Artificial Noise-Aided Secrecy Beamforming Optimization Method for MISO Wiretap Channels

Ruixin Li
School of Electronic Information, Zhengzhou University of Light Industry, Zhengzhou, Henan, China

Abstract: Physical layer security technologies, which do not rely on complex key management and utilize the inherent physical characteristics of wireless channels to achieve secure information transmission, are a critical means of ensuring the confidentiality of future wireless communications. Artificial noise-aided beamforming design in Multiple-Input Single-Output (MISO) wiretap channels offers significant advantages in combating passive eavesdropping; however, existing optimization methods still suffer from shortcomings in relaxation accuracy, convergence efficiency, and robustness. This paper addresses the secrecy rate maximization problem in artificial noise-aided MISO wiretap channels. It constructs a non-convex optimization model incorporating total power constraints, null-space orthogonality constraints, sparse directional constraints, and dual robustness constraints. Simulation results demonstrate that the proposed solution framework integrating alternating optimization and semidefinite relaxation can significantly improve the system's secrecy rate and achieve faster convergence. Even in scenarios with channel estimation errors and eavesdropper location uncertainty, the algorithm maintains stable secrecy performance, verifying its superior robustness.

Keywords: MISO Wiretap Channel; Artificial Noise; Alternating Optimization; Semidefinite Relaxation

1. Introduction

With the development of 5G/6G wireless communication technologies and the large-scale deployment of Internet of Things (IoT) devices, wireless communication security has become increasingly critical. Given the vast scale of these communication networks, traditional cryptography-based security mechanisms are inadequate in resource-constrained wireless environments due to their high computational complexity and key-distribution challenges. Physical layer security (PLS), a novel security paradigm that leverages the inherent physical properties of wireless channels for secure information transmission, offers a new approach to wireless communication security.

The MISO wiretap channel is a classic model in physical layer security research, with significant theoretical value and application potential for secure communications. Artificial-noise-aided secrecy beamforming interferes with the eavesdropper's reception by transmitting information signals and artificial noise simultaneously at the transmitter without compromising the communication quality of legitimate users. Relevant schemes have been widely verified in MISO, MISOME, and intelligent reflecting surface-assisted scenarios [1-3]. However, most existing optimization methods for the secrecy rate maximization problem suffer from low relaxation accuracy, slow convergence, and poor robustness, especially when facing non-ideal channel state information [4,5]. To address these issues, this paper proposes a secrecy beamforming optimization scheme that combines alternating optimization with semidefinite relaxation. Based on reasonable modeling, we formulate a non-convex optimization problem with multiple constraints and introduce two robustness constraints to enhance the algorithm's robustness, thereby providing a feasible method for beamforming design in physical layer secure communications.

2. System Model and Problem Formulation

2.1 System Model

Consider a typical MISO wiretap channel system consisting of a transmitter equipped with N_t antennas, a single-antenna legitimate receiver, and a single-antenna eavesdropper. The channel vector from the transmitter to the legitimate receiver is $\mathrm{h}_d \in C^{N_t \times 1}$,and the channel vector

from the transmitter to the eavesdropper is $h_e \in C^{N_t \times 1}$. All channels are independent Rayleigh flat fading channels, with channel coefficients following an independent and identically distributed complex Gaussian distribution $CN(0, 1)$. The additive white Gaussian noise powers at the legitimate receiver and the eavesdropper are and , respectively. The eavesdropper is a passive eavesdropper, and the transmitter has no access to the instantaneous channel state information of the eavesdropper. The specific system structure is shown in Figure 1.

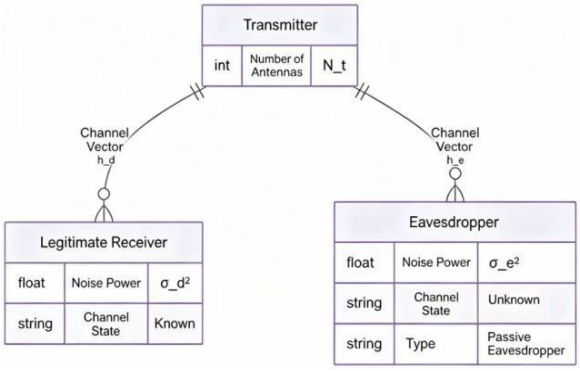

Figure 1. System Model of Artificial Noise-Aided MISO Wiretap Channel

In the artificial noise-aided MISO wiretap channel system, the transmitter adopts a composite transmission structure of "confidential information signal + artificial noise". The transmitted signal can be expressed as:

$$x=ws+Vn$$

where is the beamforming vector for confidential information, is the normalized confidential information symbol satisfying $E[|s|^2]=1$; is the beamforming matrix for artificial noise, and is the artificial noise vector. To ensure that artificial noise does not interfere with legitimate users, the null-space orthogonality constraint must be satisfied, meaning that artificial noise is restricted to the null space of the legitimate channel. The signal received by the legitimate user is:

$$y_d=\mathrm{h}_d^H w s+n_d$$

where is additive white Gaussian noise. Since $\mathrm{h}_d^H V=0$, The artificial noise term is eliminated on the legitimate link. Therefore, the signal-to-interference-plus-noise ratio (SINR) at the legitimate user is: $\mathrm{SINR}_d=\frac{|\boldsymbol{h}_d^H \boldsymbol{w}|^2}{\sigma_d^2}$

Correspondingly, the legitimate channel capacity is:

$$C_d=\log_2(1+\mathrm{SINR}_d)$$

The signal received by the eavesdropper is:

$$y_e=\mathrm{h}_e^H w s+\mathrm{h}_e^H V n+n_e,$$

where is the eavesdropping channel vector,$n_e \sim CN(0, \sigma_e^2)$ is the received noise at the eavesdropper. Since the eavesdropper cannot know the specific direction of h_d , it cannot remove the artificial noise from the received signal. Therefore, the effective SINR at the eavesdropper is:

$$\mathrm{SINR}_e=\frac{|\boldsymbol{h}_e^H \boldsymbol{w}|^2}{|\boldsymbol{h}_e^H \boldsymbol{V}|^2+\sigma_e^2}$$

Correspondingly, the eavesdropper's channel capacity is:

$$C_e=\log_2(1+\mathrm{SINR}_e)$$

Based on Shannon's secrecy capacity theory, the system's secrecy rate is:

$$R_s=log_2(1+SINR_d)-log_2(1+SINR_e)$$

Further consider a multi-eavesdropper scenario with K independent passive eavesdroppers. Let the channel of the k-th eavesdropper be$h_{e,k}$, and its corresponding eavesdropping capacity is:

$$C_{e,k}=log_2(1+SINR_{e,k})$$

Then, the system's secrecy rate is defined under the worst-case assumption as:

$$R_s^{multi}=C_d-\max_{1\le k\le K} C_{e,\ k}$$

Due to channel estimation errors and eavesdropper location uncertainty, the transmitter can only obtain the nominal channel vectors and h_e.The actual channels satisfy:

$\tilde{\mathrm{h}}_d=\mathrm{h}_d+\Delta\mathrm{h}_d, \|\Delta\mathrm{h}_d\|\le\varepsilon_d,$

$\tilde{\mathrm{h}}_e=\mathrm{h}_e+\Delta\mathrm{h}_e, \|\Delta\mathrm{h}_e\|\le\varepsilon_e$,或 $\|\Delta\mathrm{h}_{e,loc}\|\le\varepsilon_{loc}$

Where ε_d, ε_e, are given uncertainty radii. In the presence of channel uncertainty, the system's secrecy rate should be defined as the worst-case achievable rate, i.e., the minimum value over all possible channels.

2.2 Problem Formulation

In the context of wireless communication security, based on the above system model and the secrecy rate expression, this paper proposes a joint optimization problem to maximize the secrecy rate, with optimization variables including the information beamforming vector, the artificial noise matrix, and the power allocation coefficient[6].

The information beamforming vector is set as the primary optimization variable, as it directly determines the spatial transmission characteristics of the useful signal and the reception performance of legitimate users. The artificial noise matrix is an auxiliary

optimization variable that generates directional interference in the null space to degrade the signal quality received by eavesdroppers. Let the maximum total transmit power be and define the power allocation coefficient to adjust the power allocation ratio between the information signal and artificial noise, such that:

$\| w\|^2 \le \rho P_{max}$,$tr(VV^H) \le (1-\rho)P_{max}$

These three variables are interrelated: and jointly determine the information transmission efficiency; and together determine the interference suppression capability; and and must also satisfy the null-space orthogonality constraint $\mathrm{h}_d^H V=0$, to ensure that artificial noise does not affect legitimate users. Meanwhile, the transmitter knows the nominal channels of legitimate users and eavesdroppers h_e; however, due to channel estimation errors and eavesdropper location uncertainty, the actual channels have bounded uncertainty:

$$\mathscr{H}_d=\{\tilde{\boldsymbol{h}}_{\boldsymbol{d}}=\boldsymbol{h_d}+\Delta\boldsymbol{h_d} \mid \| \Delta\boldsymbol{h_d} \| \le \varepsilon_d\}$$

$$\mathscr{H}_e=\{\tilde{\boldsymbol{h}}_{\boldsymbol{e}}=\boldsymbol{h_e}+\Delta\boldsymbol{h_e} \mid \| \Delta\boldsymbol{h_e} \| \le \varepsilon_e\}$$

$$\mathscr{H}_{e,\mathrm{loc}}=\{\tilde{\boldsymbol{h}}_e \mid \| \tilde{\boldsymbol{h}}_e-\boldsymbol{h}_e \| \le \varepsilon_{\mathrm{loc}}\}$$

Where and are the channel estimates, and are the channel estimation errors, and and are the corresponding upper bounds of the errors. To characterize the system's robust security, all channel-related constraints must hold for all possible channels within the uncertainty set, and the secrecy rate is taken as the worst-case value. This leads to the following robust optimization problem:

$$(\mathrm{P1}):\max_{\mathbf{w},\mathbf{V},\rho}\Big[\min_{\substack{\tilde{\mathbf{h}}_\mathrm{d}\in\mathscr{H}_\mathrm{d}\\ \tilde{\mathbf{h}}_\mathrm{e}\in\mathscr{H}_\mathrm{e}\cup\mathscr{H}_{\mathrm{e,loc}}}} \log_2\Big(1+\frac{|\tilde{\mathbf{h}}_\mathrm{d}^\mathrm{H}\mathbf{w}|^2}{\sigma_\mathrm{d}^2}\Big)-\log_2\Big(1+\frac{|\tilde{\mathbf{h}}_\mathrm{e}^\mathrm{H}\mathbf{w}|^2}{|\tilde{\mathbf{h}}_\mathrm{e}^\mathrm{H}\mathbf{V}|^2+\sigma_\mathrm{e}^2}\Big)\Big]_+$$

$$s.t.C1: \| w\|^2 \le \rho P_{max}, tr(VV^H) \le (1-\rho)P_{max}$$

$$C2: \boldsymbol{h}_d^H \boldsymbol{V}=\mathbf{0}$$

$$C3: 0<\rho<1$$

$$C4: \| \boldsymbol{V}\|_1 \le \delta$$

$$C5: \forall \tilde{\mathrm{h}}_\mathrm{e}\in\mathscr{H}_\mathrm{e}\cup\mathscr{H}_{\mathrm{e,loc}}: \ |\tilde{\mathrm{h}}_e^H w \mid \le \eta$$

Where is the maximum total transmit power at the transmitter, is the sparsity constraint threshold for the artificial noise matrix, and is the upper bound on the allowed eavesdropper leakage power (replacing the original exact zero-forcing condition). Constraint C1 explicitly allocates the total power between the information beam and artificial noise, ensuring that effectively participates in the optimization; C2 is the null-space orthogonality constraint for artificial noise, ensuring that artificial noise does not interfere with legitimate user reception; C3 is the power allocation coefficient constraint, limiting the range of the power allocation ratio; C4 is the sparse directional constraint for artificial noise, controlling its spatial sparsity; C5 is modified from exact zero-forcing to robust approximate zero-forcing to accommodate channel uncertainty, and all constraints hold for $\forall \tilde{\mathrm{h}}_d\in\mathscr{H}_d, \forall \tilde{\mathrm{h}}_e\in\mathscr{H}_e\cup\mathscr{H}_{e,\mathrm{loc}}$. Optimization problem (P1) is a highly coupled non-convex optimization problem. Both the objective function and constraints contain highly coupled optimization variables($\boldsymbol{w},\boldsymbol{V}$, $\boldsymbol{\rho}$)and since the objective function is in the form of a logarithmic difference and the constraints contain nonlinear terms, it is difficult to solve directly.

3. Solution to the Optimization Problem

This paper proposes a hybrid solution framework integrating Alternating Optimization (AO), Semidefinite Relaxation (SDR), and robust transformation (S-procedure/Schur complement). The core idea of this framework is to first decouple and then convexify the problem, iteratively approximating a local optimal solution. First, the original problem is decomposed into three subproblems to optimize and respectively; each subproblem uses the S-procedure to transform an infinite number of robust constraints into a finite number of Linear Matrix Inequalities (LMIs), and combines SDR to discard non-convex rank-one constraints, thereby converting it into a convex Semidefinite Programming (SDP) problem; finally, a feasible solution is reconstructed from the relaxed solution using a rank-one recovery strategy. The algorithm updates variables sequentially until convergence, thereby obtaining the optimal solution.

3.1 Overall Solution Framework and Variable Decoupling

The difficulty of Problem (P1) lies in: the objective function is in max-min form with an internal logarithmic difference; variables w、V and are highly coupled in power constraints and eavesdropper SINR; and robust constraints must hold for all possible channels, constituting semi-infinite constraints. To address these challenges, we first introduce auxiliary variables and to equivalently transform the max-min objective. Let and denote the worst-case SINR for the legitimate user and the eavesdropper, respectively. The original problem is then

reformulated as:

$$\max_{\mathbf{w},\mathbf{V},\rho,\gamma_d,\gamma_e} [\log_2(1+\gamma_d)-\log_2(1+\gamma_e)]_+$$

s.t. $\forall \tilde{\mathrm{h}}_\mathrm{d} \in \mathscr{H}_d$: $\frac{|\tilde{\mathbf{h}}_\mathrm{d}^\mathrm{H}\mathbf{w}|^2}{\sigma_\mathrm{d}^2} \geq \gamma_d$

$$\forall \tilde{\mathrm{h}}_\mathrm{e} \in \mathscr{H}_\mathrm{e} \cup \mathscr{H}_{\mathrm{e,loc}}: \quad \frac{|\tilde{\mathbf{h}}_\mathrm{e}^\mathrm{H}\mathbf{w}|^2}{|\tilde{\mathbf{h}}_\mathrm{e}^\mathrm{H}\mathbf{V}|^2+\sigma_\mathrm{e}^2} \leq \gamma_e$$

C1-C5, $\gamma_\mathrm{d} \geq 0$, $\gamma_\mathrm{e} \geq 0$

Since is monotonically increasing with respect to and monotonically decreasing with respect to γ_e, the optimal solution must lie on the boundary of the constraints. Therefore, the problem can be decomposed into an outer search over the pair (γ_d, γ_e) and an inner feasibility check with (γ_d, γ_e) fixed. For simplicity, this paper employs alternating optimization to directly decouple w、V and by fixing the other variables and updating the current variable at each step, while embedding a binary search to adjust and to improve convergence speed.

The variable update sequence for alternating optimization is as follows:

1. Fix and ρ, update w;
2. Fix and ρ, update V;
3. Fix and V, update ρ.

Each subproblem is converted into a convex optimization problem.

3.2 Convexification and Robust Transformation of Subproblems

3.2.1 Subproblem 1:Fix and ρ, optimize w

In this case, the constraints related to are: $\| w\|^2 \leq \rho P_{max}$, $\forall \tilde{\mathrm{h}}_\mathrm{e} \in \mathscr{H}_\mathrm{e} \cup \mathscr{H}_{\mathrm{e,loc}}$:$|\tilde{\mathrm{h}}_\mathrm{e}^\mathrm{H}\mathrm{w}| \leq \eta$, as well as the lower bound of the legitimate user's robust SINR and the upper bound of the eavesdropper's robust SINR. For brevity, define $\mathrm{W}=\mathrm{ww}^\mathrm{H}$, then and rank(W)=1. We use SDR to discard the rank-one constraint and first solve the relaxed SDP.

(a) Transformation of the legitimate user's robust SINR constraint

We require that $\forall \, // \boldsymbol{\Delta h_d} \| \leq \varepsilon_d$, $|\,(\mathrm{h}_d+\Delta \mathrm{h}_d)^H w\,|^2 \geq \gamma_d \sigma_d^2$. Using the S-procedure, this infinite constraint is equivalent to the existence of such that:

$$\begin{bmatrix} -\lambda_d \mathrm{I}_{N_t}-\mathrm{W} & -\mathrm{W}\mathrm{h}_d \\ -\mathrm{h}_d^H\mathrm{W} & -\mathrm{h}_d^H\mathrm{W}\mathrm{h}_d+\gamma_d\sigma_d^2+\lambda_d\varepsilon_d^2 \end{bmatrix} \succeq 0$$

(b) Transformation of the eavesdropper's robust SINR upper bound

We require that $\forall \tilde{\mathrm{h}}_\mathrm{e} \in \mathscr{H}_\mathrm{e} \cup \mathscr{H}_{\mathrm{e,loc}}, |\tilde{\mathbf{h}}_e^H\mathbf{w}|^2 \leq \gamma_e(|\tilde{\mathbf{h}}_e^H\mathbf{V}|^2+\sigma_e^2)$.

Let $Z=VV^H$, then the constraint can be written as:

$$\tilde{\mathbf{h}}_e^H\left(\frac{1}{\gamma_e}\mathbf{W}-\mathbf{Z}\right)\tilde{\mathbf{h}}_e \leq \sigma_e^2$$

Since and $// \boldsymbol{\Delta h_e} // \leq \varepsilon_e$, this quadratic inequality holds for all $\Delta \mathrm{h}_e$ .Similarly, it can be converted into an LMI using the S-procedure. Taking as an example, there exists such that:

$$\begin{bmatrix} \mu_e\mathbf{I}-\frac{1}{\gamma_e}\mathbf{W}+\mathbf{Z} & -\left(\frac{1}{\gamma_e}\mathbf{W}-\mathbf{Z}\right)\mathbf{h}_e \\ -\mathbf{h}_e^H\left(\frac{1}{\gamma_e}\mathbf{W}-\mathbf{Z}\right) & \sigma_e^2-\mathbf{h}_e^H\left(\frac{1}{\gamma_e}\mathbf{W}-\mathbf{Z}\right)\mathbf{h}_e-\mu_e\varepsilon_e^2 \end{bmatrix} \succeq 0$$

(c) Robust approximate zero-forcing constraint C5

The constraint holds for all $\forall \tilde{\mathrm{h}}_\mathrm{e} \in \mathscr{H}_\mathrm{e} \cup \mathscr{H}_{\mathrm{e,loc}}$, which is equivalent to $\tilde{\mathbf{h}}_e^H\mathbf{W}\tilde{\mathbf{h}}_e \leq \eta^2$ .Similarly, using the S-procedure to transform into an LMI, we have:

$$\begin{bmatrix} \mu_e\mathbf{I}-\mathbf{W} & -\mathbf{W}\mathbf{h}_e \\ -\mathbf{h}_e^H\mathbf{W} & \eta^2-\boldsymbol{h}_e^H\mathbf{W}\mathbf{h}_e-\mu_e\varepsilon_e^2 \end{bmatrix} \succeq 0$$

In summary, the relaxed formulation of Subproblem 1 is: given V,ρ,γ_d, and γ_e, solve the SDP (with variables and auxiliary scalars λ_d , μ_e ,etc.)with the objective of maximizing $\log_2(1+\gamma_\mathrm{d})-\log_2(1+\gamma_\mathrm{e})$ .We can use binary search to find while converting the objective into a feasibility problem. After obtaining the optimal solution W^* , if rank(W^*)=1 ,we directly take the principal eigenvector $\mathrm{w}^* = \sqrt{\lambda_{\max}}\mathrm{u}_{\max}$;otherwise, we use Gaussian randomization (generate several candidate and select the one that maximizes the original objective while satisfying the constraints).

Initialize

Given current $\boldsymbol{V}^i$,ρ^i,γ_d^i,γ_e^i , set interior-point method precision ε , maximum iterations K , initial λ_d=0,μ_e=0,μ_{loc}=0, internal count k=0

repeat

Construct the SDP for and λ_d,μ_e,μ_{loc}:

$\mathrm{tr}(\boldsymbol{W}) \leq \rho^i P_{\max}$,

LMI (legitimate user robust SINR lower bound),

LMI (eavesdropper robust SINR upper bound),

LMI (approximate zero-forcing constraint C5)

Call SDP solver to obtain $\boldsymbol{W}^*$

if then

$\boldsymbol{w}=\sqrt{\lambda_{\max}}\boldsymbol{u}_{\max}$ (principal eigenvector decomposition)

else

Generate candidate using Gaussian randomization, select the one that maximizes and satisfies robust constraints

end if

$\boldsymbol{w}^{k+1}=\boldsymbol{w}$

k=k+1
until or $k \geq K$
$\boldsymbol{w}^{i+1}=\boldsymbol{w}^{k}$
Return $\boldsymbol{w}^{i+1}$

3.2.2 Subproblem 2: Fix and ρ, optimize V

This paper employs the proximal gradient method to directly optimize rather than to avoid the complex coupling between rank and sparsity. After fixing and ρ, the constraints related to are limited to:

Power constraint: $tr(VV^H) \leq (1-\rho)P_{max}$;

Null-space constraint: $\mathrm{h}_d^H V=0$

Sparsity constraint:$\| \boldsymbol{V} \|_1 \leq \delta$

Eavesdropper robust upper bound constraint, which can be equivalently reformulated as:

$$\tilde{\boldsymbol{h}}_e^H \left(\frac{1}{\gamma_e} \boldsymbol{w}\boldsymbol{w}^H - \boldsymbol{V}\boldsymbol{V}^H \right) \tilde{\boldsymbol{h}}_e \leq \sigma_e^2, \quad \forall \tilde{\mathrm{h}}_e \in \mathscr{H}_e \cup \mathscr{H}_{e,\mathrm{loc}}$$

The objective is to maximize the secrecy rate given γ_e, i.e., to minimize γ_e, or directly find a feasible that satisfies all constraints. This paper adopts a feasibility checking combined with an outer-layer binary search method; therefore, the core of Subproblem 2 lies in determining, given γ_e, whether there exists a that satisfies the above constraints.

To convexify the non-convex problem, we introduce semidefinite relaxation: let and $Q \succeq 0$, then rank(Q)$\leq N_t-1$ (since $\mathrm{V} \in \mathrm{C}^{\mathrm{N_t} \times (\mathrm{N_t}-1)}$, normally rank(Q)=N_t-1). Ignoring the rank constraint, we solve the convex relaxation problem with respect to Q.

The power constraint is transformed into:

$$\mathrm{tr(Q)} \leq (1-\rho)P_{max}$$

The null-space constraint is equivalent to $V^H \mathrm{h_d}=0$, which implies $\mathrm{Qh_d}=VV^H \mathrm{h}_d=0$. Since $\mathrm{Q} \succeq 0$, this linear constraint can be written as:

$$\mathrm{Qh_d}=0$$

Let $\mathrm{M}=\frac{1}{\gamma_e}\mathrm{ww}^H-\mathrm{Q}$, then then the eavesdropper's robust SINR upper bound constraint can be written as:

$$\tilde{\mathbf{h}}_e^H \mathbf{M} \tilde{\mathbf{h}}_e \leq \sigma_e^2, \quad \forall \tilde{\mathrm{h}}_e \in \mathscr{H}_e \cup \mathscr{H}_{e,\mathrm{loc}}$$

Taking as an example, we require that this inequality holds for all $/\!/ \Delta \mathrm{h_e} /\!/ \leq \varepsilon_e$. According to the S-Procedure, this semi-infinite constraint is equivalent to the existence of $\mu_e \geq 0$ such that:

$$\begin{bmatrix} \mu_e \mathrm{I}-\mathrm{M} & -\mathrm{Mh}_e \\ -\mathrm{h}_e^H \mathrm{M} & -\mathrm{h}_e^H \mathrm{M} \mathrm{h}_e + \sigma_e^2 - \mu_e \varepsilon_e^2 \end{bmatrix} \succeq 0$$

For $\mathscr{H}_{\mathrm{e,loc}}$, simply replace with the nominal channel vector, replace with $\varepsilon_{\mathrm{loc}}$, and introduce the corresponding auxiliary variable $\mu_{\mathrm{loc}} \geq 0$, to obtain a similar LMI.

Ignoring the sparsity constraint and rank constraint, the feasibility check for Subproblem 2 is: given γ_{e}, determine whether there exist $\mathrm{Q} \succeq 0$, $\mu_e \geq 0$, and $\mu_{\mathrm{loc}} \geq 0$ such that $\mathrm{tr(Q)} \leq (1-\rho)P_{max}$,$\mathrm{Qh_d}=0$, and the above LMIs are satisfied. This is a standard SDP problem that can be efficiently solved using interior-point methods (such as SeDuMi or SDPT3) or first-order algorithms.

If the SDP is feasible, let its optimal solution be $\mathbf{Q}^*$ .Since the rank(Q)$\leq N_t-1$ and sparsity constraints were discarded during relaxation, the following steps are required to recover that satisfies the original constraints:

Perform eigenvalue decomposition on $\mathbf{Q}^*$, take the N_t-1 largest eigenvalues and their corresponding eigenvectors, and construct:

$$\tilde{\mathbf{V}}=\mathbf{U}_r \mathbf{\Lambda}_r^{1/2} \in C^{N_t \times (N_t-1)}$$

Where contains the first eigenvectors, and $\mathbf{\Lambda}_r$ is a diagonal matrix containing the corresponding eigenvalues. Then $\tilde{\mathbf{V}}\tilde{\mathbf{V}}^H \approx \mathbf{Q}^*$, and rank($\tilde{\mathbf{V}}$)$\leq N_t-1$.

Enforce $\mathrm{h}_d^H \mathrm{V}=0$. Let be the projection matrix onto the orthogonal complement of h_d, then:

$$\mathbf{V}_{\mathrm{orth}}=\mathbf{P}\tilde{\mathbf{V}}$$

This operation satisfies $\mathrm{h_d^H V_{orth}}=0$ and does not alter the orthogonality of the column space of $\mathbf{V}_{\mathrm{orth}}$.

To satisfy $\| \boldsymbol{V} \|_1 \leq \delta$, use the soft thresholding operator:

$$[S_\lambda(\mathbf{X})]_{ij}=\mathrm{sgn}(X_{ij}) \cdot \ max(|X_{ij}|-\lambda,0)$$

Use binary search to find such that $\| S_\lambda(\mathbf{V}_{\mathrm{orth}}) /\!/_1 \leq \delta$, and set $\mathbf{V}_{\mathrm{sparse}}=S_\lambda(\mathbf{V}_{\mathrm{orth}})$. If the power constraint is violated, scale proportionally:

$$\mathbf{V}_{\mathrm{sparse}} \leftarrow \mathbf{V}_{\mathrm{sparse}} \cdot \sqrt{\frac{(1-\rho)P_{max}}{\| \mathbf{V}_{\mathrm{sparse}} \|_F^2}}$$

and repeat the sparse projection.

Substitute the final into the original robust constraint for verification: randomly sample M channels from the uncertainty set and check whether all sampled points satisfy the inequality. If successful, output V; otherwise, appropriately increase and re-solve the SDP.

Initialize

Given current $\boldsymbol{w}^{i+1}$, ρ^i, γ_e^i, sparsity threshold δ, maximum iterations K, initial $\mu_e=0$,$\mu_{\mathrm{loc}}=0$, internal count

repeat

Construct the SDP for and :

$$\&\mathrm{tr}(\boldsymbol{Q})\le(1-\rho^{i})P_{\max},$$
$$\&\boldsymbol{Q}\boldsymbol{h}_{d}=\boldsymbol{0},$$

&LMI (eavesdropper robust SINR upper bound)
Call SDP solver to obtain

Perform eigenvalue decomposition on $\boldsymbol{Q}^{*}$,take the first principal components to obtain $\widetilde{\boldsymbol{V}}$

$$\boldsymbol{V}_{\mathrm{orth}}=\left(\boldsymbol{I}-\frac{\boldsymbol{h}_{d}\boldsymbol{h}_{d}^{H}}{\|\boldsymbol{h}_{d}\|^{2}}\right)\widetilde{\boldsymbol{V}}$$

Binary search to make $\| S_{\lambda}(\boldsymbol{V}_{\mathrm{orth}})\|_{1}\le\delta$, set
If

$$\boldsymbol{V}_{\mathrm{sparse}}\leftarrow\boldsymbol{V}_{\mathrm{sparse}}\cdot\sqrt{(1-\rho^{i})P_{\max}/\,/\,\boldsymbol{V}_{\mathrm{sparse}}\|_{F}^{2}}$$

$\boldsymbol{V}^{k+1}=\boldsymbol{V}_{\mathrm{sparse}}$
end if
$k=k+1$
until or

$$\boldsymbol{V}^{i+1}=\boldsymbol{V}^{k}$$

Return $\boldsymbol{V}^{i+1}$

3.2.3 Subproblem 3: Fix and V, optimize ρ

In the t-th iteration of alternating optimization, given the information beamforming vector $w(\mathrm{t})$ and artificial noise matrix $V(\mathrm{t})$, the power allocation coefficient appears only in the total power constraint C1. The objective of this subproblem is to minimize the proportion of information power (thereby allocating the remaining power to artificial noise), while ensuring that the choice of does not degrade the secrecy rate. Since the objective function has no direct dependency on after fixing and (ρ does not affect the SINR expression), Subproblem 3 is essentially a feasibility check and power allocation ratio adjustment problem.

From constraint C1: $\| w\|^{2}\le\rho P_{max}$, $tr(VV^{H})\le(1-\rho)P_{max}$, combined with $0<\rho<1$, we obtain that must simultaneously satisfy:

$$\rho\ge\frac{\|\mathbf{w}\|^{2}}{P_{max}},\rho\le1-\frac{\mathrm{tr}(\mathbf{V}\mathbf{V}^{H})}{P_{max}},0<\rho<1$$

Therefore, a feasible exists if and only if:

$$\frac{\|\mathbf{w}\|^{2}}{P_{max}}+\frac{\mathrm{tr}(\mathbf{V}\mathbf{V}^{H})}{P_{max}}\le1$$

This condition is equivalent to the total transmission power of the current and not exceeding P_{max} ,which is naturally satisfied during algorithm iterations due to constraint C1 in the original problem.

To maximize the interference capability of artificial noise in subsequent iterations, power should be allocated to artificial noise as much as possible, i.e., the smallest feasible should be selected. At the same time, should not be less than $\frac{\|\mathbf{w}\|^{2}}{P_{max}}$, otherwise the power constraint would be violated. Therefore, the optimal solution is:

$$\rho^{*}=\frac{\|\mathbf{w}\|^{2}}{P_{max}}$$

This value ensures that the information beam uses exactly the allocated power, with the remaining power$(1-\rho^{*})P_{max}$entirely allocated to artificial noise. Furthermore, we need to verify whether satisfies the upper bound constraint:

$$\frac{\|\mathbf{w}\|^{2}}{P_{max}}\le1-\frac{\mathrm{tr}(\mathbf{V}\mathbf{V}^{H})}{P_{max}}\Leftrightarrow//\mathbf{w}\|^{2}+\mathrm{tr}(\mathbf{V}\mathbf{V}^{H})\le P_{max}$$

This is precisely the original form of C1, so it holds. If numerical errors cause a slight violation, a projection can be applied:

$$\rho^{*}=min(max(\frac{//\mathbf{w}//^{2}}{P_{max}},\varepsilon),1-\varepsilon)$$

Where is a small positive number (e.g., 10^{-6}) to avoid boundary degeneracy.

Initialize

Given current $\boldsymbol{w}^{i+1},\boldsymbol{V}^{i+1}$, total power $P_{\max}$, boundary constant $\varepsilon=10^{-6}$

$\rho^{i+1}=\min\ \left(\max(\rho_{\mathrm{temp}},\varepsilon),1-\varepsilon\right)$

Return ρ^{i+1}

4. Simulation Results

4.1 Simulation Parameter Settings

To verify the effectiveness of the proposed robust secrecy beamforming algorithm for artificial noise-aided MISO wiretap channels, Monte Carlo simulation experiments were conducted in the MATLAB R2023b environment. The simulations used the CVX 2.2 toolbox to solve convex optimization problems. All comparison algorithms employed the same channel realizations and parameter settings to ensure a fair comparison. The specific simulation parameters are shown in Table 1.

Table 1. Simulation Parameter Settings

Parameter	Symbol	Value
Number of Transmitter Antennas	N_t	4
Maximum Transmit Power	P_{max}	20 dBm (100 mW)
Legitimate User Noise Power	σ_d^2	1
Eavesdropper Noise Power	σ_e^2	1
Legitimate User Channel Error Radius	ε_d	0.1
Eavesdropper Channel Estimation Error Radius	ε_e	0.1
Eavesdropper Location Uncertainty Radius	ε_{loc}	0.1

Artificial Noise Sparsity Threshold	δ	0.8
Robust Approximate Zero-Forcing Leakage Upper Bound	η	5×10^{-4}
Maximum Iterations for Alternating Optimization	max_iter	20
Convergence Tolerance	tol	10^{-2}
Number of Monte Carlo Trials	num_real	100
Number of Monte Carlo Trials for Robustness Testing	num_robust	50
Number of Worst-Case SINR Samples	N_s	500

This paper selects the following four typical algorithms for performance comparison:

Proposed algorithm: The secrecy beamforming algorithm proposed in this paper, which integrates alternating optimization, semidefinite relaxation, and dual robustness constraints

Non-robust algorithm: Identical in structure to the proposed algorithm, but ignoring all channel uncertainties(ε_d=ε_e=ε_{loc}=0)

No artificial noise algorithm: Uses only Maximum Ratio Transmission (MRT) beamforming without transmitting artificial noise

Random null-space artificial noise algorithm: Uses MRT beamforming and transmits uniform random artificial noise within the legitimate channel's null space; the power allocation coefficients are the same as those in the proposed algorithm

4.2 Convergence Analysis

First, we analyze the convergence performance of the proposed algorithm. Figure 2 shows the curve of the proposed algorithm's secrecy rate versus the number of iterations under a single typical channel realization.

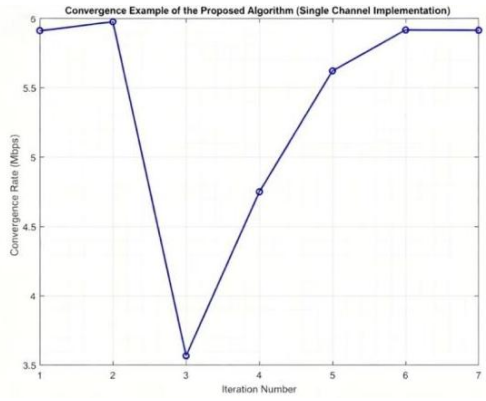

Figure 2. Convergence Example of the Proposed Algorithm (Single Channel Realization)

As shown in Figure 2, the algorithm exhibits slight fluctuations in the early stages of iteration due to the coupling between the information beam and artificial noise; this is a normal phenomenon in alternating optimization algorithms. After a brief performance dip at the third iteration, the algorithm quickly adjusted and continued to rise, stabilizing after the sixth iteration, with the final secrecy rate maintaining around 5.9 bps/Hz.

Figure 3 shows the histogram of the number of iterations of the proposed algorithm in 100 Monte Carlo experiments.

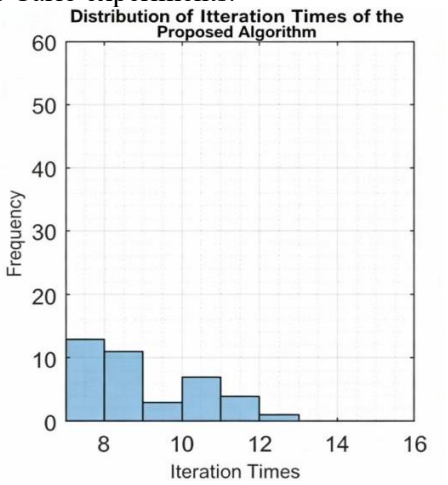

Figure 3. Distribution of Iteration Counts of the Proposed Algorithm

The statistical results show that the proposed algorithm requires an average of 7.8 iterations, with all samples converging within 13 iterations. Approximately 70% of the samples converged within 7–10 iterations, and none required more than 15 iterations. This indicates that the alternating optimization framework proposed in this paper exhibits good convergence properties and can find satisfactory local optimal solutions in a small number of iterations, thereby meeting the requirements of real-time communication systems.

4.3 Secrecy Rate Performance Comparison

Figure 4 shows the Cumulative Distribution Function (CDF) curves for the secrecy rate of the four algorithms based on 100 Monte Carlo simulations.

As shown in Figure 4, the performance of the proposed algorithm is significantly better than that of the algorithm without artificial noise. At CDF = 0.5 (i.e., the secrecy rate achievable in 50% of channel realizations), the proposed algorithm's secrecy rate is slightly higher than that of the random artificial noise algorithm and

significantly higher than that of the no-artificial-noise algorithm. In the high-reliability region at CDF = 0.9 (i.e., the secrecy rate achievable in 90% of channel realizations), the proposed algorithm's secrecy rate is comparable to that of the non-robust algorithm and far exceeds that of the no-artificial-noise algorithm.

Figure 5 presents a bar chart comparing the average secrecy rates of the four algorithms.

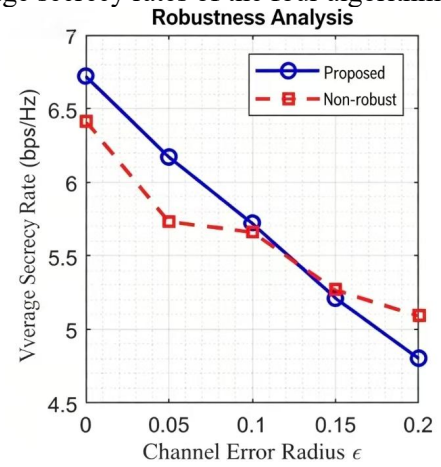

Figure 4. Cumulative Distribution of Secrecy Rates

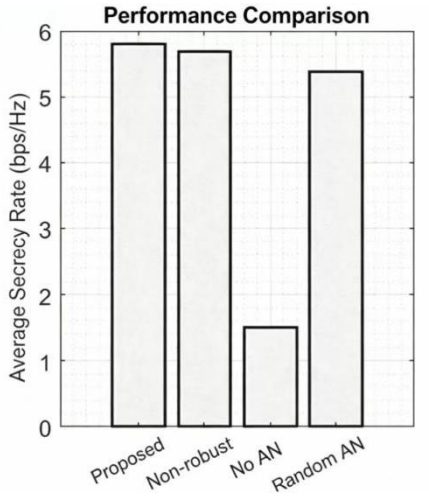

Figure 5. Average Secrecy Rates (bps/Hz)

The specific numerical results are shown in Table 2.

As shown in Table 2, the proposed algorithm achieves the highest average secrecy rate, reaching 5.79 bps/Hz. The non-robust algorithm, which does not account for channel uncertainty, has an average secrecy rate of 5.69 bps/Hz, approximately 1.73% lower than that of the proposed algorithm. The random artificial noise algorithm has an average secrecy rate of 5.38 bps/Hz, which is approximately 7.1% lower than the proposed algorithm. The no-artificial-noise algorithm has the lowest average secrecy rate, at only 1.51 bps/Hz, which is approximately 73.9% lower than the proposed algorithm.

Table 2. Average Secrecy Rate Comparison

Algorithm	Average Secrecy Rate (bps/Hz)	Performance Loss Relative to the Proposed Algorithm
Proposed algorithm	5.79	0%
Non-robust algorithm	5.69	1.73%
Random artificial noise algorithm	5.38	7.10%
No artificial noise algorithm	1.51	73.90%

It should be noted that although the average rates of the proposed algorithm and the non-robust algorithm are relatively close, the proposed algorithm demonstrates a significant performance advantage in the high-reliability region (CDF > 0.9). In practical communication systems, performance in the high-reliability region is more critical than the average rate, as it determines the quality of secure communication the system can provide in the vast majority of cases. This result validates the effectiveness of the joint optimization framework proposed in this paper: by simultaneously optimizing the information beamforming vector, artificial noise matrix, and power allocation coefficients, the proposed algorithm maximizes interference with the eavesdropper's signal reception while ensuring the communication quality of legitimate users, thereby significantly improving the system's secrecy performance.

4.4 Robustness Analysis

To verify the robustness of the proposed algorithm under non-ideal channel conditions, this paper tests the average secrecy rate performance under different channel error radii. The channel error radius ranges from 0 to 0.2, with a step size of 0.05. For each error radius, 50 Monte Carlo simulations are performed, and the results are averaged.

Figure 6 shows the comparison curves of the average secrecy rates between the proposed algorithm and the non-robust algorithm under different channel error radii.

As shown in Figure 6, the secrecy rates of all algorithms decrease as the channel error radius increases. This is because greater channel uncertainty leads to less accurate estimates of the true channel by the transmitter, resulting in reduced effectiveness of beamforming and artificial noise design.

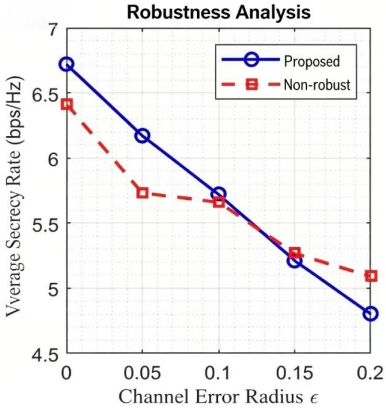

Figure 6. Robustness Analysis

However, the rate of decline for the proposed algorithm is significantly slower than that of the non-robust algorithm. When (ideal channel), the performance of the two algorithms is similar: the proposed algorithm achieves a secrecy rate of approximately 6.7 bps/Hz, while the non-robust algorithm achieves approximately 6.5 bps/Hz. When ε=0.1, the proposed algorithm's secrecy rate remains around 5.7 bps/Hz, with a decrease of approximately 14.9%; whereas the secrecy rate of the non-robust algorithm has dropped to 5.6 bps/Hz, representing a decrease of approximately 13.8%. When ε=0.2, the secrecy rate of the proposed algorithm remains around 4.8 bps/Hz, representing a decrease of approximately 28.4%; whereas the secrecy rate of the non-robust algorithm has dropped to 5.1 bps/Hz, representing a decrease of approximately 21.5%.

Due to the randomness of Monte Carlo sampling, individual data points exhibit slight fluctuations; however, the overall trend clearly indicates that the proposed algorithm, by simultaneously considering channel estimation errors and eavesdropper location uncertainty and transforming the robust constraints into linear matrix inequalities, is capable of maintaining stable secrecy performance under non-ideal channel conditions. In contrast, the non-robust algorithm, which assumes perfectly ideal channel state information, experiences a more rapid decline in performance under channel uncertainty and fails to meet the requirements of practical communication systems.

5. Conclusion

This paper investigates physical layer secure communication in artificial noise-aided MISO wiretap channels, where the system includes legitimate receiving users and illegal eavesdroppers. Considering total transmit power constraints, artificial noise null-space orthogonality constraints, and sparse directional constraints, we introduce dual robustness constraints under channel estimation error and eavesdropper location uncertainty. With the objective of maximizing the system's secrecy rate, we jointly optimize the information beamforming vector, artificial noise matrix, and power allocation coefficients. Alternating optimization, semidefinite relaxation, and S-procedure convex transformation algorithms are employed to solve the highly coupled non-convex optimization problem. Analysis of simulation results indicates that, compared to existing schemes, the proposed method exhibits faster convergence and higher secrecy rates, maintains stable secrecy performance even in scenarios with channel uncertainty, and, compared to the random artificial noise scheme, directional artificial noise effectively improves interference energy utilization efficiency.

References

[1] Chen, X., Feng, Y. (2017) Security performance analysis of MISOME systems under secure outage probability constraints. *Computer Technology and Development*, 27: 83–87+92.

[2] Xu, J., Xu, S., Sun, L. (2017) Robust beamforming design assisted by artificial noise in multi-transmitter single-receiver wiretap channels. *Journal of Xi'an Jiaotong University*, 51: 124–130.

[3] Deng, Z., Dai, C., Zhang, Z. (2024) Physical layer secure communication assisted by hybrid reconfigurable intelligent surfaces and artificial noise. *Journal of Electronics & Information Technology*, 46: 3155–3164.

[4] Li, J., Lü, B. (2023) MISO wireless secure transmission based on active intelligent reflecting surfaces and artificial noise assistance. *Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition)*, 43: 61–71.

[5] Wang, S., Da, X. (2017) Robust secure transmission design for multi-beam satellite communications under non-ideal channel conditions. *Journal of Electronics & Information Technology*, 39: 92–100.

[6] Shi, Y., Wu, Y., Zhao, D. (2024) Secure transmission scheme based on cooperative interference, hybrid intelligent reflecting surfaces and relay assistance. *Journal of Computer Applications*, 44: 253–258.

