

$$|\boldsymbol{c}_{b,t}\boldsymbol{\omega}_z|^2 = \mathrm{Tr}\left(\boldsymbol{\Phi}_t\boldsymbol{W}_z\boldsymbol{\Phi}_t^H\mathbf{U}_t\right), \tag{10b}$$

where $\boldsymbol{W}_z$ and $\mathbf{U}_z$ represent the active and passive beamforming matrix respectively.

Proof: See Appendix A. ■

To simplify the description, define the following functions

$$\begin{aligned}\mathcal{H}_u = &\mathbf{g}_{b,r}\boldsymbol{W}_r\mathbf{g}_{b,r}^H + \mathrm{Tr}\left(\mathbf{Q}_r\mathbf{U}_r\right)\\ &+\mathbf{g}_{b,r}\boldsymbol{W}_t\mathbf{g}_{b,r}^H + \mathrm{Tr}\left(\mathbf{Q}_t\mathbf{U}_r\right) + \sigma_r^2,\end{aligned} \tag{11a}$$

$$\mathcal{H}_d = \mathbf{g}_{b,r}\boldsymbol{W}_t\mathbf{g}_{b,r}^H + \mathrm{Tr}\left(\mathbf{Q}_t\mathbf{U}_r\right) + \sigma_r^2, \tag{11b}$$

$$\mathcal{G}_u = \mathrm{Tr}\left(\boldsymbol{\Phi}_t\boldsymbol{W}_t\boldsymbol{\Phi}_t^H\mathbf{U}_t\right) + \mathrm{Tr}\left(\boldsymbol{\Phi}_t\boldsymbol{W}_r\boldsymbol{\Phi}_t^H\mathbf{U}_t\right) + \sigma_t^2, \tag{11c}$$

$$\mathcal{G}_d\left(\boldsymbol{W}_z\right) = \mathrm{Tr}\left(\boldsymbol{\Phi}_t\boldsymbol{W}_z\boldsymbol{\Phi}_t^H\mathbf{U}_t\right) + \sigma_t^2, \boldsymbol{W}_z \in \{\boldsymbol{W}_t, \boldsymbol{W}_r\}. \tag{11d}$$

Moreover, to handle to non-convexity of the objective function, we introduce the following slack variables $\{\iota_{z,u}, \iota_{z,d}, \vartheta_{z,d}, \iota_{e,u}, \iota_{e,d}, \vartheta_{e,u}\}, z \in \{t, r\}$, which satisfy the following constraints

$$2^{\iota_{r,u}} \le \mathcal{H}_u, \ \ \vartheta_{r,d} \ge \mathcal{H}_d, \tag{12a}$$

$$2^{\iota_{t,u}} \le \mathcal{G}_u, \ \ \vartheta_{t,d} \ge \mathcal{G}_d\left(\boldsymbol{W}_r\right), \tag{12b}$$

$$2^{\iota_{z,d}} \ge \vartheta_{z,d}, z \in \{t, r\}. \tag{12c}$$

Thus, we can obtain the lower bound of R_z as $\underline{R}_z = \iota_{z,u} - \iota_{z,d} \le R_z$. Similarly, we relax the eavesdropping rate as its upper bound. Define $\overline{R}_{t\to r,e} = \iota_{e,u} - \iota_{e,d} \ge R_{t\to r,e}$, where $\iota_{e,u}$ and $\iota_{e,d}$ satisfy

$$2^{\iota_{e,u}} \ge \vartheta_{e,u}, \ \ \vartheta_{e,u} \ge \mathcal{G}_u, \tag{13a}$$

$$2^{\iota_{e,d}} \le \mathcal{G}_d\left(\boldsymbol{W}_t\right). \tag{13b}$$

However, constraints (12c) and (13a) are still non-convex. Thus, we utilize first-order Taylor expansion to construct approximate linear upper bounds of $\log_2\vartheta_{z,d}$ and $\log_2\vartheta_{e,u}$, which are given by

$$\mathcal{F}\left(\vartheta, \hat{\vartheta}\right) \triangleq \log_2\hat{\vartheta} + \tfrac{1}{\hat{\vartheta}\ln 2}\left(\vartheta - \hat{\vartheta}\right) \ge \log_2\vartheta. \tag{14}$$

Thus, constraints (12c) and (13a) are converted to

$$\iota_{z,d} \ge \mathcal{F}\left(\vartheta_{z,d}, \hat{\vartheta}_{z,d}\right), z \in \{t, r\}, \tag{15a}$$

$$\iota_{e,u} \ge \mathcal{F}\left(\vartheta_{e,u}, \hat{\vartheta}_{e,u}\right), \tag{15b}$$

where $\hat{\vartheta}_{z,d}$ and $\hat{\vartheta}_{e,u}$ are the optimal solutions in the pervious iteration. Accordingly, the original optimization problem (9) can be reformulated as

$$\max_{\substack{\boldsymbol{W}_z,\mathbf{U}_z,\boldsymbol{\beta}_z,\\ \iota_{z,u},\iota_{z,d},\vartheta_{z,d},\iota_{e,u},\iota_{e,d},\vartheta_{e,u}}} \ \underline{C}_{\mathrm{sum}}, \tag{16a}$$

$$s.t.\ (12a), (12b), (13b), (15), \tag{16b}$$

$$\mathrm{Tr}\left(\boldsymbol{W}_t\right) + \mathrm{Tr}\left(\boldsymbol{W}_r\right) \le P_{\max}, \tag{16c}$$

$$\mathrm{Diag}\left(\mathbf{U}_z\right) = \boldsymbol{\beta}_z, \tag{16d}$$

$$\boldsymbol{\beta}_z\left(k\right) \in [0, 1], \forall z \in (t, r\}, k \in \mathcal{K}, \tag{16e}$$

$$\boldsymbol{\beta}_t\left(k\right) + \boldsymbol{\beta}_r\left(k\right) = 1, \forall k \in \mathcal{K}, \tag{16f}$$

$$\mathrm{Rank}\left(\mathbf{U}_z\right) = 1, \mathrm{Rank}\left(\boldsymbol{W}_z\right) = 1, \forall z \in (t, r\}, \tag{16g}$$

$$\mathbf{U}_z \succeq \mathbf{0}, \ \boldsymbol{W}_z \succeq \mathbf{0}, \forall z \in (t, r\}, \tag{16h}$$

$$\underline{R}_z \ge \eta_z, \forall z \in \{t, r\}, \tag{16i}$$

$$\underline{R}_r \ge \overline{R}_{t\to r,e}, \tag{16j}$$

where $\underline{C}_{\mathrm{sum}} = \underline{R}_r + \underline{R}_t - \overline{R}_{t\to r,e}$. Constraint (16j) guarantees the achievable secure capacity of $\boldsymbol{R}$ is always a positive value.

Remark 1: The proposed scheme can be easily extended to the cases of: 1) multiple untrusted users, where the eavesdropping rate is dependent on the maximum one; 2) the direct link between the BS and the trusted user is blocked, by replacing the signal strength in (10a) with $|\boldsymbol{c}_{b,r}\boldsymbol{\omega}_z|^2 = \mathrm{Tr}\left(\boldsymbol{\Phi}_r\boldsymbol{W}_z\boldsymbol{\Phi}_r^H\mathbf{U}_r\right)$; 3) the direct link between the BS and the untrusted user exists, by replacing the signal strength in (10b) with $|\boldsymbol{c}_{b,t}\boldsymbol{\omega}_z|^2 = \mathbf{g}_{b,t}\boldsymbol{W}_z\mathbf{g}_{b,t}^H + \mathrm{Tr}\left(\mathbf{Q}_{T,z}\mathbf{U}_t\right)$.

B. Active Beamforming Design

With given STARS transmission- and reflection- coefficient, the active beamforming optimization problem can be given by

$$\begin{aligned}\min_{\substack{\boldsymbol{W}_z,\iota_{z,u},\iota_{z,d},\vartheta_{z,d},\\ \iota_{e,u},\iota_{e,d},\vartheta_{e,u}}} \ &-\underline{C}_{\mathrm{sum}},\\ s.t.\ &\boldsymbol{W}_z \succeq \mathbf{0}, \forall z \in (t, r\},\\ &\mathrm{Rank}\left(\boldsymbol{W}_z\right) = 1, \forall z \in (t, r\},\\ &(12a), (12b), (13b), (15), (16c), (16i), (16j).\end{aligned} \tag{17}$$

Proposition 1: The rank of $\boldsymbol{W}_z$ only relies on that of $\mathbf{U}_z$, i.e., $\mathrm{Rank}\left(\boldsymbol{W}_z\right) \le \mathrm{Rank}\left(\mathbf{U}_z\right) = 1$.

Proof: Please refer to Appendix A in [3]. ■

Moreover, due to the positive transmission rate requirements in (9f), $\mathrm{Rank}\left(\boldsymbol{W}_z\right) = 1$ holds for the optimal solution. Therefore, the non-convex constraint $\mathrm{Rank}\left(\boldsymbol{W}_z\right) = 1$ can be reasonably dropped, resulting in (17) being a convex optimization problem that can be efficiently solved by CVX.

C. Penalty-based STARS Coefficient Optimization

Optimization problem with non-convex rank-one constraint $\mathrm{Rank}\left(\mathbf{U}_z\right) = 1$ is known to be NP-hard. To tackle this difficulty, we transform this constraint into its equivalent form $\|\mathbf{U}_z\|_* - \|\mathbf{U}_z\|_2 \le 0$, which is in difference of convex (DC) form and therefore still non-convex with respect to $\mathbf{U}_z$. Therefore, we utilize the penalty-based approach by moving the constraint into the objective function. As a result, with given fixed $\boldsymbol{W}_t$ and $\boldsymbol{W}_r$, we rewrite the STARS coefficient optimization problem as

$$\begin{aligned}\min_{\substack{\mathbf{U}_z,\boldsymbol{\beta}_z,\iota_{z,u},\iota_{z,d},\vartheta_{z,d},\\ \iota_{e,u},\iota_{e,d},\vartheta_{e,u}}} \ &-\underline{C}_{\mathrm{sum}} + \tfrac{1}{2\varrho}\sum_{z\in\{t,r\}}\left(\|\mathbf{U}_z\|_* - \|\mathbf{U}_z\|_2\right),\\ s.t.\ &\mathbf{U}_z \succeq 0, \forall z \in (t, r\},\\ &(12a), (12b), (13b), (15), (16d) - (16f), (16i), (16j),\end{aligned} \tag{18}$$

Algorithm 1 DLAO algorithm for Sum SC Maximization

Input: maximum iteration times T_{in}, T_{ou}, convergence threshold ε_{in}, ε_{ou}.
Output: $\boldsymbol{W}_z^*$, $\mathbf{U}_z^*$.

Initialization: iteration indexes $l = 0$, $i = 0$, feasible points $\left\{\boldsymbol{W}_z^{(0)}, \mathbf{U}_z^{(0)}\right\}$, penalty factor ϱ, discount factor $c < 1$, $\Gamma_{in} = +\infty$, $\Gamma_{ou} = +\infty$.
while $l < T_{ou}$ and $\Gamma_{ou} > \varepsilon_{ou}$ **do**
  while $i < T_{in}$ and $\Gamma_{in} > \varepsilon_{in}$ **do**
    With given $\mathbf{U}_z^{(i)}$, update $\boldsymbol{W}_z^{(i+1)}$ by solving (17);
    With given $\boldsymbol{W}_z^{(i+1)}$, update $\mathbf{U}_z^{(i+1)}$ by solving (18);
    Calculate $\Gamma_{in} = \left|\underline{C}_{\text{sum}}^{(i+1)} - \underline{C}_{\text{sum}}^{(i)}\right|$;
    $i \leftarrow i + 1$;
  end while
  Update $\left\{\boldsymbol{W}_z^{(0)}, \mathbf{U}_z^{(0)}\right\}$ with the current $\left\{\boldsymbol{W}_z^{(i)}, \mathbf{U}_z^{(i)}\right\}$, $i = 0$;
  Calculate $\Gamma_{ou} = \max\limits_{z\in\{t,r\}} \left\{\|\mathbf{U}_z\|_*^{(i)} - \|\mathbf{U}_z\|_2^{(i)}\right\}$;
  Update $\varrho^{(l+1)} = c\varrho^{(l)}$, $l \leftarrow l + 1$;
end while

where $\varrho > 0$ is a penalty factor for violating the constraint $\|\mathbf{U}_z\|_* - \|\mathbf{U}_z\|_2 \leq 0$. When ϱ is sufficiently small, the rank-one solution can be obtained by solving problem (18) [18]. Define two functions

$$F_1(\mathbf{U}_z) = \frac{1}{2\varrho}\sum_{z\in\{t,r\}} \|\mathbf{U}_z\|_* - \underline{C}_{\text{sum}}, \tag{19a}$$

$$F_2(\mathbf{U}_z) = \frac{1}{2\varrho}\sum_{z\in\{t,r\}} \|\mathbf{U}_z\|_2, \tag{19b}$$

which are both continuous convex functions. Then the objective function in (18) is converted into DC structure as $F_1(\mathbf{U}_z) - F_2(\mathbf{U}_z)$. Then we adopt the successive convex approximation (SCA) method to obtain a convex upper bound for the objective function in an iterative manner. Exploiting first-order Taylor expansion at a feasible point $\mathbf{U}_z^{(i)}, \forall z \in \{t, r\}$, the lower bound of function $F_2(\mathbf{U}_z)$ can be obtained as

$$F_2(\mathbf{U}_z) \geq \underline{F}_2(\mathbf{U}_z) \triangleq \frac{1}{2\varrho}\sum_{z\in\{t,r\}} \left\{\left\|\mathbf{U}_z^{(i)}\right\|_2 + \text{Tr}\left[\mathbf{u}_z^{(i)}\left(\mathbf{u}_z^{(i)}\right)^H\left(\mathbf{U}_z - \mathbf{U}_z^{(i)}\right)\right]\right\}, \tag{20}$$

where $\mathbf{U}_z^{(i)}$ is the optimal solution obtained in the i-th iteration of the SCA method and $\mathbf{u}_z^{(i)}$ denotes the eigenvector corresponding to the largest eigenvalue of $\mathbf{U}_z^{(i)}$. Employing this upper bound on the objective function, the STARS coefficient optimization problem is a convex optimization problem.

D. Computation Complexity Analysis

The overall DLAO algorithm for maximizing sum SC is summarized in **Algorithm 1**. The computation complexity mainly comes from solving the semi-definite programming problem in the inner loop. Thus, the overall polynomial complexity of the proposed algorithm can be approximately calculated as $\mathcal{O}\left(I_{in}I_{out}\left(2M^{3.5} + 2K^{3.5}\right)\right)$ [19], with I_{in} and I_{out} representing the number of iterations required for the convergence of Algorithm 1 for the inner and outer loop, respectively.

IV. Numerical Results

The performance of the proposed scheme will be evaluated in this section. Consider a three-dimensional coordinate system, where the BS, the STARS, ***R*** and ***T*** are respectively located at (0, 0, 5) meter (m), (30, 0, 3) m, (25, 0, 0) m and (35, 3, 0) m. The path-loss factor is $h_0 = -30$ dB, and the path-loss exponents are set as $\alpha_{b,r} = 4$ for the direct link, $\alpha_{b,s} = 2.2$ for the BS-STARS link and $\alpha_{s,r} = \alpha_{s,t} = 2.5$ for the STARS-***R*** and STARS-***T*** links. The Rician factors are set as $\kappa_{b,s} = 5$ dB and $\kappa_{s,r} = \kappa_{s,t} = 0$ for the BS-STARS link and the Rayleigh fading links, respectively. The noise power is $\sigma^2 = -105$ dBm. Furthermore, we consider the convergence threshold is $\varepsilon_{in} = \varepsilon_{out} = 10^{-3}$, the initial penalty factor $\varrho = 0.9$, and the discount factor is $c = 0.75$. The simulation results are obtained through Monte Carlo simulations over 200 channel realizations.

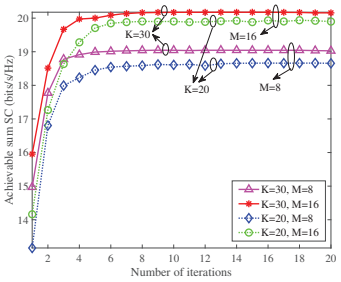

Fig. 2. Convergence performance of the proposed DLAO algorithm ($P_{\max} = 30$ dBm).

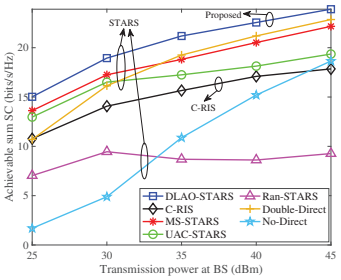

Fig. 3. The achievable sum SC versus maximum power of BS ($K = 20$, $M = 8$).

The convergence performance of the proposed algorithm under different K and M is depicted in Fig. 2. It can be seen that the achievable sum SC gradually increases in the process of iteration, and reaches a stable value within a finite number of iteration times. In addition, the improvement of K and M can enhance the security performance, which is caused by the more flexible beamforming design. Moreover, more iteration times are required for larger K and M values, increasing the computational complexity at the same time.

Fig. 3 shows the achievable sum SC obtained by different schemes, namely, the proposed DLAO-STARS scheme, conventional RISs (C-RIS), uniform amplitude control at STARS (UAC-STARS), mode switching protocol at STARS (MS-STARS) and random phase/amplitude control at STARS (Ran-STARS). Particularly, in the C-RIS scheme, one reflecting-only RIS and one transmitting-only RIS are deployed at the same location as STARS with $\frac{K}{2}$ elements. All the elements' amplitude responses should be the same in the UAC-STARS scheme, while that can only be 0 or 1 in the MS-STARS scheme. Moreover, to evaluate the impact of the presence of direct links on system secrecy performance, we consider two cases in Fig. 3: (1) No-Direct: the direct link between the BS

and $\boldsymbol{R}$ is blocked, as well as between BS and $\boldsymbol{T}$; (2) Double-Direct: there are direct links between BS and $\boldsymbol{R}$, as well as between BS and $\boldsymbol{T}$.

It can be seen that AO-STARS outperforms all other comparison schemes since STARS exploits double degrees-of-freedom than C-RIS, while has higher flexibility of amplitude coefficient optimization compared with UAC-STARS and MS-STARS, which verifies the effectiveness of the proposed scheme. Furthermore, the achievable sum SC becomes higher with the increase of transmission power except for the Ran-STARS scheme, because the random coefficient cannot always guarantee improvement of legitimate reception and reduction of information leakage. Moreover, as shown the curve named No-Direct in Fig. 3, the achievable sum SC has an obvious decline when the direct link between the BS and the untrusted user $\boldsymbol{T}$ exists, especially when the BS's transmission power is relatively small. Although Double-Direct may increase the achievable rate of $\boldsymbol{T}$, it can also cause more severe information leakage compared to the proposed framework, leading to performance degradation.

V. Conclusions

In this article, we proposed a secure transmission framework for STARS in presence of an untrusted user. Based on this framework, we formulated a sum SC maximization problem for enhancing security performance, and proposed a DLAO algorithm to implement the optimization of active beamforming at the BS and passive beamforming at the STARS. Numerical results confirmed the convergence of the proposed DLAO algorithm. Furthermore, compared with benchmark schemes, adopting the proposed DLAO-STARS scheme can obtain higher SC when internal eavesdropper exists.

Appendix A
Proof of Lemma 1

To facilitate the design, we define vectors $\boldsymbol{\mu}_z = \mathrm{Diag}(\boldsymbol{\Theta}_z) = \left[\sqrt{\beta_1^z}e^{j\theta_1^z}, \cdots, \sqrt{\beta_K^z}e^{j\theta_K^z}\right]^T \in \mathbb{C}^{K\times 1}, z \in \{t, r\}$ to denote the amplitude response and phase-shift coefficient vector of the STARS. Therefore, $\mathbf{g}_{s,z}^H \boldsymbol{\Theta}_z \mathbf{G}_{b,s} \boldsymbol{\omega}_z$ can be rewritten as $\boldsymbol{\mu}_z^H \boldsymbol{\Phi}_z \boldsymbol{\omega}_z$, where $\boldsymbol{\Phi}_z = \mathrm{diag}\left(\mathbf{g}_{s,z}^H\right) \mathbf{G}_{b,s}, \forall z \in \{t, r\}$. Moreover, define $\boldsymbol{W}_z = \boldsymbol{\omega}_z \boldsymbol{\omega}_z^H, \forall z \in \{t, r\}$ to represent the active beamforming matrix, which also satisfies $\boldsymbol{W}_z \succeq 0$ and $\mathrm{Rank}\left(\boldsymbol{W}_z\right) = 1$. Thus,

$$\begin{aligned}\left|\boldsymbol{c}_{b,r}\boldsymbol{\omega}_z\right|^2 = \mathbf{g}_{b,r}\boldsymbol{W}_z\mathbf{g}_{b,r}^H + \boldsymbol{\mu}_r^H\boldsymbol{\Phi}_r\boldsymbol{W}_z\boldsymbol{\Phi}_r^H\boldsymbol{\mu}_r \\ + \mathbf{g}_{b,r}\boldsymbol{W}_z\boldsymbol{\Phi}_r^H\boldsymbol{\mu}_r + \boldsymbol{\mu}_r^H\boldsymbol{\Phi}_r\boldsymbol{W}_z\mathbf{g}_{b,r}^H.\end{aligned} \tag{21}$$

Let $\mathbf{Q}_z = \begin{bmatrix} \boldsymbol{\Phi}_r\boldsymbol{W}_z\boldsymbol{\Phi}_r^H & \boldsymbol{\Phi}_r\boldsymbol{W}_z\mathbf{g}_{b,r}^H \\ \mathbf{g}_{b,r}\boldsymbol{W}_z\boldsymbol{\Phi}_r^H & 0 \end{bmatrix} \in \mathbb{C}^{(K+1)\times(K+1)}$, $\bar{\boldsymbol{\mu}}_r = \left[\boldsymbol{\mu}_r^T \ 1\right]^T \in \mathbb{C}^{(K+1)\times 1}$, then we have $\left|\left(\mathbf{g}_{b,r} + \boldsymbol{\mu}_r^H\boldsymbol{\Phi}_r\right)\boldsymbol{\omega}_r\right|^2 = \mathbf{g}_{b,r}\boldsymbol{W}_z\mathbf{g}_{b,r}^H + \bar{\boldsymbol{\mu}}_r^H\mathbf{Q}_z\bar{\boldsymbol{\mu}}_r$. Introduce another variable $\mathbf{U}_r = \bar{\boldsymbol{\mu}}_r\bar{\boldsymbol{\mu}}_r^H \in \mathbb{C}^{(K+1)\times(K+1)}$, satisfying $\mathbf{U}_r \succeq 0$, $\mathrm{Rank}\left(\mathbf{U}_r\right) = 1$ and $\mathrm{Diag}\left(\mathbf{U}_r\right) = \boldsymbol{\beta}_r$, where $\boldsymbol{\beta}_r \triangleq \left[\beta_1^r, \cdots, \beta_K^r, 1\right]^T$. Thus, we can get $\bar{\boldsymbol{\mu}}_r^H\mathbf{Q}_z\bar{\boldsymbol{\mu}}_r = \mathrm{Tr}\left(\mathbf{Q}_z\bar{\boldsymbol{\mu}}_r\bar{\boldsymbol{\mu}}_r^H\right) = \mathrm{Tr}\left(\mathbf{Q}_z\mathbf{U}_r\right)$, satisfying $\mathbf{U}_r \succeq 0$ and $\mathrm{rank}\left(\mathbf{U}_r\right) = 1$. Thus,

$$\left|\boldsymbol{c}_{b,r}\boldsymbol{\omega}_z\right|^2 = \mathbf{g}_{b,r}\boldsymbol{W}_z\mathbf{g}_{b,r}^H + \mathrm{Tr}\left(\mathbf{Q}_z\mathbf{U}_r\right). \tag{22}$$

Similarly, we define $\mathbf{U}_t = \boldsymbol{\mu}_t\boldsymbol{\mu}_t^H \in \mathbb{C}^{K\times K}$, which satisfies $\mathbf{U}_t \succeq 0$, $\mathrm{Rank}\left(\mathbf{U}_t\right) = 1$ and $\mathrm{Diag}\left(\mathbf{U}_t\right) = \boldsymbol{\beta}_t$, where $\boldsymbol{\beta}_t \triangleq \left[\beta_1^t, \cdots, \beta_K^t\right]^T$ denotes the transmitting amplitude response of the STARS. Thus, we have

$$\left|\boldsymbol{c}_{b,t}\boldsymbol{\omega}_z\right|^2 = \mathrm{Tr}\left(\boldsymbol{\Phi}_t\boldsymbol{W}_z\boldsymbol{\Phi}_t^H\mathbf{U}_t\right). \tag{23}$$

References

[1] Y. Liu, X. Mu, J. Xu, R. Schober, Y. Hao, H. V. Poor, and L. Hanzo, "STAR: Simultaneous transmission and reflection for 360° coverage by intelligent surfaces," *IEEE Wireless Commun.*, vol. 28, no. 6, pp. 102–109, 2021.

[2] J. Xu, Y. Liu, X. Mu, and O. A. Dobre, "STAR-RISs: Simultaneous transmitting and reflecting reconfigurable intelligent surfaces," *IEEE Commun. Lett.*, vol. 25, no. 9, pp. 3134–3138, 2021.

[3] X. Mu, Y. Liu, L. Guo, J. Lin, and R. Schober, "Simultaneously transmitting and reflecting (STAR) RIS aided wireless communications," *IEEE Trans. Wireless Commun.*, vol. 21, no. 5, pp. 3083–3098, 2022.

[4] X. Li, Y. Zheng, M. Zeng, Y. Liu, and O. A. Dobre, "Enhancing secrecy performance for STAR-RIS NOMA networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 2, pp. 2684–2688, 2023.

[5] H. Jia, L. Ma, and S. Valaee, "STAR-RIS enabled downlink secure NOMA network under imperfect CSI of eavesdroppers," *IEEE Commun. Lett.*, early access, 2023.

[6] Y. Han, N. Li, Y. Liu, T. Zhang, and X. Tao, "Artificial noise aided secure NOMA communications in STAR-RIS networks," *IEEE Wireless Commun. Lett.*, vol. 11, no. 6, pp. 1191–1195, 2022.

[7] H. Niu, Z. Chu, F. Zhou, and Z. Zhu, "Simultaneous transmission and reflection reconfigurable intelligent surface assisted secrecy MISO networks," *IEEE Commun. Lett.*, vol. 25, no. 11, pp. 3498–3502, 2021.

[8] Z. Zhu, J. Xu, G. Sun, W. Hao, Z. Chu, C. Pan, and I. Lee, "Robust beamforming design for IRS-aided secure SWIPT terahertz systems with non-linear EH model," *IEEE Wireless Commun. Lett.*, vol. 11, no. 4, pp. 746–750, 2022.

[9] H. Niu, Z. Chu, F. Zhou, Z. Zhu, L. Zhen, and K.-K. Wong, "Robust design for intelligent reflecting surface-assisted secrecy SWIPT network," *IEEE Trans. Wireless Commun.*, vol. 21, no. 6, pp. 4133–4149, 2022.

[10] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent reflecting surface: A programmable wireless environment for physical layer security," *IEEE Access*, vol. 7, pp. 82 599–82 612, 2019.

[11] G. C. Alexandropoulos, K. Katsanos, M. Wen, and D. B. Da Costa, "Safeguarding MIMO communications with reconfigurable metasurfaces and artificial noise," in *ICC 2021 - IEEE International Conference on Communications*, 2021, pp. 1–6.

[12] Z. Li, S. Wang, M. Wen, and Y.-C. Wu, "Secure multicast energy-efficiency maximization with massive RISs and uncertain CSI: First-order algorithms and convergence analysis," *IEEE Trans. Wireless Commun.*, vol. 21, no. 9, pp. 6818–6833, 2022.

[13] G. C. Alexandropoulos, K. D. Katsanos, M. Wen, and D. B. da Costa, "Counteracting eavesdropper attacks through reconfigurable intelligent surfaces: A new threat model and secrecy rate optimization," *arXiv*, 2022.

[14] K. Cao, B. Wang, H. Ding, T. Li, J. Tian, and F. Gong, "Secure transmission designs for NOMA systems against internal and external eavesdropping," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2930–2943, 2020.

[15] Z. Zhu, Z. Li, Z. Chu, G. Sun, W. Hao, P. Liu, and I. Lee, "Resource allocation for intelligent reflecting surface assisted wireless powered IoT systems with power splitting," *IEEE Trans. Wireless Commun.*, vol. 21, no. 5, pp. 2987–2998, 2022.

[16] M. Abbasi Msleh, F. Heliot, and R. Tafazolli, "Ergodic capacity analysis of reconfigurable intelligent surface assisted MIMO systems over rayleigh-rician channels," *IEEE Commun. Lett.*, vol. 27, no. 1, pp. 75–79, 2023.

[17] M. A. ElMossallamy, H. Zhang, L. Song, K. G. Seddik, Z. Han, and G. Y. Li, "Reconfigurable intelligent surfaces for wireless communications: Principles, challenges, and opportunities," *IEEE Trans. Cogn. Commun. Netw.*, vol. 6, no. 3, pp. 990–1002, 2020.

[18] X. Yu, D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, "Robust and secure wireless communications via intelligent reflecting surfaces," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2637–2652, 2020.

[19] I. Pólik and T. Terlaky, "Interior point methods for nonlinear optimization," in *Nonlinear optimization*. Springer, 2010, pp. 215–276.