Downlink physical layer security transmission confronted with synergistic eavesdroping

XU Zhaoye [1, a], LU Ruimin [2,b]

[1] Institute of Communications Engineering PLA University of Science & Technology Nanjing, China

[2] Nanjing Telecommunication Technology Institute Nanjing, China

[a]xvzhaoye@yeah.net, [b]lrmmail@189.cn

Keywords: Physical layer security, Multi-downlinks, Synergistic eavesdroping, Zero-sum game.

Abstract. The most of existing physical layer security research focus on the situation where decentralized nodes transmit signals to the Base Station(BS). But considering a scenario where nonorthogonal transmission is allowed, when the BS transmits signals to decentralized nodes, the multi-downlinks will interfere each other, decreasing the signal-to-interference-plus-noise ratios (SINRs) at receivers. Focusing on the above problem, this paper optimizes the downlink beamforming and power allocation jointly to meet the SINRs requirement. On this basis, when confronted with synergistic eavesdroping where a malicious jammer helps the eavesdropper to eavesdrop, the BS transmits the artificial noise(AN) to improve the secrecy rate. Then zero-sum game model is proposed to obtain the strategies and corresponding expectation value of the secrecy rate when system reaches the mixed strategy equilibrium. By simulation, this method will obtain a good secrecy rate.

1. Introduction

In 1975, Wyner firstly proposed the Wire-tap channel model based on Shannon's information theory in [1]. This model showed that when the eavesdropper channel is a degraded version of the main channel, the source and the destination can exchange perfectly secure messages at a non-zero rate, which is the basement of following physical layer security research.

Focusing on the network consisting of eavesdroppers and friendly jammers, [2] builds up the utility function based on secrecy rate, and then Stackelberg type of game is proposed to obtain the optimal jamming power that maximize the system utility. When there are many decentralized nodes and a BS in the network, [3] divides all the decentralized nodes into some coalitions to transmit signals to the BS cooperatively, improving the secrecy rate. Then in [4], authors optimize the coalitions by using no-cooperation games to improve the secrecy rate based on [3]. In the situation where the eavesdropper is smart and it can chose to jam or to eavesdrop, [5] proposes zero-sum game and investigates the existence of pure strategy equilibrium and mixed strategy Nash equilibrium. When the smart malicious jammer helps the eavesdropper, [6] solves the power allocation problem by

using zero - sum game and Stackelberg type of game is proposed in [7] to obtain the optimal value of utility and to analyze the intercept probability.

These above literatures study the complex interaction among interdependent rational players by using the game theory. However there are some shortages cannot be neglected: these literatures only take uplink communication with many decentralized nodes into consideration, but the physical layer security problems in downlink are also important. When in scenarios with nonorthogonal channel, the interference among multi-downlinks will decrease the SINRs at receivers.

In [8][9][10], the downlink secrecy transmission problem is addressed. [8] considers a scenario where a BS transmits signals to a legal receiver. When an eavesdropper tries to eavesdrop the transmitted date from the BS, the BS improves the secrecy rate by selecting beamforming mode. In [9], a method based on singular value decomposition (SVD) is derived to get a beamfroming vector that is orthometric to other downlink channels for a specific downlink channel. A orthogonalization method was proposed in [10] to solve the downlink physical layer security: at the beginning of each time slot, the BS equipped with N_t antennas randomly generates $M\left(1 \le M \le N_t\right)$ N_t-dimensional normalized orthogonal vectors, then each decentralized node selects one vector that maximize its received SINR . Finally, the BS selects an optimal node with largest SINR for each beam. Thereafter, the BS communicates with the selected M nodes. However, above cited papers only focus on how to obtain proper beamforming vectors for each downlink channel to improve secrecy rate but neglect the secrecy rate improvement by optimizing the transmission power allocation to each downlink channel.

In his paper, we first propose an algorithm using uplink-downlink duality to optimize the beamforming and power allocation of downlink jointly, then on this basis, we use zero-sum game to obtain the system mixed strategy Nash equilibrium and the corresponding secrecy rate.

2. System Model

Let us consider a downlink scenario where a BS equipped with M antennas sends independent information signals to K decentralized terminals such as Unmanned Aerial Vehicles (UAVs) equipped with single antenna. An eavesdropper Eve tries to eavesdrop from the BS and a malicious jammer helps the eavesdropper, as is shown in Fig.1

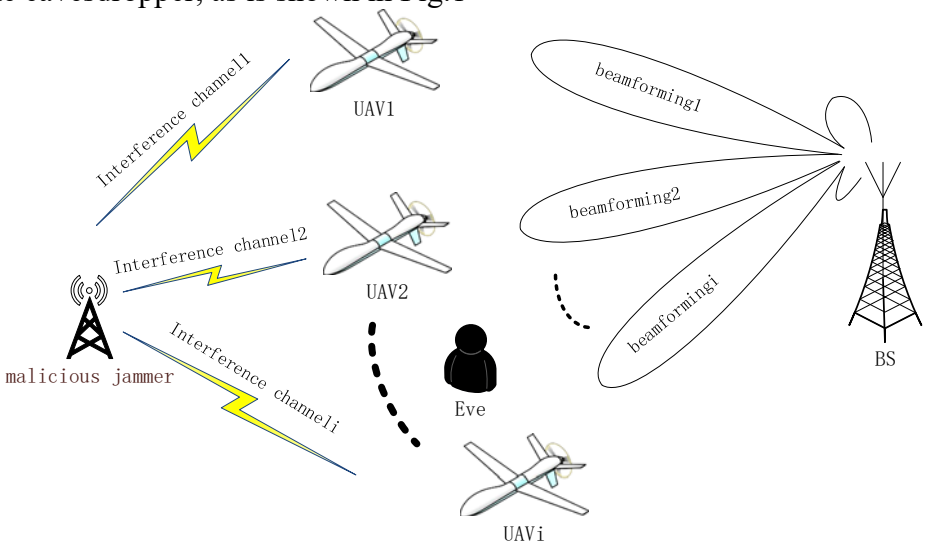

Fig.1. System model

Let the certain target threshold in each receiver is: $\Upsilon_1, \Upsilon_2, \cdots \Upsilon_K$. The total transmission power available at malicious jammer is limited by $P_{RJ\max}$. In order to jam the Eve, the BS transmits AN limited by $P_{J\max}$, which can be diminished by UAVs. And the maximal power at BS to transmit signals is $P_{\max}$.

The signal transmitted from the BS is $\mathbf{x} = \sum_{i=1}^{K} \mathbf{w}_i s_i + \mathbf{z}$, $1 \le i \le K$. Where $\mathbf{w}_i \in \mathbb{C}^{M\times 1}, 1 \le i \le K$, $\|\mathbf{w}_i\| = 1$, are the beamforming vectors that map all signals onto the antenna array and can be collected in a matrix $\mathbf{W} = [\mathbf{w}_1, \ldots, \mathbf{w}_K]$. $s_i, 1 \le i \le K$, are the independent information signals sended from the BS to K decentralized receivers, the downlink transmission powers are given by $p_i = E\left\{|s_i|^2\right\}$, $1 \le i \le K$,which can be stacked in a vector $\mathbf{p} = [p_1, \ldots, p_K]$. $\mathbf{z} \sim CN(0, \mathbf{R}_J)$ is the AN that is independent to the transmitted signals from the BS, with $\mathbf{R}_J = E\left(\mathbf{z}\mathbf{z}^H\right) \succ 0$ representing the AN covariance matrices and $p_J = tr(\mathbf{R}_J)$ is the AN power.

Since the AN can be diminished by the decentralized receivers, the signals received at the i th reciever and at the Eve can be written as respectively:

$$y_i = n_{si} + \mathbf{h}_{si}^H \mathbf{x} + h_{Ri} z_{RJ} = n_{si} + \mathbf{h}_{si}^H \sum_{k=1}^{K} \mathbf{w}_k s_k + h_{Ri} z_{RJ} \tag{1}$$

$$y_e = n_{se} + \delta \mathbf{h}_{se}^H \mathbf{x} = n_{se} + \delta \mathbf{h}_{se}^H \sum_{i=1}^{K} \mathbf{w}_i s_i + \delta \mathbf{h}_{se}^H \mathbf{z} \tag{2}$$

Where $n_{si} \sim CN\left(0, \sigma_i^2\right)$ and $n_{se} \sim CN\left(0, \sigma_e^2\right)$ are the additive noises at i th receiver and Eve, respectively. We use $\mathbf{h}_{si} \in \mathbb{C}^{M\times 1}$ to denote the legitimate channel from the BS to the i th receiver, whose elements are i.i.d. zero mean and unit variance complex Gaussian random variables. The downlink spatial covariance matrice is $\mathbf{R}_i = E\left\{\mathbf{h}_{si}\mathbf{h}_{si}^H\right\}$. Similarly, we use $\delta \mathbf{h}_{se}$ to denote the eavesdropper channel from the BS to the eavesdropper, where δ is the relative path loss, and $\mathbf{h}_{se} \in \mathbb{C}^{M\times 1}$ denotes the small-scale fading vector with i.i.d. zero mean and unit variance complex Gaussian distributed entries. The corresponding spatial covariance matric is $\mathbf{R}_{se} = E\left\{\delta^2 \mathbf{h}_{se}\mathbf{h}_{se}^H\right\}$. We denote by h_{Ri} the baseband complex channel gain between the malicious jammer and the i th receiver. z_{RJ} is the malicious interfering noise transmitted by the malicious jammer, and $p_{RJ} = E\left\{|z_{RJ}|^2\right\}$ is the malicious interfering power.

In the following superscripts DL and UL refer to downlink and uplink quantities, respectively.From (1) and (2), the SINR at the i th receiver is $\mathrm{SINR}_i^{DL} \triangleq \dfrac{p_i \mathbf{w}_i^H \mathbf{R}_i \mathbf{w}_i}{\sum_{\substack{k=1 \\ k\ne i}}^{K} p_k \mathbf{w}_k^H \mathbf{R}_k \mathbf{w}_k + p_{RJ}|h_{Ri}|^2 + \sigma_i^2}$ and the SINR at the eavesdropper is $\mathrm{SINR}_E = \dfrac{\sum_{i=1}^{K} p_i \mathbf{w}_i^H \mathbf{R}_{se} \mathbf{w}_i}{tr(\mathbf{R}_J \mathbf{R}_{se}) + \sigma_e^2}$.The secrecy rate can be written as:

$$C_s = W\left(\sum_{i=1}^{K} \log\left(1 + \mathrm{SINR}_i^{DL}\right) - \log\left(1 + \mathrm{SINR}_E\right)\right)^+, i = 1 \ldots K. \tag{3}$$

3. Downlink Optimazation

In the downlink scenario, the joint optimaization of downlink beamforming and power allocation can be expressed as:

$$\min_{\mathbf{W},\mathbf{p}} \sum_{i=1}^{K} p_i, i = 1 \ldots K. \tag{4}$$

$$s.t.\ \ \mathrm{SINR}_i^{DL}(\mathbf{W},\mathbf{p}) \geq \Upsilon_i \tag{5}$$

$$p_i \geq 0; \sum_{i=1}^{K} p_i \leq P_{\max}; \|\mathbf{w}_i\| = 1$$

To solve the above problem, we propose an iterative algorithm composed of two steps: First by susing uplink-downlink duality proved in [11][12], we seek proper beamforming matrix and power allocation that make K decentralized receivers achieve individual target SINRs showed in (5) when the total transmission power is $P_{\max}$. Then using beamforming matrix obtained in the first step we minimize the total transmission power based on (4).

A. Step One.

In downlink scenario where nonorthogonal transmission is allowed, the SINR values of decentralized receivers are coupled, making it more complicated to optimal beamformers jointly. Paper [11][12] obtain the optimal downlink beamforming matrix by solving a dual uplink problem.

Considering an uplink scenario with the same total transmission power and malicious interference, the equal reciver noise,the same targets and the same fixed beamforming matrix, then the uplink SINRs are $\mathrm{SINR}_i^{UL}(\mathbf{w}_i,\mathbf{q}) \triangleq \dfrac{q_i \mathbf{w}_i^H \mathbf{R}_i \mathbf{w}_i}{\mathbf{w}_i^H \left(\sum_{\substack{k=1 \\ k \neq i}}^{K} q_k \mathbf{R}_k + \left(p_{RJ} |h_{Ri}|^2 + \sigma_i^2 \right) \mathbf{I} \right) \mathbf{w}_i}$, $\forall i$,where $\mathbf{q} = [q_1, \ldots, q_K]$ is the uplink power allocation matrix. We define $C^{UL}(\widetilde{\mathbf{W}},\mathbf{q}) = \max_{\mathbf{q}} \min_{1 \leq i \leq K} \dfrac{\mathrm{SINR}_i^{UL}}{\Upsilon_i}$ under the maximal power constraint $\|\mathbf{q}\| = P_{\max}$.

Let $\mathbf{q}_{ext} = [\mathbf{q}^T, 1]^T$ and $\Lambda(\mathbf{W},\mathbf{q}) = \begin{bmatrix} \mathbf{D}\boldsymbol{\Psi}^T(\mathbf{W}) & \mathbf{D}\boldsymbol{\sigma} \\ \dfrac{1}{P_{\max}} \mathbf{1}^T \mathbf{D}\boldsymbol{\Psi}^T(\mathbf{W}) & \dfrac{1}{P_{\max}} \mathbf{1}^T \mathbf{D}\boldsymbol{\sigma} \end{bmatrix}$ be the extended uplink coupling matrix, where $\boldsymbol{\sigma} = [p_{RJ} |h_{R1}|^2 + \sigma_1^2, \ldots, p_{RJ} |h_{RK}|^2 + \sigma_K^2]^T$, $\left[\boldsymbol{\Psi}(\mathbf{W})\right]_{ik} = \begin{cases} \mathbf{w}_k^H \mathbf{R}_i \mathbf{w}_k, k \neq i \\ 0, k = i \end{cases}$ and $\mathbf{D} = diag\left\{ \left(\Upsilon_1 / \left(\widetilde{\mathbf{w}}_1^H R_1 \widetilde{\mathbf{w}}_1 \right) \right), \ldots, \left(\Upsilon_K / \left(\widetilde{\mathbf{w}}_K^H R_K \widetilde{\mathbf{w}}_1 \right) \right) \right\}$.

Then we have the equation:

$$\Lambda(\widetilde{\mathbf{W}},\tilde{\mathbf{q}}) \tilde{\mathbf{q}}_{ext} = \frac{1}{C^{UL}(\widetilde{\mathbf{W}},\tilde{\mathbf{q}})} \tilde{\mathbf{q}}_{ext} \tag{6}$$

It has been proved in [12] that $C^{UL}(\widetilde{\mathbf{W}},\tilde{\mathbf{q}})$ is a reciprocal eigenvalue of Λ, and $C_{opt}^{DL}(P_{\max})$ is associated with the maximal eigenvector of Λ, so we have:

$$C_{opt}^{DL}(P_{\max}) = \max C^{UL}(\widetilde{\mathbf{W}},\tilde{\mathbf{q}}) = \frac{1}{\min_{\mathbf{W}} \lambda_{\max}(\Lambda(\mathbf{W},P_{\max}))} \tag{7}$$

The optimal power allocation $\mathbf{q}$ is obtained as the first K components of the dominant eigenvector of Λ,which can be scaled so that its last component equals one.

B. Step Two.

For given $\mathbf{q}_{ext}$, $\min_{\mathbf{W}} \lambda_{\max}\left(\Lambda\left(\mathbf{W}, P_{\max}\right)\right)$ can be obtained by independent maximization of the uplink SINRs, and [12] has reduced the joint optimization problem to K decoupled problems equivalent to the scaled MMSE beamforming solution:

$$\widehat{\mathbf{w}}_i = \arg\max_{\mathbf{w}_i} \frac{\mathbf{w}_i^H \widetilde{\mathbf{R}}_i \mathbf{w}_i}{\mathbf{w}_i^H \mathbf{Q}_i(\mathbf{q}) \mathbf{w}_i} \tag{8}$$

$$s.t.\ \ \|\mathbf{w}_i\|_2 = 1,\ \forall i$$

Where $\mathbf{Q}_i(\mathbf{q}) = \sum_{\substack{k=1 \\ k\neq i}}^{K} [\mathbf{q}]_k \widetilde{\mathbf{R}}_k + \mathbf{I}$, $\widetilde{\mathbf{R}}_l = \mathbf{R}_l / \left(p_{RJ} |h_{Rl}|^2 + \sigma_l^2\right)$, $l = i, k$.

By solving (8) we obtain $\mathbf{W}$ that make constraints in (5) fulfilled. According paper [11],for given $\mathbf{W}$, the optimal power allocation that minimize the transmission power is characterized by $\mathrm{SINR}_i^{UL} = \Upsilon_i$, $1 \le i \le K$, from which $\mathbf{q}$ can be solved as $\mathbf{q} = \left(\mathbf{I} - \mathbf{D}\boldsymbol{\Psi}^T \mathbf{W}\right)^{-1} \mathbf{D1}$ [12],where $\mathbf{1} = [1, \ldots 1]^T$.

Then make $P_{\max} = \|\mathbf{q}\|_1$ as the total transmission power and repeat A and B until $\max_{1\le i\le K}\left(SINR_i^{UL} / \Upsilon_i\right) = \min_{1\le i\le K}\left(SINR_i^{UL} / \Upsilon_i\right)$, and finally we can obtain the downlink power allocation[12]:

$$\mathbf{p} = \left(\mathbf{I} - \mathbf{D}\boldsymbol{\Psi}\mathbf{W}\right)^{-1} \mathbf{D1} \tag{9}$$

The Zero-sum Game

We can build the zero-sum game utility function as:

$$U_s = C_s - \beta\left(P_{sig} + P_J\right) + \beta P_{RJ} \tag{10}$$

Where $\beta > 0$. $\beta\left(P_{sig} + P_J\right)$ represents the cost of improving the power of transmission and AN, and βP_{RJ} is the cost of the malicious jammer decreaseing the secrecy rate. The goal of the BS is to maximize the U_s while the malicious jammer is to minimize U_s, and it is a zero-sum game.

Paper [15][16] investigate the method to convert the continuous state games to discrete games, and [17] introduces conclusions about zero-sum matrix. In this paper, we build the discrete strategy sets of the BS and malicious jammer as, respectively:

$$\mathrm{B} = \left\{0, \Delta p_J, 2\Delta p_J, \ldots, P_{J\max} - \Delta p_J, P_{J\max}\right\} \tag{11}$$

$$\mathrm{M} = \left\{0, \Delta p_{RJ}, 2\Delta p_{RJ}, \ldots, P_{RJ\max} - \Delta p_{RJ}, P_{RJ\max}\right\} \tag{12}$$

n is the number of strategies in set B and m is the number in set M. $\mathbf{C} \in \mathbf{R}^{n\times m}$ is a nonnegative utility matrix, each element in which corresponds to a strategy combination of B and M.

Let $\mathbf{u} = \left\{u_1, u_2, \ldots, u_n\right\}, |\mathbf{u}| = 1$, is the probability distribution according to which the BS chose the strategies in B ,and $\mathbf{v} = \left\{v_1, v_2, \ldots, v_m\right\}, |\mathbf{v}| = 1$ is the probability distribution according to which the malicious jammer chose the strategies in M. So the system utility function in mixed strategy can be written as:

$$U_s = \sum_{k=1}^{n} \sum_{l=1}^{m} u_k \mathbf{C} v_l = \mathbf{u}^T \mathbf{C} \mathbf{v} \tag{13}$$

For the BS, the problem is[17]:

$$\max \min_{v_i, i=1,\ldots m} \left(\mathbf{C}^T \mathbf{u}\right)_{v_i} \tag{14}$$

$$s.t.\ \ \mathbf{v} \succ 0, \mathbf{1}^T \mathbf{v} = 1$$

For the malicious jammer, the problem is[17]:

$$\min \max_{u_i, i=1,\ldots n} \left(\mathbf{C}\mathbf{v}\right)_{v_i} \tag{15}$$

$$s.t.\ \ \mathbf{u} \succ 0, \mathbf{1}^T \mathbf{u} = 1$$

[17] has proved that(14)is equivalent to(15), so $\mathbf{u}$ and $\mathbf{v}$ can be obtained by solving (14)or(15).

4. Numerical Simulations

The simulation is set up as follows: $M = 4$, $K = 5$, $W = 1, \beta = 4$, the relative path loss is $\delta = 1$, the maximal power of AN is $P_{RJ\max} = 120\text{mW}$, the maximal transmission power is $P_{\max} = 1400\text{mW}$, the maximal malicious interfering power is $P_{RJ\max} = 300\text{mW}$,the noise level is -80dBm, the certain target threshold in the each receiver is: $\Upsilon_1 = \cdots = \Upsilon_K = 3\text{dB}$, and $\Delta p_J = \Delta p_{RJ} = 1\text{mW}$.

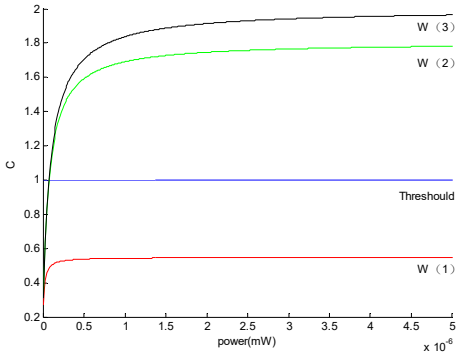

Fig.2. Illustration of the iterative algorithm

Fig.2 illustrates the iterative algorithm proposed in this paper. When $\mathbf{W}(1)$ obtained in the 1th iteration is used to optimize the power allocation, the result of convergence is $C < 1$, which means that the target thresholds can't be achieved. When $\mathbf{W}(2)$ or $\mathbf{W}(3)$ is proposed, the target thresholds can be achieved, but $\mathbf{W}(3)$ have the maximal C. That means the iterative algorithm is effective.

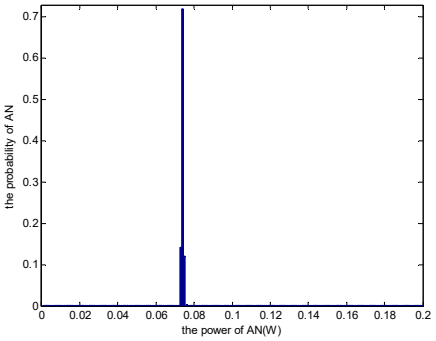

Fig.3. The probability of AN

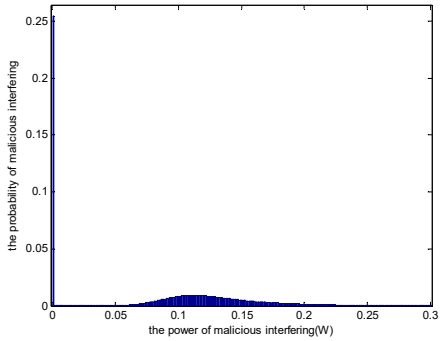

Fig.4. The probability of malicious interfering

By simulation, Fig.3 and Fig.4 show the probability of AN and of malicious interfering respectively when system reaches the mixed strategy equilibrium. And in the mixed strategy equilibrium, the power expectation of AN is 0.0741W , the power expectation of malicious interfering is 0.0987W , and the corresponding secrecy rate expectation is 1.9119bit/s/Hz .

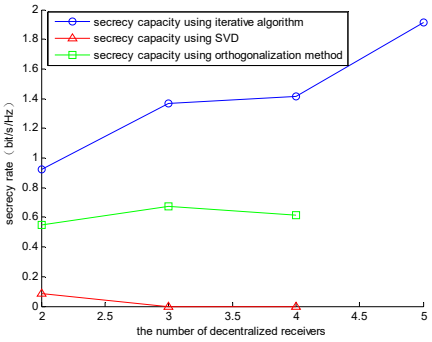

Fig.5. Comparison with other methods

For given the same total transmission power, the same malicious interfering power, the same AN power and the same amount of decentralized receivers, Fig.5 shows the comparison with methods in [9] and [10]. We can conclude that SVD method in [9] can hardly guarantee secrecy communication, orthogonalization method in [10] can obtain a good secrecy rate, and the method in this paper can achieve the most secrecy rate. Also, because of the limitation of SVD method and orthogonalization method, when the antenna number of the BS is 4, [9][10] only can communicate with 4 decentralized receivers simultaneously at most, but by using the method in this paper, the BS can communicate with 5 decentralized receivers simultaneously and get more secrecy rate.

5. Conclusions

This paper takes multi-downlinks physical layer security transmission confronted with synergistic eavesdroping into consideration. By using an iteration algorithm based on uplink-downlink duality and zero-sum game, this paper can obtain more secrecy rate and can communicate with more receiver simultaneously than [9][10].

References

[1] Wyner A D.The wiretap channel[J].Bell System Technical Journal,1975,54(8):1355-1387.

[2] Han Zhu, Marina Ninoslav, Merouane Debbah, Are Hjorungnes. Physical Layer Security Game: Interaction between Source, Eavesdropper and Friendly Jammer[J].EURASIP Journal on Wireless Communication and Networking Mar. 2009(11):1-10.

[3] W. Saad, Z. Han, T. Basar, M. Debbah and A. Hjorungnes, "Physical layer security: Coalitional games for distributed cooperation," *2009 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks*, Seoul, 2009, pp. 1-8.

[4] FU Xiao-mei, YAO Xiao-ming, ZONG Qun. Relay selection and power optimization in cooperative coalitions [J]. Sysems Engineering and Electronics, 2016,05:1176-1181.

[5] A. Mukherjee and A. L. Swindlehurst, "Jamming Games in the MIMO Wiretap Channel With an Active Eavesdropper," in *IEEE Transactions on Signal Processing*, vol. 61, no. 1, pp. 82-91, Jan.1, 2013.

[6] M. Ara, H. Reboredo, S. A. M. Ghanem and M. R. D. Rodrigues, "A zero-sum power allocation game in the parallel Gaussian wiretap channel with an unfriendly jammer," *2012 IEEE International Conference on Communication Systems (ICCS)*, Singapore, 2012, pp. 60-64.

[7] FANG He, XU Li, SU Binting, LIN Hui. Anti-jamming and Eavesdropping in Wireless Multi-channel Networks [J]. JOURNAL OF SICHUAN UNIVERSITY (ENGINEERING SCIENCE EDITION),2016,01:119-125.

[8] X. Chen and L. Lei, "Energy-Efficient Optimization for Physical Layer Security in Multi-Antenna Downlink Networks with QoS Guarantee," in IEEE Communications Letters, vol. 17, no. 4, pp. 637-640, April 2013.

[9] X. Chen and R. Yin, "Performance Analysis for Physical Layer Security in Multi-Antenna Downlink Networks with Limited CSI Feedback," in IEEE Wireless Communications Letters, vol. 2, no. 5, pp. 503-506, October 2013.

[10] X. Chen; Y. Zhang, "Mode Selection in MU-MIMO Downlink Networks: A Physical-Layer Security Perspective," in IEEE Systems Journal , vol.PP, no.99, pp.1-9 doi: 10.1109/JSYST.2015.2413843

[11] H. Boche and M. Schubert, "A general duality theory for uplink and downlink beamforming," *Proceedings IEEE 56th Vehicular Technology Conference*, 2002.

[12] M. Schubert and H. Boche, "Solution of the multiuser downlink beamforming problem with individual SINR constraints," in *IEEE Transactions on Vehicular Technology*, vol. 53, no. 1, pp. 18-28, Jan. 2004.

[13] M. Pesavento, D. Ciochina and A. B. Gershman, "Iterative dual downlink beamforming for cognitive radio networks," *2010 Proceedings of the Fifth International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, Cannes, 2010, pp. 1-5.

[14] Tamer B, Geert O. Dynamic non-cooperative game theory [M]. Information Forensics and Security, 2011, 6(3): 818-830.

[15] LIN Shang-bin, HUANG Kai-zhi, WANG Wen, LI Ming-liang. A Physical Layer Security Transmission Method based on Contimuous Zero-sum Game in the Presence of a Malicious Jammer[J]. JOURNAL OF SIGNAL PROCESSING, 2015,06:720-726.

[16] Liu Z Q, Yu J S, Li J F. The properties and equilibrium in mixed strategy of continuous game theory [J]. Journal of Capital Normal University，2007，,2（2）：13-18.

[17] Boyd. S. Convex Optimization.[M]. TISINGHUA UNICERSITY RESS, 2013,1(1): 222-224.