Artificial Noise Assisted Interference Alignment for Physical Layer Security Enhancement

Lin Hu, Junxiang Peng, Yan Zhang†, Hong Wen*, Shuai Tan, and Jiabing Fan
School of Communications and Information Engineering, Chongqing University of Posts and Telecommunication, Chongqing, China
†School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China
*School of Aeronautics and Astronautics, University of Electronic Science and Technology of China, Chengdu, China
Emails: lin.hu@ieee.org, sunlike@uestc.edu.cn, {junxiang.peng.cqupt, yixianqianzy, shuai.tan.cqupt, jiabing.fan.cqupt}@gmail.com

GLOBECOM 2022 - 2022 IEEE Global Communications Conference | 978-1-6654-3540-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/GLOBECOM48099.2022.10000712

***Abstract*—Secure transfer of wireless information is becoming a critical issue in multi-user interference networks. In this paper, we consider secure transmission from a source (Alice) to a legitimate destination (Bob), coexisting with a passive eavesdropper (Eve) and K transceiver pairs. By assuming that only statistical channel state information (CSI) of Eve and local CSIs of legitimate users are known, a secrecy beamforming scheme with artificial noise (AN) is designed for secure transmission, and a modified interference alignment (IA) scheme is proposed for secrecy enhancement. Unlike the conventional AN-aided IA approaches which may lead to private signal cancellation, we propose a novel design modification with security protection. Moreover, a definite connection between improperness and infeasibility of IA is established, to provide guiding insights on IA requirements. Based on a strict mathematical analysis, we further characterize the impact of transmit power on transceiver design and secrecy performance. Numerical results confirm that our design enables high transmission security with performance guarantee, and thus is suitable and stable for physical layer security (PLS) in multi-user interference networks.**

***Index Terms*—Physical layer security, interference networks, interference alignment, secrecy rate, secrecy outage probability, artificial noise.**

I. Introduction

Wireless communication is particularly vulnerable and susceptible to security attacks (e.g., malicious interception and eavesdropping) due to the broadcast characteristics of wireless medium. Thus guarantying confidentiality is one of the top issues in wireless networks [1]–[6]. As a complement to the cryptography-based encryption method, by exploiting the physical properties of wireless channel, physical layer security (PLS) can support secrecy communication, and is identified as an important complement to cryptographic techniques.

Artificial noise (AN) is an intuitive and effective method for secure communication. More precisely, AN aided beamforming and cooperative jamming for secrecy rate maximization (SRM) problem are designed in [7], [8]. It turns out that this scheme can enhance both secrecy rate and secure energy efficiency. The authors in [9] investigate the worst-case scenario so that omit the noise at eavesdropper (Eve). The difference is that the work [10] takes the noise term into consideration and obtains an optimal solution. The problem of minimizing the secrecy outage probability (SOP) is considered in [11], [12].

On the other hand, interference is a fundamental nature of multi-user networks, which is harmful for secure communication. Therefore, interference management becomes important. The seminal work can be traced back to the interference alignment (IA)-a promising solution for interference management in wireless networks are proposed in [13]. Consequently, minimizing interference leakage (MinIL) algorithm was proposed in [14] to solve the problem of IA with low computational complexity. In [15], some works were done to introduce the alternating minimization (AM) algorithm for IA with arbitrary antennas, number of users, or spatial streams in the MIMO interference channel.

From the point of networks based on IA, the multi-user interference network seems more secure. In [16], secure communication based on IA is proposed in the multi-user interference network, by assuming the interference and the AN from legitimate base station are aligned at target users to be eliminated. Based on this work, a novel AN scheme for the anti-eavesdropping in the multi-user interference network is studied [17]. In this scheme, the interference and the AN from different legitimate transmitters are aligned into two different subspaces at legitimate receivers. Then the scheme can both enhance the desired signal and make Eves more confused. Moreover, the authors in [18] combine secure communication with green communication, and further studies the energy harvesting efficiency in the multi-user interference network. In addition, AN aided IA for secure transmit design is investigated in [19].

Our work is significantly different from the existing secrecy-enhancing transmit schemes [7]–[11] and secure communication for interference networks [16]–[19] in the following aspects:

1) The security schemes [7]–[11] do not consider the interference mitigation, and thus cannot be directly applied to the multi-user interference networks. To enhance secrecy performance in multi-user scenario, we propose a secure transmit design based on IA, which align the interference at legitimate user while disrupting the potential eavesdropping. Different from conventional schemes in [16]–[19] which do not take into account the secrecy outage event, we investigate the SRM problem under the SOP constraint. When the instantaneous CSI of wiretapping channel is not available, the SOP cannot be prevented with absolute certainty.

2) The authors in [16] study the proper condition to achieve IA. However, there does not exist a definite link between properness and feasibility. In fact, determining the feasibility of IA is NP-hard. To circumvent this difficulty, we establish a condition to develop a direct connection between improperness and infeasibility. Our intuition is that the improper systems are almost surely infeasible.

3) Unlike traditional AN aided IA approaches which may lead to private signal cancellation, we propose a modified IA algorithm to avoid this impediment. Numerical results show that the proposed method is more stable and effective than conventional methods.

II. System Model and Problem Formulation

Consider the multi-user wireless network, as show in Fig. 1, where Alice intends to transmit a confidential message to Bob, in the presence of a passive Eve and K transmitter–receiver pairs. Assume that all transmitter and receiver are equipped with M and N antennas, respectively, nevertheless Eve is equipped with a single antenna. Due to the passive nature of Eve, we assume that the statistical CSI is available. Furthermore, we presume that local CSI is available for each user, namely, each transmitter j knows the local channel matrices $\mathbf{H}_{kj}$ to all receivers k, where $k, j \in \{1, 2, ..., K\}$. Assume that Alice sends both confidential message and AN. Thus we can construct $\mathbf{s}_a$ as

$$\mathbf{s}_a = \sqrt{P_a\phi}\mathbf{v}_a x_a + \sqrt{P_a(1-\phi)/d_{an}}\mathbf{W}_a\mathbf{z}_a, \tag{1}$$

where the transmit power of Alice is P_a. Let $\phi \in [0, 1]$ express the fraction of P_a assigned to the private signal. Besides, x_a and $\mathbf{v}_a \in \mathbb{C}^M$ denote the data symbol and corresponding beamforming vector. Similarly, $\mathbf{z}_a \in \mathbb{C}^{d_{an}}$ and $\mathbf{W}_a \in \mathbb{C}^{M\times d_{an}}$ corresponds to the vector that contain d_{an} streams of AN generated by Alice and its precoding matrix.

In addition, we assume the transmit power of each transmitter is P. Then, the signal vector $\mathbf{s}_j$ transmitted from the transmitter j can be expressed as

$$\mathbf{s}_j = \sqrt{P}\mathbf{v}_j x_j, \tag{2}$$

where the transmitted secret-free signal is x_j and its beamforming vector is $\mathbf{v}_j \in \mathbb{C}^M$.

Then, the received signal after filtering at Bob can be formulated as

$$\begin{aligned} y_b =& \mathbf{u}_a^H\mathbf{H}_{ba}\mathbf{s}_a + \sum_{j=1}^{K}\mathbf{u}_a^H\mathbf{H}_{bj}\mathbf{s}_j + \mathbf{u}_a^H\mathbf{n}_b \\ =& \underbrace{\sqrt{P_a\phi}\mathbf{u}_a^H\mathbf{H}_{ba}\mathbf{v}_a x_a}_{\text{desired signal}} + \underbrace{\sum_{j=1}^{K}\sqrt{P}\mathbf{u}_a^H\mathbf{H}_{bj}\mathbf{v}_j x_j}_{\text{interferences}} \\ &+ \underbrace{\sqrt{P_a(1-\phi)/d_{an}}\mathbf{u}_a^H\mathbf{H}_{ba}\mathbf{W}_a\mathbf{z}_a}_{\text{artificial noise}} + \mathbf{u}_a^H\mathbf{n}_b, \end{aligned} \tag{3}$$

where channels from Alice to Bob and j-th transmitter to Bob are expressed by $\mathbf{H}_{ba} \in \mathbb{C}^{N\times M}$ and $\mathbf{H}_{bj} \in \mathbb{C}^{N\times M}$, respectively. In addition, $\mathbf{n}_b$ represents additive complex white Gaussian noises (AWGN) at Bob.

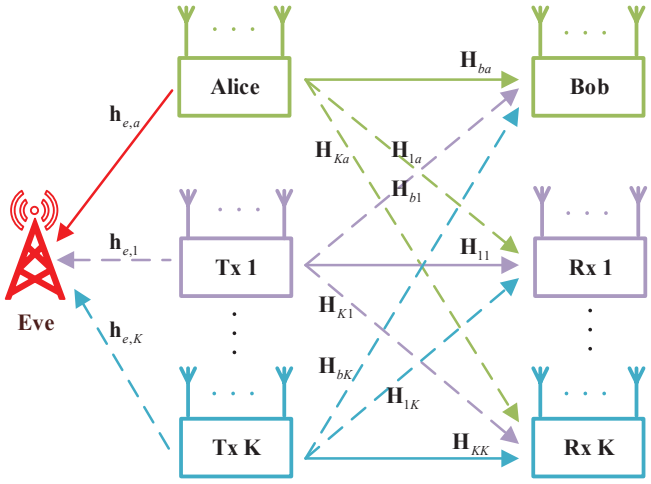

Fig. 1. K-user MIMO interference channel with external eavesdropper.

To avoid private signal cancellation, we design the beamformer at Alice (Bob) by choosing $\mathbf{u}_a$ ($\mathbf{v}_a$) as the left (right) singular vector, corresponding to the largest singular value of $\mathbf{H}_{ba}$. This transmission scheme is referred to as the max-eigenmode transmission, and can effectively avoid private signal cancellation. Moreover, the received signal after filtering at receiver k, and Eve can be expressed as

$$y_k = \sum_{j=1}^{K}\mathbf{u}_k^H\mathbf{H}_{bj}\mathbf{s}_j + \mathbf{u}_k^H\mathbf{H}_{ka}\mathbf{s}_a + \mathbf{u}_k^H\mathbf{n}_k, \tag{4}$$

$$y_e = \mathbf{h}_{ea}^H\mathbf{s}_a + \sum_{j=1}^{K}\mathbf{h}_{ej}^H\mathbf{s}_j + n_e, \tag{5}$$

where channels from Alice to k-th receiver and Eve are denoted by $\mathbf{H}_{ka} \in \mathbb{C}^{N\times M}$ and $\mathbf{h}_{ea} \in \mathbb{C}^M$, respectively. Likewise, the channels form j-th transmitter to k-th receiver and Eve are expressed by $\mathbf{H}_{kj} \in \mathbb{C}^{N\times M}$ and $\mathbf{h}_{ej} \in \mathbb{C}^M$, respectively. Moreover, $\mathbf{n}_k$ and n_e represent AWGN at k-th receiver and Eve, respectively. In order to avoid the inter-user interference, the following conditions should be satisfied.

$$\mathbf{u}_a^H\mathbf{H}_{bj}\mathbf{v}_j = 0,\ \mathbf{u}_k^H\mathbf{H}_{ka}\mathbf{v}_a = 0,\ \mathbf{u}_k^H\mathbf{H}_{kj}\mathbf{v}_j = 0,\ \forall j \neq k, \tag{6}$$

$$\mathbf{u}_a^H\mathbf{H}_{ba}\mathbf{W}_a = \mathbf{0},\ \mathbf{u}_k^H\mathbf{H}_{ka}\mathbf{W}_a = \mathbf{0}. \tag{7}$$

The multi-user interference networks based on IA is called feasible if there exist beamforming vector $\mathbf{v}_j$, received combining vector $\mathbf{u}_k$ and precoding matrix $\mathbf{W}_a$ such that (6) and (7) are satisfied. However, checking feasibility of IA is an open probelm [20]. To circumvent this difficulty, we propose a condition to establish a definite link between improperness and infeasibility, by simply comparing the total number of equations and the total number of variables may suffice.

According to [16], [20], the total number of variables in the vectors $\mathbf{u}_k,\ \mathbf{v}_k,\ k = 1, 2, \ldots, K$, can be denoted as

$$N_1 = K(M + N - 2). \tag{8}$$

In addtion, the number of variables in $\mathbf{W}_a$ is given by

$$N_2 = d_{an}(M - d_{an}). \tag{9}$$

Thus, the total number of variables in (6) and (7) can be calculated as

$$N_V = N_1 + N_2 = K\left(M+N-2\right) + d_{an}\left(M-d_{an}\right). \quad (10)$$

Likewise, the total number of equations in (6) and (7) can be denoted as

$$N_E = \left(K+d_{an}\right)\left(K+1\right). \quad (11)$$

Thus, we can know that an asymmetric system is improper if $N_V < N_E$ according to [20]. Then

$$K\left(M+N-2\right) + d_{an}\left(M-d_{an}\right) < \left(K+d_{an}\right)\left(K+1\right). \quad (12)$$

Remark 1: The guiding intuition is that the improper systems are almost surely infeasible, then we develop a direct connection between improperness and infeasibility. Extensive experiments verify that the system configuration dissatisfy the improper condition, then the perfect IA could be achieved, i.e., AN and interference can be eliminated at the receivers.

In order to eliminate interference with AN together at the receivers, we will adopt AM algorithm in [15] with some necessary modifications.

1) We start with arbitrary beamforming vectors $\mathbf{v}_j$ and $\mathbf{W}_a$ satisfying $\mathbf{v}_j^H\mathbf{v}_j = 1$ and $\mathbf{W}_a^H\mathbf{W}_a = \mathbf{I}_{d_{an}}$. Besides, we fix $\mathbf{u}_a\left(\mathbf{v}_a\right)$ as the max-eigenmode beamforming.
2) Let the columns of matrix $\mathbf{S}_k$ be the $N-1$ dominant eigenvectors of $\mathbf{H}_{ka}\mathbf{v}_a\mathbf{v}_a^H\mathbf{H}_{ka}^H + \mathbf{H}_{ka}\mathbf{W}_a\mathbf{W}_a^H\mathbf{H}_{ka}^H + \sum_{j=1,j\neq k}^{K}\mathbf{H}_{kj}\mathbf{v}_j\mathbf{v}_j^H\mathbf{H}_{kj}^H$, where the matrix $\mathbf{S}_k$ represents an orthonormal basis for the interference subspace at Rx k. Then the projection matrix of Rx k would be formed by $\mathbf{F}_k = \mathbf{I} - \mathbf{S}_k\mathbf{S}_k^H$.
3) Let the columns of $\mathbf{W}_a$ be the d_{an} least dominant eigenvectors of $\mathbf{H}_{ba}^H\mathbf{u}_a\mathbf{u}_a^H\mathbf{H}_{ba} + \sum_{k=1}^{K}\mathbf{H}_{ka}^H\mathbf{F}_k\mathbf{H}_{ka}$, and let $\mathbf{v}_k$ be the least dominant eigenvectors of $\mathbf{H}_{bj}^H\mathbf{u}_a\mathbf{u}_a^H\mathbf{H}_{bj} + \sum_{k=1,k\neq j}^{K}\mathbf{H}_{kj}^H\mathbf{F}_k\mathbf{H}_{kj}$.
4) Repeat steps 2,3 until convergence.

We assume that interference and AN are eliminated at legitimate users with the above modified IA. Then the signal-to-interference-plus-noise ratios (SINRs) at Bob and Eve can be expressed as

$$\gamma_{\mathrm{b}}\left(\phi\right) = P_a\phi\left|\mathbf{u}_a^H\mathbf{H}_{ba}\mathbf{v}_a\right|^2, \quad (13)$$

$$\gamma_{\mathrm{e}}\left(\phi\right) = \frac{P_a\phi\left|\mathbf{h}_{ea}^H\mathbf{v}_a\right|^2}{1+\sum_{j=1}^{K}P\left|\mathbf{h}_{ej}^H\mathbf{v}_j\right|^2 + \frac{P_a(1-\phi)}{d_{an}}\left\|\mathbf{h}_{ea}^H\mathbf{W}_a\right\|^2}. \quad (14)$$

Let $C_B \triangleq \log_2\left(1+\gamma_b\left(\phi\right)\right)$ be the main channel capacity, and let $C_E \triangleq \log_2\left(1+\gamma_{\mathrm{e}}\left(\phi\right)\right)$ be the eavesdropper channel capacity. When transmitters can not achieve the instantaneous CSI of wiretapping channel, then the perfect secure transmission cannot always be guaranteed and secrecy outage occurs. The secrecy outage probability [9] is defined as

$$p_{out} = \Pr\left\{R_S > C_B - C_E\right\}, \quad (15)$$

where R_S denote a target secrecy rate.

Note that our primary goal is to design AN-assisted IA scheme for secure communication with privacy protection. Thus we adopt secrecy rate as the objective function, then the SOP constrained SRM problem can be formulated as

$$\max\ R_S \quad \text{s.t. } p_{out} \leq \varepsilon_{th};\ 0 \leq \phi \leq 1. \quad (16)$$

where the predefined thresholds ε_{th} denote the maximum allowable the SOP between Alice and Bob, ϕ is the optimized parameter of the SRM problem.

III. Solution to SRM Under A Secrecy Constraint

The SRM problem in formula (16) is difficult to solve directly. The main trouble lies in the probability SOP constraint. In this section, we divide the solution process into three steps. First, we derive a closed form expression for the SOP constraint. Then, we transfer (16) into a tractable power allocation problem. Finally, the optimal solution is obtained by developing an efficient numerical method.

A. Formulation of the Explicit SOP Constraint

For a given ϕ, the SOP will increase with secrecy rate as expressed in (15). Hence, the SOP in problem (16) must hold with equality at the maximum secrecy rate. We define variables $\mu \triangleq 2^{C_B-R_S}-1$, thus the SOP constraint can be rewritten as

$$\Pr\left(\gamma_{\mathrm{e}}\left(\phi\right) > \mu\right) = \varepsilon_{th}. \quad (17)$$

To simplify analysis, we define new variables as follows

$$X \triangleq P_a\phi\left|\mathbf{h}_{ea}^H\mathbf{v}_a\right|^2,\ X_1 \triangleq \sum\nolimits_{j=1}^{K}P\left|\mathbf{h}_{ej}^H\mathbf{v}_j\right|^2, \quad (18)$$

$$X_2 \triangleq \frac{P_a\left(1-\phi\right)}{d_{an}}\left\|\mathbf{h}_{ea}^H\mathbf{W}_a\right\|^2,\ Y \triangleq X_1 + X_2. \quad (19)$$

Note that $\mathbf{h}_{ea} \sim \mathcal{CN}\left(\mathbf{0},\mathbf{I}_N\right)$ and $\mathbf{h}_{ej} \sim \mathcal{CN}\left(\mathbf{0},\mathbf{I}_N\right)$. Then we can verify that $X \sim \mathrm{Exp}\left(\lambda\right), X_1 \sim \Gamma\left(\alpha_1,\beta_1\right), X_2 \sim \Gamma\left(\alpha_2,\beta_2\right)$, where $\alpha_1 \triangleq K, \alpha_2 \triangleq d_{an}, \lambda \triangleq 1/P_a\phi$, $\beta_1 \triangleq P, \beta_2 \triangleq P_a\left(1-\phi\right)/d_{an}$. Moreover, $\mathrm{Exp}\left(\lambda\right)$ denote exponential distribution with parameter λ and $\Gamma\left(\alpha,\beta\right)$ denote gamma distribution with a shape parameter α and an inverse scale parameter β.

Proposition 1: A closed form expression for the SOP constraint can be expressed as

$$\varepsilon_{th} = \frac{1}{e^{\lambda\mu}}\left(\frac{1}{1+\lambda\mu\beta_1}\right)^{\alpha_1}\left(\frac{1}{1+\lambda\mu\beta_2}\right)^{\alpha_2}. \quad (20)$$

Proof: Please refer to Appendix A for details. ■

Then taking the logarithm of both sides of formula (20), and rearranging terms, we can obtain that

$$\begin{aligned}\ln\left(\frac{1}{\varepsilon_{th}}\right) =& \frac{w}{P_a} + \alpha_1\ln\left(1+\frac{P}{P_a}w\right) \\ &+ \alpha_2\ln\left(1+\frac{1-\phi}{\alpha_2}w\right),\end{aligned} \quad (21)$$

where $w \triangleq \mu/\phi$.

B. Reformulation of the SRM Problem

To simplify analysis, let $\gamma_B \triangleq P_a\left|\mathbf{u}_a^H\mathbf{H}_{ba}\mathbf{v}_a\right|^2$ represent the effective SINR at Bob. Then the objective function of (16) can be expressed as

$$R_S = C_B - \log_2(1+\mu) = \log_2\left(\frac{1+\phi\gamma_B}{1+\phi w}\right). \tag{22}$$

Note that R_S depends on both parameters w and ϕ. Furthermore, given (21), w can be considered as an implicit function of ϕ, which can be expressed as $w(\phi)$. Specifically, it can be verified that $w(\phi) > 0$. Therefore, the problem (16) can be reformulated as

$$\max\ R_S(\phi) = \log_2\left(\frac{1+\phi\gamma_B}{1+\phi w(\phi)}\right)\ \text{s.t.}\ (21);\ 0 \le \phi \le 1. \tag{23}$$

C. Power Allocation for SRM Problem

System parameters has been provided by Proposition 1. To be specific, by analyzing (21) we can obtain useful properties for problem (23). Then we analyze the above properties in the following Lemma.

Lemma 1: The function $w(\phi)$ is monotonically increasing with ϕ.

Proof: First, we can verify that $w(\phi) > 0$ by (21). Then, taking the first-order derivative on both sides of (21) with respect of ϕ, $w'(\phi)$ is calculated and bounded as in (24). Finally we obtain $w'(\phi) > 0$. This completes the proof of Lemma 1. ∎

Lemma 2: The function $h(\phi) = w'(\phi)/w(\phi)$ is monotonically increasing with ϕ.

Proof: According to (24), the function $h(\phi)$ can be expressed as in (25) shown at the bottom of this page. Based on Lemma 1, both the first and third terms on the right-hand of (21) increase with ϕ. Hence, in order to satisfy (21), $(1-\phi)w(\phi)$ must decrease with ϕ. Then the denominator of $h(\phi)$ strictly decreases with ϕ, and hence establishing the desired result. ∎

Proposition 2: The objective function in problem (23) is a strictly concave of ϕ.

Proof: Please refer to Appendix B for details. ∎

Proposition 3: The function $R_S(\phi)$ in (23) is a strictly decreasing function when $R_S'(0) \le 0$, and a strictly increasing function when $R_S'(1) \ge 0$.

Proof: Based on Proposition 2, we can obtain that $R_S'(\phi) < R_S'(0) \le 0$ for all $\phi \in (0,1]$ when $R_S'(0) \le 0$. On the other hand, we have $R_S'(\phi) > R_S'(1) \ge 0$ for all $\phi \in [0,1)$ when $R_S'(1) \ge 0$. This completes the proof of Proposition 3. ∎

Based on the above Propositions, a numerical method for solving the problem (23) can be proposed. Specifically, three different cases are described as follows.

- *Case 1:* From Proposition 3, we can know that the function $R_S(\phi)$ is a monotonically increasing with ϕ when $R_S'(1) \ge 0$ and hence the optimal solution is $\phi_{op} = 1$. Thus, the condition $R_S(1) > R_S(0) = 0$ can be guaranteed in this case, then we have a positive secrecy rate. Besides, it means that the secrecy beamforming without AN is the optimal strategy.
- *Case 2:* By Proposition 3, it shows that $R_S(\phi)$ is a monotonically decreasing function with ϕ when $R_S'(0) \le 0$. Thus, the optimal solution is $\phi_{op} = 0$. As a result, the corresponding secrecy rate is $R_S(\phi_{op}) = 0$.
- *Case 3:* According to Proposition 2, we can obtain that $R_S(\phi)$ is a strictly concave function of ϕ. Thus there must exist a unique optimal solution $\phi_{op} \in (0,1)$ such that $R_S'(\phi_{op}) = 0$ when $R_S'(1) < 0$ and $R_S'(0) > 0$. Moreover, if $\phi \in (0, \phi_{op})$, it can be verified that $R_S'(\phi) > 0$. Therefore, a positive secrecy rate can be obtained by $R_S(\phi_{op}) > R_S(0) = 0$.

Remark 2: For Case 3, it is difficult to obtain an analytical expression for ϕ_{op}. Nevertheless, a numerical method can be developed by solving simultaneous equations composed of $R_S'(\phi_{op}) = 0$ and (21). In particular, when secure transmission is performed in the high SNR region (e.g., P_a is large), ϕ_{op} can be approximated as (26).

$$\phi_{op} \approx \frac{1}{1+\sqrt{\left(\varepsilon_{th}^{-\frac{1}{\alpha_2}}-1\right)\alpha_2}}. \tag{26}$$

Proof: Please refer to Appendix C for details. ∎

Accordingly, the execution process to solve the problem (23) can be summarized in Algorithm 1.

Algorithm 1 Solve SRM Problem in (23)

1: Input: P_a, P, ε_{th}, γ_B, d_{an}.
2: Calculate $R_S'(0)$ and $R_S'(1)$ according to (29).
3: **if** $R_S'(0) \le 0$, **then**
4: Obtain $\phi_{op} = 0$.
5: **else if** $R_S'(1) \ge 0$, **then**
6: Obtain $\phi_{op} = 1$.
7: **else** $R_S(\phi)$ has a unique optimal solution on $(0,1)$.
8: Obtain ϕ_{op} by solving $R_S'(\phi_{op}) = 0$.
9: **end if**
10: Output: ϕ_{op} and $R_S(\phi_{op})$.

$$w'(\phi) = \frac{P_a\alpha_2 w(\phi)\left(P_a + Pw(\phi)\right)}{\left[\alpha_2 + (1-\phi)w(\phi)\right]\left(P_a+Pw(\phi)\right) + P_a\alpha_2(1-\phi)\left(P_a+Pw(\phi)\right) + PP_a\alpha_1\left[\alpha_2+(1-\phi)w(\phi)\right]}. \tag{24}$$

$$h(\phi) = \frac{P_a\alpha_2}{\alpha_2 + (1-\phi)w(\phi) + P_a\alpha_2(1-\phi) + P_aP\alpha_1\frac{\alpha_2+(1-\phi)w(\phi)}{P_a+Pw(\phi)}}. \tag{25}$$

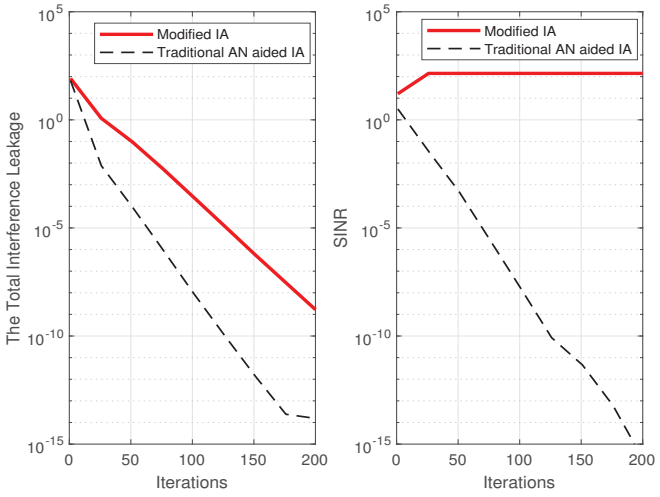

Fig. 2. The total interference leakage and SINR at Bob, $P = P_a = 10$ dB.

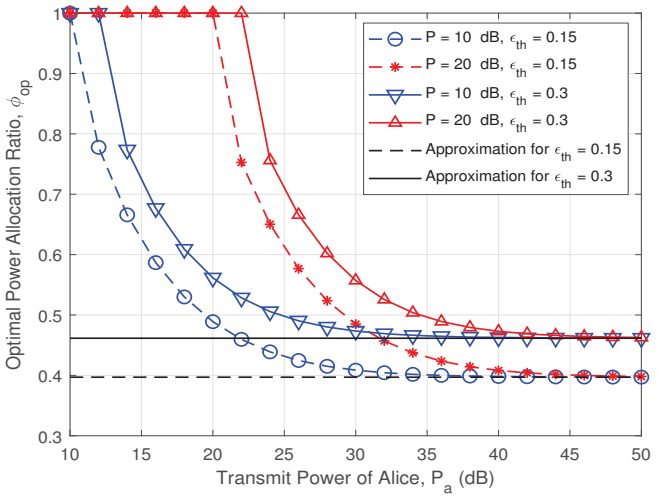

Fig. 4. Optimal power allocation ratio vs. transmit power of Alice.

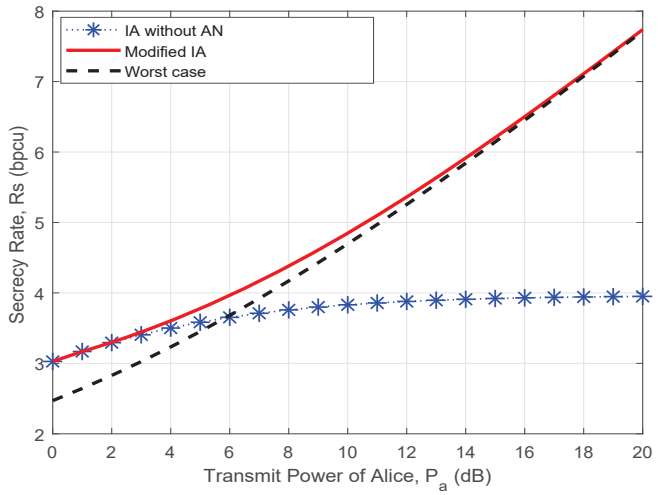

Fig. 3. Secrecy rate vs. transmit power of Alice, $P = 0$ dB.

IV. Numerical Results

In this section, we verify the performance of the proposed modified IA scheme. Unless otherwise provided, system parameters are set as $M = 8$, $N = 4$, $d_{an} = 5$, $K = 3$, and $\varepsilon_{th} = 0.1$, respectively. Furthermore, the secrecy rate is measured by bits per channel use (bpcu).

Fig. 2 compares the proposed modified IA scheme and the traditional IA scheme with respect to the total interference leakage as well as the SINR at Bob. It can be observed that both methods can achieve IA, i.e., both interference and AN are aligned and eliminated at legitimate receivers, which is consistent with Remark 1. Fig. 2 also illustrates the inefficiency in terms of private information protection of the traditional scheme. Note that in the modified IA scheme, the max-eigenmode transmission is adopted, leading to the higher SINR at Bob. The modified IA achieves a robust and reliable performance, and thus is more suitable for multi-user interference networks.

Fig.3 shows the secrecy rate performance with different schemes, including the modified IA scheme, the worst case scenario designed in [9] by ignoring the noise at Eve, as well as the IA without AN transmission. From Fig. 3, the secrecy rate of the proposed scheme outperforms the other schemes in a wide range of P_a. In low SNR region, the secrecy rate of the proposed scheme equals to that of IA scheme without AN. This is due to the fact that the optimal power allocation ratio is 1, as analyzed for the Case 1 in SECTION III. C.

Fig. 4 presents the optimal power allocation ratio. It can be verified that it is preferable for Alice to allocate more power to private signal as other transmitters increase transmit power. In addition, as P_a increases, the probability of information leakage also increases, implying that it is preferable to perform AN-assisted transmission for Alice. Furthermore, when P_a becomes large, the optimal power allocation ratio will converge to a constant value, as discussed in Remark 2. It can also be verified that the approximation is quite accurate.

V. Conclusion

The main contribution of this paper is the proposition of an artificial noise (AN) assisted interference alignment (IA), taking both security and performance guarantee into account. Specifically, a modified IA scheme was designed to avoid the private signal cancellation caused by the traditional scheme. The relationship between improperness and infeasibility of IA was established to provide insights into IA requirements. Moreover, an explicit solution to the secrecy rate maximization (SRM) problem was obtained by optimizing the power allocation ratio between the private signal and the AN signal.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (No. 61801060, 61901089, and 62002052) and in part by the National Key Research and Development Program of China (No. 2019YFB1803204). The corresponding author is Hong Wen.

APPENDIX A
PROOF OF PROPOSITION 1

Proof: According to [21], the probability density function (PDF) of Y can be calculated as

$$\begin{aligned} f_Y(y) =& \int_{-\infty}^{\infty} f_{X_1}(y-x_2) f_{X_2}(x_2)\, dx_2 \\ =& \frac{y^{\alpha_1+\alpha_2-1}}{\beta_1^{\alpha_1}\beta_2^{\alpha_2} e^{\frac{y}{\beta_1}} \Gamma(\alpha_1+\alpha_2)} \\ & \times {}_1F_1\left(\alpha_2; \alpha_1+\alpha_2; \left(\frac{1}{\beta_1}-\frac{1}{\beta_2}\right) y\right), \end{aligned} \tag{27}$$

where $y > 0$ and ${}_1F_1(\alpha;\ \gamma;\ z)$ is the confluent hypergeometric function [22, 9.210.1]. By (27), the complementary cumulative distribution function (CCDF) of $\gamma_{\mathrm{e}}(\phi)$ is given by

$$\begin{aligned} \bar{F}_{\gamma_{\mathrm{e}}}(\mu) =& \Pr(X > \mu + \mu Y) \\ =& \frac{1}{e^{\lambda\mu}} \left(\frac{1}{1+\lambda\mu\beta_1}\right)^{\alpha_1} \left(\frac{1}{1+\lambda\mu\beta_2}\right)^{\alpha_2}. \end{aligned} \tag{28}$$

This completes the proof of Proposition 1. ∎

APPENDIX B
PROOF OF PROPOSITION 2

Proof: From (22), $R_S'(\phi)$ can be calculated as

$$\begin{aligned} R_S'(\phi) =& \left(\frac{\gamma_B}{1+\phi\gamma_B} - \frac{w(\phi)+\phi w'(\phi)}{1+\phi w(\phi)}\right) \frac{1}{\ln(2)} \\ =& \left(\frac{\gamma_B - w(\phi)}{(1+\phi\gamma_B)[1+\phi w(\phi)]} - \frac{h(\phi)}{1+\frac{1}{\phi w(\phi)}}\right) \frac{1}{\ln(2)}. \end{aligned} \tag{29}$$

Based on Lemmas 1 and 2, the first and second terms on the right-hand side of (29) are strictly decreasing and increasing function of ϕ, respectively. In consequence, $R_S''(\phi) < 0$. By the second order condition, we have Proposition 2. ∎

APPENDIX C
APPROXIMATION IN (28)

Proof: Based on (29), we can obtain that

$$R_S'(0) = \frac{\gamma_B - w(0)}{\ln(2)} > 0 \Leftrightarrow \gamma_B > w(0). \tag{30}$$

Then by Case 2, it can be verified that $\phi_{op} > 0$.

When P_a is large, the constraint in (21) is approximated as

$$\ln\left(\frac{1}{\varepsilon_{th}}\right) = \alpha_2 \ln\left(1 + \frac{1-\phi}{\alpha_2} w(\phi)\right). \tag{31}$$

After rearranging terms in (31), we can have that

$$w'(\phi) = \frac{1}{(1-\phi)^2} \left(\varepsilon_{th}^{-\frac{1}{\alpha_2}} - 1\right) \alpha_2. \tag{32}$$

If P_a is large, $R_S'(\phi)$ in (29) can be approximated as

$$R_S'(\phi) = \frac{1-\phi^2 w'(\phi)}{\phi(1+\phi w(\phi))\ln(2)}. \tag{33}$$

From (32), $w'(\phi) \to \infty$ as $\phi \to 1$. Hence we can establish $R_S'(1) < 0$. Then by Case 2, it can be shown that $\phi_{op} < 1$. Substituting (32) into (33), we have the following equation

$$1 - \left(\frac{\phi}{1-\phi}\right)^2 \left(\varepsilon_{th}^{-\frac{1}{\alpha_2}} - 1\right) \alpha_2 = 0. \tag{34}$$

By solving the equation (34), we can obtain (26). ∎

REFERENCES

[1] H. Wen, *Physical Layer Approaches for Securing Wireless Communication Systems*. New York, NY, USA: Springer-Verlag, 2013.

[2] C. Gong, X. Yue, Z. Zhang, X. Wang, and X. Dai, "Enhancing physical layer security with artificial noise in large-scale NOMA networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2349–2361, Mar. 2021.

[3] L. Hu, H. Wen, B. Wu, J. Tang, and F. Pan, "Adaptive base station cooperation for physical layer security in two-cell wireless networks," *IEEE Access*, vol. 4, pp. 5607–5623, 2016.

[4] X. Luo, Y. Liu, H.-H. Chen, and W. Meng, "Artificial noise assisted secure mobile crowd computing in intelligently connected vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 8, pp. 7637–7651, Aug. 2021.

[5] J. Su, Z. Sheng, A. X. Liu, Y. Han, and Y. Chen, "Capture-aware identification of mobile RFID tags with unreliable channels," *IEEE Trans. Mobile Comput.*, vol. 21, no. 4, pp. 1182–1195, Apr. 2022.

[6] S. Kavaiya, D. K. Patel, Z. Ding, Y. L. Guan, and S. Sun, "Physical layer security in cognitive vehicular networks," *IEEE Trans. Commun.*, vol. 69, no. 4, pp. 2557–2569, Apr. 2021.

[7] L. Hu, H. Wen, B. Wu, J. Tang, and F. Pan, "Adaptive secure transmission for physical layer security in cooperative wireless networks," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 524–527, Mar. 2017.

[8] L. Hu, H. Wen, B. Wu, J. Tang, F. Pan, and R.-F. Liao, "Cooperative-jamming-aided secrecy enhancement in wireless networks with passive eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2108–2117, Mar. 2018.

[9] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.

[10] B. Wang, P. Mu, and Z. Li, "Secrecy rate maximization with artificial-noise-aided beamforming for MISO wiretap channels under secrecy outage constraint," *IEEE Commun. Lett.*, vol. 19, no. 1, pp. 18–21, Jan. 2015.

[11] D. Hu, P. Mu, W. Zhang, and W. Wang, "Minimization of secrecy outage probability with artificial-noise-aided beamforming for MISO wiretap channels," *IEEE Commun. Lett.*, vol. 24, no. 2, pp. 401–404, Feb. 2020.

[12] L. Hu *et al.*, "Cooperative jamming for physical layer security enhancement in Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 219–228, Feb. 2018.

[13] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the K-user interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.

[14] K. Gomadam, V. R. Cadambe, and S. A. Jafar, "A distributed numerical approach to interference alignment and applications to wireless interference networks," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3309–3322, Jun. 2011.

[15] S. W. Peters and R. W. Heath, "Interference alignment via alternating minimization," in *Proc. IEEE ICASSP*, Apr. 2009, pp. 2445–2448.

[16] N. Zhao, F. R. Yu, M. Li, and V. C. M. Leung, "Anti-eavesdropping schemes for interference alignment (IA)-based wireless networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5719–5732, Aug. 2016.

[17] C. Tian, P. Ren, Q. Du, L. Sun, and Y. Wang, "An artificial noise-based security scheme for interference alignment-based wireless networks," in *Proc. IEEE GLOBECOM*, Dec. 2017, pp. 1–6.

[18] Z. Xie *et al.*, "Secured green communication scheme for interference alignment based networks," *J. Commun. Networks.*, vol. 22, no. 1, pp. 23–36, Feb. 2020.

[19] H. Xia, X. Zhou, S. Han, C. Li, and Y. Chai, "Joint secure transceiver design and power allocation for AN-assisted MIMO networks," *IEEE Trans. Wireless Commun.*, vol. 21, no. 1, pp. 477–488, Jan. 2022.

[20] C. M. Yetis, T. Gou, S. A. Jafar, and A. H. Kayran, "On feasibility of interference alignment in MIMO interference networks," *IEEE Trans. Signal Process.*, vol. 58, no. 9, pp. 4771–4782, Oct. 2010.

[21] R. B. Ash, *Basic Probability Theory*. Mineola, NY, USA: Dover, 2008.

[22] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 8th ed. New York, NY, USA: Academic, 2014.