第 21 卷　第 2 期　　太赫兹科学与电子信息学报　　Vol.21，No.2
2023 年 2 月　　Journal of Terahertz Science and Electronic Information Technology　　Feb.，2023

文章编号：2095-4980(2023)02-0195-08

A novel optimization scheme for artificial-noise-aided MU-MISOME broadcast secure communication system in slow fading channel environment

YAO Li[1]，LIU Youjiang[1]，ZHANG Jian[2]

(1.Institute of Electronic Engineering，China Academy of Engineering Physics，Mianyang Sichuan 621999，China；
2.School of Electronic Science and Engineering，University of Electronic Science and Technology of China，
Chengdu Sichuan 611731，China)

Abstract: This study investigates artificial noise aided Multiuser Multiple-Input Single-Output (MU-MISO) broadcast wiretap system designs in slow fading channel environment. We adopt a beamforming technique with artificial noise to achieve secure multiuser communication and optimize system performance. To overcome the complexity of this model, a novel optimization scheme using semi-closed-form expressions and Monte Carlo method is employed to derive the relationship between transmission parameters and secure transmission performance. In this article, we detail the procedure of our new method, and conduct some heuristic simulation works. The simulation results reveal how power allocation ratio and information rate influence the multiuser system secure transmission probability and effective secrecy throughput of the multiuser system. We compare the multiuser system security and throughput performance with each user's performance, which helps us to verify the security ability of our method. Our research results extend the traditional single-user artificial noise design method to multi-user scenarios, and provide ideas for solving the optimization problem of multi-user broadcast communication.

Keywords: physical layer security; artificial noise; beamforming; multiuser communication; broadcast system

CLC number: TN929.5　　**Document code:** A　　**doi:** 10.11805/TKYDA2020568

1 Introduction

Due to the broadcasting nature of electromagnetic waves, private data is vulnerable for potential eavesdroppers, especially in multiuser communication scenarios. Traditionally, cryptographic algorithms are widely used to ensure system security. However, because of the neglect of channel's physical layer characteristics, the perfect secrecy of cryptographic algorithms cannot be always guaranteed, especially in the scenario that eavesdroppers have infinite computational ability. Physical-layer security prevents eavesdropping by taking advantage of physical properties of wireless channels. This technique is based on perfect secrecy theory introduced by Shannon[1], and was first proposed in [2]. Following these studies, an increasing number of researchers has engaged in this new field.

Enhancing security by worsening the eavesdropper's channel is a novel approach to achieve physical-layer security. In [3], Goel and Negi proposed to confuse the eavesdropper by Artificial Noise(AN). They blend the information-bearing signal with artificially made noise signal which lies in the null space of the legitimate receiver. After that, the authors of [4] worked out fast fading channel optimal power allocation issue via closed-form expressions, and considered the impact of imperfect Channel State Information(CSI). Different from fast fading channel scenes, slow fading channel scenarios, in which the channel coherence time is longer than the codeword length, and burst errors may appear suddenly, seems more challenging, and closer to reality. The authors of [5] proposed the effective secrecy throughput as a performance metric in the design of secure transmission using artificial noise over slow fading. They derived closed-form expressions for the effective secrecy throughput and determined the optimal power allocation and optimal secrecy rate for on-off transmission scheme and adaptive transmission scheme to maximize the secure transmission performance. Based on previous research results,

Received date: 2020-10-30; **Revised date:** 2021-01-14

Foundation: National Natural Science Foundation of China(61601425)

researchers of [6] examined the secrecy performance of three AN-aided secure transmission schemes, namely, the partially-adaptive, fully-adaptive, and on-off schemes. And a power allocation approach for artificial noise aided beamforming was proposed in MISO wiretap channels in [7].

The above-mentioned articles are all about traditional point-to-point communication system, namely, one transmitter conveys messages to one receiver. For multiuser security communication system with artificial noise, some problems are still open. The authors in [8] researched on secrecy outage constraint artificial noise aided multiuser communication system. Atallah and his partner in [9] proposed a new location-based multicasting technique to improve the security in the presence of non-colluding passive eavesdroppers. However, the fore-mentioned articles were aimed at multicast channel where a common message is transmitted to multiple receivers. While for multiuser broadcast channels where a unique data symbol is transmitted to each of all users, multiuser beamforming technique is always used to eliminate inter-user interference. [10] proposed zero-forcing beamforming in broadcast channels. Minimum Mean Square Error(MMSE) broadcast beamforming technique was studied in [11]. The authors of [12] proposed the optimal beamforming design for multiuser broadcast secure transmission under secrecy outage probability constraint with artificial noise technique for different users, which has different priorities and importance. And the outage performance of cooperative Non-Orthogonal Multiple Access(NOMA) under multiuser and multi-relay system was studied in reference [13].

Based on the above-mentioned articles, this work combines multiuser beamforming and artificial noise to achieve multiuser broadcast secure communication. We focus on a multiuser, Multiple-Input, Single-Output per user, and Multi-antenna Eavesdropper(MU-MISOME) wiretap channel, and build a complete model for AN-aided MU-MISOME secure communication system. We suppose a slow fading channel scene, and adopt a more popular pre-coding method in recent articles like [5] and [6]. Then, the expression about Signal-to Noise-Ratio(SNR) of each user and eavesdropper is derived, which is a basic step in physical security optimization problems.

A new solution to the MU-MISOME broadcast wiretap channel optimization problem is proposed. Since it's hard to get optimal parameters by a closed-form method in this system, Monte-Carlo algorithm is employed to show the influence of system parameters on system security performance.

We investigate the general principle underlying the relationship of secure transmission probability and effective secrecy throughput with power allocation factor and information rate by simulation. It's easy to get optimal parameters by this means. Moreover, we compare the system performance with each user's performance, which will help us to verify the security ability of our method.

Notation: scalar variables are denoted by italic symbols. Vectors and matrices are denoted by lowercase and uppercase boldface symbols, respectively. $(\cdot)^{\mathrm{T}}$ denotes the transpose, $(\cdot)^{\mathrm{H}}$ denotes the complex conjugate transpose, $(\cdot)^{-1}$ denotes the inverse, and $\|\cdot\|$ denotes the Frobenius norm of matrix.

2 System model of MU-MISOME broadcast wiretap channel

We consider a MU-MISOME broadcast system. As shown in Fig.1, the transmitter Alice with M_{T} antennas transmits information signal $\boldsymbol{s}$ to K single-antenna users, Bob-1, Bob-2, $\cdots$, Bob-K. $\boldsymbol{s}=[s_1\ s_2\ \dots\ s_j\ \dots\ s_K]^{\mathrm{T}}$, $j=1,2,\cdots,K$, s_j represents Bob-j's information signal. The channel between Alice and Bob is defined as main channel, and the CSI of main channel is a $K\times M_{\mathrm{T}}$ matrix $\boldsymbol{H}$, $\boldsymbol{H}=[\boldsymbol{h}_1^{\mathrm{T}}\ \boldsymbol{h}_2^{\mathrm{T}}\ \dots\ \boldsymbol{h}_j^{\mathrm{T}}\ \dots\ \boldsymbol{h}_K^{\mathrm{T}}]^{\mathrm{T}}$, the $1\times M_{\mathrm{T}}$ vector $\boldsymbol{h}_j^{\mathrm{T}}$ represents the channel matrix between Alice and Bob-j. We assume that the instantaneous CSI $\boldsymbol{H}$ is perfectly known by Bobs and is sent to Alice with feedback links. Transmitted information is overheard by a passive eavesdropper Eve with M_{E} antennas. The channel matrix between Alice and Eve is a $M_{\mathrm{E}}\times M_{\mathrm{T}}$ matrix $\boldsymbol{G}$. The instantaneous CSI of $\boldsymbol{G}$ is not available to Alice. And with an extreme hypothesis,

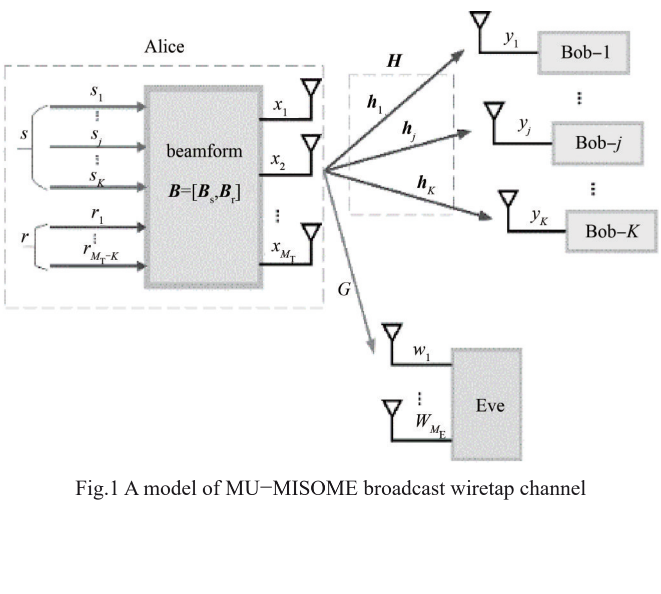


Fig.1 A model of MU-MISOME broadcast wiretap channel

Eve can get the perfect instantaneous CSI of $\boldsymbol{H}$ because of the unsafe feedback links from Bobs to Alice. The Eve's channel and the main channels are all modeled as independent and identically distributed (i.i.d.) Rayleigh fading, and subject to slow fading.

According to usual assumption in MU–MISOME broadcast system, we have $M_{\mathrm{T}} > K$ and $M_{\mathrm{T}} > M_{\mathrm{E}}$. If the assumption is violated, artificial noise signal may be eliminated by Eve, and detailed explanation is listed in former researching articles like [7] and [9]. To ensure security, Alice transmits artificial noise signal $\boldsymbol{r}$ in conjunction with information signal $\boldsymbol{s}$, where $\boldsymbol{r}$ is a $\left(M_{\mathrm{T}} - K\right) \times 1$ zero–mean complex Gaussian random vector, $\boldsymbol{r} = \left[r_1 \ r_2 \ \ldots \ r_{M_{\mathrm{T}}-K}\right]^{\mathrm{T}}$, and the variance of its entries is σ_r^2. The total transmit power is assumed to be P_{T}, and we denote the total information signal power as σ_s^2. Assuming that Alice equally distributes the transmit power to every user, the variance of s_j is $\sigma_j^2 = \sigma_s^2/K$. Given $\varnothing$ to represent power allocation factor, namely the ratio of information signal power to the total power, we have $\sigma_j^2 = \varnothing P_{\mathrm{T}}/K$, $\sigma_r^2 = \left(1 - \varnothing\right) P_{\mathrm{T}}/\left(M_{\mathrm{T}} - K\right)$, where $0 < \varnothing \leqslant 1$.

To mix artificial noise signal with information signal and convey information to multiple users, we use beamforming matrix $\boldsymbol{B}$ as pre–coding procedure, $\boldsymbol{B} = [\boldsymbol{B}_{\mathrm{s}} \quad \boldsymbol{B}_{\mathrm{r}}]$. $\boldsymbol{B}_{\mathrm{s}}$ is a $M_{\mathrm{T}} \times K$ zero–forcing beamforming matrix for transmitting information signal $\boldsymbol{s}$ to Bobs, $\boldsymbol{B}_{\mathrm{s}} = \boldsymbol{H}^{\mathrm{H}}\left(\boldsymbol{H}\cdot\boldsymbol{H}^{\mathrm{H}}\right)^{-1} = [\boldsymbol{b}_1 \ \boldsymbol{b}_2 \ldots \ \boldsymbol{b}_K]$. $\boldsymbol{B}_{\mathrm{r}}$ is the artificial noise pre–coding matrix, which keeps artificial noise lies in the null space of main channels. Alice performs eigenvalue decomposition on matrix $\boldsymbol{H}^{\mathrm{H}} \cdot \boldsymbol{H}$, and let $\boldsymbol{B}_{\mathrm{r}}$ be eigenvectors corresponding to zero eigenvalue of $\boldsymbol{H}^{\mathrm{H}} \cdot \boldsymbol{H}$. The transmission signal $\boldsymbol{x}$ on M_{T} antennas is

$$\boldsymbol{x} = \frac{1}{\|\boldsymbol{B}\|}\cdot[\boldsymbol{B}_{\mathrm{s}} \quad \boldsymbol{B}_{\mathrm{r}}]\cdot\begin{bmatrix}\boldsymbol{s}\\ \boldsymbol{r}\end{bmatrix} = \frac{1}{\|\boldsymbol{B}\|}\cdot\left(\boldsymbol{B}_{\mathrm{s}}\cdot\boldsymbol{s} + \boldsymbol{B}_{\mathrm{r}}\cdot\boldsymbol{r}\right) = \delta\cdot\left(\boldsymbol{B}_{\mathrm{s}}\cdot\boldsymbol{s} + \boldsymbol{v}\right) \tag{1}$$

where $\boldsymbol{v} = \boldsymbol{B}_{\mathrm{r}}\cdot\boldsymbol{r}$ represents the whole artificial noise for M_{T} antennas, and $\delta = 1/\|\boldsymbol{B}\|$ is the power normalization parameter.

After $\boldsymbol{x}$ passing the main channel, the received signal at Bob–j is

$$y_j = \boldsymbol{h}_j^{\mathrm{T}} \cdot \boldsymbol{x} + \xi_j = \delta \cdot \left(\boldsymbol{h}_j^{\mathrm{T}} \cdot \boldsymbol{b}_j \cdot s_j + \boldsymbol{h}_j^{\mathrm{T}} \cdot \sum_{i \neq j}^{K} \boldsymbol{b}_i \cdot s_i + \boldsymbol{h}_j^{\mathrm{T}} \cdot \boldsymbol{v}\right) + \xi_j = \delta \cdot \boldsymbol{h}_j^{\mathrm{T}} \cdot \boldsymbol{b}_j \cdot s_j + \xi_j = \delta \cdot s_j + \xi_j \tag{2}$$

where ξ_j is the Additive White Gaussian Noise(AWGN) of Bob–j's receiver. In this article, we assume that all users' AWGNs have the same variance, namely σ^2. Therefore, the instantaneous SNR of Bob–j is

$$\gamma_j = \frac{\delta\cdot\sigma_j^2}{\sigma^2} = \frac{\delta\cdot\varnothing P_{\mathrm{T}}}{K\cdot\sigma^2} = \varnothing\bar{\gamma}_j \tag{3}$$

where $\bar{\gamma}_j = \delta\cdot P_{\mathrm{T}}/K\cdot\sigma^2$, and we can define this constant as the average *SNR* of Bob–j. At Eve, we assume an extreme situation that the receiver noise is zero. Hence the received signal for Eve is

$$\boldsymbol{w} = \boldsymbol{G}\cdot\boldsymbol{x} = \delta\cdot\boldsymbol{G}\cdot\left(\boldsymbol{B}_{\mathrm{s}}\cdot\boldsymbol{s} + \boldsymbol{v}\right) \tag{4}$$

$\boldsymbol{w} = \left[w_1 \quad w_2 \quad \ldots \quad w_{M_E}\right]^{\mathrm{T}}$. To overhear all users' signal, Eve needs to eliminate influence caused by beamforming matrix. As we have assumed Eve can get the perfect instantaneous CSI of $\boldsymbol{H}$, it can also obtain beamforming matrix used by Alice easily. In this article, it is assumed Eve can use the knowledge of $\boldsymbol{H}$ to eliminate beamforming, or we call it ‘de–beamforming’. As shown in Fig.2, the ‘de–beamforming’ $K \times M_{\mathrm{E}}$ matrix $\boldsymbol{D} = \left(\boldsymbol{G}\cdot\boldsymbol{B}_{\mathrm{s}}\right)^{+} = [\boldsymbol{d}_1^{\mathrm{T}} \ \boldsymbol{d}_2^{\mathrm{T}} \ \ldots \ \boldsymbol{d}_j^{\mathrm{T}} \ \ldots \ \boldsymbol{d}_K^{\mathrm{T}}]^{\mathrm{T}}$. $\boldsymbol{D}$ is the pseudo inverse matrix for $\boldsymbol{G}\cdot\boldsymbol{B}_{\mathrm{s}}$. After ‘de–beamforming’, Eve can get the eavesdropping signal z as

$$\boldsymbol{z} = \boldsymbol{D}\cdot\boldsymbol{w} = \delta\cdot\left(\boldsymbol{G}\boldsymbol{B}_{\mathrm{s}}\right)^{-1}\cdot\boldsymbol{G}\boldsymbol{B}_{\mathrm{s}}\cdot\boldsymbol{s} + \delta\cdot\left(\boldsymbol{G}\boldsymbol{B}_{\mathrm{s}}\right)^{-1}\cdot\boldsymbol{G}\cdot\boldsymbol{v} = \delta\cdot\boldsymbol{s} + \delta\cdot\boldsymbol{D}\cdot\boldsymbol{G}\cdot\boldsymbol{v}. \tag{5}$$

The $K \times 1$ vector $\boldsymbol{z} = [z_1 \ z_2 \ldots \ z_j \ \ldots \ z_K]^{\mathrm{T}}$, where $z_j = \delta\cdot\left(s_j + \boldsymbol{d}_j^{\mathrm{T}}\cdot\boldsymbol{G}\cdot\boldsymbol{v}\right)$. To this, the instantaneous receiving *SNR* of Bob–j's

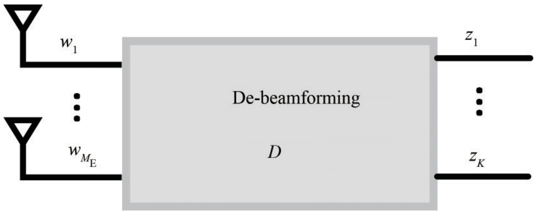


Fig.2 Procedure of ‘De–beamforming’ in Eve

signal in Eve is

$$\gamma_{E_j}=\frac{\sigma_j^2}{\left\|\boldsymbol{d}_j^{\mathrm{T}}\cdot\boldsymbol{G}\cdot\boldsymbol{v}\right\|^2}=\frac{\varnothing P_{\mathrm{T}}/K}{\left\|\boldsymbol{d}_j^{\mathrm{T}}\cdot\boldsymbol{G}\cdot\boldsymbol{B}_{\mathrm{r}}\right\|^2\cdot\frac{(1-\varnothing)P_{\mathrm{T}}}{M_{\mathrm{T}}-K}}=\frac{\varnothing}{1-\varnothing}\cdot\frac{1}{\rho\cdot\left\|\boldsymbol{d}_j^{\mathrm{T}}\cdot\boldsymbol{G}\cdot\boldsymbol{B}_r\right\|^2} \tag{6}$$

where $\rho=\frac{K}{M_{\mathrm{T}}-K}$. Based on (5) and (6), it can be seen that the AN component behaves as noise to the eavesdropping signal.

3 Secure transmission optimization by Monte Carlo method

In this section, we first introduce the principle about system secrecy and throughput performance of MU-MISOME broadcast wiretap channel. Then the means of performance optimization by Monte Carlo method is presented.

3.1 Secrecy and throughput performance of MU-MISOME broadcast system

In MU-MISOME broadcast system, the Bob-j's achievable secrecy rate C_j can be expressed as

$$C_j=\begin{cases}C_{B_j}-C_{E_j},\gamma_j>\gamma_{E_j}\\0, \qquad\qquad \gamma_j\leqslant\gamma_{E_j}\end{cases} \tag{7}$$

where $C_{B_j}=\log_2\left(1+\gamma_j\right)$ is the channel capacity of Bob-j, and $C_{E_j}=\log_2\left(1+\gamma_{E_j}\right)$ is the channel capacity of Eve about Bob-j's signal. In this article, we use the on-off transmission scheme in [9], and we express secure transmission probability as

$$P_{\sec}=Pr\left(C\geqslant R_{\mathrm{s}}\right) \tag{8}$$

where C is the channel capacity of the whole system, and R_{S} is the transmitting information rate in Alice. In multiuser system, to ensure security of every user, we choose the minimum channel capacity of all Bobs as the system capacity, namely $C=\min\limits_K C_j$. We have

$$P_{\sec}=Pr\left(\min_K C_j\geqslant R_{\mathrm{s}}\right)=Pr\left(\max_K\gamma_{E_j}\leqslant\frac{1+\gamma_j}{2^{R_{\mathrm{s}}}}-1\right) \tag{9}$$

People can also use the effective secrecy throughput to quantify the average rate of the messages that are securely transmitted from Alice to Bob[4]. We can express the effective secrecy throughput as

$$U=R_{\mathrm{s}}P_{\sec} \tag{10}$$

Based on (3),(6),(7) and (9),(10), we know that the security performance of system is determined by power allocation factor $\varnothing$ and information rate R_{s}. The authors of article [9] derived closed-form expressions of $P_{\sec}$ and U about $\varnothing$ and R_{s} for MISOME slow fading wiretap system. But in MU-MISOME system, it's hard to get closed-form expressions about Probability Density Functions(PDFs) of γ_{E_j} in equation (6) since the distribution of $\left\|\boldsymbol{d}_j\cdot\boldsymbol{G}\cdot\boldsymbol{B}_{\mathrm{r}}\right\|^2$ is difficult to derive. That problem inspires us to find a new route to obtain optimal $\varnothing$ and R_{s}.

3.2 Monte Carlo optimization method

To calculate the system secure transmission probability in any given $(\varnothing \quad R_{\mathrm{s}})$, we propose to simulate the secure transmission probability by Monte-Carlo method. The feasibility of this method is based on the reality that Alice can get the distribution of eavesdropper's channel matrix since Eve locates in the same environment as Bobs, this reality is also available in recent articles like [9] and [10]. Steps of our simulation method is given as Table1.

4 Simulation results

By the Monte-Carlo method proposed above, simulation work has been carried out. In our simulation work, we suppose a $10\times4\times5$(namely $M_{\mathrm{T}}=10$, $K=4$, and $M_{\mathrm{E}}=5$) MU-MISOME system. $\overline{\gamma}_j=15\,\mathrm{dB}$, moreover, there is no AWGN in Eve. We also employ Monte-Carlo coefficient $\beta=100\,000$, namely it created 100 000 samples of eavesdropper's channel. The main channel $\boldsymbol{H}$ and Eve's channel $\boldsymbol{G}$ are both subject to Rayleigh distribution.

Table1 Procedure of Monte–Carlo method for MU–MISOME optimization

1:Input system constants like M_{T}, K, M_{E}, $\bar{\gamma}_j$, and the instantaneous main channel CSI $\boldsymbol{H}$.

2:Setting Monte–Carlo coefficient β, and the range of R_{s} (namely the maximum of information rate $R_{\mathrm{s,max}}$).

3:Generate samples of eavesdropper's channel $\boldsymbol{G}$, the number of samples is β.

4:For a given $(\varnothing_i \quad R_{\mathrm{s},i})$, we calculate every user's γ_{E_j} using (6) by every sample of $\boldsymbol{G}$. Then we can get $\beta\,\gamma_{E_j}$ samples. For every sample, it can be judged whether secure or not by (9). Checking all β samples, then we simulate to get secure transmission probability of given $(\varnothing_i \quad R_{\mathrm{s},i})$ as $P_{\mathrm{sec}}(\varnothing_i \quad R_{\mathrm{s},i})$, and effective secrecy throughput $U(\varnothing_i \quad R_{\mathrm{s},i})$.

5:Vary $\varnothing$ from 0 to 1, R_s from 0 to $R_{\mathrm{s,max}}$, one can derive the whole relationship of P_{sec} and U with $(\varnothing \quad R_{\mathrm{s}})$.

Our simulation result is shown as Fig.3. The Z axis represents effective secrecy throughput(U), X axis and Y axis represent power ratio$(\varnothing$) and transmission information rate$\left(R_{\mathrm{s}}\right)$ respectively. It's easy to see that effective secrecy throughput increases firstly, then decreases with the increase of both $\varnothing$ and R_{s}, namely there is a peak in the 3D figure.

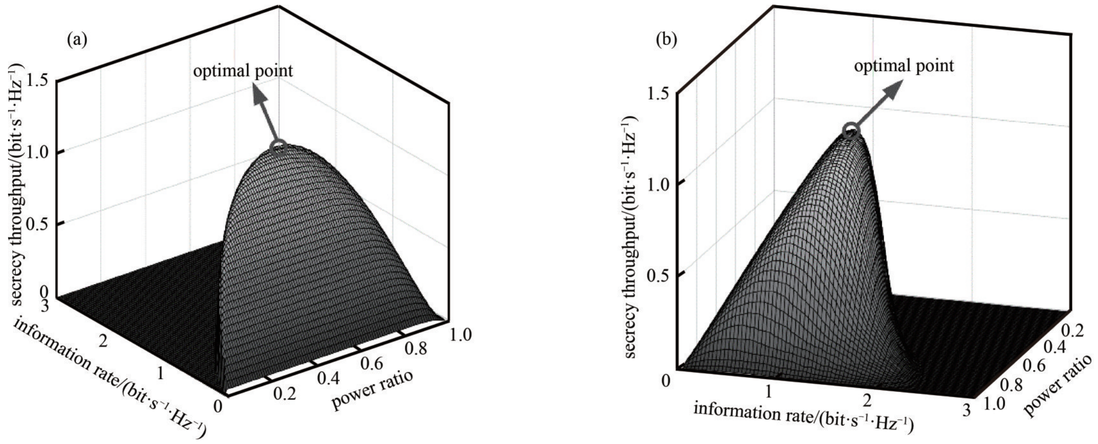


Fig.3 3D figures of the relationship about effective secrecy throughput(U) with power ratio($\varnothing$) and information rate(R_{s})

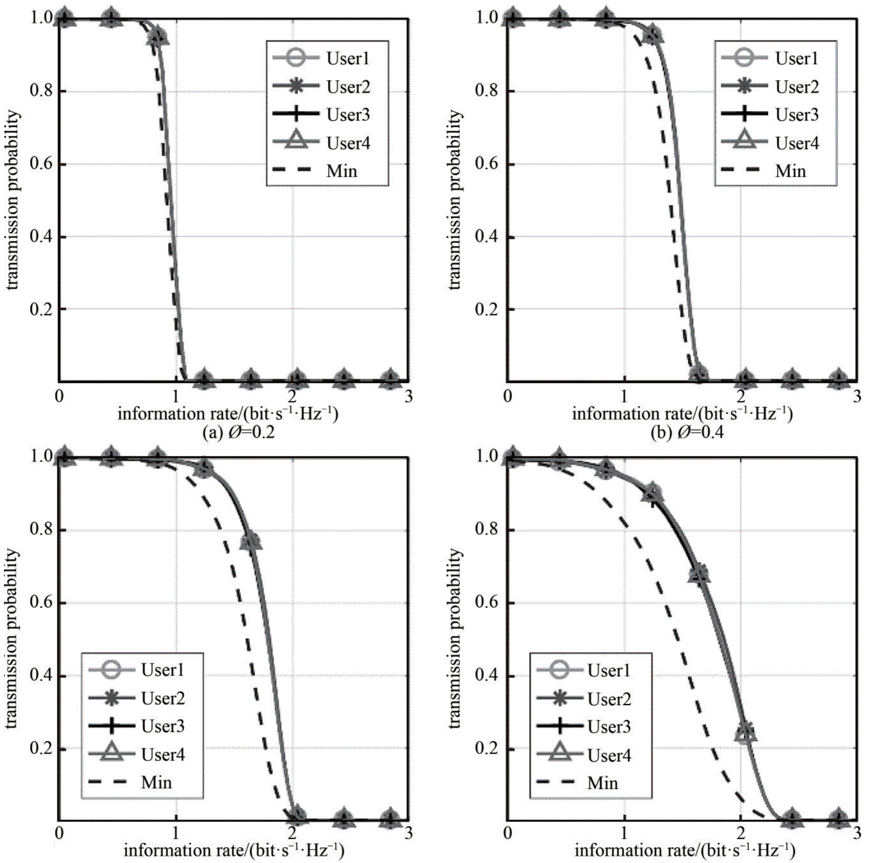
Therefore, we can get an optimal parameters pair that makes the effective secrecy throughput maximum, as circled by the red line in Fig.3.

After that, some disciplines of secure transmission probability with different $\varnothing$ and R_{s} were inspected. In following figures, we apply the legend "User 1" to "User 4" for expressing the simulation result of Bob-1 to Bob-4, and the legend "min" as the simulation result of the whole system. Fig.4 shows the relationship of P_{sec} versus R_{s} by different $\varnothing$. We can see that P_{sec} keeps 1 before a threshold. It's just because the transmitting data rate is so slow that the system secure capacity is always larger than R_{s}, and no outage will occur. After the threshold, however, P_{sec} decreases rapidly and tends to zero.

We also studied the system secure transmission probability and single user's secure transmission probability. Since we choose the minimum channel capacity of all Bobs as the system capacity, the system's P_{sec} is always lower than single user's secure transmission probability. When a system P_{sec} threshold(for example, $P_{\mathrm{sec}} \geqslant 0.95$) is set, the corresponding R_{s} can always keep all users' secure transmission probability higher than the threshold, as shown in Fig. 4. This will keep every user's communication secure.

Fig.5 shows how P_{sec} changes with increasing $\varnothing$ for different R_{s}. P_{sec} keeps zero when $\varnothing$ is too small, because low information signal power will cause low user SNR. After a threshold, P_{sec} first increases, then decreases as $\varnothing$ increases. We can also notice that the optimal $\varnothing$ nearly keeps constant for different R_{s}. This conclusion also coincides with articles like [8] and [9].

Fig.6 is the trend of effective secrecy throughput U with increasing R_{s} for different $\varnothing$. It's a profile of a given $\varnothing$ in Fig.3(b). From this figure, it's obvious that before R_{s} reaching the peak, U linearly increases with R_{s}. After the maximum, U decreases to zero quickly. We also notice that the system optimal R_{s}(information rate corresponding to maximum system effective secrecy throughput) is smaller than each user's optimal R_{s}. That means when we set R_{s} as the system's optimal information, single user can hardly achieve its best transmission performance. Therefore, although this method can ensure security of the whole system, there are still improvement spaces when we want to strengthen a specific user's secure transmission ability.



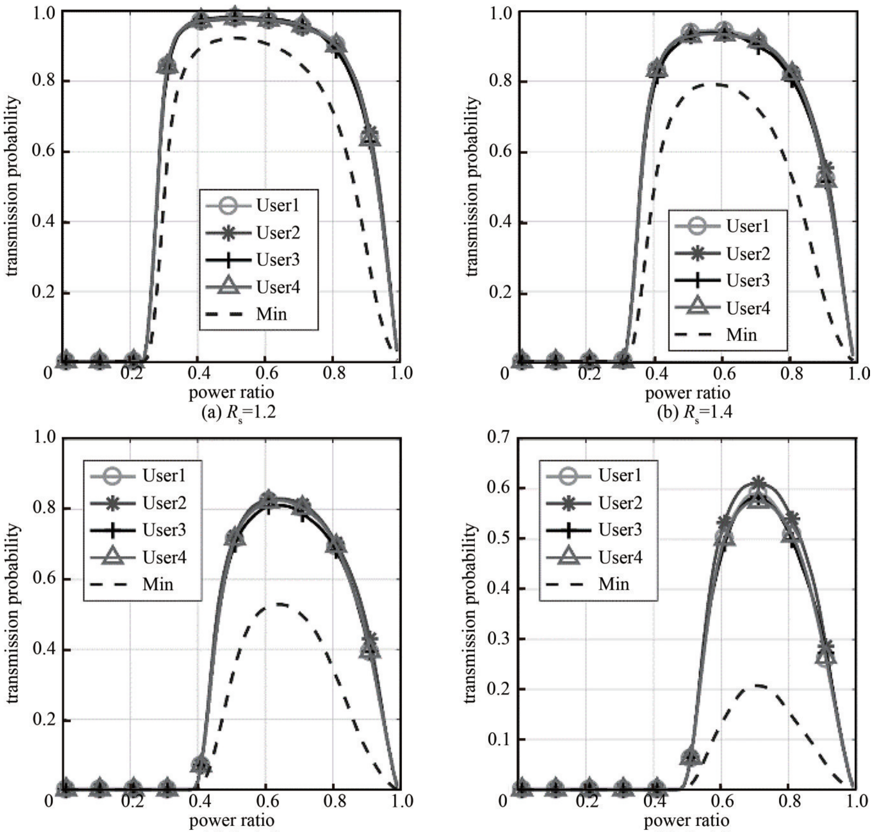
(a) $\varnothing$=0.2

(b) $\varnothing$=0.4

(c) $\varnothing$=0.6

(d) $\varnothing$=0.8

Fig.4 Relationship of secure transmission probability with information rate by different power ratios in a 10×4×5 multiuser system



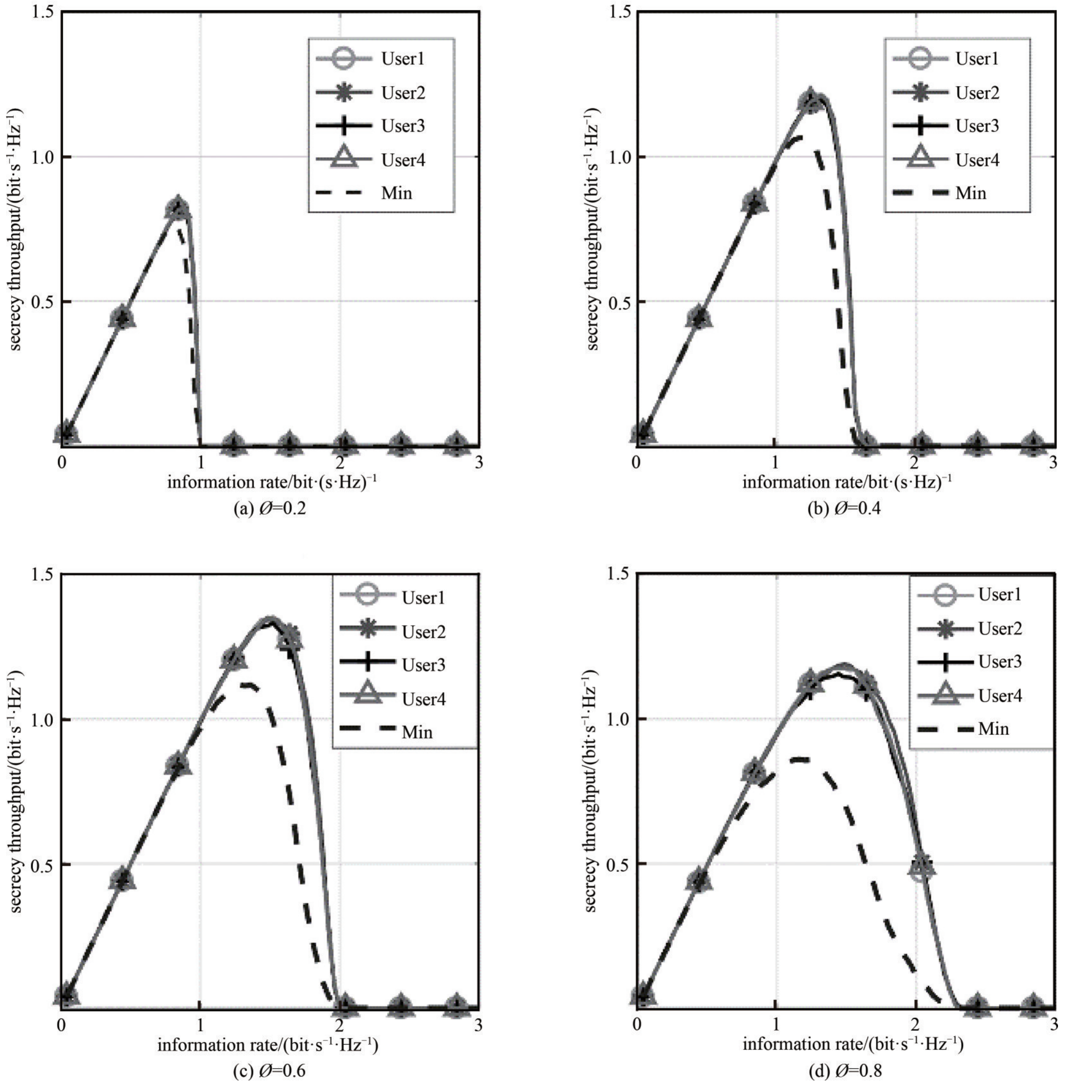
(a) R_s=1.2

(b) R_s=1.4

(c) R_s=1.6

(d) R_s=1.8

Fig.5 Relationship of secure transmission probability with power ratio by different information rates in a 10×4×5 multiuser system



(a) $\varnothing$=0.2

(b) $\varnothing$=0.4

(c) $\varnothing$=0.6

(d) $\varnothing$=0.8

Fig.6 Relationship of effective secrecy throughput with information rate by different power ratios in a 10×4×5 multiuser system

5 Conclusion

In this article, we investigated performance optimization in AN-aid MU-MISOME secure communication system. We first built a new MU-MISOME model in slow fading channels, and derived some expressions of system performance. To overcome difficult problem of closed-form optimization method, we employed Monte-Carlo method to simulate the secure transmission probability for different system parameters, and optimized system secure transmit throughput. Furthermore, we inspected influence on secure transmission probability and effective secrecy throughput by different power ratios and information rates, which will help us to achieve an optimal multiuser secure communication system in practice.

References:

[1] SHANNON C E. Communication theory of secrecy systems[J]. The Bell System Technical Journal, 1949,28(4):656-715. doi:10.1002/j.1538-7305.1949.tb00928.x.

[2] WYNER A D. The wire-tap channel[J]. The Bell System Technical Journal, 1975,54(8):1355-1387. doi:10.1002/j.1538-7305.1975.tb02040.x.

[3] GOEL S,NEGI R. Guaranteeing secrecy using artificial noise[J]. IEEE Transactions on Wireless Communications, 2008,7(6):2180-2189. doi:10.1109/TWC.2008.060848.

[4] ZHOU X,MCKAY M R. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation[J]. IEEE Transactions on Vehicular Technology, 2010,59(8):3831-3842. doi:10.1109/TVT.2010.2059057.

[5] YANG N,ELKASHLAN M,DUONG T Q,et al. Optimal transmission with artificial noise in MISOME wiretap channels[J]. IEEE Transactions on Vehicular Technology, 2016,65(4):2170-2181. doi:10.1109/TVT.2015.2419318.

[6] YAN S, YANG N, LAND I, et al. Three artificial-noise-aided secure transmission schemes in wiretap channels[J]. IEEE Transactions on Vehicular Technology, 2018,67(4):3669-3673. doi:10.1109/TVT.2017.2779508.

[7] HU D,MU P,ZHANG W,et al. Minimization of secrecy outage probability with artificial-noise-aided beamforming for MISO wiretap channels[J]. IEEE Communications Letters, 2020,24(2):401-404. doi:10.1109/LCOMM.2019.2957121.

[8] WANG B,MU P. Artificial noise-aided secure multicasting design under secrecy outage constraint[J]. IEEE Transactions on Communications, 2017,65(12):5401-5414. doi:10.1109/TCOMM.2017.2748118.

[9] ATALLAH M,KADDOUM G. Secrecy analysis in wireless network with passive eavesdroppers by using partial cooperation[J]. IEEE Transactions on Vehicular Technology, 2019,68(7):7225-7230. doi:10.1109/TVT.2019.2913934.

[10] YOO T,GOLDSMITH A. On the optimality of multiantenna broadcast scheduling using zero-forcing beamforming[J]. IEEE Journal on Selected Areas in Communications, 2006,24(3):528-541. doi:10.1109/JSAC.2005.862421.

[11] CHRISTENSEN S S,AGARWAL R,DE CARVALHO E,et al. Weighted sum-rate maximization using weighted MMSE for MIMO-BC beamforming design[J]. IEEE Transactions on Wireless Communications, 2008,7(12):4792-4799. doi:10.1109/TWC.2008.070851.

[12] YAO Li,LIU Youjiang,ZHANG Jian,et al. Secure beamforming method for artificial-noise-aided multiuser broadcast system with users of different importance under secrecy outage probability constraint[J]. IET Communications, 2020,14(19):3380-3387. doi:10.1049/iet-com.2020.0277.

[13] 刘凯,李新颖,郝浩. 多用户多中继系统下协作NOMA的中断性能[J]. 太赫兹科学与电子信息学报, 2020,18(4):586-594. (LIU Kai,LI Xinying,HAO Hao. Outage performance of cooperative NOMA under multiuser and multi-relay system[J]. Journal of Terahertz Science and Electronic Information Technology, 2020,18(4):586-594.) doi:10.11805/TKYDA2019007.

Biographies:

YAO Li(1990-), Ph.D., his main research direction is secure communication and physical layer security. email:519055375@qq.com.

LIU Youjiang(1987-), Ph. D., Professor. His research interests include signal generation, processing, and circuit design for advanced RF front-ends.

ZHANG Jian(1968-), Ph.D., Professor. His current research involves physics-based electronics and optoelectronics, MMW and Terahertz technology.