SCO-AN:Improve Secrecy Capacity for Secure Transmission Using Power Allocation

Yebo Gu (280968341@qq.com)
harbin institue of technology https://orcid.org/0000-0002-4847-7567
Zhilu Wu
Harbin Institute of Technology
Zhendong Yin
Harbin Institute of Technology
Bowen Huang
jushri Technologies,INC

Research

Keywords: physical layer security, artificial noise, secrecy capacity optimization artificial noise, power allocation

Posted Date: March 16th, 2020

DOI: https://doi.org/10.21203/rs.3.rs-17295/v1

RESEARCH

SCO-AN:Improve Secrecy Capacity for Secure Transmission Using Power Allocation

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

Abstract

Artificial noise(AN) is a core technique in physical layer security field which has been widely studied.AN reduces the channel capacity of eavesdroppers without affecting the channel capacity of the communicator so that AN can increase secrecy capacity.Secrecy capacity is defined as channel capacity of the communicator minus channel capacity of eavesdroppers.The AN is prohibited from affecting the channel capacity of the legal receiving channel. This condition brings good performance to AN as well as limitations.Recently, the secrecy capacity optimization artificial noise (SCO-AN) is proposed to increase the secrecy capacity more effectively.SCO-AN can reduce the channel capacity of the communicator to a small extent while greatly reducing the channel capacity of the eavesdropper. So, SCO-AN can further expand the secrecy capacity on the basis of AN. Due to the limitation of transmit power, SCO-AN cannot be added indefinitely, so it is an important issue to increase the secrecy capacity as much as possible under a certain power limit.In this paper, a secrecy capacity function with SCO-AN added under certain power constraints is established.Because this function is non-convex, the traditional convex optimization algorithm cannot be applied. A sequence quadratic program(SQP) is adopted to solve this power allocation problem.Simulation results show that SQP can effectively improve the secrecy capacity under a certain power limit.

Keywords: physical layer security; artificial noise; secrecy capacity optimization artificial noise; power allocation

1 Introduction

Information technology has developed rapidly in recent years. As people demand higher information transmission speeds, more requirements have been put forward for the secure transmission of information. The information encryption technology is used to realize the secure transmission of information for a long time. Due to the limitation of computing speed, the encrypted information is difficult to decipher.With the development of computer technology, the deciphering of information has become more and more simple. In theory, as long as the computer's calculation speed is fast enough, there is no encrypt information that cannot be deciphered. So traditional information encryption techniques have encountered limitations. The emergence of physical layer security technology has proposed new methods for solving information security problems.

*Correspondence: felton20@163.com
[1]School of Electronics and Information Engineering, Harbin Institute of Technology , Xidazhi street, 150001 harbin, China
Full list of author information is available at the end of the article
†Equal contributor

The physical layer security technology is fundamentally different from the information encryption technology. The physical layer security technology is mainly based on the randomness of the transmission channel. The use of coding and modulation technology to realize the secure transmission of information is an important research content for the realization of wireless network security in the next generation of communications. Beamforming and artificial noise are the main technologies for achieving physical layer security. Beamforming is mainly used to encode the transmitted information to "point" the receiver to reduce the information received by eavesdroppers. Artificial noise is to add a signal in the eavesdropper's channel that has no effect on the transmission channel so that the signal received by the eavesdropper is disturbed. In the physical layer security technology, the capacity is usually used to judge the quality of the physical layer technology. In the AN and beamforming technology, secrecy capacity refers to the difference between the channel capacity of the legitimate receiver and the channel capacity of the eavesdropper.

The research on the secrecy capacity of eavesdropping channel is the basis of the research on the physical layer security technology, and also the guidance of the research on the physical layer information security mechanism. If the secrecy capacity is greater than zero, it means that part of the information cannot be received by the eavesdropper which means part of the information can not be "deciphered". In summary, one of the goals of the physical layer security technology is to maximize the secrecy capacity.

The study of physical layer security originated from Shannon. In his paper, unconditional confidential transmission is proposed, which is also the ultimate goal of physical layer security technology research [1]. After shannon, Wyner first researched the secure transmission of information from the perspective of information theory. Wyner defines the communication model with the eavesdropping channel, and secrecy capacity was also first proposed in his paper [2]. Csiszer and Korner continue to study the physical layer security technology on the basis of wyner, in paper [3], a broadcast channel model with confidential messages is proposed to extend Wyner's work. For a long time in the past, the physical layer security technology has not been concerned. Until the application of Multiple-Input Multiple-Out-put(MIMO) technology, physical layer security technology has developed rapidly. In particular, the proposal of artificial noise technology makes the physical layer security technology easier to apply to MIMO technology [4]. AN technology adds a signal the transmitted signal which is orthogonal to the legitimate channel. The additional signal does not affect the capacity of legitimate channel, but it will reduce the channel capacity of the eavesdropper and increase the secrecy capacity of the wireless communication system.

On the basis of AN technology, scholars have done a lot of outstanding work. The optimal power allocation for artificial noise and achievable rates in MIMO-OFDM wiretap communication system are proposed in [5]. In [6] and [7], The artificial noise and interference alignment technology are creatively merged together, and artificial noise with interference alignment characteristics is proposed, which expands the application field of artificial noise. In [8], the upper limit of the secrecy capacity of artificial noise wireless communication systems subject to transmit power is proposed.

AN technology has excellent performance. Because AN is orthogonal to legitimate channel so that the legal channel is not affected. There is no need to add any additional signal processing device to the receiver. At the same time, the eavesdropper's channel capacity is reduced effectively. We assume that the channel capacity of the legitimate channel is A and the channel capacity of the eavesdropper is B. The principle of AN is to reduce B so that the difference between A and B becomes larger while keeping A unchanged.

In our previous work [9], the secrecy capacity optimization artificial noise(SCO-AN) is proposed. SCO-AN adds an additional signal-global artificial noise (GAN) to the signal based on AN. The role of GAN is to reduce the small part of A and reduce the B by a large amount. So the difference between A and B is enlarged. SCO-AN is a tool to convert the noise immunity of communication systems into secrecy capacity. When we transmit important information, we can use the anti-noise ability encoding technology to send confidential information, and at the same time add GAN to the channel to interfere with the eavesdropper as much as possible to achieve confidential transmission.

Limited by the transmit power of the antenna system, it is an important issue to maximize the secrecy capacity with limited power. Therefore, we study the power allocation problem of SCO-AN in this paper. Because the Hessian matrix of the SCO-AN power allocation function is not positive definite, SCO-AN power allocation function is a non-convex function. The maximum value of the SCO-AN power allocation function can not be obtained by gradient descent method. In this paper, an iterative method is used to find the extreme value of the power allocation function within a certain range. The main contributes of this paper are summarized as follows:

- In this paper, in order to use the limited transmission power to maximize the secrecy capacity, the power allocation problem of SCO-AN is described for the first time, and the optimization conditions of the power allocation function are strictly limited to ensure that the optimization results meet the realistic constraints.
- Based on [9], the design of SCO-AN has been changed. SCO-AN and AN have a common basis. This greatly simplifies the calculation of the power allocation algorithm and improves the operation efficiency of the algorithm.
- Due to the numerous and complicated constraints, it is difficult for traditional iterative algorithms to guarantee the validity of the calculation. So in this paper, an iterative algorithm is used to optimize the objective function of SCO-AN. Simulation results prove that this iterative algorithm is very effective.

Paper structure is as follows: In section 2, the artificial noise and analyzed its technical principles are introduced briefly. In the third section, we introduced the secrecy capacity optimization artificial noise and briefly analyzed its advantages over artificial noise. The power problem of SCO-AN is explained in detail.

The model of SCO-AN power allocation is first proposed, and its convergence is also analyzed in detail. At the same time, the SQP algorithm is explained in section 3. we introduced the algorithm flow of SCO-AN using SQP algorithm. Simulation results are shown in section 4, and conclusions are drawn in section 5.

2 Method

2.1 system model

Figure 1 the wireless communication model with eavesdropper

In this section, we introduce AN and SCO-AN technology in detail.

Fig.1 shows a wireless communication system model with information sender, legitimate receiver and eavesdroppers. In this model, Alice(A) is the sender of the signal, Bob(B) is the legitimate receiver of signal, and Eve(E) is the eavesdropper who taps signal. Here we assume that A has N_A transmitting antennas, B has N_B receiving antennas, and eavesdropper E has N_E receiving antennas. $\mathbf{H}$ is the channel state information(CSI) of legitimate channel(A to B), $\mathbf{G}$ is CSI of eavesdropper channel(Alice to Eve). Channel estimation is usually performed to obtain channel state information by inserting pilots into the transmitted signal.As shown in FIG. 1, for the convenience of discussion, a feedback channel is set between A and B. A can obtain the channel state information H from B accurately without delay. At the same time, we also assume that G can be accurately obtained by A without delay. $\mathbf{H}_t$ and $\mathbf{G}_t$ are the CSI of H and G at time t. The element $h_{i,j}(g_{i,j})$ in H(or G) represnts the channel gain between the i_{th} transmitter antenna and the j_{th} receiver(eavesdropper) antenna. $\mathrm{x}_t \in \mathbb{C}^{N_\mathbf{A}}$ represents the signal sent by Alice at time slot t, $\mathrm{y}_t \in \mathbb{C}^{N_\mathbf{B}}$ represents the signal received by Bob at time slot t,$\mathrm{z}_t \in \mathbb{C}^{N_\mathbf{E}}$ represents the signal received by Eve at time slot t,respectively, so that

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

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

Where $\mathbf{n}_t$ and $\mathbf{e}_t$ are independent and identically distributed(i.i.d) additive white Gaussian noise(AWGN) with variance of σ_n^2 and σ_e^2. The block fading is assumed to exist so that each element in $\mathbf{H}_t$ and $\mathbf{G}_t$,$\mathbf{H}_\mathrm{t} \in \mathbb{C}^{\mathbf{N}_A\times\mathbf{N}_B}$,$\mathbf{G}_\mathrm{t} \in \mathbb{C}^{\mathbf{N}_A\times\mathbf{N}_E}$.$h_{i,j}$ $g_{i,j}$ are independent complex constants. $h_{i,j}$ and $g_{i,j}$ are assumed to be independent complex constants. For convenience of discussion, the channel estimation of $\mathbf{H}_t$ and $\mathbf{G}_t$ is assumed to be error-free.The maximum transmitting power is assumed to be P_0 , $E[\mathrm{x}_t^\dagger \mathrm{x}_t] \le P_0$.

The secrecy capacity of the communication model with eavesdroppers is[3]:

$$\mathrm{SecrecyCapacity} = \log(1+\frac{|\mathbf{H}_\mathrm{t}x_\mathrm{t}|^2}{\sigma_\mathrm{n}^2}) - \log(1+\frac{|\mathbf{G}_\mathrm{t}x_\mathrm{t}|^2}{\sigma_\mathrm{e}^2}), \tag{3}$$

Secrecy capacity of the MIMO communication system is the difference between capacity of H and capacity of G.

2.2 the artificial noise

Since AN(w_t) is orthogonal to H($H_t w_t = 0$), AN does not affect Bob's reception of information. For Eve, AN is a noise that will reduce Eve's channel capacity. So Alice sends AN $\mathrm{w}_t \in \mathbb{C}^{N_\mathbf{A}}$ while sending the normal signal s_t so that

$$\mathbf{x}_t = \mathbf{w}_t + \mathbf{s}_t, \tag{4}$$

w_t is artificial noise which designed to put in the null space of H_t so that $\mathrm{H}_t\mathrm{w}_t$=0. Z_t is an standard orthonormal basis for H_t and v_t satisfies $\mathbf{w}_t = \mathbf{Z}_t\mathbf{v}_t$ and $\mathrm{Z}_t^\dagger\mathrm{Z}_t = I$, v_t is a complex random variables with variance of σ_t^2. So the signals received by Bob and Eve are:

$$\begin{aligned}\mathbf{z}_t &= \mathbf{H}_t\mathbf{x}_t + \mathbf{n}_t \\ &= \mathbf{H}_t\mathbf{w}_t + \mathbf{H}_t\mathbf{s}_t + \mathbf{n}_t, \\ &= \mathbf{H}_t\mathbf{s}_t + \mathbf{n}_t,\end{aligned} \tag{5}$$

$$\mathbf{y}_t = \mathbf{G}_t\mathbf{s}_t + \mathbf{G}_t\mathbf{w}_t + \mathbf{e}_t, \tag{6}$$

y_t is the signal received by Eve and z_t is the signal received by Bob. Because w_t is in the null space of $\mathbf{H}_t$, artificial noise has no effect on Bob, while Eve is affected by AN when receiving information due to extra artificial noise in the received signals.

In [4], the transmitted signal is designed to be $\mathbf{s}_t = \mathbf{p}_t\mathbf{u}_t$ where u_t is the information signal and p_t obeys the independent Gaussian distribution. p_t is designed to satisfy the following conditions a)$\mathbf{H}_t\mathbf{p}_t \neq 1$,b)$\|\mathbf{p}_t\| = 1$.

So the lower bound of secrecy capacity after adding artificial noise is :

$$\begin{aligned}&\mathrm{SecrecyCapacity}_t \ge C_{sec}^a = I(Z;U) - I(Y;U) \\ &= \log(1+\tfrac{|\mathbf{H}_t\mathrm{p}_t|^2\sigma_u^2}{\sigma_n^2}) - \log(1+\tfrac{|\mathbf{G}_t\mathrm{p}_t|^2\sigma_u^2}{\mathrm{E}|\mathbf{G}_t\mathrm{w}_t|^2+\sigma_e^2}),\end{aligned} \tag{7}$$

where $\mathrm{E}|\mathbf{G}_t\mathbf{w}_t|^2 = (\mathbf{G}_t\mathbf{Z}_t\mathbf{Z}_t^\dagger\mathbf{G}_t^\dagger)\sigma_t^2$.

Notation: $\mathrm{A}^{\dagger}$ denotes the conjugate transpose of matrix A. $\mathbb{C}^{M\times N}$ represents the space of complex $M\times N$ matrices.E$(\cdot)$ represents the expectations.

2.3 the secrecy capacity optimization artificial noise

One of the goals of physical layer security is to increase the secrecy capacity of the communication system as much as possible. In a communication system with eavesdroppers, since the channel capacity of a legitimate receiver cannot be increased, only the channel capacity of the eavesdropper can be reduced. The essence of artificial noise is to reduce the capacity of eavesdroppers while maintaining the legitimate channel capacity. Inspired by AN, we added an additional artificial noise to the wireless communication system-the secrecy capacity optimization artificial noise (SCO-AN). SCO-AN reduces the legal channel capacity on the basis of AN while the capacity of eavesdropping channels is greatly reduced to increase the system's secrecy capacity.

With the development of communication technology and the emergence of new channel coding technology, the anti-noise performance of wireless communication systems has been greatly improved, which provides suitable conditions for the application of SCO-AN technology. SCO-AN can greatly increase the secrecy capacity of the system while increasing the noise of the system slightly.

SCO-AN consists of artificial noise and global artificial noise(GAN). Alice sends SCO-AN ($\mathbf{w}_g$) while sending the normal signal

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

Where s_t represents the signal sent by Alice and $\mathrm{w}_g \in \mathbb{C}^{N_{\mathbf{A}}}$ consists of GAN and artificial noise:

$$\mathbf{w}_g = \mathbf{w}_t + \mathbf{w}_m, \tag{9}$$

$\mathrm{w}_m \in \mathbb{C}^{N_{\mathbf{A}}}$ represents GAN which improves the secrecy capacity of the system and $\mathrm{w}_t \in \mathbb{C}^{N_{\mathbf{A}}}$ represents the artificial noise. To facilitate calculations, we assume that $\mathrm{w}_m = \mathrm{Z}_t\mathrm{v}_m$ and Z_t is a standard orthonormal basis for H_t which is described in second section. v_m is designed to be i.i.d complex random variables with variance σ_m^2. So the messages received by the Alice and Bob are :

$$\mathbf{z}_t = \mathbf{H}_t\mathbf{s}_t + \mathbf{H}_t\mathbf{w}_g + \mathbf{n}_t, \tag{10}$$

$$\mathbf{y}_t = \mathbf{G}_t\mathbf{s}_t + \mathbf{G}_t\mathbf{w}_g + \mathbf{e}_t, \tag{11}$$

Because of $\mathbf{H}_t\mathbf{w}_t$=0, so

$$\begin{aligned}\mathbf{z}_t &= \mathbf{H}_t\mathbf{s}_t + \mathbf{H}_t\mathbf{w}_g + \mathbf{n}_t = \mathbf{H}_t\mathbf{s}_t + \mathbf{H}_t\mathbf{w}_t + \mathbf{w}_m + \mathbf{n}_t \\ &= \mathbf{H}_t\mathbf{s}_t + \mathbf{H}_t\mathbf{w}_t + \mathbf{H}_t\mathbf{w}_m + \mathbf{n}_t \\ &= \mathbf{H}_t\mathbf{s}_t + \mathbf{H}_t\mathbf{w}_m + \mathbf{n}_t,\end{aligned} \tag{12}$$

$$\begin{aligned}\mathbf{y}_t &= \mathbf{G}_t\mathbf{s}_t + \mathbf{G}_t\mathbf{w}_g + \mathbf{e}_t \\ &= \mathbf{G}_t\mathbf{s}_t + \mathbf{G}_t(\mathbf{w}_t + \mathbf{w}_m) + \mathbf{e}_t \\ &= \mathbf{G}_t\mathbf{s}_t + \mathbf{G}_t\mathbf{w}_t + \mathbf{G}_t\mathbf{w}_m + \mathbf{e}_t\end{aligned} \tag{13}$$

So the lower bound of secrecy capacity after adding SCO-AN is:

$$\begin{aligned}&\mathrm{Secrecy_s} \geq C_{\mathrm{sec}^a} = I(Z;U) - I(Y;U) \\ &= \log(1 + \tfrac{|\mathbf{H}_t p_t|^2\sigma_u^2}{\sigma_n^2 + E|\mathbf{H}_t w_m|^2}) - \log(1 + \tfrac{|\mathbf{G}_t \mathbf{p}_t|^2\sigma_u^2}{\mathrm{E}|\mathbf{G}_t\mathbf{w}_t|^2 + \mathrm{E}|\mathbf{G}_t\mathbf{w}_m|^2 + \sigma_e^2}),\end{aligned} \tag{14}$$

where $\mathrm{E}|\mathbf{H}_t\mathbf{w}_m|^2 = (\mathbf{H}_t\mathbf{Z}_t\mathbf{Z}_t^{\dagger}\mathbf{H}_t^{\dagger})\sigma_m^2$,
$\mathrm{E}|\mathbf{G}_t\mathbf{w}_t|^2 = (\mathbf{G}_t\mathbf{Z}_t\mathbf{Z}_t^{\dagger}\mathbf{G}_t^{\dagger})\sigma_t^2$,$\mathrm{E}|\mathbf{G}_t\mathbf{w}_m|^2 = (\mathbf{G}_t\mathbf{Z}_t\mathbf{Z}_t^{\dagger}\mathbf{G}_t^{\dagger})\sigma_m^2$.

From the previous discussion, it is obvious that H_t, G_t, p_t and Z_t are known. So $\mathbf{G}_t\mathbf{Z}_t\mathbf{Z}_t^{\dagger}\mathbf{G}_t^{\dagger}$, $|\mathbf{H}_t p_t|^2$, $|\mathbf{G}_t p_t|^2$ and $\mathbf{H}_t\mathbf{Z}_t\mathbf{Z}_t^{\dagger}\mathbf{H}_t^{\dagger}$ are constants that can be calculated. We assume that $|\mathbf{H}_t p_t|^2 = H_p^t$,$|\mathbf{G}_t p_t|^2 = G_p^t$,$\mathbf{H}_t\mathbf{Z}_t\mathbf{Z}_t^{\dagger}\mathbf{H}_t^{\dagger} = H_z^t$ and $\mathbf{G}_t\mathbf{Z}_t\mathbf{Z}_t^{\dagger}\mathbf{G}_t^{\dagger} = G_z^t$. H_p^t , G_p^t , H_z^t and G_p^t are constants. In order to express the gain of the SCO-AN to the system conveniently, C_t represents the change in the secrecy capacity of the system after adding the SCO-AN. We subtract (7) from (14), so the increments of secrecy capacity after adding SCO-AN is:

$$\begin{aligned}C_t = &\log_2(1 + \tfrac{H_p^t\sigma_u^2}{H_z^t\sigma_m^2 + \sigma_n^2}) - \log_2(1 + \tfrac{G_p^t\sigma_u^2}{G_z^t(\sigma_m^2 + \sigma_t^2) + \sigma_e^2}) \\ &-[(\log_2(1 + \tfrac{H_p^t\sigma_u^2}{\sigma_n^2}) - \log_2(1 + \tfrac{G_p^t\sigma_u^2}{G_z^t\sigma_t^2 + \sigma_e^2})],\end{aligned} \tag{15}$$

To ensure that SCO-AN is valid, C_t should be greater than zero. In (15), C_t is a non-convex function about σ_m^2, so the extreme values of C_t can be obtained within a certain range, which is analyzed in detail in the paper [9]. In other words, SCO-AN can be added to the communication system without limit theoretically. However, it is impossible because the unlimited addition of noise will reduce the communication quality of the system and even cause communication failure, so we can only Add SCO-AN within the range allowed by the system's noise immunity.

3 Power allocation problem of SCO-AN

The transmission power of wireless communication systems is limited. It is very important to get the max-

imum secrecy capacity under the limited transmission power.

We assume the power per transmission is P. Since $\|\mathbf{p}_t\|=1$ and Z_t are standard orthonormal basis for H_t, So

$$\sigma_m^2+\sigma_t^2+\sigma_u^2\le P, \tag{16}$$

we assume that x denotes σ_u^2, y denotes σ_m^2 and z denotes σ_t^2 and the initial state of x, y, z before power allocation is x_0, y_0,z_0. The secrery capacity that only adds AN without power allocation is P0. So

$$\log_2(1+\frac{H_p^t x_0}{\sigma_n^2})-\log_2(1+\frac{G_p^t x_0}{G_z^t z_0+\sigma_e^2})=P_0 \tag{17}$$

So the power distribution problem of SCO-AN is written as:

$$\begin{aligned}
\min\ & \log_2(1+\tfrac{G_p^t x}{G_z^t(p-x)+e})-\log_2(1+\tfrac{H_p^t x}{H_z^t y+n})\\
s.t\ & \log_2(1+\tfrac{G_p^t x}{G_z^t z+e})-\log_2(1+\tfrac{H_p^t x}{H_z^t y+n})\\
& -\log_2(1+\tfrac{H_p^t x}{n})+\log_2(1+\tfrac{G_p^t x}{G_z^t(p-x)+e})>0\\
& \log_2(1+\tfrac{H_p^t x}{n})-\log_2(1+\tfrac{G_p^t x}{G_z^t z+e})>P_0\\
& x+y+z\le P\\
& x>0\\
& y>0\\
& z>0
\end{aligned} \tag{18}$$

In (18), condition $\log_2(1+\frac{H_p^t x}{n})-\log_2(1+\frac{G_p^t x}{G_z^t z+e})>P_0$ is added when setting the limit function. Bacause the role of the original framework should not be reduced in the optimization of a large range, so the secrecy capacity of AN should not be reduced.

The hessian matrix of the objective function is non-positive definite, so the extremum of the objective function can not be obtained by the method of partial derivative. An sequence quadratic program(SQP) is adopted to optimize power allocation to maximize system secrecy capacity. The basic idea of SQP is: at each iterative step, a quadratic programming subproblem is solved to establish a descent direction to reduce the value function to obtain compensation, and these steps are repeated until the original problem solution is obtained.

The Lagrange function of (18) is:

$$\begin{aligned}
&L(x,y,z,\mu,\lambda)=f(x,y,z)-\mu_1 h_1(x,y,z)\\
&-\sum_{j=1,2,3,4,5}\lambda_j g_j(x,y,z),
\end{aligned} \tag{19}$$

where

$$\begin{aligned}
f(x,y,z)=\ & \log_2(1+\tfrac{G_p^t x}{G_z^t(p-x)+e})-\log_2(1+\tfrac{H_p^t x}{H_z^t y+n})\\
g_1(x,y,z)=\ & \log_2(1+\tfrac{G_p^t x}{G_z^t z+e})-\log_2(1+\tfrac{H_p^t x}{H_z^t y+n})\\
& -\log_2(1+\tfrac{H_p^t x}{n})+\log_2(1+\tfrac{G_p^t x}{G_z^t(p-x)+e})\\
g_2(x,y,z)=\ & \log_2(1+\tfrac{H_p^t x}{n})-\log_2(1+\tfrac{G_p^t x}{G_z^t z+e})-P_0\\
g_3(x,y,z)=\ & x\\
g_4(x,y,z)=\ & y\\
g_5(x,y,z)=\ & z\\
h_1(x,y,z)=\ & x+y+z-P
\end{aligned} \tag{20}$$

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

$$\begin{aligned}
&\tfrac{\partial L}{\partial X}\big|_{x=x^*}=0 && (a)\\
&\lambda_j\ne 0, && (b)\\
&u_t\ge 0, && (c)\\
&u_t g_t(x*)=0, && (d)\\
&h_i(x*)=0 \qquad i=1 && (e)\\
&g_j(x*)=0 \qquad j=1,2,3,4,5 && (f)
\end{aligned} \tag{21}$$

(21) are Karush–Kuhn–Tucker conditions(KKT conditions), (a) is a necessary condition when the extreme value of Lagrange function is taken, (b) is Lagrange coefficient constraint, (c) is inequality constraint case, and (d) is complementary Relaxation conditions, (e) and (f) are the original constraints.

For general problems, the KKT condition is a necessary condition for a set of solutions to be the optimal solution. When the original problem is a convex problem, the KKT condition is a sufficient condition as well.

Regarding condition (c), We construct the $L(x,\lambda,\mu)$ function, we hope $L(x,\lambda,\mu)\le f(x)$. In $L(x,\lambda,\mu)$, μ is 0, so λ is less than or equal to 0, and the coefficient 0 must be satisfied, which is the condition (c) as well.

Regarding condition (d), the minimum value of $L(x,\lambda,\mu)$must be the minimum value of the three formula terms, and the minimum value of the third term is when the value is equal to 0.

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

$$\begin{aligned}
\min\ & \tfrac{1}{2}d^T B_t d+\nabla f(x_t,y_t,z_t)^T d\\
s.t\ & h(x_t,y_t,z_t)+A_t^{\varepsilon} d=0\\
& g(x_t,y_t,z_t)+A_t^{\Gamma} d\ge 0,
\end{aligned} \tag{22}$$

where $A_t^{\varepsilon}=\nabla h(x_t,y_t,z_t)$,$A_t^{\Gamma}=\nabla g(x_t,y_t,z_t)$,$B_t$ is a positive definite matrix, d_t is optimal solution of quadratic programming subproblems.

Theorem 3.1 *A KKT point x^* of the optimization constraint problem and its corresponding Lagrangian multiplier vector$\lambda^*, \mu^* \geq 0$. Assuming at x, the following conditions hold:*

(1)Effectively constrained jacobi matrix is row full rank.

(2)The strict complementary relaxation condition holds, that is, $g_i(x^*) \geq 0, \lambda_i^* \geq 0, g_i(x^*)\lambda_i^* = 0, g_i(x^*) + \lambda_i^* > 0$.

(3)A sufficient second-order optimality condition holds, that is, for any vector $d \neq 0$ that satisfies $A(x^*)d = 0$, The following conditions are true:

$$d^T B(x^*, \mu^*, \lambda^*)d > 0$$

where $B(x, \mu, \lambda)$ is a positive definite matrix, If (x_t, μ_t, λ_t) is sufficiently close to (x^*, μ^*, λ^*), the quadratic programming sub-problem (22) 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^*.

Using Karush-Kuhn-Tucker Conditions, (21)is equivalent to:

$$H_1(d, \mu, \lambda) = B_t - (A_t^{\varepsilon})^T \mu - (A_t^{\Gamma})^T \lambda + \nabla f(x_t, y_t, z_t), \tag{23}$$

$$H_2(d, \mu, \lambda) = h(x_t, y_t, z_t) + (A_t^{\varepsilon})^T d, \tag{24}$$

$$\begin{aligned} &\lambda \geq 0, \\ &g(x_t, y_t, z_t) + A_t^{\Gamma} d \geq 0, \\ &\lambda[g(x_t, y_t, z_t) + A_t^{\Gamma} d] = 0, \end{aligned} \tag{25}$$

Note that formula (19) is a linear complementarity problem, we define smooth FB-function:

$$\varphi(\varepsilon, a, b) = a + b - \sqrt{a^2 + b^2 + 2\varepsilon^2}, \tag{26}$$

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

$$\Phi(\varepsilon, d, \lambda) = (\varphi_1(\varepsilon, d, \lambda), \varphi_2(\varepsilon, d, \lambda) ... \varphi_m(\varepsilon, d, \lambda))^T, \tag{27}$$

in (26),

$$\begin{aligned} \varphi_i(\varepsilon, d, \lambda) = \lambda_i + [g_i(x_t) + (A_t^{\Gamma})_i d] \\ - \sqrt{\lambda_i^2 + [g_i(x_t) + (A_t^{\Gamma})_i d]^2 + 2\varepsilon^2}, \end{aligned} \tag{28}$$

Where $(A_t^{\Gamma})_i$ is the i-th row of A_t^{Γ}. (21) and (22) are equivalent to

$$H(z) := H(\varepsilon, d, \mu, \lambda) = \begin{pmatrix} \varepsilon \\ H_1(d, \mu, \lambda) \\ H_2(d, \mu, \lambda) \\ \Phi(\varepsilon, d, \lambda) \end{pmatrix} = 0, \tag{29}$$

the Jacobian matrix of (H_z) is

$$H'(z) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & B_t & -(A_t^{\varepsilon})^T & -(A_t^{\Gamma})^H \\ 0 & A_t^{\varepsilon} & 0 & 0 \\ \nu & D_2(z)A_t^{\Gamma} & 0 & D_1(z) \end{pmatrix}, \tag{30}$$

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

$$\nu_i = -\frac{2\varepsilon}{\sqrt{\lambda_i^2 + [g_i(x_t) + (A_t^{\Gamma})_i d]^2 + 2\varepsilon^2}}, \tag{31}$$

$$\begin{aligned} D_1(z) = diag(a_1(z), a_2(z), ..., a_m(z)), \\ D_2(z) = diag(b_1(z), b_2(z), ..., b_m(z)), \end{aligned} \tag{32}$$

,where

$$\begin{aligned} a_i(z) = 1 - \frac{\lambda_i}{\sqrt{\lambda_i^2 + [g_i(x_t) + (A_t^{\Gamma})_i d]^2 + 2\varepsilon^2}}, \\ b_i(z) = 1 - \frac{g_i(x_t) + (A_t^{\Gamma})_i d}{\sqrt{\lambda_i^2 + [g_i(x_t) + (A_t^{\Gamma})_i d]^2 + 2\varepsilon^2}}, \end{aligned} \tag{33}$$

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

$$\psi(z) = \gamma \|H(z)\| \min\{1, \|H(z)\|\}, \tag{34}$$

The full SQP is as follows:

Algorithm 1 SQP

step0:set β=0.5 ,σ=0.2,ε=1×10^{-6},the initial vector $d0 = (1, 1, 1)^{\mathrm{T}}$,$\mu_0 = 0$,$\lambda_0 = (0, 0, 0)^T$,$z_0 = (\varepsilon_0, d_0, \mu_0, \lambda_0)$,$\overline{z}_0 = (\varepsilon_0, 0, 0, 0)$,$i = 0$
step1:if $\|H(z_i)\| \leq 0$,stop iteration, else,$\psi_i = \psi(z_i)$,ψ_i is shown in (34),$H(z_i)$ is shown in (29).
step2: Solve the following equations:
$H(z_i) + H'(z_i)\Delta z_i = \psi\overline{z}_0$,then get the solution of the equations:$\Delta z_i = (\Delta\varepsilon_i, \Delta d_i, \Delta\mu_i, \Delta\lambda_i)$
step3: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 $\alpha_i = \rho^{m_i}$, $z_{i+1} = z_i + \alpha_i \Delta z_i$
step4:$i = i + 1$,go to step1

4 Results and Discussion

4.1 simulation environment

In the simulation experiment, the number of transmitting antennas is set to two(N_A=2), the number of receiving antennas is set to two(N_B=2), and the number of antennas of the eavesdropper is set to two(N_E=2). Channels H and G are Rayleigh fading channels, and the transmitted signals are completely random. The transmit power is 10(P=10).

4.2 simulation results

Fig.2 shows the secrecy capacity of SCO-AN in (14) and (18) with different Signal-to-noise ratio(SNR) . The abscissa represents the SNR, the SNR ranges from -10 to +20, and the ordinate represents the secrecy capacity. Simulation experiments on the same communication model containing eavesdroppers. In the simulation , H_t and G_t are unchanged. σ_n^2, σ_e^2 are adjusted according to different SNR. σ_m^2 , σ_t^2 and σ_u^2 is adjusted in power allocation. From the Fig.2 we see that under the same SNR, the secrecy capacity of SCO-AN after power allocation is always greater than that without power allocation. At the same time, the secrecy capacity of the SCO-AN after power allocation is always greater than the secrecy capacity without power allocation is increased with the increase of SNR.

Fig.3 shows the secrecy capacity of SCO-AN in (14) and (18) with different channnels. The abscissa represents the serial number of the simulation experiment, that is, the abscissa of 1 represents the first experiment, and the abscissa of 2 represents the second experiment, etc. The ordinate represents the value of the secrecy capacity. The simulation experiment randomly simulated 10 different channel models containing eavesdroppers. In Fig.3, we see that after power allocation, the secrecycapacity of SCO-AN is increased in each experiment. This fully illustrates the effectiveness of SQP.

Fig.4 shows mean of the secrecy capacity with different channnel models obtained after 100 simulations. The abscissa in Fig.4 represents the interval where the experiment number is located. For example, abscissa 1 represents the first to tenth experiments, and abscissa 2 represents the eleventh to twentieth experiments,etc. The ordinate represents the interval Mean value of secrecy capacity of SCO-AN obtained from internal simulation. The channel model with eavesdroppers in each experiment is completely random. From the figure we can see that after the power allocation algorithm, the mean of secrecy capacity are increased.

Fig.5 shows sum of the secrecy capacity with different channnel models obtained after 100 simulations. The abscissa in Fig.5 represents the interval in which the experiment number is located. For example, abscissa 1 represents the first to tenth experiments, abscissa 2 represents the first to twentieth simulation experiments, and the ordinate represents the sum of the secrecy capacity of the SCO-AN obtained from the simulation experiment.It can be seen in Fig. 5 that the total secrecy capacity of the SCO-AN after power allocation is greater than that before power allocation.

In Table 1, (x,y,z) represents original coordinates, (x',y',z') represents coordinates after SQP processing, andrepresents improved by SQP. From Table 1, we see that has improved to a certain extent after entering the SQP for power allocation, and (x,y,z) is within a limited range, which indicates that SQP is a very effective power allocation algorithm.It should be noted that in Table 1, after some experiments, the sum of the transmission power after power allocation is less than ten. Although the secrecy capacity of SCO-AN becomes larger, the sum of powers less than ten indicates that the transmission power is not fully utilized, and The SQP algorithm has converged . It is a good research content to use the extra power to increase the secrecy capacity in the future.

5 Conclusion

It is the research focus of the physical layer security technology to maximize the secrecy capacity under the limited transmission power. In this paper, the power allocation technology of Secrecy Capacity Optimization artificial noise is studied.Because the objective function of power allocation is non-convex, the traditional convex optimization algorithm cannot effectively solve the power allocation problem of SCO-AN. Therefore, in this paper, the sequence quadratic program method is adopted to solve the SCO-AN. The power allocation problem of AN has been proved by simulation experiments that SQP can effectively improve the secrecy capacity of SCO-AN under a certain power limit. Due to the limitation of the SQP algorithm itself, it is only possible to find the maximum value of the SCO-AN secrecy capacity within a certain range .This result is obviously not the best. Finding the maximum value of SCO-AN's secrecy capacity under certain power constraints is still a challenge. Related studies have used statistical methods to determine the maximum value of AN's secrecy capacity under certain power constraints using the physical conditions of multi-antenna transmission. In the future research, we will continue to study the possibility of using statistical methods to find the maximum value of the secrecy capacity of SCO-AN under a certain power limit. Table 1 shows that SQP did not fully utilize the transmit power when performing power allocation, and using redundant transmit power to further increase the secrecy capacity of SCO-AN is also our future research content.

6 Abbreviations

List of 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

7 Declarations

7.1 Availability of data and materials

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

7.2 Competing interests

The authors declear that they have no competing interests.

7.3 Authors' contributes

YG proposed the framework of the whole algorithm. ZW handled all the simulations. ZY was a major contributor in writing the manuscript. BW made all figures and tables in the manuscript.

7.4 Funding

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

Author details

[1]School of Electronics and Information Engineering, Harbin Institute of Technology , Xidazhi street, 150001 harbin, China. [2]Jushri Technologies,INC, jinzhong road, 200335 shanghai, China.

References

1. Shannon C. Communication theory of secrecy system.Bell Syst Tech J,1949,28(4):655 715
2. Wyner A D. The wire-tap channel[J]. Bell Syst.tech.j, 1975, 54(8):1355-1387.
3. Csiszar I, Korner J. Broadcast channels with confidential messages[J]. IEEE Transactions on Information Theory, 2003, 24(3):339-348.
4. Negi R, Goel S. Secret communication using artificial noise[C]. IEEE Vehicular Technology Conference. 2005.
5. Zhou, X., and McKay, M. R. "Secure Transmission With Artificial Noise Over Fading Channels: Achievable Rate and Optimal Power Allocation." IEEE Transactions on Vehicular Technology (2010).
6. Zhao N , Yu F R , Li M , et al. Anti-Eavesdropping Schemes for Interference Alignment (IA)-Based Wireless Networks[J]. IEEE Transactions on Wireless Communications, 2016, 15(8):5719-5732.
7. Cao Y , Zhao N , Yu F R , et al. An anti-eavesdropping interference alignment scheme with wireless power transfer[C]. IEEE International Conference on Communication Systems. IEEE, 2017.
8. Wei Li, Mounir Ghogho, Bin Chen, et al. (2012). Secure communication via sending artificial noise by the receiver: outage secrecy capacity/region analysis. IEEE Communications Letters, 16(10), 1628-1631.
9. Yebo G , Zhilu W , Zhendong Yin, et al. The Secrecy Capacity Optimization Artificial Noise: A New Type of Artificial Noise for Secure Communication in MIMO System." IEEE Access 7 (2019): 58353 - 58360.
10. Li Q, Yang Y, Ma W K, et al. Robust Cooperative Beamforming and Artificial Noise Design for Physical-Layer Secrecy in AF Multi-Antenna Multi-Relay Networks[J]. IEEE Transactions on Signal Processing, 2014, 63(1):206-220.
11. Chae S H, Wan C, Lee J H, et al. Enhanced Secrecy in Stochastic Wireless Networks: Artificial Noise With Secrecy Protected Zone[J]. Information Forensics and Security IEEE Transactions on, 2014, 9(10):1617-1628.
12. Marzban, Mohamed F., et al. "Security-enhanced SC-FDMA transmissions using temporal artificial-noise and secret key aided schemes." IEEE Access 7 (2019): 14807-14824.
13. Liao, Wei-Cheng, et al. "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach." IEEE Transactions on Signal Processing 59.3 (2010): 1202-1216.
14. Li, Qiang, and Wing-Kin Ma. "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization." IEEE Transactions on Signal Processing 61.10 (2013): 2704-2717.
15. Zeng, Ming, et al. "Securing downlink massive MIMO-NOMA networks with artificial noise." IEEE Journal of Selected Topics in Signal Processing 13.3 (2019): 685-699.
16. Romero-Zurita, Nabil, Mounir Ghogho, and Des McLernon. "Outage probability based power distribution between data and artificial noise for physical layer security." IEEE Signal Processing Letters 19.2 (2011): 71-74.
17. Lin, Pin-Hsun, et al. "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels." IEEE Journal on Selected Areas in Communications 31.9 (2013): 1728-1740.
18. Zhang, Xi, Xiangyun Zhou, and Matthew R. McKay. "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels." IEEE Transactions on Vehicular Technology 62.5 (2013): 2170-2181.
19. Jeongseok H A, Sangseok Y U N, Sanghun I M. Apparatus and method for secure communication using artificial noise scheme: U.S. Patent Application 16/162,014[P]. 2019-7-25
20. Zheng T X, Wang H M, Yuan J, et al. Multi-Antenna Transmission With Artificial Noise Against Randomly Distributed Eavesdroppers[J]. IEEE Transactions on Communications, 2015, 63(11):4347-4362.
21. Singh P, Trivedi A. NOMA and massive MIMO assisted physical layer security using artificial noise precoding[J]. Physical Communication, 2020, 39: 100977.
22. Wong, Cheong Yui, et al. "Multiuser OFDM with adaptive subcarrier, bit, and power allocation." IEEE Journal on selected areas in communications 17.10 (1999): 1747-1758.
23. Tse, D. N. "Optimal power allocation over parallel Gaussian broadcast channels." Proceedings of IEEE International Symposium on Information Theory. IEEE, 1997.
24. Zhao, Yi, Raviraj Adve, and Teng Joon Lim. "Improving amplify-and-forward relay networks: optimal power allocation versus selection." 2006 IEEE International Symposium on Information Theory. IEEE, 2006.
25. Jiang, Yuhan, et al. "Power Allocation for Intelligent Interference Exploitation Aided Physical-Layer Security in OFDM-Based Heterogeneous Cellular Networks." IEEE Transactions on Vehicular Technology (2020).
26. Zhou, Xiangyun, and Matthew R. McKay. "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation." IEEE Transactions on Vehicular Technology 59.8 (2010): 3831-3842.
27. Tsai, Shang-Ho, and H. Vincent Poor. "Power allocation for artificial-noise secure MIMO precoding systems." IEEE transactions on signal processing 62.13 (2014): 3479-3493.
28. Zhou, Xiangyun, and Matthew R. McKay. "Physical layer security with artificial noise: Secrecy capacity and optimal power allocation." 2009 3rd International Conference on Signal Processing and Communication Systems. IEEE, 2009.
29. Zhang, Erqing, Sixing Yin, and Huisheng Ma. "Stackelberg Game-Based Power Allocation for V2X Communications." Sensors 20.1 (2020): 58.
30. Yang, Yunchuan, et al. "Transmitter beamforming and artificial noise with delayed feedback: Secrecy rate and power allocation." Journal of Communications and Networks 14.4 (2012): 374-384.
31. Li, Na, Xiaofeng Tao, and Jin Xu. "Artificial noise assisted communication in the multiuser downlink: Optimal power allocation." IEEE communications letters 19.2 (2014): 295-298.
32. Van Chien, Trinh, Emil Björnson, and Erik G. Larsson. "Joint power allocation and load balancing optimization for energy-efficient Cell-free Massive MIMO networks." arXiv preprint arXiv:2002.01504 (2020).
33. Goswami, Debjani, and Suvra Sekhar Das. "Iterative Sub-Band and Power Allocation in Downlink Multiband NOMA." IEEE Systems Journal (2020).
34. Hasna, Mazen O., and M-S. Alouini. "Optimal power allocation for relayed transmissions over Rayleigh-fading channels." IEEE

Transactions on Wireless communications 3.6 (2004): 1999-2004.
35. Yan, Junkun, et al. "Collaborative detection and power allocation framework for target tracking in multiple radar system." Information Fusion 55 (2020): 173-183.
36. Qin, Haohao, et al. "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs." IEEE Transactions on Wireless Communications 12.6 (2013): 2717-2729.

Figures

Figure 2 Secrecy capacity in (14) and (18) versus different SNR

Figure 3 Secrecy capacity in (14) and (18) versus different channel models

Figure 4 The mean of secrecy capacity in (14) and (18) obtained after 100 simulations

Figure 5 The sum of secrecy capacity in (14) and (18) obtained after 100 simulations

Tables

Table 1 The coordinates and secrecy capacity before and after the SQP.

(x,y,z)	(x',y',z')	before	after
(2,4,4)	(1.8246 3.9107 3.8930)	0.0595	0.0733
(2,2,6)	(1.7771 1.7749 5.9320)	0.0509	0.0523
(3,1,6)	(2.8638 0.4580 5.9795)	0.0456	0.0549
(5,3,2)	(4.2260 1.6668 1.6631)	0.3684	0.5057
(3,2,5)	(2.1938 1.1219 3.7771)	0.0770	0.2444
(3,4,3)	(2.6635 3.3499 0.4547)	0.0670	0.0787
(5,1,8)	(0.9993 0.9993 8.0000)	0.0025	0.0153
(2,3,5)	(1.7184 2.8065 4.8242)	0.4797	0.6225

Figures

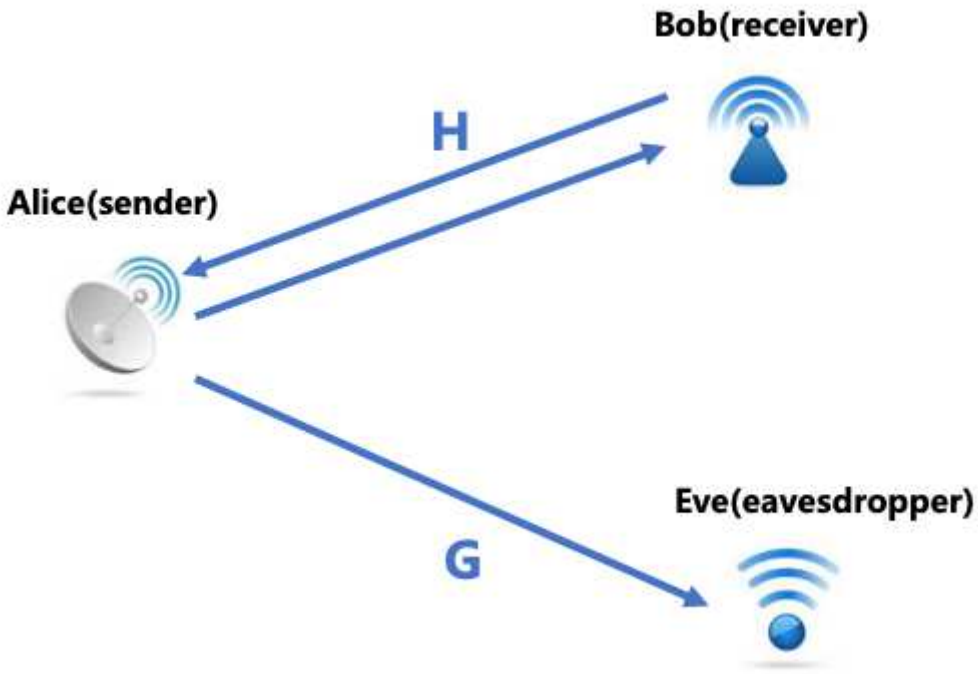

Figure 1

The wireless communication model with eavesdropper

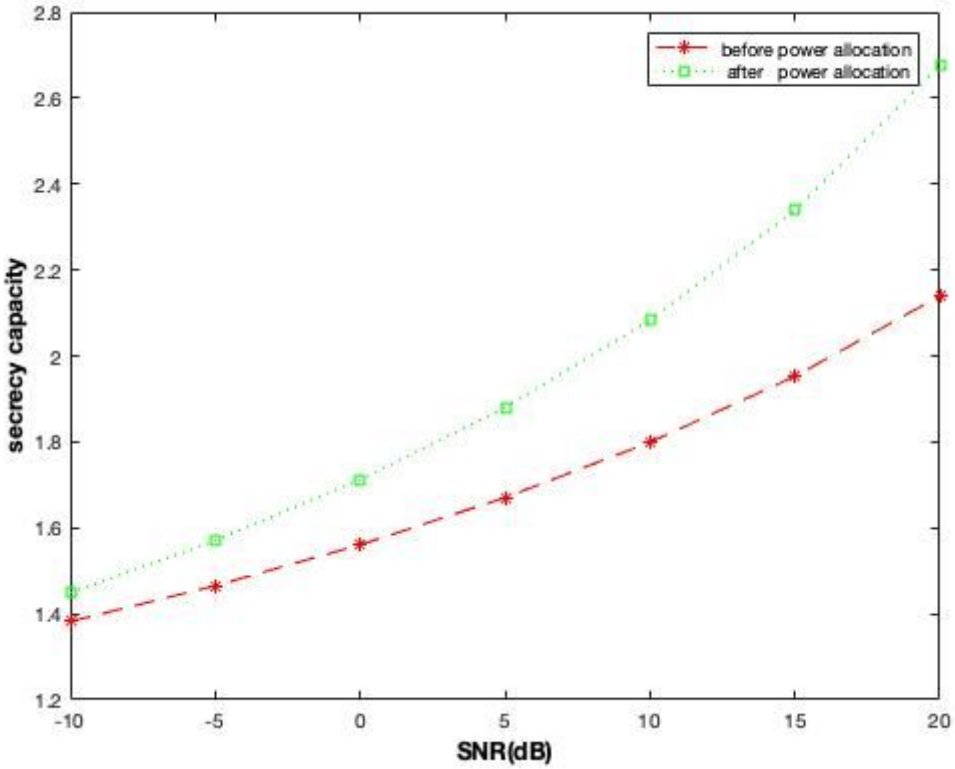

Figure 2

Secrecy capacity in (14) and (18) versus different SNR

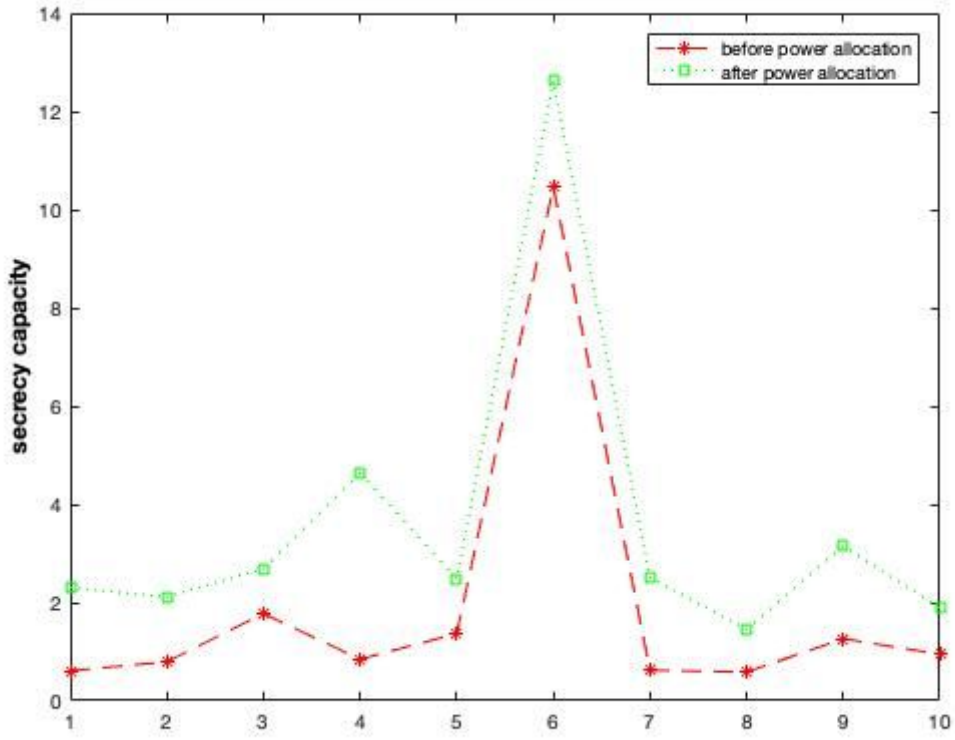

Figure 3

Secrecy capacity in (14) and (18) versus different channel models

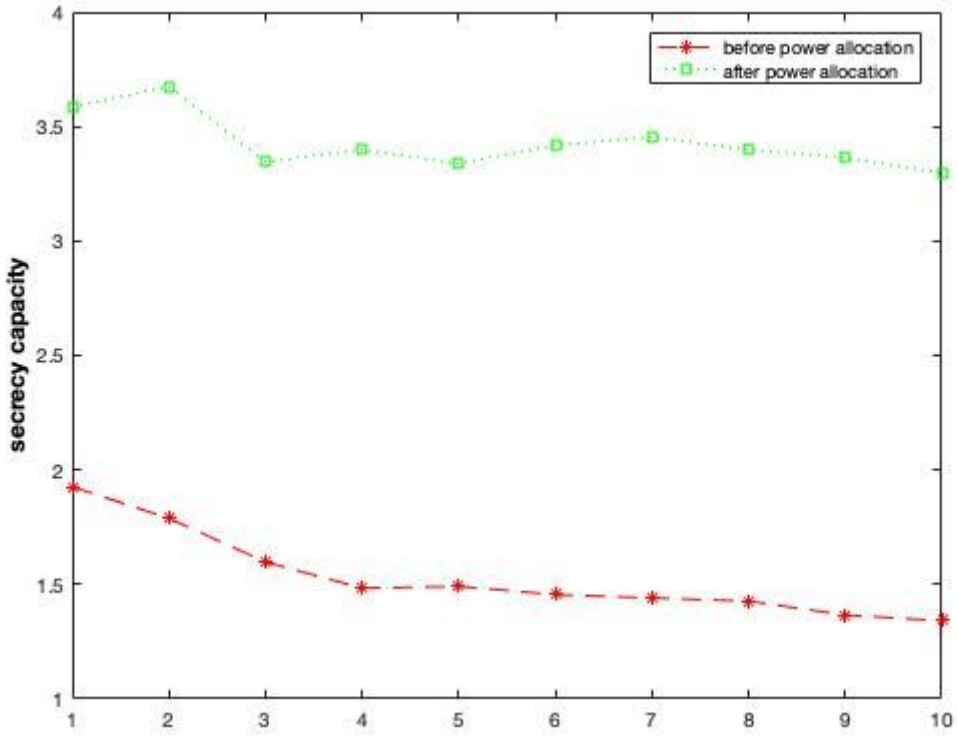

Figure 4

The mean of secrecy capacity in (14) and (18) obtained after 100 simulations

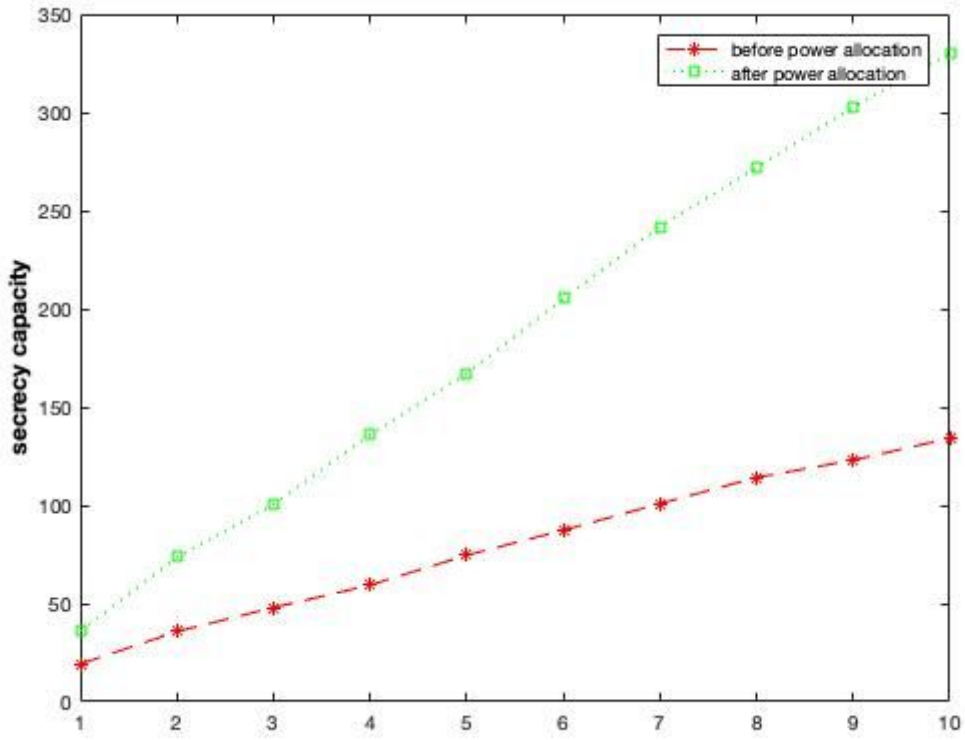

Figure 5

The sum of secrecy capacity in (14) and (18) obtained after 100 simulations