Power Allocation for Physical Layer Security Among Similar Channels

Xiangxue Tai[1], Shuai Han[1(✉)], Xi Chen[2], and Qingli Zhang[1]

[1] Harbin Institute of Technology, Harbin, China
hanshuai@hit.edu.cn
[2] Flatiron Institute, Simons Foundation, New York, NY, USA

Abstract. Physical layer security technologies are used to ensure the secure communication when eavesdroppers use infinite computing capabilities to launch brute force attacks. Traditional physical layer security technologies utilized the difference between legitimate channels and eavesdropping channels. However, in certain scenarios, the legitimate channels are similar to eavesdropping channels so that the communication become insecure. In this paper, we especially studied the physical layer security communication among similar channels. An interference relay model was proposed to ensure the security of communication and at the same time, optimize the power allocation by maximizing the lower bound of the secrecy outage probability. The theoretical secrecy outage probability of the proposed power allocation scheme was derived. Simulation results show that the proposed scheme is superior to a uniform power allocation scheme on channel security performance under the same condition. Furthermore, using simulation, we demonstrated that the derivation of secrecy outage probability for the proposed power allocation scheme is valid.

Keywords: Physical layer security · Similar channels
Power allocation · Interference relay

1 Introduction

Physical layer security is an information theoretical approach to achieving confidentiality at the physical layer [1]. Physical layer security technologies can resist quantum attack and play a key role in secure communications. Currently, there are several studies discussing physical layer security technologies. Precoding/beamforming technologies played a vital role physical layer security. In paper [2], two novel schemes were proposed to enhance the security performance using precoding-aided spatial modulation (PSM): one used the random antenna selection (RAS) technique to generate zero-forcing precoding matrices with randomly

This work is supported by the National Natural Science Foundation of China (No. 91438205 and No. 61471143).

J. Zheng et al. (Eds.): ADHOCNETS 2018, LNICST 258, pp. 247–257, 2019.
https://doi.org/10.1007/978-3-030-05888-3_23

activated transmit antennas; the other was an improved version of RAS-PSM by introducing the time-varying artificial noise into RAS-PSM. Another precoding scheme was proposed for multiple input multiple output (MIMO) system [3] where two cases were analyzed as: (1) all CSI (Channel State Information) with legitimate channels at the transmitter could maximize the signal to noise ratio (SNR) of the receiver and the secret rate: (2) the transmitter used an improved Lloyd algorithm to construct the codebook. This scheme quantified the precoding and finally obtained a low-complexity postcode scheme to offset the SNR loss. Moreover, in recent years artificial noise technologies became more important in physical layer security communication. Artificial noise tech-nologies can jam the eavesdropper so as to improve the security capacity. Nowadays, artificial noise technologies mainly included zero-space noise based on MIMO and noise base station deployment based on random geometric model [4]. Artificial noise technologies were often combined with beamforming [5,6]. By jointly optimizing beamforming and the artificial noise vector of all base stations, they minimized the total transmit power, ensured the QoS (Quality of Service) of authorized users and prevented unauthorized users from intercepting information. Some existing conclusions about single antenna eavesdroppers were extended to multi-antenna eavesdroppers. It has been proved that the traditional zero-space artificial noise scheme is the best choice given any system parameters. Random beamforming technology is also used for physical layer security in some cases since it only used partial CSI but can effectively improve the system security. Exploiting full duplexity to enhance physical layer security has received considerable attention [7]. Besides, physical layer security is studied for the fifth generation communication system (5G), where beamforming based on massive MIMO [8] and secure transmission for millimeter wave systems [9] were both studied.

Physical layer security technologies make the information transmit securely by modelling the difference of channel status information (CSI, you should move this to the place where CSI was mentioned for the first time) between legitimate channels and eavesdropping channels. However, if the distance from legitimate receiver to the eavesdropper is too short compared to the distance between the transmitter to legitimate receiver or eavesdropper, the CSI of the legitimate channel will be very similar to that of the wiretap channel. In such cases, existing physical layer security schemes cannot perform transmission securely any more.

In this paper, to solve the security transmission problem when legal channels are similar to wiretap channels, we proposed a power allocation scheme based on a physical layer security model with interference relays. Key performance measurements of physical layer security include the ergodic secrecy capacity and the secrecy outage probability. We derived the expression of optimal power allocation parameters by maximizing the lower bound of ergodic secrecy capacity. In the meanwhile, the secrecy outage probability was also derived to evaluate the performance of the proposed power allocation scheme.

The rest of this paper is organized as follows. The system model is provided in Sect. 2. In section Sect. 3, power allocation to realize physical layer security com-

munication among similar channels is optimized and a optimal power allocation scheme is proposed. Theoretical analysis is performed in Sect. 4 and the secrecy outage probability based on the proposed optimal power allocation scheme is derived. Simulation results are provided in Sect. 5 to evaluate the secrecy performance of the uniform power allocation scheme and the proposed power allocation scheme. We also verify the accuracy of the secrecy outage probability based on optimal power allocation scheme we derived. Section 6 draws the conclusion of this paper.

Our notations are as follows. In this paper, we use x, $\mathbf{x}$, $\mathbf{X}$ to denote a scalar, a vector and a matrix, respectively. $||\mathbf{x}||^2$ represent 2-norm of vector $\mathbf{x}$. If $\mathbf{X} \in \mathbb{C}^{N\times M}$ denotes that $\mathbf{X}$ is a $N \times M$ dimensional complex matrix. $\mathcal{CN}(0, \sigma^2)$ denotes the circular symmetric complex Gaussian distribution with zero mean and covariance σ^2. $\{x\}^+ = \max(0, x)$. $E(x)$ denotes the mathematical expectation of x.

2 System Model

In order to bring difference to legal channels and wiretap channels, we consider adding interference relays to the system, as shown in Fig. 1. The interference node relays interfering signals, which are orthogonal to the channels from the interference relay node to the legitimate receivers. Then, the interfering signals will only reduce the eavesdropper's signal quality.

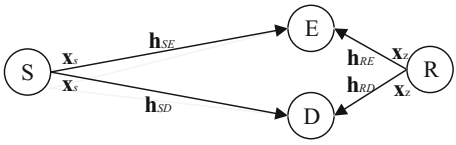

Fig. 1. The physical layer security communication interference relay model for the specific indifference channels

Figure 1 is the proposed physical layer security communication interference relay model for the scenario when channels are not differential enough to ensure secure communication. Source node S represents the transmitter, destination node D represents the legitimate receiver, eavesdropping node E represents the eavesdropping receiver, and relay node R represents the interference relay. The distance from S to D or E is very long so that the distance between D and E can be ignored. Then, S-D channel and S-E channel are very similar. In Fig. 1, we assume that the distance between R and D or R and E is not that long such that the distance between D to E is comparable with it. Then, S-D channel and S-E channel are differential. $\mathbf{h}_{SD}$ denotes the CSI vector from S to D, $\mathbf{h}_{SD} \in \mathbb{C}^{N_s\times 1}$, where N_s is the number antennas of transmitter S. $\mathbf{h}_{SE}$ is the CSI vector from S to E, $\mathbf{h}_{SE} \in \mathbb{C}^{N_s\times 1}$. Especially, $\mathbf{h}_{SE} = \mathbf{h}_{SD}$. $\mathbf{h}_{RD}$ is the CSI vector from R to

D, $\mathbf{h}_{RD} \in \mathbb{C}^{N_r \times 1}$. $\mathbf{h}_{RE}$ is the CSI vector from R to D, $\mathbf{h}_{RE} \in \mathbb{C}^{N_r \times 1}$. $\mathbf{x}_s$ is the useful signal which S transmits to D, $\|\mathbf{x}_s\|^2 = 1$. $\mathbf{x}_z$ is the interference which R transmits to E. $\mathbf{x}_z$ is pseudo random complex Gaussian noise and is orthogonal to $\mathbf{h}_{RD}$, namely $\mathbf{h}_{RD}\mathbf{x}_z = 0$. Besides, $\|\mathbf{x}_z\|^2 = 1$.

Assume that the total power constraint of the system is P which is the sum of the transmitting power of S and R. We introduce a power allocation factor as λ so that the power of S is λP and the power of R is $(1-\lambda)P$. Assume that the receiving antenna gain of E and D are the same. Then the signals received at D and E can be respectively expressed as:

$$y_d = \sqrt{\lambda P}\mathbf{h}_{SD}^H \mathbf{x}_s + \sqrt{(1-\lambda)P}\mathbf{h}_{RD}^H \mathbf{x}_z + n_d, \tag{1}$$

$$y_e = \sqrt{\lambda P}\mathbf{h}_{SE}^H \mathbf{x}_s + \sqrt{(1-\lambda)P}\mathbf{h}_{RE}^H \mathbf{x}_z + n_e, \tag{2}$$

where y_d is the signal received at the destination node D and y_e is the signal received at the eavesdropping node E. n_d is the complex Gaussian random noise received at the destination node D, $n_d \sim \mathcal{CN}(0, \sigma_d^2)$. n_e is the complex Gaussian random noise received at the eavesdropping node E, $n_e \sim \mathcal{CN}(0, \sigma_e^2)$.

Because $\mathbf{h}_{RD}\mathbf{x}_z = 0$, the signal to noise ratio γ_d at the destination node D can be expressed as

$$\gamma_d = \frac{\lambda P \|\mathbf{h}_{SD}\|^2}{\sigma_d^2}. \tag{3}$$

And the signal to noise ratio γ_e at the eavesdropping node E can be expressed as

$$\gamma_e = \frac{\lambda P \|\mathbf{h}_{SE}\|^2}{(1-\lambda)P\|\mathbf{h}_{RE}\|^2 \cos\theta + \sigma_e^2}, \tag{4}$$

where θ is the angle which obeys uniform distribution between $\mathbf{h}_{RE}$ and $\mathbf{x}_z$, $\theta \in (-\frac{\pi}{2}, \frac{\pi}{2})$.

Then the instantaneous secrecy capacity can be expressed as

$$C_s(\lambda) = [\log_2(1+\gamma_d) - \log_2(1+\gamma_e)]^+. \tag{5}$$

Due to $\mathbf{h}_{SE} = \mathbf{h}_{SD}$, $\sigma_d^2 = \sigma_e^2$, $(1-\lambda)P\|\mathbf{h}_{RE}\|^2 \cos\theta > 0$, we can get $\gamma_d > \gamma_e$. Hence, $C_s > 0$. Therefore, the system model can achieve physical layer security communication among indifference channels.

3 A Optimal Power Allocation Scheme to Realize Physical Layer Security Communication Among Similar Channels

3.1 Power Allocation Optimization

The secrecy performance of system is relevant to the secrecy outage probability. The bigger the secrecy outage probability is, the better the secrecy performance is. Hence, it is meaningful to optimize secrecy outage probability.

Assume that the minimum transmission rate that ensures normal system secure operation is R_s, the secrecy outage probability can be expressed as

$$P_{out}(R_s) = Pr[C_s(\lambda) < R_s]. \tag{6}$$

Let $\gamma_{SD} = \frac{P\|\mathbf{h}_{SD}\|^2}{\sigma_d^2}$, $\gamma_{RD} = \frac{P\|\mathbf{h}_{RD}\|^2}{\sigma_d^2}$, $\gamma_{SE} = \frac{P\|\mathbf{h}_{SE}\|^2}{\sigma_e^2}$ and $\gamma_{RE} = \frac{P\|\mathbf{h}_{RE}\|^2 \cos\theta}{\sigma_e^2}$, then the Eqs. (3) and (4) can be expressed as

$$\gamma_d = \lambda\gamma_{SD}, \tag{7}$$

$$\gamma_e = \frac{\lambda\gamma_{SE}}{(1-\lambda)\gamma_{RE} + 1}. \tag{8}$$

Submitting Eqs. (3), (4) and (5) into Eq. (6) and simplifying, the secrecy outage probability can be rewritten as

$$P_{out}(R_s) = Pr[g(\lambda) < 2^{R_s} - 1]. \tag{9}$$

where

$$g(\lambda) = (1 - 2^{R_s})\lambda\gamma_{SD} + (1 - 2^{R_s})(1-\lambda)\gamma_{RE} + \lambda(1-\lambda)\gamma_{SD}\gamma_{RE}.$$

In [10], $Pr[g(x) \le t] \ge 1 - E(x)/t$. Hence, we can get

$$P_{out}(R_s) \ge 1 - \frac{E[g(\lambda)]}{2^{R_s} - 1}. \tag{10}$$

The lower bound of the secrecy outage probability can be expressed as $1 - \frac{E[g(\lambda)]}{2^{R_s} - 1}$. Because it is difficult to maximize the secrecy outage probability, we try to maximize the lower bound of the secrecy outage probability. Then, the optimal power allocation factor λ^* should make the secrecy outage probability maximum, which can be expressed as

$$\lambda^* = \arg\min_{0<\lambda<1}(1 - \frac{E[g(\lambda)]}{2^{R_s} - 1}). \tag{11}$$

The Eq. (11) is equivalent to

$$\lambda^* = \arg\max_{0<\lambda<1} E[g(\lambda)]. \tag{12}$$

Above all, the $E[g(\lambda)]$ can be expressed as

$$\begin{aligned} E[g(\lambda)] = &-E[\gamma_{SD}]E[\gamma_{RE}]\lambda^2 + [(1 - 2^{R_s})(E[\gamma_{SD}] - E[\gamma_{RE}]) \\ &+E[\gamma_{SD}]E[\gamma_{RE}]]\lambda + (1 - 2^{R_s})E[\gamma_{RE}]. \end{aligned} \tag{13}$$

According to Eq. (13), $E[g(\lambda)]$ is a quadratic function. The maximum point is its extreme point. Namely, the optimal power allocation factor λ^* is the extreme

point of $E[g(\lambda)]$. Hence, the optimal power allocation factor λ^* can be expressed as

$$\lambda^* = \frac{1}{2} + \frac{2^{R_s}-1}{2P}\left(\frac{1}{E[\|\mathbf{h}_{SD}\|^2]} - \frac{\pi}{E[\|\mathbf{h}_{RE}\|^2]}\right). \tag{14}$$

From Eq. (14), we can see that the optimal power allocation factor λ^* is relevant to $E[\|\mathbf{h}_{SD}\|^2]$, $E[\|\mathbf{h}_{RE}\|^2]$, P and R_s. Hence, when P and R_s is fixed, the optimal power allocation factor λ^* will not change until the statistics channel state information of channel $\mathbf{h}_{SD}$ and $\mathbf{h}_{RE}$ change. Besides, when $P \to \infty$, $\frac{2^{R_s}-1}{2P}\left(\frac{1}{E[\|\mathbf{h}_{SD}\|^2]} - \frac{\pi}{E[\|\mathbf{h}_{RE}\|^2]}\right) \to 0$, $\lambda^* \to \frac{1}{2}$. Therefore, when the total power constraints P is large enough, this optimal power allocation based on the lower bound of secrecy outage probability has the same secrecy performance on secrecy outage probability as the fixed uniform power allocation scheme of which power allocation factor λ^* is equal to 0.5.

3.2 A Power Allocation Scheme

According to the optimal power allocation factor λ^*, a power allocation scheme is proposed which is summarized in the following procedure.

1: Source node S gets the channel state information from S to D ($E[\|\mathbf{h}_{SD}\|^2]$). Relay node R feeds back the channel state information from R to E ($E[\|\mathbf{h}_{RE}\|^2]$) to the source node E.
2: Source node S calculates the power allocation factor λ^* according to the equation (14).
3: Source node S infroms the λ^* to the Relay node R.
4: Send the useful data safely. The transmitting power of the source node S is λP and the transmitting power of the interference relay is $(1-\lambda)P$. Meanwhile, Source node S checks whether the statistics channel static information has changed.
5: If the statistics channel static information has changed, return to perform step 2. channel static information has changed.

The power allocation factor λ^* is determined at S with the statistics CSI. Then the power allocation factor is fed back to R. The system conduct the transmission in a secure way and check if the statistics CSI has changed at the same time. S will update λ^* if the statistics CSI has changed.

This proposed power allocation scheme has the following characteristics. First, this scheme achieves the physical layer security communication when the distance between a legitimate receiver and a eavesdropping receiver is too short if compared to the distance between a transmitter and a legitimate receiver/eavesdropping receiver. It solves the security issue when legal channels are similar to eavesdropping channels. Second, it can get a better security performance on erodgic secrecy capacity and secrecy outage probability compared

to the uniform power allocation scheme (as demonstrated in the next section). Third, compared to the power allocation scheme using instantaneous CSI, this scheme only requires the statistics CSI, which is available in most applications. Finally, this scheme only updates the power allocation factor when the statistics CSI changes. It will save signaling overhead.

4 Performance Theoretical Analysis

Due that the optimal power allocation is based on the lower bound of secrecy outage probability. Hence, it is meaningful to derive the secrecy outage probability under this power allocation scheme.

The expression of secrecy outage probability has been given in Eq. (9). Let $\gamma_{SD} = \frac{P\|\mathbf{h}_{SD}\|^2}{\sigma_d^2}$, $\gamma_{RD} = \frac{P\|\mathbf{h}_{RD}\|^2}{\sigma_d^2}$, $\gamma_{SE} = \frac{P\|\mathbf{h}_{SE}\|^2}{\sigma_e^2}$ and $\gamma_{RE} = \frac{P\|\mathbf{h}_{RE}\|^2 \cos\theta}{\sigma_e^2}$, the power allocation can be rewritten as

$$P_{out}(R_s) = P_r[ax_1 + bx_2\cos\theta + cx_1x_2\cos\theta < t], \tag{15}$$

where

$$\begin{aligned} a &= \frac{(1-2^{R_s})\lambda P}{\sigma_d^2},\ b = \frac{(1-2^{R_s})(1-\lambda)P}{\sigma_e^2} \\ c &= \frac{\lambda(1-\lambda)P^2}{\sigma_d^2\sigma_e^2},\ t = 2^{R_s} - 1 \\ x_1 &= \|\mathbf{h}_{SD}\|^2, \qquad x_2 = \|\mathbf{h}_{RE}\|^2 \end{aligned} \tag{16}$$

Obviously, $a < 0$, $b < 0$, $c > 0$, $t > 0$. Besides, they are all const. Hence, the secrecy outage probability can be triple integrals which is

$$P_{out}(R_s) = \iiint_Q p(x_1)p(x_2)p(\theta)dx_1dx_2d\theta, \tag{17}$$

where Q is the restrictions and follows

$$Q: ax_1 + bx_2\cos\theta + cx_1x_2\cos\theta < t, \tag{18}$$

$p(x_1)$, $p(x_2)$ and $p(\theta)$ are respectively the probability density functions of x_1, x_2 and θ. Furthermore, We can get the integration interval more intuitively in Fig. 2.

Due to each element in $\mathbf{h}_{SD}$ and $\mathbf{h}_{RE}$ obeys the complex Gaussian random distribution, $\|\mathbf{h}_{SD}\|^2$ and $\|\mathbf{h}_{RE}\|^2$ follow χ^2 distribution. Assume that θ follows uniform distribution. Then the probability density functions of x_1, x_2 and θ can be expressed as

$$p(x_1) = \begin{cases} \frac{1}{2^{N_r}\Gamma(2N_r)\sigma_{SD}^{2N_r}} x_1^{N_r-1} e^{-\frac{x_1}{2\sigma_{SD}^2}}, & x_1 > 0 \\ 0, & x_1 \le 0 \end{cases} \tag{19}$$

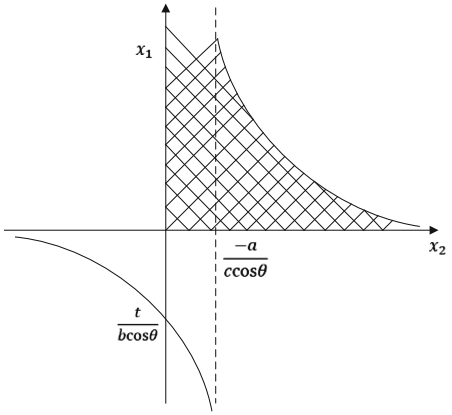

Fig. 2. The integration interval Q

$$p\left(x_2\right)=\begin{cases}\dfrac{1}{2^{N_r}\Gamma(N_r)\sigma_{RE}^{2N_r}}{x_2}^{N_r-1}e^{-\dfrac{x_2}{2\sigma_{RE}^2N_r}}, & x_2>0\\ 0, & x_2\le 0\end{cases} \tag{20}$$

$$p(\theta)=\begin{cases}\dfrac{1}{\pi},\ \theta\in(-\dfrac{\pi}{2},\dfrac{\pi}{2})\\ 0,\ \ otherwise\end{cases} \tag{21}$$

where $\sigma_{RE}^2=\dfrac{E[||\mathbf{h}_{RE}||^2]}{2N_r}$ and $\sigma_{SD}^2=\dfrac{E[||\mathbf{h}_{SD}||^2]}{2N_r}$.

Then the final expression of the secrecy outage probability is

$$\begin{aligned}P_{out}\left(R_s\right)&=\frac{1}{\pi}\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}}(1-e^{\bigtriangledown_1}\sum_{k=0}^{N_r-1}\frac{1}{k!}(-\bigtriangledown_1)^k d\theta\\&+\frac{1}{\pi}\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}}\int_{-\frac{a}{c\cos\theta}}^{\infty}p(x_2)[1-e^{-\bigtriangledown_2}\sum_{k=0}^{N_r-1}\frac{1}{k!}\bigtriangledown_2{}^k]\,dx_2\,d\theta,\end{aligned} \tag{22}$$

where $\bigtriangledown_1$ and $\bigtriangledown_2$ are respectively

$$\bigtriangledown_1=\frac{a}{2c\cos\theta\sigma_{RE}^2}, \tag{23}$$

$$\bigtriangledown_2=\frac{t-bx_2\cos\theta}{2(cx_2\cos\theta+a)\sigma_{SD}^2}. \tag{24}$$

5 Numerical Results and Analysis

In this section, we conduct simulations and evaluate the erodgic secrecy capacity and the secrecy outage probability of the proposed physical layer security scheme.

The secrecy outage probability of the system using the optimal power allocation scheme ($\lambda = \lambda^*$) has been compared to the fixed uniform power allocation scheme ($\lambda = 0.5$).

5.1 Analysis of Secrecy Outage Probability

Figure 3 shows the erodgic secrecy capacity performance against total transmit power P for the proposed power allocation scheme ($\lambda^* = 0.5$) and the fixed uniform power allocation scheme ($\lambda = 0.5$). We assume that $N_s = N_r = 2, 4, 8$, $N_d = 1$ and $N_e = 1$. All the channels of the system are the Rayleigh fading channels. The noise power at D or E is normalized, as $P = P/\sigma^2$. Hence, the signal-to-noise ratio of the total transmitted power varies from 1 dB to 15 dB. We set the minimum transmission rate R_s=1.5 bit/s/Hz.

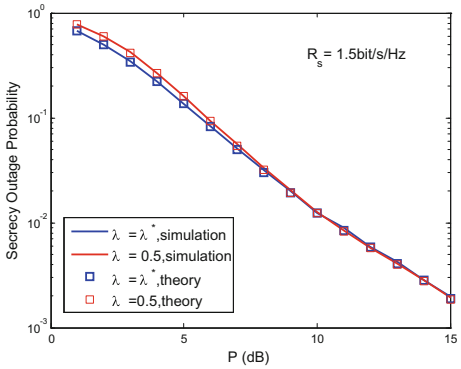

Fig. 3. Secrecy outage probability against total transmit power P for the proposed power allocation scheme and the fixed uniform power allocation scheme

In Fig. 3, it can be seen that the total power constraint P has a positive effect on the secrecy outage probability. When the total power constraint P is fixed, the secrecy outage probability of the system using the optimal power allocation scheme is smaller than the system using the uniform power allocation scheme. And for our power allocation scheme, the secrecy outage probability curve of the simulation results fits the one of Eq. (22) theoretical numerical results, based on which, it can be derived that the theoretical result of secrecy outage probability is correct.

5.2 Analysis of Ergodic Secrecy Capacity

Simulation conditions are the same as those in section A. Here, the minimal data rate R_s to ensure the system communication keeping secret is set to 1.5 bit/s/Hz, which also means if the data rate is smaller than R_s, the system cannot communicate in secure way. The secrecy outage probability against total

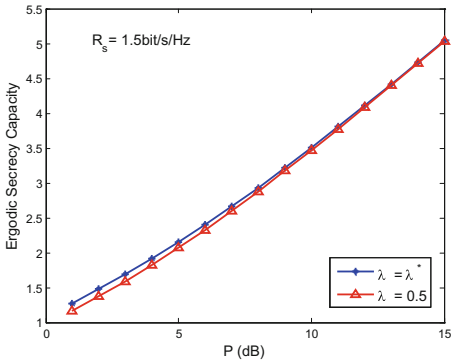

Fig. 4. Erodgic secrecy capacity against total transmit power P for the proposed power allocation scheme and the fixed uniform power allocation scheme

transmit power P for the proposed power allocation scheme ($\lambda^* = 0.5$) and the fixed uniform power allocation scheme ($\lambda = 0.5$) are shown in Fig. 4.

We can see that the greater the total power constraint P, the better the erodgic secrecy capacity performance of the system will be. Moreover, when the total power allocation constraint P is fixed, the optimal power allocation scheme we proposed can ensure a bigger erodgic secrecy capacity than the uniform power allocation scheme. Hence, as for the erodgic secrecy capacity performance, our proposed power allocation scheme is better than the fixed uniform power allocation scheme.

6 Conclusion

In this paper, we solved the challenging problem existing in traditional physical layer security communications, when the difference between legal and eavesdropping channels is not enough to meet the security requirement for information transmission. We specifically studied the power allocation between source node and interference relay node in physical layer security communication with interference relay. We optimized the power allocation through the minimization of lower bound of secrecy outage probability. Further, we developed a power allocation scheme, analyzed its advantages and derived its theoretical secrecy outage probability. Simulation results demonstrated that the proposed power allocation scheme has a better ergodic secrecy capacity and a lower secrecy outage probability than a uniform power allocation scheme.

References

1. Liang, Y., Poor, H.V., Shamai (Shitz), S.: Information theoretic security. Found. Trends Commun. Inf. Theory **5**(4–5), 355–580 (2008)
2. Huang, Y., Zheng, B., Wen, M., et al.: Improving physical layer security via random precoding. In: IEEE GLOBECOM Workshops, pp. 1–6 (2017)
3. Geraci, G., Egan, M., Yuan, J.H., et al.: Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding. IEEE Trans. Commun. **60**(11), 3472–3482 (2012)
4. Wang, H.M., Wang, C., Zheng, T.X., Quek, T.Q.S.: Impact of artificial noise on cellular networks: a stochastic geometry approach. IEEE Trans. Wirel. Commun. **6**(99), 1–5 (2016)
5. Lu, Y., Xiong, K., Fan, P., Zhong, Z.: Optimal coordinated beamforming with artificial noise for secure transmission in multi-cell multi-user networks. In: 2017 IEEE International Conference on Communications (ICC), France, Paris, pp. 1–6 (2017)
6. Mei, W., Chen, Z., Fang, J.: Artificial noise aided energy efficiency optimization in MIMOME system with SWIPT. IEEE Commun. Lett. **21**(8), 1795–1798 (2017)
7. Li, Q., Zhang, Y., Lin, J., et al.: Full-duplex bidirectional secure communications under perfect and distributionally ambiguous eavesdroppers CSI. IEEE Trans. Sig. Process. **65**(17), 4684–4697 (2017)
8. Yaacoub, E., Al-Husseini, M.: Achieving physical layer security with massive MIMO beamforming. In: 2017 11th European Conference on Antennas and Propagation (EUCAP), Paris, France, pp. 1753–1757 (2017)
9. Ying, J., Wang, H.-M., Zheng, T.-X., et al.: Secure transmissions in millimeter wave systems. IEEE Trans. Veh. Technol. **66**(9), 7809–7817 (2017)
10. Abramowitz, M., Stegun, L.A.: Handbook of Mathematical Functions with Formulaes, Graphs, and Mathematical Tables. Dover Publications Inc., New York (1974)