applied sciences

MDPI

Article

Power Allocation for Secrecy-Capacity-Optimization-Artificial-Noise Secure MIMO Precoding Systems under Perfect and Imperfect Channel State Information

Yebo Gu [1], Bowen Huang [2] and Zhilu Wu [1,*]

[1] School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin 150001, China; 16B305002@hit.edu.cn
[2] JushriTechnologies Inc., Shanghai 200335, China; bowen.huang@jushri.com
* Correspondence: wuzhilu@hit.edu.cn

Abstract: In this paper, we consider the physical layer security problem of the wireless communication system. For the multiple-input, multiple-output (MIMO) wireless communication system, secrecy capacity optimization artificial noise (SCO−AN) is introduced and studied. Unlike its traditional counterpart, SCO−AN is an artificial noise located in the range space of the channel state information space and thus results in a significant increase in the secrecy capacity. Due to the limitation of transmission power, making rational use of this power is crucial to effectively increase the secrecy capacity. Hence, in this paper, the objective function of transmission power allocation is constructed. We also consider the imperfect channel estimation in the power allocation problems. In traditional AN research conducted in the past, the expression of the imperfect channel estimation effect was left unknown. Still, the extent to which the channel estimation error impacts the accuracy of secrecy capacity computation is not negligible. We derive the expression of channel estimation error for least square (LS) and minimum mean squared error (MMSE) channel estimation. The objective function for transmission power allocation is non-convex. That is, the traditional gradient method cannot be used to solve this non-convex optimization problem of power allocation. An improved sequence quadratic program (ISQP) is therefore applied to solve this optimization problem. The numerical result shows that the ISQP is better than other algorithms, and the power allocation as derived from ISQP significantly increases secrecy capacity.

Keywords: physical layer security; secure transmission; secrecy capacity; secrecy capacity optimization artificial noise; power allocation; channel estimation error

Citation: Gu, Y.; Huang, B.; Wu, Z. Power Allocation for Secrecy-Capacity-Optimization-Artificial-Noise Secure MIMO Precoding Systems under Perfect and Imperfect Channel State Information. *Appl. Sci.* **2021**, *11*, 4558. https://doi.org/10.3390/app11104558

Academic Editor: Cheonshik Kim

Received: 2 April 2021
Accepted: 13 May 2021
Published: 17 May 2021

1. Introduction

Secure transmission is a fundamental problem in wireless communications due to the broadcast nature of the wireless medium. Along with the rapid advancement of information technology, the higher information transmission rate has called for a stricter standard of information transmission security. For a long time, the primary method of guaranteeing the secure transmission of information has been via encryption technology. Encryption technology utilizes the limitation in computing speed to prevent the eavesdropper from deciphering all encrypted information in a limited time. However, as computer technology advances with faster computation, the decryption of information becomes more straightforward. In theory, no encrypted information is indecipherable if the computer's calculation speed is fast enough. This indeed is the inherent flaw in the current information encryption technology. Therefore, the physical layer security technology has been proposed to solve the problems of secure information transmission.

The physical layer security technology differs substantially from the information encryption technology. Unlike encryption technology, which relies on the limitation in computation speed, the physical layer security technology has its basis in the randomness

of the wireless communication channel. The physical layer security technology tries to prevent eavesdroppers from decoding information, regardless of the amount of time or the computing speed. One of the most innovative physical layer security technologies is artificial noise (AN). AN adds extra noise to the information. This noise solely impacts the eavesdropper's channel but does not affect the legitimate receiver channel. That is, only the signal received by the eavesdropper is reduced in this method. The effectiveness of the physical layer technology is then evaluated by secrecy capacity.

The study of physical layer security begins from [1]. This paper proposes unconditional secure transmission as the ultimate goal of physical layer security technology study.

After [1,2] is the first paper to study the secure transmission of information from the perspective of information theory. In [2], wiretap communication model with the eavesdropping channel is proposed, and the aforementioned secrecy capacity was also first proposed in this paper. Paper [3] studies the physical layer security technology based on [2]. In [3], a broadcast channel model with confidential messages is proposed to extend Wyner's work.

Currently, the physical layer security technology has not been at the center of public attention, primarily due to a strict restriction that the eavesdropper's channel must be strictly worse than the legitimate channel. Considering the following cases: the eavesdropper is closer to the transmitter, or the eavesdropper has more antennas than the transmitter. These mentioned conditions will make the eavesdropper's channel better than the legitimate channel and thus reduces the effectiveness of the physical layer security technology.

To help with the issue above, AN technology is introduced. The proposal of AN technology reduces the difficulty of applying the physical layer security technology in the multiple-input, multiple-output (MIMO) communication system [4]. AN is in the null space of the legitimate channel, which mean the legitimate channel is not affected. There is no need to employ any additional signal processing device to the legitimate receiver. Meanwhile, the eavesdropper's channel capacity is reduced significantly. To show this result quantitatively, let A denote the channel capacity of the legitimate receiver and B denote the channel capacity of the eavesdropper. The principle of AN is to increase the difference $A - B$ by reducing B and keeping A constant.

There have been many outstanding works in the realm of AN technology. In [5,6], AN and the interference alignment technology are creatively merged to introduce AN featuring interference alignment. In [7], the lower bound on the secrecy capacity of artificial noise wireless communication systems subject to transmit power is proposed. Ref. [8] proposes the secrecy capacity expression with imperfect channel estimation. This expression is non-convex, so the gradient descent method cannot be used for this optimization problem. Therefore, it is impossible to get the optimal solution of the secrecy capacity expression. The study in [9–12] consider the effects of active eavesdropper. The active eavesdropper can interfere with pilot to reduce the secrecy capacity of the wire-tap system. This is something that hasn't been explored in previous studies.

The past research on AN is summarized into two main aspects:

(1) Research on AN noise technology under different communication modes [13–21]: examples include the AN power allocation problem in OFDM, GSM, and other communication modes [22] and the application of AN under intelligent reflecting surface [23]. The simplified communication model is $Y = HX + e$, where Y denotes the received signal, H denotes the channel, X denotes the transmitted signal, and e is the noise. The above researches focus on "H".

(2) Reshaping certain features of AN. For example, Ref. [24] designs an artificial noise that has interference alignment characteristics. The research focused on "X" from the equation above [25–28].

Still, there has been little to no research attention on redesigning the core of AN. Therefore, our research focus on creating a new kind of AN. Our research shows that our new artificial noise has a better performance compared to its traditional counterpart.

In [29], the secrecy capacity optimization artificial noise (SCO−AN) is proposed. The core of AN technology is to design a noise in the null space of the channel state information space. Unlike the traditional AN, which ignores the range space of the channel state information space, SCO−AN is located in that range space. While SCO−AN may slightly impact the channel capacity of the legitimate receiver, SCO−AN significantly reduces the channel capacity of the eavesdropper. Therefore, this method still increases the difference between the legitimate channel capacity and the eavesdropping channel capacity. SCO−AN is a tool to convert the noise immunity of communication systems into secrecy capacity.

As there is a limitation in the transmission power, it is critical to draw an optimization problem to maximize the secrecy capacity under that limitation. The power allocation problem becomes essential. Therefore, in this paper, we study the power allocation problem of SCO−AN. The Hessian matrix of the SCO−AN power allocation objective function is not positive definite, which means the objective function is non-convex. The maximum value of the SCO−AN power allocation function cannot be obtained by the gradient descent method. An improved sequential quadratic programming (ISQP) is proposed to solve this problem. With the effects of imperfect channel estimation considered, the objective power allocation function containing imperfect channel estimation parameters is constructed.

The main contributions of this paper are summarized as follows:

(1) In reality, the secrecy capacity of a wireless communication system using SCO−AN is limited by transmission power. Considering this limitation, this paper constructs a power distribution function for SCO−AN and the information-bearing signal.
(2) Since the power allocation objective function is non-convex, it is difficult to optimize the power distribution function using a power optimization scheme based on gradient descent. ISQP is then proposed to allocate power between SCO−AN and the information-bearing signal. ISQP improves the traditional iterative algorithm and reduces the computational complexity by simplifying the initial iterative matrix and improving computational efficiency.
(3) Due to the influence of Gaussian white noise in the channel, there is an error in the channel estimation, resulting in an error in the SCO−AN design. The channel estimation error affects the accuracy of the power allocation optimization. This paper considers the imperfect channel state information for power allocation. The power allocation objective function of SCO−AN and the information-bearing signal containing channel estimation errors is constructed. The expression for the channel estimation errors is derived for the first time. This expression can then be applied to future physical layer security research examining imperfect channel estimation.The power allocation function is then converted to a function with only one variable–the SCO−AN–simplifying the function's overall computational complexity.

This paper is structured as follows:

- In Section 2, the system model and the framework are introduced.
- In Section 3, the objective function for the power allocation between SCO−AN and the information-bearing signal, with and without considering imperfect channel estimation, is proposed. ISQP is then applied to optimize the power allocation. The algorithm flow of ISQP algorithm is constructed.
- In Section 4, simulation results are shown and discussed.
- In Section 5, the conclusion is drawn, and the suggestions for future work are presented.

In this paper, the following notations are used: Boldface upper case denotes matrices, boldface lower case denotes vectors, italics case denotes numbers; $[\cdot]^T$ denotes the matrix transpose operation; $[\cdot]^*$ denotes the complex conjugate operation; $[\cdot]^\dagger$ denotes the conjugate transpose operation (conjugate complex number) for the matrix (number) "$\cdot$"; $E\{\cdot\}$ denotes the mathematical expectation; $\|\cdot\|$ denotes the norm of a vector; and $|\cdot|$ denotes the determinant of a matrix.

2. Related Work and System Model

2.1. Related Work–Wireless Communication Model with Eavesdroppers

In this section, we review the artificial noise technology and the method of SCO−AN. Moreover, the effects of imperfect channel estimation are analyzed in detail.

Figure 1 shows a wireless communication system model with an eavesdropper. In this model, Alice is the transmitter of the message, Bob is the legitimate receiver, and Eve is the eavesdropper. Alice has N_A antennas, Bob has N_B antennas and Eve has N_E antennas. $\mathbf{H}$ represents the channel state information (CSI) of the legitimate channel (Alice to Bob), while $\mathbf{G}$ represents the CSI of the eavesdropper channel (Alice to Eve). $\mathbf{H}_k$ and $\mathbf{G}_k$ represent the CSI of $\mathbf{H}$ and $\mathbf{G}$ at time k respectively. The element $h_{i,j}$ (or $g_{i,j}$) in $\mathbf{H}$ (or $\mathbf{G}$) is the channel gain coefficient between the i_{th} transmitter antenna and the j_{th} receiver's (or eavesdropper's) antenna. $\mathbf{x}_k \in \mathbb{C}^{N_A}$ represents the signal transmitted by Alice at time k; $\mathbf{y}_k \in \mathbb{C}^{N_E}$ represents the signal received by Bob at time k; and $\mathbf{z}_k \in \mathbb{C}^{N_B}$ represents the signal received by Eve at time k.

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{x}_k + \mathbf{n}_k, \tag{1}$$

$$\mathbf{y}_k = \mathbf{G}_k \mathbf{x}_k + \mathbf{e}_k, \tag{2}$$

where $\mathbf{n}_k$ and $\mathbf{e}_k$ are independent and identically distributed (i.i.d) additive Gaussian white noise (AGWN) with the variance of σ_n^2 and σ_e^2 respectively. For the convenience of discussion, we assume that the CSI of $\mathbf{G}$ and $\mathbf{H}$ can be obtained by Alice without delay. The maximum transmitting power is assumed to be P, where $E[\mathbf{x}_k^\dagger \mathbf{x}_k] \leq P$.

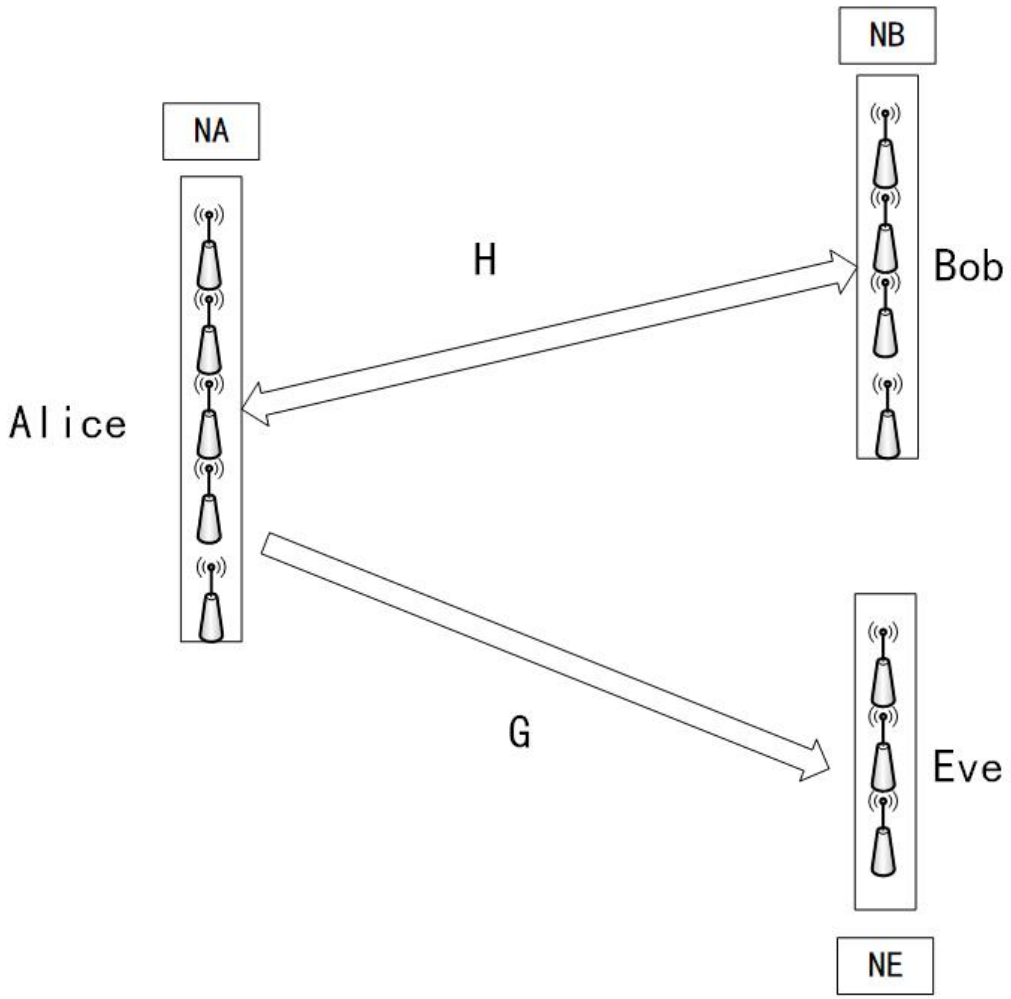


Figure 1. Wireless communication model with eavesdropper.

2.2. Related Work–The Artificial Noise

Located in the null space of legitimate channel (i.e., Bob's channel), AN does not affect Bob's reception of information. For Eve, however, AN reduces Eve's channel capacity significantly. Alice sends AN simultaneously while sending the information-bearing signal; that is,

$$\mathbf{x}_k = \mathbf{w}_k + \mathbf{s}_k, \tag{3}$$

In (3), $\mathbf{w}_k \in \mathbb{C}^{N_A}$ denotes AN; $\mathbf{s}_k \in \mathbb{C}^{N_A}$ denotes the information-bearing signal; and $\mathbf{w}_k$ is artificial noise, which is located in the null space of $\mathbf{H}_k$, such that $\mathbf{H}_k\mathbf{w}_k = 0$. Let $\mathbf{Z}_k$ be a standard orthonormal basis for $\mathbf{H}_k$ and $\mathbf{v}_k$ be a complex random variable with the variance of σ_v^2 such that $\mathbf{w}_k = \mathbf{Z}_k\mathbf{v}_k$ and $\mathbf{Z}_k^\dagger\mathbf{Z}_k = \mathbf{I}$. Then, the signals received by Bob and Eve are:

$$\begin{aligned} \mathbf{z}_k &= \mathbf{H}_k\mathbf{x}_k + \mathbf{n}_k \\ &= \mathbf{H}_k\mathbf{w}_k + \mathbf{H}_k\mathbf{s}_k + \mathbf{n}_k \\ &= \mathbf{H}_k\mathbf{s}_k + \mathbf{n}_k, \end{aligned} \tag{4}$$

$$\mathbf{y}_k = \mathbf{G}_k\mathbf{s}_k + \mathbf{G}_k\mathbf{w}_k + \mathbf{e}_k, \tag{5}$$

where $\mathbf{y}_k$ is the signal received by Eve, and $\mathbf{z}_k$ is the signal received by Bob. $\mathbf{y}_k$ and $\mathbf{z}_k$ are Gaussian vectors. As $\mathbf{w}_k$ is in the null space of $\mathbf{H}_k$, we have $\mathbf{H}_k\mathbf{w}_k = 0$ and the term with $\mathbf{w}_k$ vanishes in (4). That is, the artificial noise does not impact Bob, while Eve is affected.

In [4], the transmitted signal is chosen as $\mathbf{s}_k = \mathbf{p}_k\mathbf{u}_k$, where $\mathbf{u}_k$ is the information signal with the variance of σ_u^2 and $\mathbf{p}_k$ obeys the independent Gaussian distribution. Here, $\mathbf{p}_k$ is chosen such that: (a) $\mathbf{H}_k\mathbf{p}_k \neq 1$, and (b) $\|\mathbf{p}_k\|$=1.

In [4], Goel considers two scenarios:

(a) A single-input, single-output (SISO) wireless communication system where the transmitter, the receiver, and the eavesdropper equip one antenna each, i.e., $N_A = N_B = N_R = 1$; and

(b) A MIMO wireless communication system where the the transmitter, the receiver, and the eavesdropper each equip multiple antennas, i.e., $N_A = N_B = N_R > 1$.

For scenario a, the variables in (4)–(6) are Gaussian complex variables. $\log_e(*)$ is used to calculate entropy, so the lower bound on secrecy capacity after adding artificial noise is given by:

$$\begin{aligned} C_{sec}^a &= \mathrm{I}(Z;S) - \mathrm{I}(Y;S) \\ &= \log\left(1 + \frac{|H_k p_k|^2\sigma_u^2}{\sigma_n^2}\right) - \log\left(1 + \frac{|G_k p_k|^2\sigma_u^2}{E|G_k w_k|^2 + \sigma_e^2}\right), \end{aligned} \tag{6}$$

where $\mathrm{E}|G_k w_k|^2 = (G_k Z_k Z_k^\dagger G_k^\dagger)\sigma_k^2$. C_{sec}^a denotes the secrecy capacity after adding artificial noise, and $\mathrm{I(A;B)}$ denotes mutual information entropy of A and B.

For scenario b, $\mathbf{G}_k$ and $\mathbf{H}_k$ are Gaussian complex matrices. The elements in $\mathbf{G}_k$ and $\mathbf{H}_k$ are Gaussian complex variables. The other variables in (4)–(6) are Gaussian vectors. It then follows that the lower bound on secrecy capacity after adding artificial noise is given by:

$$\begin{aligned} C_{\mathrm{sec}}^a &= I(Z;S) - I(Y;S) \\ &= \log\left|\mathbf{I}\sigma_n^2 + \mathbf{H}_k E[\mathbf{s}_k\mathbf{s}_k^\dagger]\mathbf{H}_k^\dagger\right| - \log\left(\frac{|\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger\sigma_v^2 + \mathbf{G}_k E[\mathbf{s}_k\mathbf{s}_k^\dagger]\mathbf{G}_k^\dagger|}{|\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger\sigma_v^2 + \mathbf{I}\sigma_e^2|}\right). \end{aligned} \tag{7}$$

2.3. Related Work–SCO−AN: Perfect Channel Estimation

SCO−AN is proposed in [29]. In this section, SCO−AN is introduced in detail.

The goal of physical layer security is to maximize the secrecy capacity of a communication system. In the wireless wiretap communication model, it is not possible to increase the channel capacity of the legitimate receiver. AN is then proposed to reduce the eavesdropper's channel capacity while the legitimate receiver's channel capacity remains intact. Inspired by AN, the secrecy capacity optimization artificial noise (SCO−AN) is

proposed in [29]. Unlike the traditional AN, SCO−AN has a slight impact on the legitimate receiver's channel capacity but reduces the capacity of eavesdropping channels much more significantly. Hence, the system's overall secrecy capacity increases.

Next, we compute the analytical expression of using SCO−AN, in a manner parallel to our computations of AN above. Alice adds SCO−AN to the transmission signal:

$$\mathbf{x}_k = \mathbf{w}_g + \mathbf{s}_k, \tag{8}$$

In [29], the transmitted signal is $\mathbf{s}_k = \mathbf{p}_k \mathbf{u}_k$, where $\mathbf{u}_k$ is the information-bearing signal with variance of σ_u^2 and $\mathbf{p}_k$ obeys the Gaussian distribution. $\mathbf{p}_k$ satisfies the following conditions: (a) $\mathbf{H}_k \mathbf{p}_k \neq 1$; and (b)$\|\mathbf{p}_k\|$=1. $\mathbf{w}_g \in \mathbb{C}^{N_A}$ denotes the SCO−AN. To facilitate calculations, we assume that $\mathbf{w}_g = \mathbf{Z}_k \mathbf{v}_g$, where $\mathbf{Z}_k$ is a standard orthonormal basis of $\mathbf{H}_k$ and $\mathbf{v}_g$ is a complex random variables with variance σ_g^2. The signals received by the Bob and Eve are:

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{s}_k + \mathbf{H}_k \mathbf{w}_g + \mathbf{n}_k, \tag{9}$$

$$\mathbf{y}_k = \mathbf{G}_k \mathbf{s}_k + \mathbf{G}_k \mathbf{w}_g + \mathbf{e}_k, \tag{10}$$

where $\mathbf{z}_k$ denotes the signal received by Bob and $\mathbf{y}_k$ denotes the signal received by Eve.

For the SISO wireless communication system, all the elements in (8)–(10) are complex variables. So the lower bound on secrecy capacity after adding SCO−AN is:

$$\begin{aligned} C_{\text{sec}}^g &= I(Z;S) - I(Y;S) \\ &= \log\left(1 + \frac{|H_k p_k|^2 \sigma_u^2}{E|H_k w_g|^2 + \sigma_n^2}\right) - \log\left(1 + \frac{|G_k p_k|^2 \sigma_u^2}{E|G_k w_g|^2 + \sigma_e^2}\right), \end{aligned} \tag{11}$$

where $\mathrm{E}\left|H_k w_g\right|^2 = (H_k Z_k Z_k^\dagger H_k^\dagger)\sigma_g^2$, and $\mathrm{E}\left|G_k w_g\right|^2 = (G_k Z_k Z_k^\dagger G_k^\dagger)\sigma_g^2$. C_{sec}^g denotes the secrecy capacity after adding SCO−AN. In (11), C_{sec}^g is a non-convex function about σ_g^2.

For the MIMO wireless communication system, $\mathbf{H}_k$ and $\mathbf{G}_k$ are gaussian complex martixs, $\mathbf{x}_k$, $\mathbf{w}_g$, $\mathbf{s}_k$, $\mathbf{n}_k$ and $\mathbf{e}_k$ are gaussian vectors. So the lower bound on secrecy capacity after adding SCO−AN is:

$$\begin{aligned} C_{\text{sec}}^g &= I(Z;S) - I(Y;S) \\ &= \log\left(\frac{|(\mathbf{H}_k \mathbf{Z}_k \mathbf{Z}_k^\dagger \mathbf{H}_k^\dagger)\sigma_g^2 + \mathbf{I}\sigma_n^2 + \mathbf{H}_k \mathbf{Z}_k \mathbf{Z}_k^\dagger \mathbf{H}_k^\dagger \sigma_u^2|}{|(\mathbf{H}_k \mathbf{Z}_k \mathbf{Z}_k^\dagger \mathbf{H}_k^\dagger)\sigma_g^2 + \mathbf{I}\sigma_n^2|}\right) \\ &\quad - \log\left(\frac{|(\mathbf{G}_k \mathbf{Z}_k \mathbf{Z}_k^\dagger \mathbf{G}_k^\dagger)\sigma_g^2 + \mathbf{I}\sigma_e^2 + \mathbf{G}_k \mathbf{Z}_k \mathbf{Z}_k^\dagger \mathbf{G}_k^\dagger \sigma_u^2|}{|(\mathbf{G}_k \mathbf{Z}_k \mathbf{Z}_k^\dagger \mathbf{G}_k^\dagger)\sigma_g^2 + \mathbf{I}\sigma_e^2|}\right) \end{aligned} \tag{12}$$

(12) is a function of σ_g^2.

For the convenience of discussion, C_{sec}^k represents the change of secrecy capacity after adding the SCO−AN when compared to simply adding traditional AN. For the case of SCO−AN, to ensure the effectiveness of physical security, (13) must be guaranteed.

$$C_{\text{sec}}^k = C_{\text{sec}}^g - C_{\text{sec}}^a > 0, \tag{13}$$

In (13), for the SISO communication system, C_{sec}^a is given by (6) and C_{sec}^g is given by (11). For the MIMO communication system, C_{sec}^a is given by (7) and C_{sec}^g is given by (12).

In Figure 2, the dashed line represents the secrecy capacity of AN calculated by (7), and the solid line is the secrecy capacity of SCO−AN calculated by (12). The legitimate channel $\mathbf{H}$ and the eavesdropper channel $\mathbf{G}$ are Rayleigh fading channels. The signal $\mathbf{x}_k$ is a complex covector. Figure 2 shows that SCO−AN provides more secrecy capacity than AN does. The noise in $\mathbf{H}$ and $\mathbf{G}$ are Gaussian white noise. The secrecy capacity increases with higher SNR.

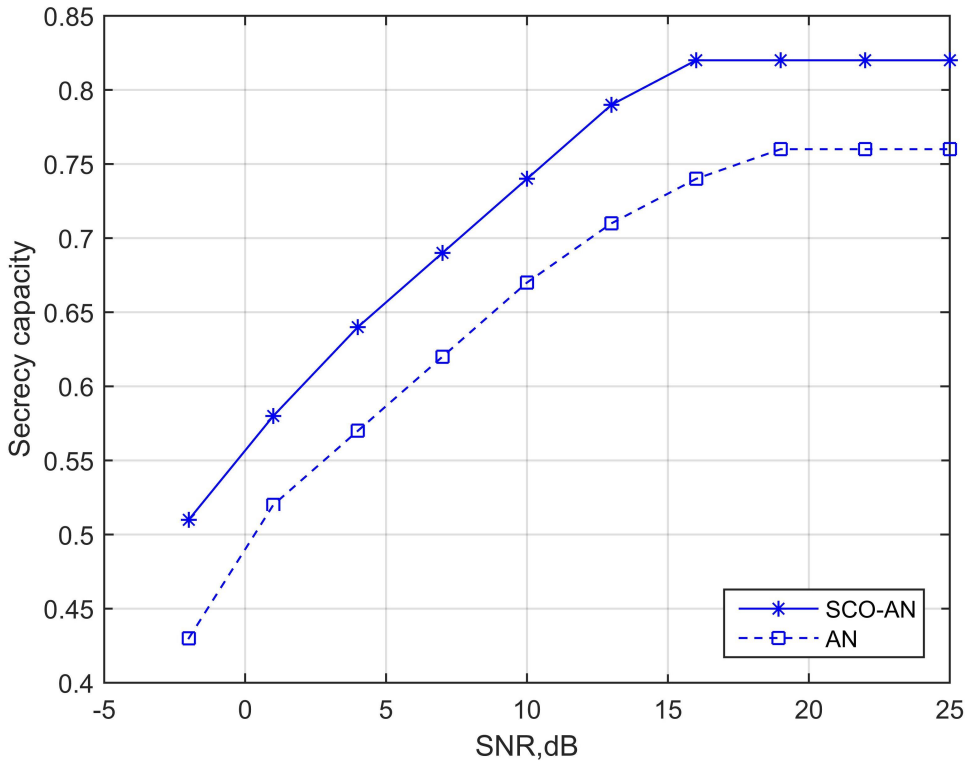


Figure 2. Secrecy capacity comparison of the AN and SCO−AN versus different SNR.

2.4. SCO−AN: Imperfect Channel Estimation

The Gaussian white noise causes the error of channel estimation. The effect of the imperfect channel estimation should be considered.

For the SISO communication system, H_{eo} denotes channel estimation error. The channel state information received by Alice is $\widetilde{H}$:

$$H_k = H_{eo} + \widetilde{H}, \tag{14}$$

The signal received by Bob after adding SCO−AN is:

$$z_k^* = (H_{eo} + \widetilde{H})s_k + (H_{eo} + \widetilde{H})w_g + n_k, \tag{15}$$

For MIMO communication system, $\mathbf{H}_{eo}$ denotes channel estimation error. The channel state information received by Alice is $\widetilde{\mathbf{H}}$:

$$\mathbf{H}_k = \mathbf{H}_{eo} + \widetilde{\mathbf{H}}, \tag{16}$$

The signal received by Bob after adding SCO−AN is:

$$\mathbf{z}_k^* = (\mathbf{H}_{eo} + \widetilde{\mathbf{H}})\mathbf{s}_k + (\mathbf{H}_{eo} + \widetilde{\mathbf{H}})\mathbf{w}_g + \mathbf{n}_k, \tag{17}$$

We assume that the channel estimation of $\mathbf{G}$ is perfect.

For the SISO communication system, H_{eo}, $\widetilde{H}$, and Z_k are independent. Therefore, $|H_{eo}Z_k|^2 = |H_{eo}|^2|Z_k|^2$, $\left|\tilde{H}Z_k\right|^2 = \left|\tilde{H}\right|^2|Z_k|^2$. The lower bound on secrecy capacity after adding SCO−AN under imperfect channel estimation is:

$$\begin{aligned} C_{sec,eo}^{g} &= I(Z;S) - I(Y;S) \\ &= \log\left(1 + \frac{\left|\tilde{H}p_k\right|^2\sigma_u^2}{\sigma_n^2+|H_{eo}p_k|^2\sigma_u^2+E\left|\tilde{H}w_g\right|^2+E\left|H_{eo}w_g\right|^2}\right) - \log\left(1 + \frac{|G_k p_k|^2\sigma_u^2}{E|G_k w_g|^2+\sigma_e^2}\right) \\ &= \log\left(1 + \frac{\left|\tilde{H}p_k\right|^2\sigma_u^2}{\sigma_n^2+|H_{eo}p_k|^2\sigma_u^2+\left|\tilde{H}Z_k\right|^2\sigma_g^2+|H_{eo}Z_k|^2\sigma_g^2}\right) - \log\left(1 + \frac{|G_k p_k|^2\sigma_u^2}{|G_k Z_k|^2\sigma_g^2+\sigma_e^2}\right) \\ &= \log\left(1 + \frac{\left|\tilde{H}p_k\right|^2\sigma_u^2}{\sigma_n^2+|H_{eo}p_k|^2\sigma_u^2+\left|\tilde{H}\right|^2|Z_k|^2\sigma_g^2+|H_{eo}|^2|Z_k|^2\sigma_g^2}\right) - \log\left(1 + \frac{|G_k p_k|^2\sigma_u^2}{|G_k|^2|Z_k|^2\sigma_g^2+\sigma_e^2}\right) \end{aligned} \tag{18}$$

In (18), we see that the channel estimation error will affect the channel capacity of the legitimate channel. Meanwhile, the secrecy capacity of the wireless communication system is reduced.

For the MIMO system, the lower bound on secrecy capacity after adding SCO−AN under imperfect channel estimation is:

$$\begin{aligned} C_{\text{sec},eo}^{g} &= I(Z;S) - I(Y;S) \\ &= \log\left(\frac{|\mathbf{K}_H + (\mathbf{H}_{eo}+\tilde{\mathbf{H}})\mathbf{Z}_k\mathbf{Z}_k^{\dagger}(\mathbf{H}_{eo}+\tilde{\mathbf{H}})^{\dagger}\sigma_u^2|}{|\mathbf{K}_H|}\right) - \log\left(\frac{|\mathbf{K}_G + \mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^{\dagger}\mathbf{G}_k^{\dagger}\sigma_u^2|}{|\mathbf{K}_G|}\right) \end{aligned} \tag{19}$$

In (19), $\mathbf{K}_H = ((\mathbf{H}_{eo}+\tilde{\mathbf{H}})\mathbf{Z}_k\mathbf{Z}_k^{\dagger}(\mathbf{H}_{eo}+\tilde{\mathbf{H}})^{\dagger})\sigma_g^2 + \mathbf{I}\sigma_n^2$ and $\mathbf{K}_G = (\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^{\dagger}\mathbf{G}_k^{\dagger})\sigma_g^2 + \mathbf{I}\sigma_e^2$.

2.5. Comprison of AN and SCO−AN

The artificial noise must be in the null space of the CSI matrix, this condition makes the artificial noise design very challenging. Artificial noise is the solution of homogeneous linear equations $\mathbf{H}_k\mathbf{w}_k = 0$. If the rank of the matrix $\mathbf{H}_k$ is r and the dimension is $n \times m(n \geq m)$, only when $r < m$, the homogeneous linear equation system $\mathbf{H}_k\mathbf{w}_k = 0$ has no solutions, when $r = m$, the homogeneous linear equations have only zero solutions. In the environment of natural communication, the probability of occurrence of $r = m$ is almost zero, that is to say, in the conditions of natural communication, the design of artificial noise is almost impossible.

For example, in MIMO, when the number of transmitting antennas is less than the number of eavesdropping antennas, artificial noise cannot be designed; when the number of transmitting antennas is equal to the number of eavesdropping antennas, artificial noise can be designed under the condition $|\mathbf{H}| = 0$. When the number of transmitting antennas is greater than the number of eavesdropping antennas, artificial noise cannot be designed. This is exactly the opposite of the original intention of AN. AN is designed to solve the condition that the eavesdropping channel must be a weaken version of the legitimate channel.

Therefore, the previous researches discussed some of the characteristics of AN theoretically and ignored its applicability.

For SISO, H_k is a constant and w_k is a constant as well. If $H_k W_k = 0$ has a non-zero solution, H = 0 must be guaranteed. Therefore, AN is not applicable in SISO wireless communication system.

SCO−AN is located in the range space of the legitimate CSI space, so, $\mathbf{H}_k\mathbf{w}_g \neq 0$.

There are countless non-zero solutions to $\mathbf{w}_g$, so we don't worry about to design $\mathbf{w}_g$.

We try to design AN under the condition of Rayleigh fading channels, and carry out a total of 1000 experiments, and all experiments fail. When we try to design SCO−AN, all experiments are successful.

In Table 1, we compare SCO−AN and AN in detail, and briefly summarize the characteristics and applicability of SCO−AN and AN. It can be seen that SCO−AN is better than AN in every aspect.

Table 1. Comprison of AN and SCO−AN.

Method	Design Difficulty	Secrecy Capacity Improvement	Application	Connection with H	Connection with G
AN	tough	normal	normal	in null space	in range space
SCO−AN	easy	good	good	in range space	in range space

3. Power Allocation of SCO−AN

The transmission power of the wireless communication system is limited. It is essential to allocate secrecy capacity under limited transmission power.

3.1. Objective Function of Power Allocation

3.1.1. Objective Function of Power Allocation for SISO Communication System

$\|\mathbf{p}_k\|^2$=1 and $\mathbf{Z}_k$ is a standard orthonormal basis for $\mathbf{H}_k$, which means $\mathbf{Z}_k\mathbf{Z}_k^\dagger = \mathbf{I}$ for MIMO and $Z_k Z_k^\dagger = 1$ for SISO. We assume that the transmission power is P.

$$\sigma_g^2 + \sigma_u^2 \leq P. \tag{20}$$

We use x instead of σ_u^2 and y instead of σ_g^2. The initial states of x and y are x_0 and y_0 respectively. For the SISO communication system, the secrecy capacity before power allocation is C_{sec}^0. Therefore:

$$\log\left(1 + \frac{|H_k|^2 x_0}{\sigma_n^2 + |H_k|^2 y_0}\right) - \log\left(1 + \frac{|G_k|^2 x_0}{|G_k|^2 y_0 + \sigma_e^2}\right) = C_{sec}^0. \tag{21}$$

There are no variables except x_0 and y_0 in (21). The power allocation problem of SCO−AN for SISO is written as:

$$\begin{aligned}
\min \quad & \log\left(1 + \frac{|G_k|^2 x}{|G_k|^2 y + \sigma_e^2}\right) - \log\left(1 + \frac{|H_k|^2 x}{\sigma_n^2 + |H_k|^2 y}\right) \\
\text{s.t.} \quad & \log\left(1 + \frac{|H_k|^2 x}{\sigma_n^2 + |H_k|^2 y}\right) - \log\left(1 + \frac{|G_k|^2 x}{|G_k|^2 y + \sigma_e^2}\right) > C_{sec}^0 \\
& \log\left(\frac{|H_k|^2 x}{\sigma_n^2 + |H_k|^2 y}\right) \geq K \\
& x + y \leq P \\
& x > 0 \\
& y > 0
\end{aligned} \tag{22}$$

In (22), a restricted condition $\log\left(1 + \frac{|H_k|^2 x}{\sigma_n^2 + |H_k|^2 y}\right) - \log\left(1 + \frac{|G_k|^2 x}{|G_k|^2 y + \sigma_e^2}\right) > C_{sec}^0$ is added to make sure that the optimal direction is correct. SCO−AN is an extra noise for Bob the receiver as well. K is the minimum signal-to-noise ratio (SNR) for normal communication. We add another restricted condition $\log\left(1 + \frac{|H_k|^2 x}{\sigma_n^2 + |H_k|^2 y}\right) \geq K$ to ensure normal communication. The value of K varies among different communication systems.

The objective function in (22) is $\log\left(1 + \frac{|G_k|^2 x}{|G_k|^2 y + \sigma_e^2}\right) - \log\left(1 + \frac{|H_k|^2 x}{\sigma_n^2 + |H_k|^2 y}\right)$. The Hessian matrix of the objective function in (22) is not positive definite, so the extremum of the objective function cannot be obtained by the partial derivative method. An improved sequence quadratic program (ISQP) is adopted to optimize power allocation. The basic idea of ISQP is that, at each iterative step, a quadratic programming problem is solved to

establish a descent direction, which reduces the value function to obtain compensation. The iterative steps are repeated until the solution of the original problem is obtained.

The Lagrange function of (22) is:

$$L(x,y,\mu,\lambda) = f(x,y) - \mu_1 h_1(x,y) - \sum_{j=1,2,3,4} \lambda_j g_j(x,y), \tag{23}$$

where

$$\begin{aligned} f(x,y) &= -\log\left(1+\tfrac{|H_k|^2 x}{\sigma_n^2+|H_k|^2 y}\right)+\log\left(1+\tfrac{|G_k|^2 x}{|G_k|^2 y+\sigma_e^2}\right) \\ g_1(x,y) &= \log\left(1+\tfrac{|H_k|^2 x}{\sigma_n^2+|H_k|^2 y}\right)-\log\left(1+\tfrac{|G_k|^2 x}{|G_k|^2 y+\sigma_e^2}\right)-C_{sec}0 \\ g_2(x,y) &= x \\ g_3(x,y) &= y \\ g_4(x,y) &= \log\left(\tfrac{|H_k|^2 x}{\sigma_n^2+|H_k|^2 y}\right)-\mathrm{K} \\ h_1(x,y) &= x+y-P. \end{aligned} \tag{24}$$

For the case of imperfect channel estimation, the initial states of x and y are x_0 and y_0 respectively. The initial secrecy capacity is C_{sec}^{eo}.

$$\log\left(1+\frac{\left|\tilde{H}\right|^2 x}{\sigma_n^2+|H_{eo}|^2 x+\left|\tilde{H}\right|^2 y+|H_{eo}|^2 y}\right)-\log\left(1+\frac{|G_k|^2 x_0}{|G_k|^2 y_0+\sigma_e^2}\right)=C_{sec}^{eo} \tag{25}$$

The power allocation problem of SCO−AN for SISO under imperfect channel estimation is written as:

$$\begin{aligned} \min \quad & -\log\left(1+\frac{\left|\tilde{H}\right|^2 x}{\sigma_n^2+|H_{eo}|^2 x+\left|\tilde{H}\right|^2 y+|H_{eo}|^2 y}\right)+\log\left(1+\frac{|G_k|^2 x}{|G_k|^2 y+\sigma_e^2}\right) \\ \text{s.t.} \quad & \log\left(1+\frac{\left|\tilde{H}\right|^2 x}{\sigma_n^2+|H_{eo}|^2 x+\left|\tilde{H}\right|^2 y+|H_{eo}|^2 y}\right)-\log\left(1+\frac{|G_k|^2 x}{|G_k|^2 y+\sigma_e^2}\right)>C_{sec}^{eo} \\ & \log\left(1+\frac{\left|\tilde{H}\right|^2 x}{\sigma_n^2+|H_{eo}|^2 x+\left|\tilde{H}\right|^2 y+|H_{eo}|^2 y}\right)\geq K \\ & x+y\leq P \\ & x>0 \\ & y>0 \end{aligned} \tag{26}$$

The Lagrange function of (26) is:

$$L(x,y,\mu,\lambda) = f(x,y) - \mu_1 h_1(x,y) - \sum_{j=1,2,3,4} \lambda_j g_j(x,y), \tag{27}$$

where

$$\begin{aligned} f(x,y) &= -\log\left(1+\tfrac{\left|\tilde{H}\right|^2 x}{\sigma_n^2+|H_{eo}|^2 x+\left|\tilde{H}\right|^2 y+|H_{eo}|^2 y}\right)+\log\left(1+\tfrac{|G_k|^2 x}{|G_k|^2 y+\sigma_e^2}\right) \\ g_1(x,y) &= \log\left(1+\tfrac{\left|\tilde{H}\right|^2 x}{\sigma_n^2+|H_{eo}|^2 x+\left|\tilde{H}\right|^2 y+|H_{eo}|^2 y}\right)-\log\left(1+\tfrac{|G_k|^2 x}{|G_k|^2 y+\sigma_e^2}\right)-C_{sec}^{eo} \\ g_2(x,y) &= x \\ g_3(x,y) &= y \\ g_4(x,y) &= \log\left(\tfrac{\left|\tilde{H}\right|^2 x}{\sigma_n^2+|H_{eo}|^2 x+\left|\tilde{H}\right|^2 y+|H_{eo}|^2 y}\right)-K \\ h_1(x,y) &= x+y-P, \end{aligned} \tag{28}$$

The most frequently used methods for channel estimation are least square (LS) channel estimation and minimum mean square error (MMSE) channel estimation.

LS channel estimation is a classic algorithm for non-blind channel estimation. The pilot symbols are used to estimate the channel.

The LS channel estimation is given as:

$$\tilde{\mathbf{H}}_{LS} = \mathbf{z}_k(\mathbf{x}_k)^{-1}. \tag{29}$$

For the MIMO communication system, the LS channel estimation is:

$$\begin{aligned} \left\|\mathbf{H}_{eo}^{LS}\right\|^2 &= \left\|\mathbf{H} - \tilde{\mathbf{H}}_{LS}\right\|^2 \\ &= \left\|(\mathbf{z}_k - \mathbf{n})\mathbf{x}_k^{-1} - \mathbf{x}_k\mathbf{x}_k^{-1}\right\|^2 \\ &= \left\|\mathbf{n}\mathbf{x}_k^{-1}\right\|^2. \end{aligned} \tag{30}$$

In (30), $\mathbf{H}_{eo}^{LS}$ denotes the error of LS channel estimation and $\left\|\mathbf{H}_{eo}^{LS}\right\|^2$ denotes the second norm of the LS channel estimation error. $\left\|\mathbf{H}_{eo}^{LS}\right\|^2$ is in proportion to the SNR of the legitimate channel.

For the SISO communication system, the LS channel estimation is:

$$\left|H_{eo}^{LS}\right|^2 = \left|H - \tilde{H}_{LS}\right|^2 = \left|nx_k^{-1}\right|^2. \tag{31}$$

For the MIMO communication system, similar to LS estimation, it is easy to obtain (32):

$$\begin{aligned} \left\|\mathbf{H}_{eo}^{MMSE}\right\|^2 &= \left\|\mathbf{H} - \tilde{\mathbf{H}}_{\mathbf{MMSE}}\right\|^2 \\ &= \left\|\mathbf{H} - R_{\mathbf{H}\tilde{\mathbf{H}}}\left(R_{\mathbf{HH}} + \frac{\sigma_n^2}{\sigma_x^2}I\right)^{-1}\tilde{\mathbf{H}}_{LS}\right\|^2 \\ &= \left\|\mathbf{H} - R_{\mathbf{H}\tilde{\mathbf{H}}}\left(R_{\mathbf{HH}} + \frac{\sigma_n^2}{\sigma_x^2}I\right)^{-1}\mathbf{y}_k\mathbf{x}_k^{-1}\right\|^2, \end{aligned} \tag{32}$$

where $\mathbf{H}_{eo}^{MMSE}$ denotes the error of MMSE channel estimation and $R_{\mathbf{AB}}$ denotes the cross-correlation matrix of $\mathbf{A}$ and $\mathbf{B}$.

For SISO communication system, R_{AB} denotes the cross-correlation coefficient of A and B.

$$\begin{aligned} \left|H_{eo}^{MMSE}\right|^2 &= \left|H - \tilde{H}_{MMSE}\right|^2 \\ &= \left|H - R_{H\tilde{H}}\left(R_{HH} + \frac{\sigma_e^2}{\sigma_x^2}\right)^{-1}\tilde{H}_{LS}\right|^2 \\ &= \left|H - R_{H\tilde{H}}\left(R_{HH} + \frac{\sigma_n^2}{\sigma_x^2}\right)^{-1}y_k x_k^{-1}\right|^2. \end{aligned} \tag{33}$$

For the SISO communication system, according to the analysis above, every parameter in (18) except σ_g^2 is available. (31) and (33) are applicable conclusions. However, for MIMO communication system, the expansion of matrices is too complex, rendering (30) and (32) inapplicable.

3.1.2. Objective Function of Power Allocation for MIMO Communication System

For the MIMO communication system, the power for each transmission is $P_{0,m}$. Therefore,

$$\sigma_g^2 + \sigma_u^2 \leq P_{0,m}. \tag{34}$$

The initial secrecy capacity is $C_{sec}^{0,m}$. For the perfect channel estimation, the initial secrecy capacity is given by:

$$\log\left|\mathbf{I}\sigma_n^2 + \mathbf{H}_k\mathbf{Z}_k\mathbf{Z}_k^{\dagger}\mathbf{H}_k^{\dagger}x_0\right| - \log\left(\frac{\left|\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^{\dagger}\mathbf{G}_k^{\dagger}y_0 + \mathbf{I}\sigma_e^2 + \mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^{\dagger}\mathbf{G}_k^{\dagger}x_0\right|}{\left|\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^{\dagger}\mathbf{G}_k^{\dagger}y_0 + \mathbf{I}\sigma_e^2\right|}\right) = C_{sec}^{0,m}. \tag{35}$$

The power allocation problem of SCO−AN for MIMO is written as:

$$\begin{aligned}
\min \quad & \log\left(\frac{|(\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger)y+\mathbf{I}\sigma_e^2+\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger x|}{|(\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger)y+\mathbf{I}\sigma_e^2|}\right)-\log\left(\frac{|(\mathbf{H}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_k^\dagger)y+\mathbf{I}\sigma_n^2+\mathbf{H}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_k^\dagger x|}{|(\mathbf{H}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_k^\dagger)y+\mathbf{I}\sigma_n^2|}\right)\\
\text{s.t.} \quad & \log\left(\frac{|(\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger)y+\mathbf{I}\sigma_e^2+\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger x|}{|(\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger)y+\mathbf{I}\sigma_e^2|}\right)-\log\left(\frac{|(\mathbf{H}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_k^\dagger)y+\mathbf{I}\sigma_n^2+\mathbf{H}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_k^\dagger x|}{|(\mathbf{H}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_k^\dagger)y+\mathbf{I}\sigma_n^2|}\right) > C_{sec}^{0,m}\\
& \log\left(\frac{|(\mathbf{H}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_k^\dagger)y+\mathbf{I}\sigma_n^2+\mathbf{H}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_k^\dagger x|}{|(\mathbf{H}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_k^\dagger)y+\mathbf{I}\sigma_n^2|}\right) > K\\
& x+y \le P_{0,m}\\
& x>0\\
& y>0
\end{aligned} \tag{36}$$

The Lagrange function of (36) is:

$$L(x,y,\mu,\lambda) = f(x,y) - \mu_1 h_1(x,y) - \sum_{j=1,2,3,4}\lambda_j g_j(x,y), \tag{37}$$

where

$$\begin{aligned}
f(x,y) &= \log\left(\frac{|(\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger)y+\mathbf{I}\sigma_e^2+\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger x|}{|(\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger)y+\mathbf{I}\sigma_e^2|}\right)-\log\left(\frac{|(\mathbf{H}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_k^\dagger)y+\mathbf{I}\sigma_n^2+\mathbf{H}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_k^\dagger x|}{|(\mathbf{H}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_k^\dagger)y+\mathbf{I}\sigma_n^2|}\right)\\
g_1(x,y) &= \log\left(\frac{|(\mathbf{H}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_k^\dagger)y+\mathbf{I}\sigma_n^2+\mathbf{H}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_k^\dagger x|}{|(\mathbf{H}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_k^\dagger)y+\mathbf{I}\sigma_n^2|}\right)-\log\left(\frac{|(\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger)y+\mathbf{I}\sigma_e^2+\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger x|}{|(\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger)y+\mathbf{I}\sigma_e^2|}\right)-C_{sec}^{0,m}\\
g_2(x,y) &= \log\left(\frac{|(\mathbf{H}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_k^\dagger)y+\mathbf{I}\sigma_n^2+\mathbf{H}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_k^\dagger x|}{|(\mathbf{H}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_k^\dagger)y+\mathbf{I}\sigma_n^2|}\right)-K\\
g_3(x,y) &= x\\
g_4(x,y) &= y\\
h_1(x,y) &= x+y-P_{0,m}\ .
\end{aligned} \tag{38}$$

For the imperfect channel estimation, the initial secrecy capacity is $C_{sec,eo}^{0,m}$. For the imperfect channel estimation, the initial secrecy capacity is given by:

$$\log\left(\frac{\left|\mathbf{K}_{H,0}^{eo}+(\mathbf{H}_{eo}+\tilde{\mathbf{H}})\mathbf{Z}_k\mathbf{Z}_k^\dagger(\mathbf{H}_{eo}+\tilde{\mathbf{H}})^\dagger x_0\right|}{\left|\mathbf{K}_{H,0}^{eo}\right|}\right)-\log\left(\frac{\left|\mathbf{K}_G+\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger x_0\right|}{|\mathbf{K}_G|}\right)=C_{sec,eo}^{0,m}\ , \tag{39}$$

In (39), $\mathbf{K}_{H,0}^{eo}=((\mathbf{H}_{eo}+\tilde{\mathbf{H}})\mathbf{Z}_k\mathbf{Z}_k^\dagger(\mathbf{H}_{eo}+\tilde{\mathbf{H}})^\dagger)y_0+\mathbf{I}\sigma_n^2$. We use x instead of σ_u^2 , y instead of σ_g^2 and the initial states of x and y are x_0 and y_0 respectively.

For the imperfect channel estimation, the power allocation problem of SCO−AN is written as:

$$\begin{aligned}
\min \quad & \log\left(\frac{\left|\mathbf{K}_H+(\mathbf{H}_{eo}+\tilde{\mathbf{H}})\mathbf{Z}_k\mathbf{Z}_k^\dagger(\mathbf{H}_{eo}+\tilde{\mathbf{H}})^\dagger x\right|}{|\mathbf{K}_H|}\right)-\log\left(\frac{\left|\mathbf{K}_G+\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger x\right|}{|\mathbf{K}_G|}\right)\\
\text{s.t.} \quad & \log\left(\frac{\left|\mathbf{K}_H+(\mathbf{H}_{eo}+\tilde{\mathbf{H}})\mathbf{Z}_k\mathbf{Z}_k^\dagger(\mathbf{H}_{eo}+\tilde{\mathbf{H}})^\dagger x\right|}{|\mathbf{K}_H|}\right)-\log\left(\frac{\left|\mathbf{K}_G+\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger x\right|}{|\mathbf{K}_G|}\right))>C_{sec,eo}^{0,m}\\
& \log\left(\frac{\left|((\mathbf{H}_{eo}+\tilde{\mathbf{H}})\mathbf{Z}_k\mathbf{Z}_k^\dagger(\mathbf{H}_{eo}+\tilde{\mathbf{H}})^\dagger)y+(\mathbf{H}_{eo}+\tilde{\mathbf{H}})\mathbf{Z}_k\mathbf{Z}_k^\dagger(\mathbf{H}_{eo}+\tilde{\mathbf{H}})^\dagger x\right|}{|\mathbf{K}_H|}\right)\ge \mathrm{K}\\
& x+y\le P_{0,m}\\
& x>0\\
& y>0
\end{aligned} \tag{40}$$

The Lagrange function of (40) is:

$$L(x,y,\mu,\lambda) = f(x,y) - \mu_1 h_1(x,y) - \sum_{j=1,2,3,4} \lambda_j g_j(x,y), \tag{41}$$

where

$$\begin{aligned}
f(x,y) &= -\log\left(\frac{\left|\mathbf{K}_H+(\mathbf{H}_{eo}+\tilde{\mathbf{H}})\mathbf{Z}_k\mathbf{Z}_k^{\dagger}(\mathbf{H}_{eo}+\tilde{\mathbf{H}})^{\dagger}x\right|}{|\mathbf{K}_H|}\right)+\log\left(\frac{\left|\mathbf{K}_G+\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^{\dagger}\mathbf{G}_k^{\dagger}x\right|}{|\mathbf{K}_G|}\right)\\
g_1(x,y) &= \log\left(\frac{\left|\mathbf{K}_H+(\mathbf{H}_{eo}+\tilde{\mathbf{H}})\mathbf{Z}_k\mathbf{Z}_k^{\dagger}(\mathbf{H}_{eo}+\tilde{\mathbf{H}})^{\dagger}x\right|}{|\mathbf{K}_H|}\right)-\log\left(\frac{\left|\mathbf{K}_G+\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^{\dagger}\mathbf{G}_k^{\dagger}x\right|}{|\mathbf{K}_G|}\right)-C_{sec,eo}^{0,m}\\
g_2(x,y) &= \log\left(\frac{\left|((\mathbf{H}_{eo}+\tilde{\mathbf{H}})\mathbf{Z}_k\mathbf{Z}_k^{\dagger}(\mathbf{H}_{eo}+\tilde{\mathbf{H}})^{\dagger})y+(\mathbf{H}_{eo}+\tilde{\mathbf{H}})\mathbf{Z}_k\mathbf{Z}_k^{\dagger}(\mathbf{H}_{eo}+\tilde{\mathbf{H}})^{\dagger}x\right|}{|\mathbf{K}_H|}\right)-\mathrm{K}\\
g_3(x,y) &= x\\
g_4(x,y) &= y\\
h_1(x,y) &= x+y-P_{0,m}
\end{aligned} \tag{42}$$

3.1.3. Objective Function of Power Allocation for SIMO Communication System with Active Eavesdroppers

In this paper, we discussed the case of the passive eavesdropper. Recently, the proposed pilot spoofing attack technology maked EVE to have the ability to attack Alice. Therefore, we will discuss the influence of active eavesdroppers.As shown in Figure 3, in the SIMO wire-tap communication system, Alice equips with N transmit antenna, N one-antenna receivers (Bobs) equip with N one-antenna Eves. Let P_N denotes the pilot symbol. P_N is known to Eve, which concurrently send the same pilot in the training phase withe the average transmission power P_e and Alice has a perfect knowledge of P_N. The relevant knowledge [30] of pilot frequency has been introduced in this paper and will not be repeated.

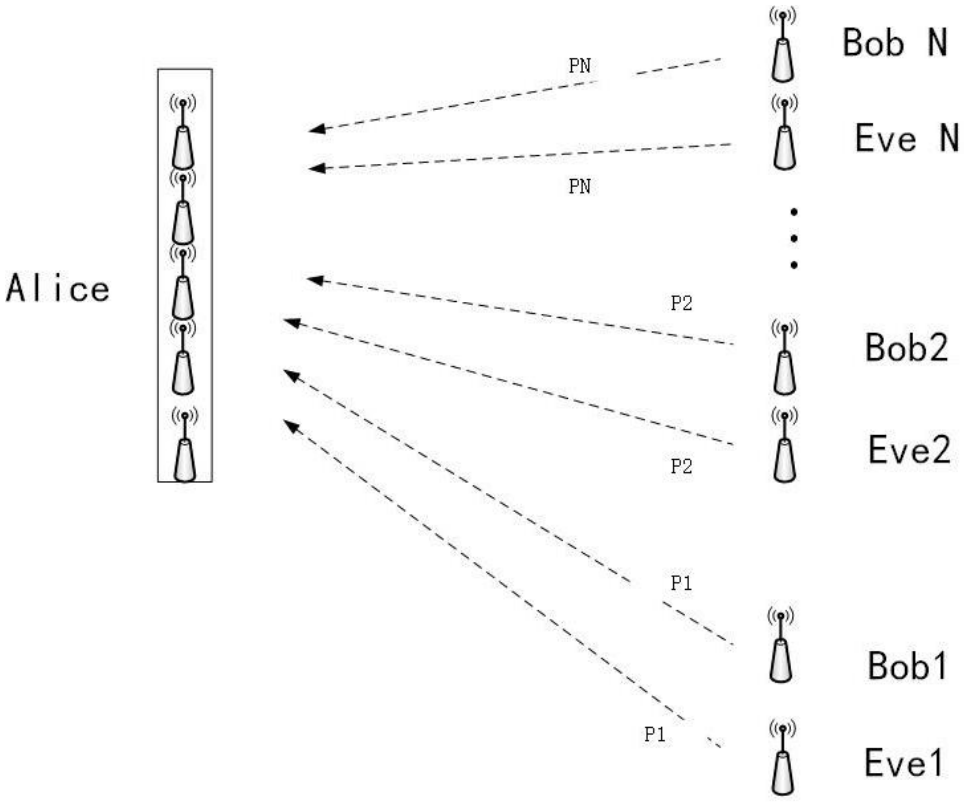


Figure 3. Single-antenna eavesdroppers launch pilot spoofing attack.

According to ([9]), for the LS estimatior,

$$\overline{\mathbf{h}}_{LS} = (\mathbf{K}_B^H \mathbf{K}_B)^{-1} \mathbf{K}_B^H z \tag{43}$$

where $\overline{\mathbf{h}}_{LS}$ denotes the estimate of $\mathbf{h}$ with LS Estimator and $\mathbf{K}_B^H \triangleq \sqrt{P_B} A_B$.

$$\mathbf{A}_B \triangleq \frac{1}{\sqrt{L_B}} \left[a(\theta_{B,1,m}), a(\theta_{B,2,m}), \ldots, a(\theta_{B,L_B,m}) \right] \tag{44}$$

$$\mathbf{A}_B \triangleq \frac{1}{\sqrt{L_B}} \left[a(\theta_{B,1,m}), a(\theta_{B,2,m}), \ldots, a(\theta_{B,L_B,m}) \right] \tag{45}$$

$$a(\theta_{B,l,m}) = \frac{\left[1, e^{-j2\pi \frac{d}{\lambda_c} \cos(\theta_{B,l,m})}, e^{-j4\pi \frac{d}{\lambda_c} \cos(\theta_{B,l,m})}, \ldots, e^{-j2n\pi \frac{d}{\lambda_c} \cos(\theta_{B,l,m})} \right]^T}{\sqrt{N}} \tag{46}$$

L_B is the number of paths between the transmitter and Alice.

For the MMSE estimatior,

$$\overline{\mathbf{h}}_{MMSE} = (\mathbf{I}_{L_B} + \mathbf{K}_B^H R_{dd}^{-1} \mathbf{K}_B)^{-1} \mathbf{K}_B^H R_{dd}^{-1} z, \tag{47}$$

where $\overline{\mathbf{h}}_{MMSE}$ denotes the estimate of $\mathbf{h}$ with MMSE Estimator and $R_{dd} \triangleq K_E K_E^H + \sigma_v^2 I_N$ The power allocation problem of SCO−AN for SIMO with active eavesdropper is written as:

$$\begin{aligned}
\min \quad & \log\left(\frac{\left| \mathbf{K}_H + (\mathbf{h}_{eo} + \tilde{\mathbf{h}}) \mathbf{Z}_k \mathbf{Z}_k^\dagger (\mathbf{h}_{eo} + \tilde{\mathbf{h}})^\dagger x \right|}{|\mathbf{K}_H|} \right) - \log\left(\frac{|\mathbf{K}_G + \mathbf{G}_k \mathbf{Z}_k \mathbf{Z}_k^\dagger \mathbf{G}_k^\dagger x|}{|\mathbf{K}_G|} \right) \\
\text{s.t.} \quad & \log\left(\frac{\left| \mathbf{K}_h + (\mathbf{h}_{eo} + \tilde{\mathbf{h}}) \mathbf{Z}_k \mathbf{Z}_k^\dagger (\mathbf{h}_{eo} + \tilde{\mathbf{h}})^\dagger x \right|}{|\mathbf{K}_H|} \right) - \log\left(\frac{|\mathbf{K}_G + \mathbf{G}_k \mathbf{Z}_k \mathbf{Z}_k^\dagger \mathbf{G}_k^\dagger x|}{|\mathbf{K}_G|} \right)) > C_{sec,eo}^{0,m} \\
& \log\left(\frac{\left| ((\mathbf{h}_{eo} + \tilde{\mathbf{h}}) \mathbf{Z}_k \mathbf{Z}_k^\dagger (\mathbf{h}_{eo} + \tilde{\mathbf{h}})^\dagger) y + (\mathbf{h}_{eo} + \tilde{\mathbf{h}}) \mathbf{Z}_k \mathbf{Z}_k^\dagger (\mathbf{h}_{eo} + \tilde{\mathbf{H}})^\dagger x \right|}{|\mathbf{K}_H|} \right) \geq \mathrm{K} \\
& x + y \leq P_{0,m} \\
& x > 0 \\
& y > 0
\end{aligned} \tag{48}$$

For SIMO communication system with active eavesdroppers, $\mathbf{h}_{eo} = \mathbf{h} - \tilde{\mathbf{h}}$ in (48). $\tilde{\mathbf{h}}$ denotes $\tilde{\mathbf{h}}_{\mathbf{LS}}$ when LS estimator is used and denotes $\tilde{\mathbf{h}}_{\mathbf{MMSE}}$ when MMSE estimator is used.

The Lagrange function of (48) is:

$$L(x, y, \mu, \lambda) = f(x, y) - \mu_1 h_1(x, y) - \sum_{j=1,2,3,4} \lambda_j g_j(x, y), \tag{49}$$

where

$$\begin{aligned} f(x,y) &= -\log\left(\frac{\left|\mathbf{K}_H+(\mathbf{h}_{eo}+\tilde{\mathbf{h}})\mathbf{Z}_k\mathbf{Z}_k^{\dagger}(\mathbf{h}_{eo}+\tilde{\mathbf{h}})^{\dagger}x\right|}{|\mathbf{K}_H|}\right)+\log\left(\frac{\left|\mathbf{K}_G+\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^{\dagger}\mathbf{G}_k^{\dagger}x\right|}{|\mathbf{K}_G|}\right) \\ g_1(x,y) &= \log\left(\frac{\left|\mathbf{K}_H+(\mathbf{h}_{eo}+\tilde{\mathbf{h}})\mathbf{Z}_k\mathbf{Z}_k^{\dagger}(\mathbf{h}_{eo}+\tilde{\mathbf{h}})^{\dagger}x\right|}{|\mathbf{K}_H|}\right)-\log\left(\frac{\left|\mathbf{K}_G+\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^{\dagger}\mathbf{G}_k^{\dagger}x\right|}{|\mathbf{K}_G|}\right)-C_{sec,eo}^{0,m} \\ g_2(x,y) &= \log\left(\frac{\left|((\mathbf{h}_{eo}+\tilde{\mathbf{h}})\mathbf{Z}_k\mathbf{Z}_k^{\dagger}(\mathbf{h}_{eo}+\tilde{\mathbf{h}})^{\dagger})y+(\mathbf{h}_{eo}+\tilde{\mathbf{h}})\mathbf{Z}_k\mathbf{Z}_k^{\dagger}(\mathbf{h}_{eo}+\tilde{\mathbf{h}})^{\dagger}x\right|}{|\mathbf{K}_H|}\right)-\mathrm{K} \\ g_3(x,y) &= x \\ g_4(x,y) &= y \\ h_1(x,y) &= x+y-P_{0,m} \end{aligned} \tag{50}$$

The power allocation problems of SCO−AN with perfect channel estimation, imperfect channel and active eavesdropper are similar. Therefore, we use the same algorithm to solve the problem.

3.2. SQP and ISQP Algorithm

μ and λ are Lagrange multipliers. To optimize the problems above, the following conditions must be satisfied:

$$\begin{aligned} &\left.\frac{\partial L}{\partial X}\right|_{x=x^*}=0 && && (a) \\ &\lambda_j \neq 0, && && (b) \\ &u_k \geq 0, && && (c) \\ &u_k g_k(x*)=0, && && (d) \\ &h_i(x*)=0 && i=1 && (e) \\ &g_j(x*)=0, && j=1,2,3,4 && (f) \end{aligned} \tag{51}$$

(51) are Karush-Kuhn-Tucker conditions (KKT conditions). (a) is a necessary condition when the extreme value of Lagrange function is taken; (b) is a Lagrange coefficient constraint; (c) is an inequality constraint case; (d) is the complementary relaxation condition; (e) and (f) are the original constraints.

The KKT condition is a necessary condition for the optimal solution.

Condition (c) constructs the $L(x,\lambda,\mu)$ function and the condition $L(x,\lambda,\mu) \leq f(x)$ should be satisfied. In $L(x,\lambda,\mu)$, μ is 0, so λ is less than or equal to 0.

A quadratic polynomial is used to approximate $f(x,y)$. By expanding the quadratic polynomial into a positive definite quadratic form, the following quadratic programming subproblem is obtained:

$$\begin{aligned} \min \quad & \tfrac{1}{2}d^T\mathbf{B}_k d+\nabla f(x_k,y_k)^T d \\ s.t \quad & h(x_k,y_k)+\mathbf{A}_k^{\varepsilon} d=0 \\ & g(x_k,y_k)+\mathbf{A}_k^{\Gamma} d \geq 0, \end{aligned} \tag{52}$$

where $\mathbf{A}_k^{\varepsilon}=\nabla h(x_k,y_k)$, $\mathbf{A}_k^{\Gamma}=\nabla g(x_k,y_k)$,$t_k$ is a positive definite matrix, and d_k is optimal solution of quadratic programming subproblems.

Let x^* denote the KKT point of the optimization constraint problem and $\lambda^*,\mu^* \geq 0$ be its corresponding Lagrange multiplier vectors. For x^*, the following conditions should be satisfied:

1. The Jacobi matrix of $L(x,\lambda,\mu)$ is row full rank.
2. The strict complementary relaxation condition should be satisfied; that is, $g_i(x^*) \geq 0$, $\lambda_i^* \geq 0, g_i(x^*)\lambda_i^*=0$, and $g_i(x^*)+\lambda_i^*>0$.
3. A sufficient second-order optimality condition should be satisfied, that is, for any vector $d \neq 0$ that satisfies $\mathbf{A}(x^*)d=0$, the following condition is satisfied:

$$d^T\mathbf{B}(x^*,y^*,\mu^*,\lambda^*)d>0, \tag{53}$$

where $\mathbf{B}(x, y, \mu, \lambda)$ is a positive definite matrix, at the beginning of the iteration, $\mathbf{B}(x, y, \mu, \lambda)$ is usually set as the identity matrix.

If $(x_k, y_k, \mu_k, \lambda_k)$ is close to $(x^*, y^*, \mu^*, \lambda^*)$ sufficiently, the quadratic programming sub-problem of (53) has a local minimum point d^*. The corresponding effective constraint index set is the same as the effective constraint index set of the original problem at (x^*, y^*). Using the KKT conditions, (52) is equivalent to:

$$H_1(d, \mu, \lambda) = \mathbf{B}_k - (\mathbf{A}_k^{\varepsilon})^T \mu - (\mathbf{A}_k^{\Gamma})^T \lambda + \nabla f(x_k, y_k), \tag{54}$$

$$H_2(d, \mu, \lambda) = h(x_k, y_k) + (\mathbf{A}_k^{\varepsilon})^T d, \tag{55}$$

$$\lambda \geq 0, g(x_k, y_k) + \mathbf{A}_k^{\Gamma} d \geq 0, \lambda[g(x_k, y_k) + \mathbf{A}_k^{\Gamma} d] = 0, \tag{56}$$

Note that Formula (20) and (23) are linear complementarity problems. We define smooth FB-function:

$$\varphi(\varepsilon, a, b) = a + b - \sqrt{a^2 + b^2 + 2\varepsilon^2}, \tag{57}$$

where $\varepsilon > 0$ is a smooth parameter, and

$$\Phi(\varepsilon, d, \lambda) = (\varphi_1(\varepsilon, d, \lambda), \varphi_2(\varepsilon, d, \lambda) \ldots \varphi_m(\varepsilon, d, \lambda))^T, \tag{58}$$

in (32),

$$\begin{aligned} \varphi_i(\varepsilon, d, \lambda) = \lambda_i + [g_i(x_k, y_k) + (A_k^{\Gamma})_i d] \\ - \sqrt{\lambda_i^2 + [g_i(x_k, y_k) + (\mathbf{A}_k^{\Gamma})_i d]^2 + 2\varepsilon^2}, \end{aligned} \tag{59}$$

where $(A_k^{\Gamma})_i$ is the i-th row of $\mathbf{A}_k^{\Gamma}$. (18) and (19), (21) and (22) are equivalent to

$$H(z) := H(\varepsilon, d, \mu, \lambda) = \begin{pmatrix} \varepsilon \\ H_1(d, \mu, \lambda) \\ H_2(d, \mu, \lambda) \\ \Phi(\varepsilon, d, \lambda) \end{pmatrix} = 0, \tag{60}$$

The Jacobian matrix of (H_z) is

$$H'(z) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \mathbf{B}_k & -(\mathbf{A}_k^{\varepsilon})^T & -(\mathbf{A}_k^{\Gamma})^H \\ 0 & \mathbf{A}_k^{\varepsilon} & 0 & 0 \\ \nu & D_2(z) A_k^{\Gamma} & 0 & D_1(z) \end{pmatrix}, \tag{61}$$

where $\nu = \nabla_{\varepsilon} \Phi(\varepsilon, d, \lambda) = (\nu_1, \nu_2, \ldots, \nu_m)^T$ and

$$\nu_i = -\frac{2\varepsilon}{\sqrt{\lambda_i^2 + [g_i(x_k, y_k) + (\mathbf{A}_k^{\Gamma})_i d]^2 + 2\varepsilon^2}}, \tag{62}$$

$$\begin{aligned} D_1(z) = diag(a_1(z), a_2(z), \ldots, a_m(z)), \\ D_2(z) = diag(b_1(z), b_2(z), \ldots, b_m(z)), \end{aligned} \tag{63}$$

where

$$\begin{aligned} a_i(z) = 1 - \frac{\lambda_i}{\sqrt{\lambda_i^2 + [g_i(x_k, y_k) + (\mathbf{A}_k^{\Gamma})_i d]^2 + 2\varepsilon^2}}, \\ b_i(z) = 1 - \frac{g_i(x_k, y_k) + (\mathbf{A}_k^{\Gamma})_i d}{\sqrt{\lambda_i^2 + [g_i(x_k, y_k) + (\mathbf{A}_k^{\Gamma})_i d]^2 + 2\varepsilon^2}}, \end{aligned} \tag{64}$$

here, we make $\gamma \in (0, 1)$ and a non-negative functions $\psi(z)$ is

$$\psi(z) = \gamma \|H(z)\| \min\{1, \|H(z)\|\}. \tag{65}$$

Sequence quadratic program (SQP) is an iterative algorithm, the basic idea of SQP is to apply approximate Newton method to the first-order optimality condition of constrained optimization problem. In each iteration step, a quadratic programming problem with the quadratic approximation of Lagrange function as the objective function and the linearization of the original constraint as the constraint condition are solved.

The full SQP is shown as follows:

Algorithm 1 SQP

Step 0: Set β=0.5, σ=0.2, ε=1×10^{-6}, the initial vector $d_0 = (1,1,1)^{\mathrm{T}}$, $\mu_0 = 0$, $\lambda_0 = (0,0,0)^T$, $z_0 = (\varepsilon_0, d_0, \mu_0, \lambda_0)$, $\bar{z}_0 = (\varepsilon_0, 0, 0, 0)$, $i = 0$
Step 1: If $\|H(z_i)\| \leq 0$, stop iteration, else, $\psi_i = \psi(z_i)$, ψ_i is shown in (37), $H(z_i)$ is shown in (32).
Step 2: Solve the equations $H(z_i) + H'(z_i)\Delta z_i = \psi \bar{z}_0$ and then get the solution of the equations: $\Delta z_i = (\Delta\varepsilon_i, \Delta d_i, \Delta\mu_i, \Delta\lambda_i)$
Step 3: Let m be the smallest non-negative integer m that satisfies the following inequality: $H(z_i + \beta^m \Delta z_i) \leq [1 - \sigma(1 - \gamma\varepsilon_0)\beta^m)]\|H(z_i)\|$ where $\alpha_i = \rho^{m_i}, z_{i+1} = z_i + \alpha_i \Delta z_i$
Step 4: $i = i + 1$, go to step1

We adopt a improved sequence quadratic program (ISQP) which is based on improvements from sequence quadratic program. At the beginning of the iteration, the initial matrix in (52), $B(x, \mu, \lambda)$ is set as the identity matrix in ISQP. In SQP, the initial matrix is designed as $W(x,y,u,\lambda) = \nabla^2(f(x,y)) - \sum_{i=1}^{l} u_i \times \nabla^2(h_i(x,y)) - \sum_{i=1}^{m} \lambda_i \times \nabla^2(g_i(x,y))$, $\nabla^2(*)$ denotes the Hessian matrix of $(*)$. A second order partial derivative should be calculated in each iteration of SQP. The complexity of $W(x,y,u,\lambda) = \nabla^2(f(x,y)) - \sum_{i=1}^{l} u_i \times \nabla^2(h_i(x,y)) - \sum_{i=1}^{m} \lambda_i \times \nabla^2(g_i(x,y))$ trivially is much larger than that of $B(x,y,\mu,\lambda)$.

3.3. Complexity Analysis

In this section, we assert the superiority of ISQP by comparing the complexity of the three algorithms: ISQP, SQP, BPA and COCOA [31]. ISQP and SQP have been introduced in detail in previous sections. The BPA algorithm is a traversal algorithm which searches all directions in each iteration and then selects the best direction. The complexity of BPA algorithm is high and the search direction is greatly affected by the step size. BPA is also likely to search in the wrong direction. The complexity of ISQP, SQP, and BPA are shown as follows. The change of angle for BPA is set as 5° so 36 rounds of calculation are needed for just one iteration. The entries in the tables indicate the calculated amount required for one iteration.

In Tables 2–5, N_{H1} denotes derivative of $g_1(x,y)$, and N_{H2} denotes derivative of $g_2(x,y)$. The amounts of computation for derivative of $g_1(x,y)$ in SISO and MIMO are different, so we use N_{H1} in place of the amounts of computation for derivative of $g_1(x,y)$. Similarly, N_{f1} denotes derivative of the objective function, and N_{f2} denotes second derivative of the objective function. Four times of calculation are needed for the second second derivative of the objective function. The objective function is a composite function, so N_{f2} is much larger than N_{f1}.

Table 2. Complexity Analysis for SISO under Perfect Channel Estimation.

Algorithm	Complexity for Each Iteration
ISQP	$16(N_{H1} + N_{H2})$+N_{f1} + 137
SQP	122 + $16(N_{H1} + N_{H2})$+N_{f1} + N_{f2}
BPA	36 N_{f2}+144

Table 3. Complexity Analysis for SISO under Imperfect Channel Estimation.

Algorithm	Complexity for Each Iteration
ISQP	$16(N_{H1} + N_{H2}) + N_{f1} + 186$
SQP	$157 + 16(N_{H1} + N_{H2}) + N_{f1} + N_{f2}$
BPA	$36\ N_{f2}$+186

Table 4. Complexity Analysis for MIMO under Perfect Channel Estimation.

Algorithm	Complexity for Each Iteration
ISQP	$16(N_{H1} + N_{H2}) + N_{f1} + 167$
SQP	$142 + 16(N_{H1} + N_{H2}) + N_{f1}$+$N_{f2}$
BPA	$36\ N_{f2} + 166$

Table 5. Complexity Analysis for MIMO under Imperfect Channel Estimation.

Algorithm	Complexity for Each Iteration
ISQP	$16(N_{H1} + N_{H2}) + N_{f1} + 216$
SQP	$192 + 16(N_{H1} + N_{H2}) + N_{f1} + N_{f2}$
BPA	$36\ N_{f2} + 234$

4. Simulation Results

4.1. Simulation Environment and Discussion

In the simulation experiment for the MIMO communication system, there are two transmitting antennas, two receiving antennas, and two eavesdropping antennas, i.e., $N_A = N_B = N_E = 2$. **H** and **G** are 2×2 Rayleigh fading channels. The distributions of **H** and **G** both have a mean value of 0 and a variance of 0.5. The information-bearing signals are random complex vectors. The transmission power is 10 (i.e., $P = 10$). The Gaussian noise in the channel changes with the SNR. The SNR of **H** increases from 0 to 30, while the SNR of **G** is 5 dB. All Parameters are shown in Table 6.

For the SISO communication system, $N_A = N_R = N_E = 1$ by definition. The information-bearing signals are a random complex number. The SNR of H increases from 0 to 30, while the SNR of G is 5 dB and $P = 10$.

Table 6. Simulation Parameters for MIMO.

Parameter	Value
Number of Transmitting Antennas	2
Number of Receiving Antennas	2
Number of Eavesdropping Antennas	2
Transmission Power	10
Mean of Channel **H** and **G**	0
Variance of Channel **H** and **G**	0.5

4.2. Numerical Simulation and Discussion

Table 7 shows the increase of secrecy capacity after one iteration for SISO under perfect channel estimation. The base value of the iteration step is $\beta = 0.5$. The imperfect channel estimation is not considered here. The secrecy capacity increases the most after one iteration of ISQP, followed closely by SQP. The secrecy capacity of the BPA algorithm has the least increase. The COCOA algorithm, another typical iterative algorithm, is also compared in Tables 7 and 8.

Table 7. Secrecy Capacity Comparison for SISO under Perfect Channel Estimation.

Algorithm	Intial Secrecy Capacity	Optimized Secrecy Capacity ($\beta = 0.5$, One Step)
ISQP	0.3643	0.4243
SQP	0.3643	0.4256
BPA	0.3643	0.3821
COCOA	0.3643	0.4109

Table 8. Complexity Comparison for SISO under Perfect Channel Estimation.

Algorithm	Amount of Computation for Each Iteration	Number of Iterations
ISQP	732	5
SQP	897	5
BPA	6624	13
COCOA	933	7

Table 8 shows the complexity comparison of algorithms for SISO under the perfect channel estimation. BPA leads to the largest calculated amount of computation and the worst optimization result. Such poor performance is owing to the lack of clear search directions for BPA. On the contrary, ISQP has the smallest calculated amount of computation and the best optimization result due to the simplicity of the initial matrix.

According to Tables 7 and 8, the optimization performance of ISQP is similar to that of SQP. However, ISQP requires much less computation. Therefore, we conclude that ISQP is a more effective and thus more desirable algorithm. ISQP and SQP requires fewer iterations than COCOA when $\varepsilon = 1 \times 10^{-6}$. The expression $\varepsilon = 1 \times 10^{-6}$ refers to the two-norm of the gradient rate for BPA and COCOA. Again, BPA requires the most iterations.

Tables 9–11 show the influence of the initial point on the optimization of secrecy capacity. The results are similar across different algorithms. The even distribution of transmission between information-bearing and SCO−AN seems to be the optimal distribution scheme. This result paves the way to an exciting field for future research.

Table 9. Influence of the Initial Point on Secrecy Capacity (ISQP).

Algorithm	(x_0, y_0)	Intial Secrecy Capacity	Optimized Secrecy Capacity
ISQP	(5, 5)	0.5612	0.6312
ISQP	(3, 7)	0.4785	0.5322
ISQP	(1, 9)	0.3821	0.4329

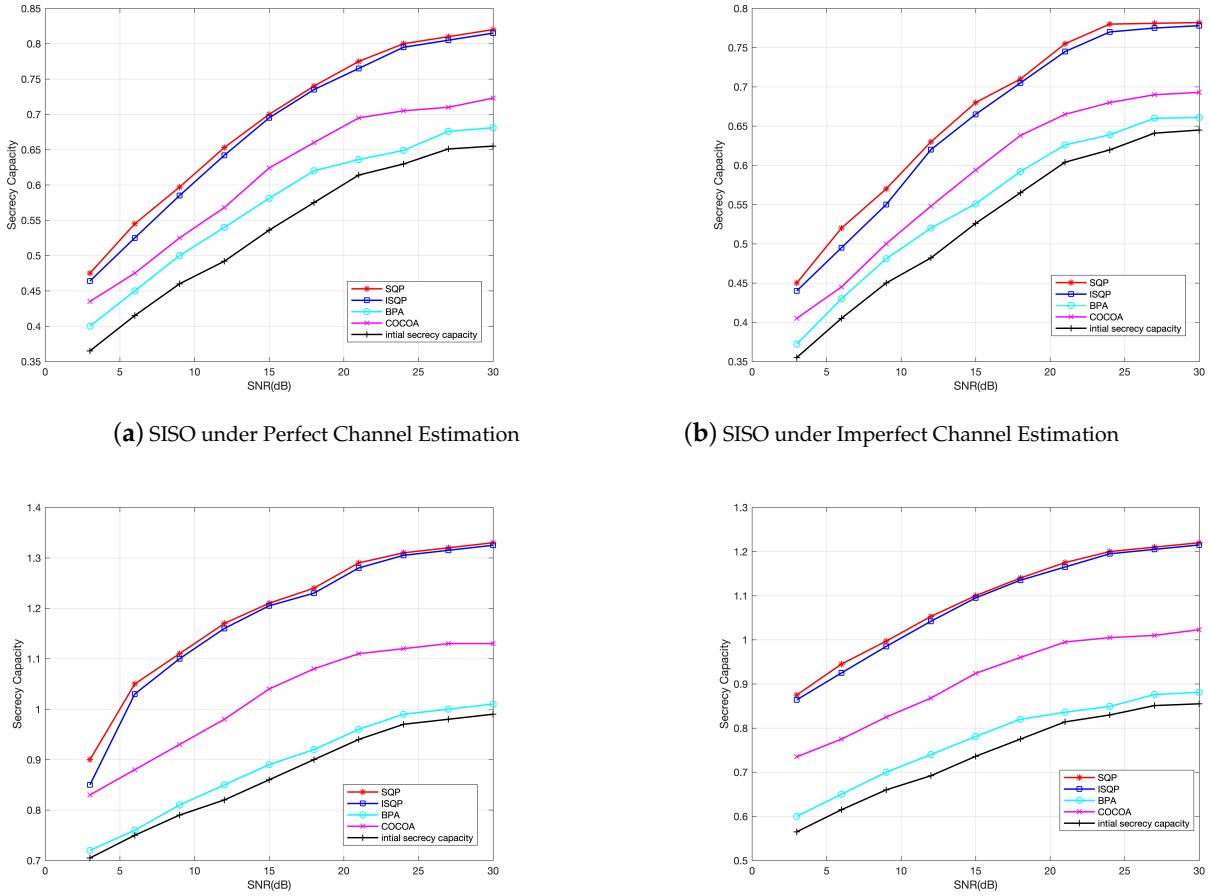
Table 10. Influence of the Initial Point on Secrecy Capacity (SQP).

Algorithm	(x_0, y_0)	Intial Secrecy Capacity	Optimized Secrecy Capacity
SQP	(5, 5)	0.5612	0.6375
SQP	(3, 7)	0.4785	0.5364
SQP	(1, 9)	0.3821	0.4357

Table 11. Influence of the Initial Point on Secrecy Capacity (BPA).

Algorithm	(x_0, y_0)	Intial Secrecy Capacity	Optimized Secrecy Capacity
BPA	(5, 5)	0.5612	0.5924
BPA	(3, 7)	0.4785	0.4922
BPA	(1, 9)	0.3821	0.4012

Figure 4 shows the performance comparison of different algorithms. Figure 4 contains four subfigures, each showing a similar trend in the results. Subfigure (a) shows the optimization performance of SISO under perfect channel estimation versus different SNR. Subfigure (b) shows the optimization performance of SISO under imperfect channel estimation versus different SNR. Subfigure (c) shows the optimization performance of MIMO under perfect channel estimation versus different SNR. Subfigure (d) shows the optimization performance of MIMO under imperfect channel estimation versus different SNR. According to Section 3, BPA requires the most computation and has the worst optimization performance. While SQP and ISQP have similar performance, SQP requires 15% more calculated amounts than ISQP. The optimization performance of COCOA is slightly better than that of BPA, but COCOA is not an excellent iterative algorithm due to the lack of efficacy.



(**a**) SISO under Perfect Channel Estimation

(**b**) SISO under Imperfect Channel Estimation

(**c**) MIMO under Perfect Channel Estimation

(**d**) MIMO under Imperfect Channel Estimation

Figure 4. Comparison of Optimization Performance under Perfect and Imperfect Channel Estimation versus Different SNR.

Figure 5 shows SCO−AN's secrecy capacity with and without allocation versus different SNR. The effects of perfect and imperfect channel estimation are also considered. The SNR of **H** increases from 2 to 30, while the SNR of G is 5 dB. ISQP allocates all the transmission power. In this figure, the solid line shows the lower bound on optimized secrecy capacity. The dashed line shows the lower bound on secrecy capacity without power allocation. The results in Figure 5 are computed according to (6) and (12), and the ISQP algorithm. The results show that the lower bound on secrecy capacity increases with power allocation, implying the high effectiveness of the ISQP algorithm. The secrecy capacity increases with SNR for **H**; that is, a low noise level improves secrecy capacity. The lower bound on the secrecy capacity of SCO−AN decreases when the effect of imperfect channel estimation is taken into consideration. The lower bound on the secrecy capacity with MMSE

channel estimation is greater than the lower bound on that with LS channel estimation. We then reach that the higher channel estimation accuracy enhances secrecy capacity.

Figure 6 shows SCO−AN's secrecy capacity with and without active eavesdropper versus different SNR. The effects of different kinds of channel estimation are also considered. The SNR of **H** increases from 2 to 30, while the SNR of G is 5 dB. ISQP allocates all the transmission power. In this figure, the solid line shows the lower bound on optimized secrecy capacity. The results in Figure 6 are computed according to (43), (47) and (48) and the ISQP algorithm. The results show that the lower bound on secrecy capacity increases with power allocation, implying the high effectiveness of the ISQP algorithm. The secrecy capacity increases with SNR for **H**; that is, a low noise level improves secrecy capacity. The lower bound on the secrecy capacity of SCO−AN decreases when the effect of active eavesdropper is taken into consideration. The lower bound on the secrecy capacity with MMSE channel estimation is greater than the lower bound on that with LS channel estimation.

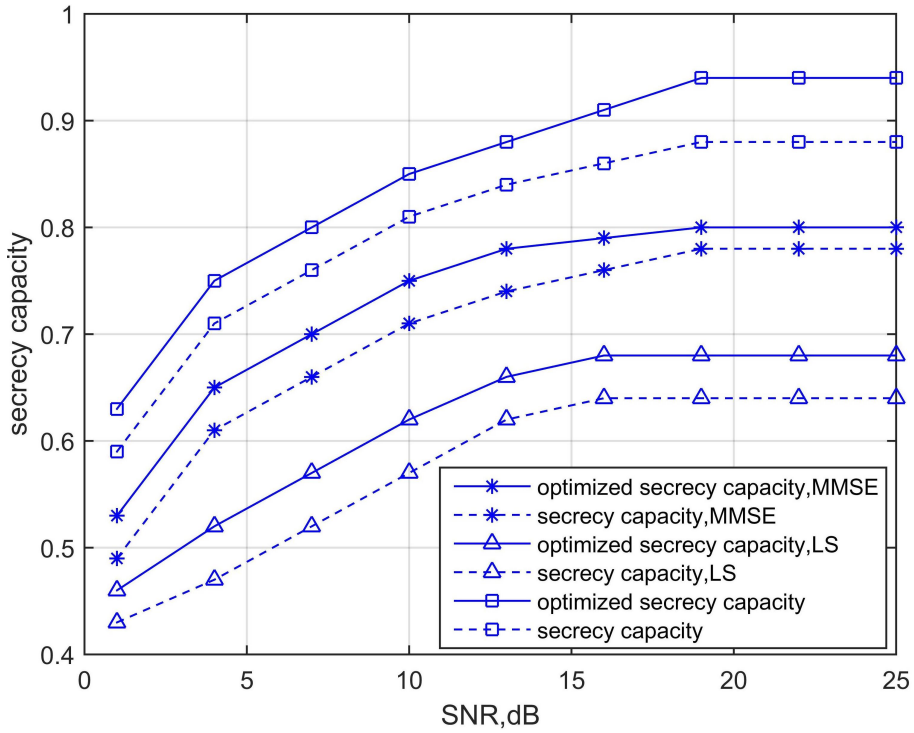


Figure 5. SCO−AN's Secrecy Capacity Before and After Power Allocation versus Different SNR and Channel Estimation Algorithm.

Figure 7 shows SCO−AN's secrecy capacity with active eavesdropper versus different P_E. The effects of different kinds of channel estimation are also considered. The power of P_E increases from 1 to 10, while the P_B is unchanged. ISQP allocates all the transmission power. The results show that the lower bound on secrecy capacity increases with power allocation, implying the high effectiveness of the ISQP algorithm. The secrecy capacity decreases with P_E; that is, a low P_E improves secrecy capacity. The lower bound on the secrecy capacity with MMSE channel estimation is greater than the lower bound on that with LS channel estimation.

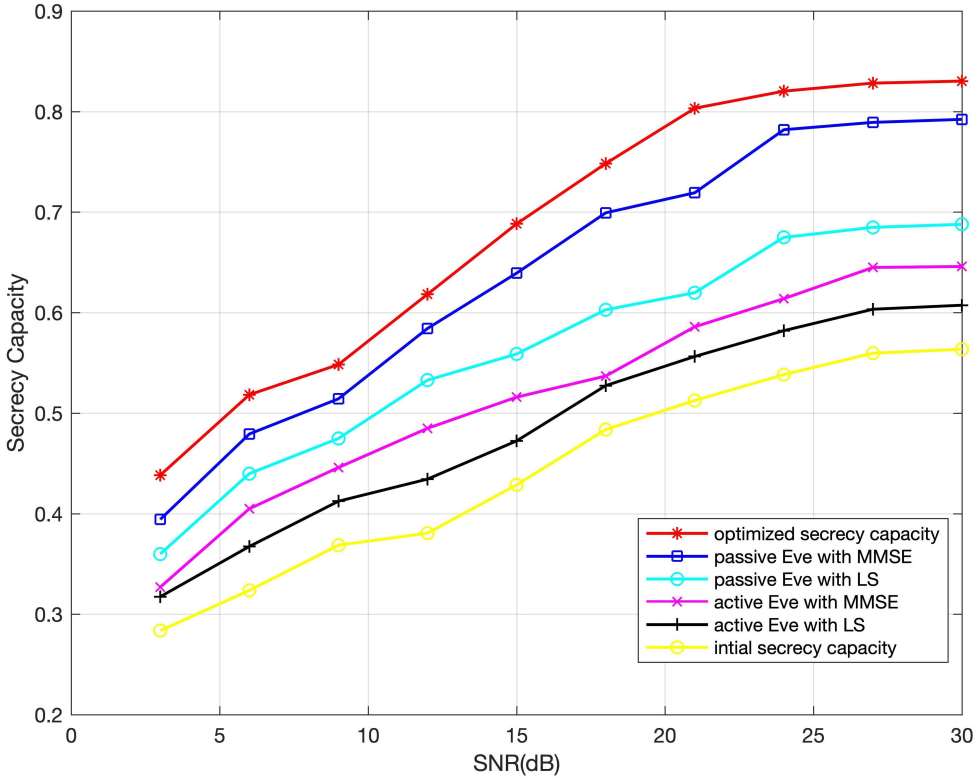


Figure 6. SCO−AN's Secrecy Capacity Before and After Power Allocation versus Different SNR and Channel Estimation Algorithm with and without active eavesdropper.

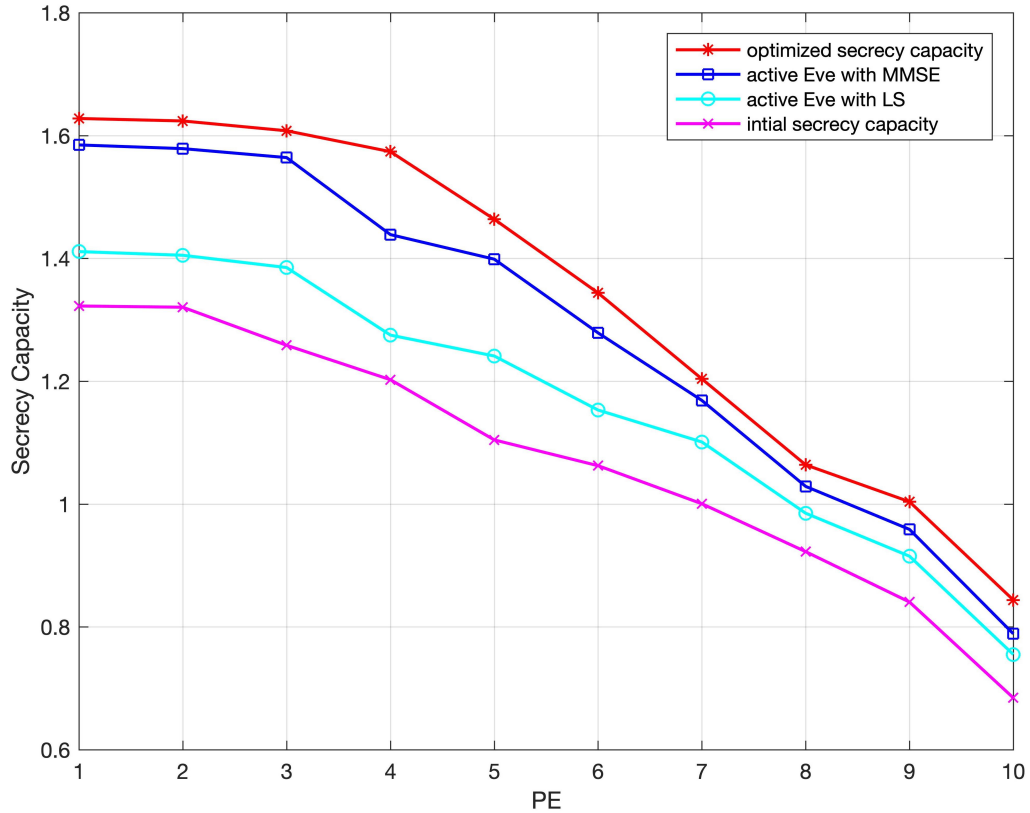


Figure 7. SCO−AN's Secrecy Capacity Before and After Power Allocation versus Different P_E and Channel Estimation Algorithm.

5. Conclusions and Future Work

In this paper, we study the power allocation problems of SCO−AN under perfect and imperfect CSI. First, the power allocation model of SCO−AN with perfect channel estimation is constructed. Then, the effect of the imperfect channel estimation error is examined. The power allocation model of SCO−AN is constructed for the first time in this paper, along with the expression of the imperfect channel estimation's effect on power allocation. The power allocation optimization problem is a crucial contribution to optimizing secrecy capacity under imperfect channel estimation. The power allocation problem's objective function is non-convex, which poses challenges to the solving process. Therefore, we solve this problem by adopting the ISQP algorithm. We compare ISQP with the other three algorithms–SQP, BPA, and COCOA. Although ISQP is slightly worse than SQP in terms of the optimization effect, the ISQP algorithm far exceeds other algorithms. Moreover, ISQP requires the least complex computation. Therefore, we decide to choose the ISQP algorithm. Our simulation results show that the secrecy capacity of SCO−AN wireless communication system increases the most under ISQP algorithm. We then conclude that the ISQP algorithm is the most effective for this purpose.

There is much room for future research. For any optimization problem, there is an upper bound to be reached. What is the upper bound on secrecy capacity for SCO−AN under a specific power? This question lays an exciting background for future research directions. Since 2019, the research on the physical layer security of reflective intelligence surfaces has become a research hotspot. The application of SCO−AN in intelligent reflector technology is one of our future research contents as well. As inspired by many papers, the features of mixing other SCO−AN signals also pose a meaningful research question, such as SCO−AN with interference alignment characteristics and SCO−AN with channel coding characteristics. Among these proposed topics for future studies, we will first study the secrecy capacity's upper bound of SCO−AN.

Author Contributions: Y.G. proposed the framework of the whole algorithm. B.H. handled all the simulations and made all figures and tables in the manuscript. Z.W. was a major contributor in writing the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: The research in this article is supported by "the National Natural Science Foundation of China" Grant nos. 61571167, 61471142, 61102084 and 61601145).

Institutional Review Board Statement: The study was conducted according to the guidelines of the Declaration of Helsinki, and approved by the Institutional Review Board (or Ethics Committee) of NAME OF INSTITUTE (protocol code XXX and date of approval).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Conflicts of Interest: The authors declear that they have no competing interests.

Abbreviations

AN	Artificial Noise
SCO−AN	Secrecy Capacity Optimization Artificial Noise
GAN	Global Artificial Noise
MIMO	Multiple-Input Multiple-Output
SQP	Sequence Quadratic Program
CSI	Channel State Information
KKT	Karush–Kuhn–Tucker
SNR	Signal-to-Noise Ratio

References

1. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 142–149. [CrossRef]
2. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
3. Csiszar, I.; Korner, J. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory* **2003**, *24*, 339–348. [CrossRef]

4. Negi, R.; Goel, S. Secret communication using artificial noise. In Proceedings of the IEEE Vehicular Technology Conference, Dallas, TX, USA, 25–28 September 2005.
5. Goel, S.; Negi, R. Secret communication in presence of colluding eavesdroppers. In Proceedings of the IEEE Military Communications Conference, Atlantic City, NJ, USA, 17–19 November 2005.
6. Dreschler, W.A.; Verschuure, H.; Ludvigsen, C.; Westermann, S. Icra noises: Artificial noise signals with speech-like spectral and temporal properties for hearing instrument assessment. *Int. Audiol.* **2001**, *40*, 148–157. [CrossRef]
7. Goeckel, D.; Vasudevan, S.; Towsley, D.; Adams, S.; Ding, Z.; Leung, K. Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks. *IEEE J. Sel. Areas Commun.* **2001**, *29*, 2067–2076. [CrossRef]
8. Rezki, Z.; Ashish, K.; Mohamed, A. On the secrecy capacity of the wiretap channel with imperfect main channel estimation. *IEEE Trans. Commun.* **2014**, *62*, 3652–3664. [CrossRef]
9. Darsena, D.; Gelli, G.; Iudice, I.; Verde, F. Design and performance analysis of channel estimators under pilot spoofing attacks in multiple-antenna systems. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3255–3269. [CrossRef]
10. Zhou, X.; Maham, B.; Hjorungnes, A. Pilot contamination for active eavesdropping. *IEEE Trans. Wirel. Commun.* **2012**, *11*, 903–907. [CrossRef]
11. Tugnait, J.K. Pilot spoofing attack detection and countermeasure. *IEEE Trans. Commun.* **2018**, *66*, 2093–2106. [CrossRef]
12. Wang, H.M.; Huang, K.W.; Tsiftsis, T.A. Multiple antennas secure transmission under pilot spoofing and jamming attack. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 860–876. [CrossRef]
13. Zhou, X.Y.; Matthew, R.M. Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation. *IEEE Trans. Veh. Technol.* **2010**, *59*, 3831–3842. [CrossRef]
14. Ciuonzo, D.; Augusto, A.; Vincenzo, C. Rician MIMO channel-and jamming-aware decision fusion. *IEEE Trans. Signal Process.* **2017**, *65*, 3866–3880. [CrossRef]
15. Cui, M.; Zhang, G.; Zhang, R. Secure wireless communication via intelligent reflecting surface. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 1410–1414. [CrossRef]
16. Zhou, F.; Chu, Z.; Sun, H.; Hu, R.Q.; Hanzo, L. Artificial noise aided secure cognitive beamforming for cooperative MISO-NOMA using SWIPT. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 918–931. [CrossRef]
17. Jiang, Y.; Zou, Y.; Guo, H.; Zhu, J.; Gu, J. Power allocation for intelligent interference exploitation aided physical-layer security in ofdm-based heterogeneous cellular networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 3021–3033. [CrossRef]
18. Zhao, N.; Yu, F.R.; Li, M.; Leung, V.C. Anti-eavesdropping schemes for interference alignment (IA)-based wireless networks. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 5719–5732. [CrossRef]
19. Cao, Y.; Zhao, N.; Yu, F.R.; Chen, Y.; Liu, X.; Leung, V.C. An anti-eavesdropping interference alignment scheme with wireless power transfer. In Proceedings of the IEEE International Conference on Communication Systems (ICCS), Shenzhen, China, 14–16 December 2016.
20. Wei, L.; Mounir, G.; Bin, C. Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis. *IEEE Commun. Lett.* **2012**, *16*, 1628–1631.
21. Bai, J.; Dong, T.; Zhang, Q.; Wang, S.; Li, N. Coordinated Beamforming and Artificial Noise in the Downlink Secure Multi-Cell MIMO Systems Under Imperfect CSI. *IEEE Wirel. Commun. Lett.* **2020**, *9*, 1023–1026. [CrossRef]
22. Liao, W.C.; Chang, T.H.; Ma, W.K.; Chi, C.Y. Qos-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach. *IEEE Trans. Signal Process.* **2011**, *59*, 1202–1216. [CrossRef]
23. Hong, S.; Pan, C.; Ren, H.; Wang, K.; Nallanathan, A. Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface. *IEEE Trans. Commun.* **2020**, *68*, 7851–7866. [CrossRef]
24. Zhang, X.; Guo, D.; An, K.; Ma, W.; Guo, K. Secure transmission and power allocation in multiuser distributed massive MIMO systems. *Wirel. Netw.* **2020**, *26*, 941–954. [CrossRef]
25. Ding, Q.; Xi, T.; Lian, Y. Joint Power Allocation Scheme for Distributed Secure Spatial Modulation in High-Speed Railway. *IEEE Syst. J.* **2020**. [CrossRef]
26. Niu, H.; Lei, X.; Xiao, Y.; Liu, D.; Li, Y.; Zhang, H. Power Minimization in Artificial Noise Aided Generalized Spatial Modulation. *IEEE Commun. Lett.* **2020**, *24*, 961–965. [CrossRef]
27. Meng, L.; Wang, Q.; Ji, Z.; Nie, M.; Ji, B.; Li, C.; Song, K. Resource allocation on secrecy energy efficiency for C-RAN with artificial noise. *Wirel. Netw.* **2020**, *26*, 639–650. [CrossRef]
28. Singh, P.; Trivedi, A. NOMA and massive MIMO assisted physical layer security using artificial noise precoding. *Phys. Commun.* **2020**, *39*, 100977. [CrossRef]
29. Gu, Y.; Wu, Z.; Yin, Z.; Zhang, X. The Secrecy Capacity Optimization Artificial Noise: A New Type of Artificial Noise for Secure Communication in MIMO System. *IEEE Access* **2019**, *7*, 58353–58360.
30. Mo, D.; Duarte, M.F. Multi-Branch Binary Modulation Sequences for Interferer Rejection. In Proceedings of the IEEE Statistical Signal Processing Workshop (SSP), Freiburg, Germany, 10–13 June 2018.
31. Bidabadi, S.; Omidi, M.J.; Kazemi, J. Energy efficient power allocation in downlink OFDMA systems using SQP method. In Proceedings of the Iranian Conference on Electrical Engineering, Shiraz, Iran, 10–12 May 2016.