Communications and Network, **2013, 5, 194-199**
http://dx.doi.org/10.4236/cn.2013.53B2037 Published Online September 2013 (http://www.scirp.org/journal/cn)

Artificial Noise Based Security Algorithm for Multi-User MIMO System

Jian-hua Peng, Kai-zhi Huang, Jiang Ji
National Digital Switching System Engineering & Technological Research Center, Zhengzhou, China
Email: hongyinghunan@126.com

Received June, 2013

ABSTRACT

The existing physical layer security algorithm, which is based on artificial noise, could affect legitimate receivers negatively when the number of users is no less than sending antennas in multi-user MIMO system. In order to improve security of multi-user MIMO system under this scenario, we propose a new multi-user MIMO system physical layer security algorithm based on joint channel state matrix. Firstly, multiple users are processed together, thus a multi-user joint channel state matrix is established. After achieving Singular Value Decomposition (SVD) of the joint channel state matrix, the minimum singular value is obtained, which can be utilized for precoding to eliminate the interference of artificial noise to legitimate receivers. Further, we also present an approach to optimize the power allocation. Simulation results show that the proposed algorithm can increase secrecy capacity by 0.1 bit/s/HZ averagely.

Keywords: Multi-user MIMO System; Joint Channel State Matrix; Secrecy Capacity; Artificial Noise; Physical Layer Security

1. Introduction

The multiple-input-multiple-output (MIMO) technology has become one of the key technologies for the next generation wireless communication systems. Besides, it has been introduced in the standards like IEEE 802.11/16 and 3GPP LTE. Due to the broadcast characteristics of the electromagnetic signal propagation and the openness of wireless channels, however, transmission of communication contents in the wireless communication system can be easily intercepted. Thusly, it has become important increasingly for protecting the multi-user MIMO system communication security.

Considering the scenario without null space in the multi-user MIMO system (number of legitimate users is more than or equal to the number of antennas at the transmitter), artificial noise for the physical layer security will introduce additional noise to the legitimate users. For this reason, available research about using artificial noise to achieve multi-user MIMO system physical layer security is conducted under the scenario of null space existing in the system. [1,2] proposed a method improving security of the legitimate users by sending artificial noise to third-party users: the potential eavesdropper's receiving could be inhibited by setting main lobe directing at the desired users at the multi-antenna transmitting terminal and transmitting artificial noise in the other beam. Communication security can be improved via combining the beam forming and the artificial noise when the locations of eavesdroppers are unknown [3]. Another way to protect the security of the legitimate users is achieved by introducing redundancy and transmitting artificial noise in the view of space and frequency domains combined [4]. An encipherment scheme under multi-user downlinks situation is proposed using artificial noise jamming the eavesdroppers [5, 6]. Especially, [5] discusses the security effectiveness of linear beam forming with artificial noise integrated respectively in the MIMO broadcast channel and the MIMO transmission multicast; besides, the noise power allocation scheme is also considered with the SINR of desired users unchanged. [7-9] provide a derivation and prove the secrecy capacity range when there are multiple legitimate users and eavesdroppers in Gaussian MIMO and MISO wiretap channel. The noise power allocation is specific researched to maximize the secrecy capacity in literature [10]. In order to ensure the existence of system null space when the number of antennas in transmitting terminal is limited, literature [11] studies how to select users from the downlink multi-users to keep the security of the system. However, the application scenarios discussed above are limited, which restrict the system users' capacity.

In the paper, a multi-user MIMO system security algorithm based on artificial noise is proposed, aiming at no null space in multi-user MIMO system scenario, and translating the problem of eliminating the interference of artificial noise to design of precoding. Firstly, multiple

legitimate users are processed together at transmitting terminal, thus a multi-user joint channel state matrix and its complement matrix are established. Then, after Singular Value Decomposition of the joint channel state matrix and the complement matrix respectively, the minimum singular value can be utilized for precoding, so as to eliminate the interference of artificial noise to legitimate receivers and multi-user. At last, the paper presented an approach to optimize the power allocation. The paper established a joint channel state matrix and sufficiently considered the problems might exist in the multi-user system, by precoding both the artificial noise affect to the legitimate users is suppressed and the interference between the multi-user is eliminated; the artificial noise is forced to be transmitted via the smallest-affect sub-channel, while the majority artificial noise falls on the eavesdropping side. Simulation results show that the proposed algorithm can increase the secrecy capacity by 0.1 bit/s/HZ averagely.

2. Security Model of the Multi-user MIMO System

The encipherment model of the multi-user MIMO system is shown as **Figure 1**. Supposing there are N_T transmitting antennas at transmitting terminal, the number of receiving antennas of each K legitimate users is present as N_R. There is also a eavesdropper whose number of receiving antennas is N_E.

Respectively, the signals received by the k-th legitimate user and the eavesdropper can be shown as:

$$y_k = H_k t_k b_k + H_k \sum_{j \neq k}^{K} t_j b_j + H_k pz + n_k \tag{1}$$

$$y_e = H_e \sum_{j=1}^{K} t_j z_j + H_e pz + n_e \tag{2}$$

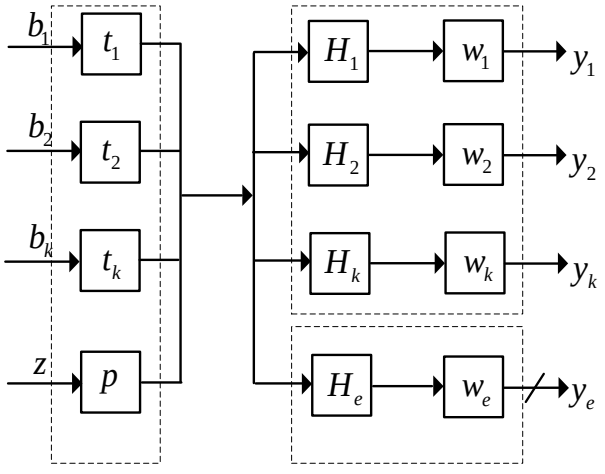

Figure 1. The Security model of multi-user MIMO system.

Among them: b_k is the transmitting signal of the k-th legitimate user, H_k is the channel state matrix of the k-th legitimate user, H_e is the channel state matrix of the eavesdropper, t_k and p, the dimension all being $N_T \times 1$, are respectively stand for the precoding of eliminating affection to legitimate users caused by multi-user interference and artificial noise, z is the artificial noise, n_k and n_e separately stand for the additive white Gaussian noise of the legitimate users and the eavesdropper.

Then, the signal estimation from the k-th legitimate user and the eavesdropper are separately:

$$\tilde{y}_k = w_k^{'} H_k t_k b_k + w_k^{'} H_k \sum_{j \neq k}^{K} t_j b_j + w_k^{'} H_k pz + w_k^{'} n_k \tag{3}$$

$$\tilde{y}_e = w_e^{'} H_e \sum_{j=1}^{K} t_j b_j + w_e^{'} H_e pz + w_e^{'} n_e \tag{4}$$

Among them: w_k and w_e are both $N_T \times 1$ dimension and stands for beam forming weight for the k-th legitimate user and the eavesdropper respectively, $w_k^{'}$ and $w_e^{'}$ are the conjugate transposed matrixes of w_k and w_e.

3. A Multi-user MIMO System Security Algorithm Based on Artificial Noise

When there is more than one legitimate user, security using artificial noise should meet two requirements: 1) to prevent mutual interference between multi-user; 2) to minimize the artificial noise affection to legitimate users. Based on the two requirements, the main idea of the security algorithm is the precoding design of p and t_k, so that the numerous artificial noise and mutual interference between multi-user could be filtered as signal is transmitted though the legitimate users' channel and the eavesdropper could not demodulate correctly due to the artificial noise affection. From (3) and (4), the legitimate users are affected by a small part of the artificial noise interference $w_k^{'} H_k pz$, and the natural additive noise from the channel $w_k^{'} n_k$. Meanwhile, the eavesdropper is effected by the mutual interference between multi-user $w_e^{'} H_e \sum_{j \neq k}^{K} t_j b_j$, the most part of the artificial noise interference $w_e^{'} H_e pz$ and the natural additive noise from the channel $w_e^{'} n_e$. As can be seen from the analysis above, precoding design of t_k and p are directly related to whether the artificial noise affection and the multi-user interference to legitimate users could be eliminated; besides, the precoding design of t_k and p are gotten though constructing complement matrix, joint channel state matrix and the Singular Value Decomposition of these two matrixes. Thus, the algorithm could be

divided into two modules: precoding based on the Singular Value Decomposition of complement matrix and precoding based on the Singular Value Decomposition of joint channel state matrix.

3.1. Precoding Based on the Singular Value Decomposition of Complement Matrix

Taking the modified Zero-Forcing beam forming method, in the receiving terminal [5], firstly, having process of beam forming and getting the weight vector w_l, then defining the complement matrix

$$\tilde{H}_l = [\tilde{h}_1....\tilde{h}_{l-1}\tilde{h}_{l+1}....\tilde{h}_K]^T,$$

in which the $\tilde{h}_l = (w_l^H H_l)^T$ is $N_T \times 1$ in dimension, so the dimension of $\tilde{H}_l$ can be known as $(K-1)\times N_T$, at last, the $\tilde{H}_l = \tilde{U}_l \tilde{D}_l \tilde{V}_l^H$ would be got by the Singular Value Decomposition of $\tilde{H}_l$. At the time of $K \le N_T$, the row number of $\tilde{H}_l$ is less than the column number, there would be a null space existing in the Singular Value Decomposition, then the right singular vector could be sequentially decomposed to $\tilde{V}_l = [\tilde{V}_l^{(s)} \tilde{V}_l^{(0)}]^H$, while the $\tilde{V}_l^{(s)}$ is the corresponding right singular vector of the nonzero singular values and the $\tilde{V}_l^{(0)}$ stands for the null space of the complement matrix. Therefore, the precoding $t_k = \tilde{V}_l^{(0)}$ based on the Singular Value Decomposition of $\tilde{H}_l$ is available.

3.2. Precoding Based on the Singular Value Decomposition of Joint Channel State Matrix

To minimize the affection of the artificial noise at the same time on the K legitimate users, the joint channel state matrix can be defined as $H_k = [\tilde{h}_1.....\tilde{h}_K]^T$, in which the $\tilde{h}_l = (w_l^H H_l)^T$ is a $N_T \times 1$ dimension vector and the H_k is $K \times N_T$ dimension, so $H_k = \tilde{U}_k \tilde{D}_k \tilde{V}_k^H$ would be got by the Singular Value Decomposition.

At the time of $K < N_T$, the row number of H_k is less than the column number, there would be a null space existing in the Singular Value Decomposition, then the right singular vector could be sequentially decomposed to $\tilde{V}_k = [\tilde{V}_k^{(s)} \tilde{V}_k^{(0)}]^H$, while the $\tilde{V}_k^{(0)}$ stands for the null space of the complement matrix. Therefore, the precoding $p = \tilde{V}_k^{(0)}$ based on the Singular Value Decomposition of H_k is available, then, the artificial noise interference to the legitimate users is zero by the precoding at the moment. At the time of $K \ge N_T$, the right singular vector could be sequentially decomposed to

$$\tilde{V}_k = [\tilde{V}_k^{(s)} \tilde{V}_k^{(0)}]^H,$$

and there would be no null space existing in the decomposition of H_k, that is, there is no null space existing in the multi-user MIMO system. To make artificial noise being transmitted via the smallest-affect to the legitimate users sub-channel and in order to reduce the affection to the legitimate users, the vector with smallest corresponding singular value in $\tilde{V}_k^{(s)}$ can be chosen as the precoding p. The specific calculation steps are as follows:

1) By the Singular Value Decomposition of h_k, select the left singular vectors to be the w_k corresponding to the largest singular value.

2) Constructing the complement matrix

$$\tilde{H}_l = [\tilde{h}_1....\tilde{h}_{l-1}\tilde{h}_{l+1}....\tilde{h}_K]^T,$$

the precoding t_k is available via the Singular Value Decomposition, which can eliminate the multi-user interference.

3) Constructing the joint channel state matrix $H_k = [\tilde{h}_1.....\tilde{h}_K]^T$, the precoding p is available via the Singular Value Decomposition, to eliminate the artificial noise affection on the legitimate users.

4. Performance Analysis

4.1. Security Performance Analysis

On the basis of definition of secrecy capacity in literature [4], the secrecy capacity of the k-th user in the multi-user MIMO system in the case of no null space existing could be derived as:

$$C_{\text{sec}} \ge \log\left(1+\frac{\left|w_k' H_k t_k\right|^2 \sigma_u^2}{\left|w_k' H_k p\right|^2 \sigma_z^2 + \sigma_n^2}\right) - \log\left(1+\frac{\left|w_e' H_e t_k\right|^2 \sigma_u^2}{\sum_{j\ne k}^{K}\left|w_e' H_e t_j\right|^2 \sigma_u^2 + \left|w_e' H_e p\right|^2 \sigma_z^2 + \sigma_e^2}\right) \quad (5)$$

Wherein, $\sigma_u^2, \sigma_z^2, \sigma_n^2, \sigma_e^2$ separately stand for the signal power, artificial noise power, noise power in the legitimate user channel and the noise power in the eavesdropper channel of the k-th user.

$$C_{\text{sec}} = \log\left(1+\frac{\left|w_k' H_k t_k\right|^2 \sigma_u^2}{\left|w_k' H_k p\right|^2 \sigma_z^2 + \sigma_n^2}\right) - \log\left(1+\frac{\left|w_e' H_e t_k\right|^2 \sigma_u^2}{\sum_{j\ne k}^{K}\left|w_e' H_e t_j\right|^2 \sigma_u^2 + \left|w_e' H_e p\right|^2 \sigma_z^2 + \sigma_e^2}\right) \quad (6)$$

As can be seen from the formula above, under the total power constrained conditions, a part of the power is used to transmit artificial noise, besides, the problem of allocation between signal power and noise power is directly affect the secrecy capacity. Assuming the power allocation among the users is uniform and the useful power allocation coefficient is φ, then the power of the k-th

user is $p_k = \frac{\varphi P}{K}$,the allocated noise power of the k-th user is $p_n = \frac{(1-\varphi)P}{K}$ and the channel capacity of the k-th user is:

$$C_{Ak} = \log(1+\frac{\left|w_k^{'} H_k t_k\right|^2 \varphi P}{\left|w_k^{'} H_k p\right|^2 (1-\varphi) P + K\sigma_n^2}) \quad (7)$$

The channel capacity of the eavesdropper is:

$$C_{Ae} = \log(1+\frac{\left|w_e^{'} H_e t_k\right|^2 \varphi P}{\sum_{j\neq k}^{K}\left|w_e^{'} H_e t_j\right|^2 \varphi P + \left|w_e^{'} H_e p\right|^2 (1-\varphi) P + K\sigma_e^2}) \quad (8)$$

Assuming:

$$A = \left|W_k^{'} H_k t_k\right|^2, B = \left|W_k^{'} H_k p\right|^2, C = K\delta_n^2, D = \left|W_e^{'} H_e t_k\right|^2,$$

$$E = \sum_{j\neq k}^{K}\left|W_e^{'} H_e t_j\right|^2, F = \left|W_e^{'} H_e p\right|^2, G = K\delta_e^2$$

Then:

$$C_{Ak} = \log(1+\frac{A\varphi P}{B(1-\varphi)P + C}) \quad (9)$$

$$C_{Ae} = \log(1+\frac{D\varphi P}{E\varphi P + F(1-\varphi)P + G}) \quad (10)$$

After derivation to the secrecy formula

$$C_{\text{sec}} = C_{Ak} - C_{Ae},$$

make it equal to zero then get a unary quadratic equation about φ:

$$(z_1 a_1 b_1 - z_2 a_2 b_2)\varphi^2 + (z_1 a_1 h_1 + z_1 b_1 h_1 - z_2 a_2 h_2 - z_2 b_2 h_2)\varphi + z_1 h_1^2 - z_2 h_2^2 = 0 \quad (11)$$

where in

$$a_1 = E - F + D, a_2 = A - B, b_1 = E - F, b_2 = -B,$$
$$h_1 = F + G,\ h_2 = B + C, z_1 = Ah_2, z_2 = dh_1$$

By the discussion and judgment of the formulas above, the value of φ which could maximize the k-th user secrecy capacity can be available.

4.2. System Performance Analysis

From (7), the k-th user's channel capacity without artificial noise, i.e. $\varphi = 1$, can be acquired.

$$C_{Ak} = \log(1+\frac{\left|w_k^{'} H_k t_k\right|^2 P}{K\sigma_n^2}) \quad (12)$$

Then, the system sum capacity without artificial noise is:

$$C = \sum_{k=1}^{K}\log(1+\frac{\left|w_k^{'} H_k t_k\right|^2 P}{K\sigma_n^2}) \quad (13)$$

Similarly, system sum capacity with artificial noise added is:

$$C_z = \sum_{k=1}^{K}\log(1+\frac{\left|w_k^{'} H_k t_k\right|^2 \varphi P}{\left|w_k^{'} H_k p\right|^2 (1-\varphi) P + K\sigma_n^2}) \quad (14)$$

So, with artificial noise security loss of system sum capacity is:

$$\Delta C = C - C_z = \sum_{k=1}^{K}\log(1+\frac{\left|w_k^{'} H_k t_k\right|^2 P}{K\sigma_n^2}) - \sum_{k=1}^{K}\log(1+\frac{\left|w_k^{'} H_k t_k\right|^2 \varphi P}{\left|w_k^{'} H_k p\right|^2 (1-\varphi) P + K\sigma_n^2}) \quad (15)$$

Obviously, from (15), the loss of system sum capacity is closely related with the receiving terminal beam forming vector w_k , the precoding eliminating the multi-user interference t_k , the precoding eliminating the artificial noise affection p and the useful power allocation coefficient φ . Taking advantages of precoding design principles in the previous section, which means the useful signal is transmitted through the primary channel and the artificial takes the secondary channel i.e. maximizing the $\left|w_k^{'} H_k t_k\right|^2$ and minimizing the $\left|w_k^{'} H_k p\right|^2$, the artificial noise affection to the legitimate users and the loss of system sum capacity can be minimized.

5. Simulation and Analysis

5.1. Secrecy Capacity

First of all, according to the method given in [6], a simulation about secrecy capacity and sum capacity is taken as the null space being existent and security being taken in the system. Assuming that the numbers of antennas in the transmitting and receiving terminal are both 4, the number of legitimate users is 3, while the channel state of legitimate users is given and normalized and total power is 500 mW constantly. The simulation results of the k-th user's secrecy capacity and sum capacity are shown in **Figures 3** and **4**.

The abscissa in **Figure 2** presents the ratio between noise power in user channel and in the eavesdropper channel, the ordinate stands for the secrecy capacity. Before artificial noise being added, part of the secrecy capacity is greater than zero due to the affection on the third-party from the multi-user interference; after artificial noise added the secrecy capacity is entirely improved which causes the secrecy capacity is always above zero in the part of $40 \le \delta_n^2 / \delta_e^2 \le 100$ and realizes the secure communication. **Figure 3** indicates that with transmitting power limited there will be some loss of the sum capacity after encryption; meanwhile, the more noise power distributed, greater the loss will be.

Secondly, raise the number of legitimate users to 4 and maintain the other simulation conditions. Now the null space will be inexistent, and the simulation results of the k-th user's secrecy capacity and sum capacity are shown in **Figures 4** and **5** following the proposed algorithm.

From **Figure 4**, when the system null space is inexistent, the system secrecy capacity can be also improved via the artificial noise, nonetheless, as the null space is inexistent, the secrecy capacity is decreased comparing with the null space existent condition. In addition, the system secure communication cannot be achieved when the useful power allocation coefficient is 0.8 and the ratio range is $70 \le \delta_n^2 / \delta_e^2 \le 100$. With the legitimate user's channel conditions deteriorated, the secrecy capacity when useful power distribution coefficient is 0.6 or 0.4 gets gradatim higher than the condition as useful power distribution coefficient being 0.8. This indicates that under certain conditions, by more artificial noise transmitted, the secrecy capacity can be improved and secure communication will be realized.

From **Figure 5**, when the system null space is inexistent, the artificial noise has partial impact on the legitimate users, so the loss of sum capacity is intensified because of the artificial noise security; the loss of sum capacity with useful power allocation coefficients being 0.8 and 0.4 is separately as much as 1/4 and 1/2 of the sum capacity without encryption. In spite of big loss of sum capacity, as the users number increasing the sum capacity after encryption is still higher than sum capacity of the null space existing system. In summary, the substance of the proposed algorithm is via a certain loss of sum capacity to improve the secrecy capacity.

5.2. Power Allocation

Assuming the total power to be 500 mW constantly, the simulation result of the k-th user secrecy capacity in the system changing with the useful signal power allocation coefficient is shown as **Figure 6**. When $\delta_n^2 / \delta_e^2 = 20$, known conditions from the simulation are:

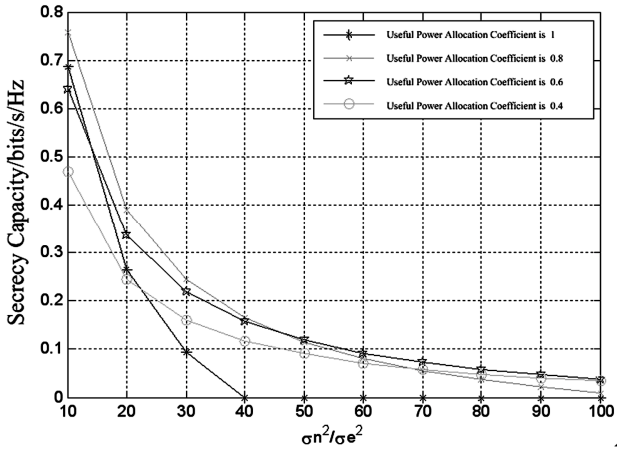

Figure 2. Secrecy capacity.

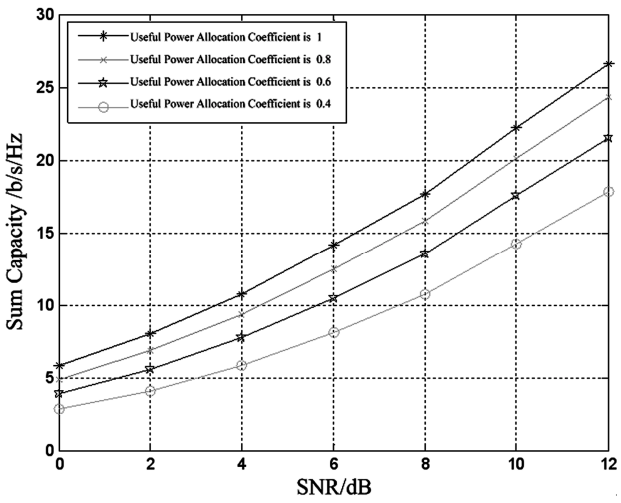

Figure 3. Sum capacity.

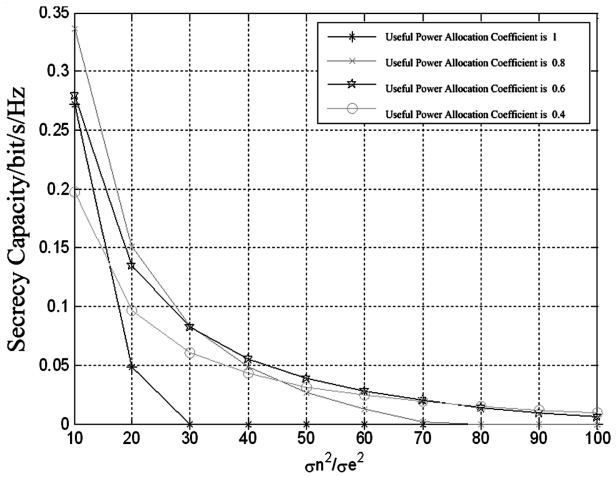

Figure 4. Secrecy capacity.

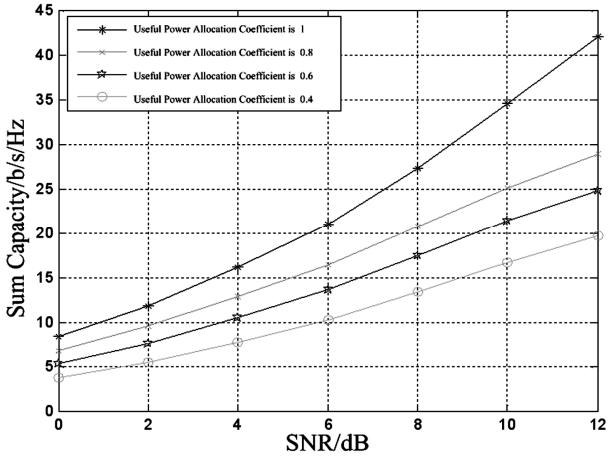

Figure 5. Sum capacity.

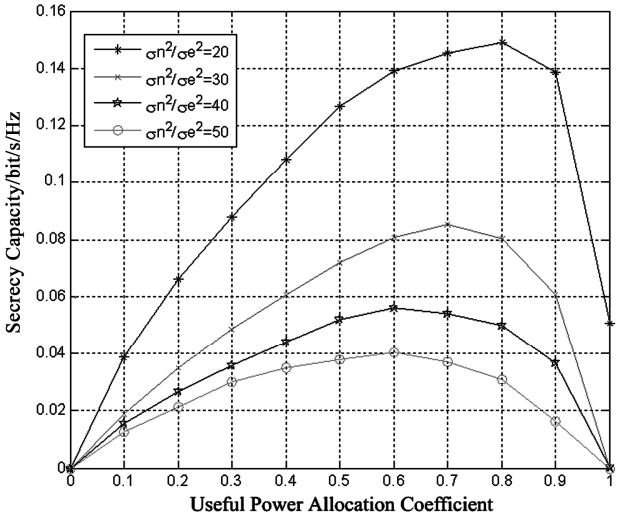

Figure 6. The Relationship between secrecy capacity and useful power allocation coefficient.

$$A = 0.0775, B = 0.0067, C = 80, D = 9.786 \times 10^{-4},$$
$$E = 1.0048,\ F = 0.0012, G = 4$$

Substituting results above into (10), the power allocation coefficient φ which maximize the secrecy capacity (i.e. maximum transmitting speed under security transmission) could be present, similarly when the δ_n^2 / δ_e^2 changes, only C need to be changed.

It is shown in **Figure 6** that in the multi-user MIMO system with null space inexistent, the secrecy capacity will decline rapidly, when the transmission power of the artificial noise is too small, especially less than the 10 percent of total power, and the secure transmission cannot be achieved if the condition getting even worse. With legitimate users' channel conditions deteriorate, the optimum allocation coefficient gradually shifts left, namely, the allocated artificial noise power will be more and more if the channel condition of the eavesdropper is better than the legitimate user.

6. Conclusions

In this paper, a multi-user MIMO system security algorithm based on artificial noise is proposed, which emphasizes the no null space in multi-user MIMO system scenario. In the algorithm, the affection of artificial noise to legitimate user is eliminated by precoding. For this purpose, the joint channel state matrix is established; then, after Singular Value Decomposition of the joint channel state matrix, the precoding is completed based on the minimum singular value; at last, an optimized power allocation scheme is proposed. As shown from simulation result, in the multi-user MIMO system with null space inexistent, with artificial noise introduced for physical layer security, the secrecy capacity will be improved efficiently by a certain sacrifice of sum capacity; especially, with the channel condition of the legitimate user getting worse, the allocated artificial noise power will be more and more to maximize the secrecy capacity.

REFERENCES

[1] R. Negi and S. Goel, Secure Communications Using Artificial Noise, IEEE Vehicle Technology Conference (VTC), Dallas, TX, September 2005, pp. 1906-1910.

[2] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communication*, Vol. 7, No. 6, 2008, pp. 2180-2189.

[3] M. Ghogho and A. Swami, "Physical Layer Secrecy of MIMO Communications in the Presence of a Poisson Random Field of Eavesdroppers," *IEEE ICC Workshop on Physical Layer Security*, Kyoto, Japan, June 2011, pp. 1-5.

[4] M. Ghogho and Ananthram, "Physical Layer Security of MIMO frequency selective channels by beamforming and noise generation," *European Signal Processing Conference*, Barcelona, Spain, Augest 2011, pp. 829-833.

[5] A. Mukherjee and A. L. Swindlehurst, "Utility of Beamforming Strategies for Secrecy in Multi-user MIMO Wiretap Channels, in Proc. of Forty-Seventh Allerton Conf., Oct 2009: 1268-1276.

[6] W. Liao, T. Chang, W. Ma and C. Chi, "Joint transmit beamforming and artificial noise design for QoS discrimination in wireless downlink," in Proc. IEEE ICASSP, Dallas, Mar 2010, pp. 256-2565.

[7] E. Ekrem and S. Ulukus, "The Secrecy Capacity Region of the Gaussian MIMO Multi-Receiver Wiretap Channel," *IEEE Transactions on Information Theory*, Vol. 57, No. 4, 2011, pp. 2083-2113. doi:10.1109/TIT.2011.2111750

[8] A. Khisti and G. W. Wornell, "Secure Transmission with Multiple Antennas Part II: The MIMOME Wiretap Channel," *IEEE Transactions on Information Theory*, Vol. 56, No. 11, 2010, pp. 5515-5532. doi:10.1109/TIT.2010.2068852

[9] A. Khisti and G. W. Wornell, "Secure Transmission with Multiple Antennas I: The MISOME Wiretap Channel," *IEEE Transactions on Information Theory*, 2010, Vol. 56, No. 11, pp. 3088-3104.doi:10.1109/TIT.2010.2048445

[10] X. Zhou and M. R. Mckay, Secure Transmission with Artificial Noise over Fading Channels: Achievable Rate and Optimal Power Allocation, International Conference Signal Processing and Communication Systems, Omaha, NE, Oct. 2010, pp. 3831-3842.

[11] A. Mukherjee and A. L. Swindlehurst, "User Election in Multi-user MIMO Systems with Secrecy Considerations," ASILOMAR Conf. on Signals, Systems, and Computers, Pacific Grove, CA, 2009, pp. 1479-1482.

