Power Optimization for Secure Communications in Full-duplex System Under Residual Self-Interference

Caidan Zhao[1], Mengsiyun Tai[1], Lianfen Huang[1], Minmin Huang[1], Xiaojiang Du[2]
[1]Dept.of Communication Engineering, Xiamen University, Xiamen, China, 361005
[2]Temple University, Philadelphia, PA 19122, USA
Email: zcd@xmu.edu.cn , dux@temple.edu

***Abstract*—This paper proposes a full-duplex physical security model with self-interference remaining. This model doesn't need the assistance of external jamming nodes and it ensures that the uplink and downlink transmission of the full-duplex system can achieve the required secrecy rate. Meanwhile, it creates a base station transmission power optimization problem with flexible constraints and a two-level method to achieve the optimization, so that power optimization can take place in the model with self-interference remaining.**

Keywords—Full-duplex communications, physical layer security, beamforming, convex optimization.

I. INTRODUCTION

With the improvement of mobile communication technology, mobile internet services develop rapidly. Meanwhile, security issues have become more serious in mobile communication systems due to the open network and characteristics of wireless transmission [1]. Traditional solutions to wireless internet security are based on key encryptions [2], which employ various encryption algorithms in the upper layer of the network protocol stack to ensure the security of data. This scheme relies on the fact that key generation can't be cracked in a short time, which requires a large amount of computation. In addition, these upper layer encryption algorithms essentially ignore the underlying useful information in the physical layer, which may become vulnerable to malicious attacks in wireless transmission. Physical layer security of communication systems is intended to make use of channel characteristics to transmit secret information. Recently, some mechanisms improving physical layer security have been widely studied [3-6], among which beamforming gradually becomes the main research direction of physical layer secure communication with the development of channel coding technology.

Now, Full-duplex wireless communication is an important component of the fifth-generation communication system for entire spectrum resource utility [8]. With the development of instrumentation and signal processing, self-interference cancellation in full-duplex wireless communication systems has been studied deeply and substantial amount system experiments have been performed on it [9]. It enables the real applications of full-duplex wireless communication systems. Full-duplex security transmission mechanisms have emerged to be a hot topic of research. Literature [10] brings forward a method with low power consumption in cases that self-interference of full-duplex communication is completely cancelled. This method uses the joint forming of information beams and noise beams. In [11], researchers assume that self-interference of full-duplex communication is totally cancelled. Because of this, they come up with a physical layer security method using artificial noise produced by full-duplex terminal antenna degrees of freedom to improve the uplink and downlink transmission security of the communication system. However, this approach only takes into account the security strategy of full-duplex base stations' receiving direction of information and ignores the security of full-duplex base stations' transmissions, which provides opportunities for Signal eavesdroppers. Full-duplex relay is used to produce interference signals in [12] so as to improve physical layer security. In [13], under the condition that self-interference exists, restraining users' SNR (signal to noise ratio), researchers design transmitting beamforming vectors to achieve the secure transmission of full-duplex systems with low power consumption. These studies are mainly used in the complete cancellation of self-interference using traditional artificial noise or external jamming nodes to improve transmission security of full-duplex communication without making full use of the co-frequency co-time characteristic of the full-duplex system.

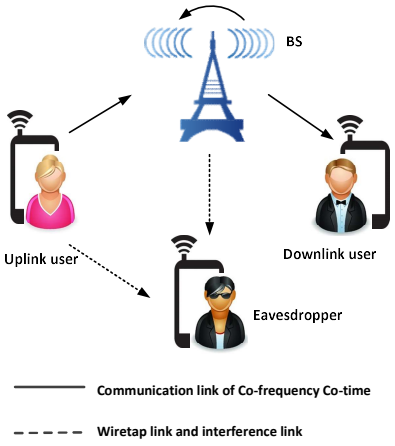

Figure 1 Full-duplex communication system

This work is partly supported by the Natural Science Foundation of Fujian Province of China (Project No. 2014J01250), 863 high technology plan(Grant No. 2015AA01A707).

In this paper, with the assumption of incomplete self-interference cancellation, we build a physical layer security model for full-duplex communication systems without the assistance of external jamming nodes. The eavesdropper wiretaps uplink and downlink transmission signals at the same time, making full use of the co-frequency co-time characteristic of the full-duplex system [14] to realize the secure transmission of uplink and downlink of the full-duplex system at the same time. This paper builds a base station power optimization model to guarantee the security and solves the optimization problem by using a two-step approach, in which the inner iteration uses a CVX toolkit [16] to deal with the non-convex problem, and the outer iteration to seek the optimizer according to a one-dimensional line search. This way, the base station transmitting power of uplink and downlink of the Full Duplex system reaches the minimal optimization.

This paper is organized as follows: Section II illustrates the model of full-duplex systems and the optimization model of base station transmitting power. The introduction of solutions to complete and incomplete self-interference cancellation are both given in Section III. Section IV shows the simulation results and comparisons. At last, the conclusion is presented in the last Section.

The symbols commonly used in this paper are as follows: $(\cdot)^{\mathrm{H}}$denotes the conjugate transpose. Tr(A) denotes the trace of matrix A. A$\succeq$0 states that A is a positive semi-definite (PSD) matrix. rank(A) denotes the rank of matrix A. I denotes the identity matrix with appropriate matrix.

II. SYSTEM MODEL

A. Wiretap channel model of full-duplex communications

Considering the residual self-interference cases, we construct the physical layer security model of full-duplex communication systems without the assistance of external jamming nodes. The base station works in full-duplex mode and the eavesdropper wiretaps uplink and downlink transmission signals at the same time. The uplinks and downlinks transmit data at the state of Co-frequency Co-time. In this case, regardless of if the eavesdropper wiretaps the information of uplink (or downlink) cellular communication, the signals corresponding to the downlink (or uplink) cellular communications link become an effective interference for eavesdroppers. That is to say, by making use of full-duplex network communications interference, the secure communication of full-duplex network communications can be effectively secured without the assistance of external jamming nodes.

In this paper, we consider a full-duplex communication system as shown in Fig. 2.1 and Fig. 2.2. The system has a full-duplex base station equipped with N(N≥1) transmitter antennas and M(M≥1) receiver antennas. A sender Tx and a receiver Rx are both equipped with signal antenna.

q_t and x_b are representing the transmitted signals of Tx and full-duplex base station respectively, where $q_t \in \mathcal{CN}(0,1)$, $x_b \in \mathcal{CN}(0,1)$.$h_r \in \mathbb{C}^{N\times 1}$, $g_e \in \mathbb{C}^{1\times 1}$, $h_e \in$ BS -Eve, Tx-BS, and Tx-Eve, respectively. $H_b \in \mathbb{C}^{N\times \mathrm{M}}$ defines the channel matrix between the receiver and the transmitter of BS.

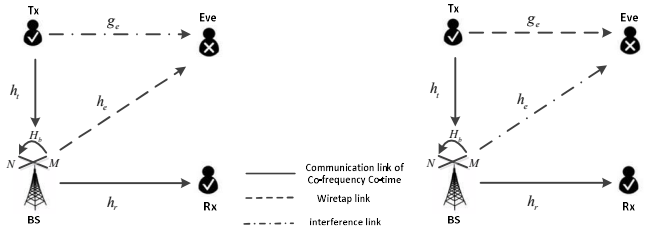

Fig.2.1 Eve wiretaps the information of down link

Fig. 2.2 Eve wiretaps the information of uplink

p_t is the transmission power of Tx.

The eavesdropper wiretaps uplink and downlink transmission signals at the same time. The received signals of Rx and Eve are y_r and y_e respectively.

$$y_r = {h_r}^H w x_b + z_r \quad (2.1)$$

$$y_e = g_e\, {p_t}^{\frac{1}{2}} q_t + {h_e}^H w x_b + z_e \quad (2.2)$$

w is the transmission beamforming vector of BS, and $\mathrm{p_t}$ is the transmit power of Tx.

Considering the residual self-interference cases, the received signals of BS can be expressed as:

$$y_b = h_t\, {p_t}^{\frac{1}{2}} q_t + k{H_b}^H w x_b + z_b \quad (2.3)$$

$k{H_b}^H w x_b$ is the self-interference between the transmitter antenna and the receiver antenna of the base station. k is the coefficient of residual self-interference. The greater the value of k is, the greater the influence from self-interference is （$0 \le k \le 1$, the self-interference was eliminated completely when k=0）.

When Eve wiretaps the information of uplink cellular communication, the signals corresponding to the downlink cellular communications link become an effective interference for eavesdroppers. Therefore, the achievable secrecy rate of uplink is：

$$R_{s1} = log\left(1 + \frac{|{h_r}^H w|}{{\sigma_r}^2}\right) - lo\,g\left(1 + \frac{|{h_e}^H w|}{{p_t}\|g_e\|^2 + {\sigma_e}^2}\right) \quad (2.4)$$

w is the transmission beamforming vector of BS. $\mathrm{p_t}$ is the transmission power of Tx.

When the eavesdropper wiretaps the information of downlink cellular communication, the signals corresponding to the uplink cellular communications link become an effective interference for eavesdroppers. Therefore, the achievable secrecy rate of downlink is：

$$R_{s2} = log\left(1 + \frac{p_t\|h_t\|^2}{{\sigma_t}^2 + k^2|{H_b}^H w|^2}\right) - log\left(1 + \frac{p_t\|g_e\|^2}{|{h_e}^H w|^2 + {\sigma_{e2}}^2}\right) \quad (2.5)$$

B. Power optimization problem of BS

The meaning of secrecy capacity [17] is that the uplink and downlink of full-duplex base stations can securely send and receive information and the eavesdropper can't get the

information from cellular communication when the value of secrecy capacity is greater than zero. This is used to realize the full duplex communication base station of the physical security. In achieving safe communication at the same time, we need to consider the power consumption of BS. We turn to an optimal problem P to minimize the power of BS and improve secrecy capacity as much as possible at the same time:

$$\begin{aligned} &\mathrm{P}: \min_{w} \|w\|^2 \\ &s.t. Pr\{\ R_{s1} \geq\ R_{m1}\} \geq 1-\rho \\ &\quad Pr\{\ R_{s2} \geq\ R_{m2}\} \geq 1-\rho \end{aligned} \tag{2.6}$$

$\mathrm{R_{m1,}}$ $\mathrm{R_{m2}}$ are the required achievable secrecy rates of uplink and downlink transmission, respectively. $\rho \in [0,1]$ is the outage probability of the secrecy rate constraint for a legitimate user. In the optimization model put forward by [13], the constraint required by SNR of the users must satisfy a certain value. But, in the optimization model proposed in this paper, we restrain the security rate and don't require the SNR of users to satisfy a certain value. That is to say our optimization model is more flexible.

By using the formula (2.4) and (2.5), the problem P can be modified as P1:

$$\begin{aligned} &P1: \min_{w} \|w\|^2 \\ &s.t. Pr\{log\left(1+\frac{|\ {h_r}^H w|^2}{{\sigma_r}^2}\right) - log\left(1+\frac{|\ {h_e}^H w|^2}{{p_t}\|\ g_e\|^2+{\sigma_e}^2}\right) \geq R_{m1}\} \geq \\ &\quad 1-\rho \end{aligned} \tag{2.7}$$

$$\begin{aligned} &Pr\left\{log\left(1+\frac{p_t\|\ h_t\|^2}{{\sigma_t}^2+k^2|\ {H_b}^H w|^2}\right) - lo\ g\left(1+\frac{p_t\|\ g_e\|^2}{|\ {h_e}^H w|^2+{\sigma_{e2}}^2}\right) \geq \right. \\ &\quad \left. R_{m2}\right\} \geq 1-\rho \end{aligned} \tag{2.8}$$

III. THE SOLUTION OF POWER OPTIMIZATION PROBLEM

A. *Power optimization under completely eliminated self-interference*

First, we consider an ideal situation where the self-interference has been eliminated completely. In this case, the coefficient of residual self-interference is zero (k=0). P1 can be modified as:

$$\begin{aligned} &\mathrm{P1}: \min_{w} \|w\|^2 \\ &\mathrm{s.t.}\ Pr\{log\left(1+\frac{|\ {h_r}^H w|^2}{{\sigma_r}^2}\right) - log\left(1+\frac{|\ {h_e}^H w|^2}{{p_t}\|\ g_e\|^2+{\sigma_e}^2}\right) \geq \\ &\quad R_{m1}\} \geq 1-\rho \end{aligned} \tag{3.1}$$

$$\begin{aligned} &Pr\{log\left(1+\frac{p_t\|\ h_t\|^2}{{\sigma_t}^2}\right) - log\left(1+\frac{p_t\|\ g_e\|^2}{|\ {h_e}^H w|^2+{\sigma_{e2}}^2}\right) \geq R_{m2}\} \geq \\ &\quad 1-\rho \end{aligned} \tag{3.2}$$

In the real situation, the transmitter can't get the perfect CSI of eavesdropper, thus, the channel state information is inaccurate.

Assume $\widetilde{\mathrm{h_e}}$ and $\widetilde{\mathrm{g_e}}$ are the estimated channels between BS and Eve, Tr and Eve, respectively. $\mathrm{h_e}$ and $\mathrm{g_e}$ can be described by the sum of estimate and error:

$$h_e = \widetilde{h_e} + e_{e1} \tag{3.3}$$

$$g_e = \widetilde{g_e} + e_{e2} \tag{3.4}$$

$e_{e1} \in (0, C_{e1})$, $e_{e2} \in (0, C_{e2})$ and C_{e1} , C_{e2} are the corresponding error covariance matrices. ($C_{e1} = \varepsilon_{e1} I$, $C_{e2} = \varepsilon_{e2} I, \varepsilon_{e1}$, ε_{e2} are the corresponding error variances).

By using S-Procedure and SDP theory, we can transform P1 to a easily solvable convex optimization problem P2:

$$\begin{aligned} &\mathrm{P2}: \min_{Q_s \geq 0} Tr(Q_s) \\ &s.t. \begin{bmatrix} A_r + \lambda_r I & u_r \\ {u_r}^H & c_r - \lambda_r {\gamma_r}^2 \end{bmatrix} \geq 0, \lambda_r \geq 0 \\ &\quad \begin{bmatrix} A_t + \lambda_{tr} I & u_t \\ {u_t}^H & c_t - \lambda_t {\gamma_t}^2 \end{bmatrix} \geq 0, \lambda_t \geq 0 \\ &\quad rank(Q_s) = 1 \end{aligned} \tag{3.5}$$

Where, $Q_s = E\{ww^H\}$, $A_r = -{C_{e1}}^{\frac{1}{2}} Q_s {C_{e1}}^{\frac{1}{2}}$, $u_r = -{C_{e1}}^{\frac{1}{2}} Q_s \widetilde{h_e}$, $c_r = -\widetilde{h_e}^H Q_s \widetilde{h_e} + 2^{-R_{m1}} \frac{{h_r}^H Q_s h_r}{t_1} t_2 + t_2(2^{-R_{m1}} - 1)$, $t_1 = {\sigma_r}^2$, $t_2 = p_t\|\ g_e\|^2 + {\sigma_e}^2$, $A_t = -{C_{e2}}^{\frac{1}{2}} Q_s {C_{e2}}^{\frac{1}{2}}$, $u_t = -{C_{e2}}^{\frac{1}{2}} Q_s \widetilde{h_e}$, $c_t = \widetilde{h_e}^H Q_s \widetilde{h_e} + 1 - \frac{t_3 \times t_4}{(1+ p_t\|\ h_t\|^2) \times 2^{-R_{m2}} - t_4}$, $t_3 = p_t\|\ g_e\|^2$ and $t_4 = {\partial_t}^2$.

The equation $\gamma_r = \sqrt{\frac{P^{-1}(1-\rho)}{2}}$ holds. $P^{-1}(x)$ is the inverse cumulative distribution function of Chi-square random variable.

The problem P2 becomes a convex problem and it can be easily solved by CVX toolkit [13] to get an optimal solution $\mathrm{Q_s}$ when we relax the rank-1 constraint. The solution of the problem can be determined through eigenvalue decomposition if $rank(Q_s) = 1$ and randomization technique if $rank(Q_s) > 1$. We finally obtain the optimal beamforming vector w^*.

B. *Power optimization under residual self-Interference*

In the current study, the self-interference of full duplex systems can be well eliminated, but, complete elimination is impossible. Therefore, the study of power optimization under residual self-interference is very meaningful.

When k isn't equal to zero, the constraint in (2.8) changes. We could not solve the problem easily by following the previous method. We need to do some transformation for solving method and transforms P1 to P3:

$$\begin{aligned} &P3: \min_{w} \|w\|^2 \\ &\mathrm{s.t.}\ Pr\{log\left(1+\frac{|\ {h_r}^H w|^2}{{\sigma_r}^2}\right) - log\left(1+\frac{|\ {h_e}^H w|^2}{{p_t}\|\ g_e\|^2+{\sigma_e}^2}\right) \geq \\ &\quad R_{m1}\} \geq 1-\rho \end{aligned} \tag{3.6}$$

$$\begin{aligned} &log\left(1+\frac{p_t\|\ h_t\|^2}{{\sigma_t}^2 + k^2\left|\ {h_e}^H w\right|^2}\right) \geq t \\ &Pr\{o\ g\left(1+\frac{p_t\|\ g_e\|^2}{|\ {h_e}^H w|^2+{\sigma_{e2}}^2}\right) \leq t - R_{m2}\} \geq 1-\rho \\ &R_{m2} \leq t \end{aligned} \tag{3.7}$$

We continue to transform the problem into a two step solution. First, we fixed t and solve an inner problem to get optimal $P^*(t)$.

$$Inner\ problem: \quad \boldsymbol{P^*(t)} = \min_{w} \|w\|^2$$

$$\text{s.t. } Pr\{log\left(1+\frac{|h_r{}^H w|^2}{\sigma_r{}^2}\right) - log\left(1+\frac{|h_e{}^H w|^2}{p_t\|g_e\|^2+\sigma_e{}^2}\right) \geq R_{m1}\} \geq 1-\rho \tag{3.8}$$

$$log\left(1+\frac{p_t\|h_t\|^2}{\sigma_t{}^2+k^2\left|H_b{}^H w\right|^2}\right)$$

$$Pr\left\{log\left(1+\frac{p_t\|g_e\|^2}{|h_e{}^H w|^2+\sigma_{e2}{}^2}\right) \leq t - R_{m2}\right\} \geq 1-\rho \tag{3.9}$$

The constraint in (3.8) can be modified as

$$Pr\{log\left(1+\frac{|h_r{}^H w|^2}{t_1}\right) - log\left(1+\frac{\left|(\widetilde{h_e}+e_{e1})^H w\right|^2}{t_2}\right) \geq R_{m1}\} \geq 1-\rho \tag{3.10}$$

Where $t_1 = \sigma_r{}^2$ and $t_2 = p_t\|g_e\|^2 + \sigma_e{}^2$. We define $Q_s = E\{ww^H\}$, the constraint in (3.10) can be modified as

$$Pr\{log\left(1+\frac{h_r{}^H Q_s h_r}{t_1}\right) - log\left(1+\frac{(\widetilde{h_e}+e_{e1})^H Q_s(\widetilde{h_e}+e_{e1})}{t_2}\right) \geq R_{m1}\} \geq 1-\rho \tag{3.11}$$

$$Pr\{e_{e1}{}^H Q_s e_{e1} + 2\Re\{e_{e1}{}^H Q_s \widetilde{h_e}\} + \widetilde{h_e}{}^H Q_s \widetilde{h_e} - [2^{-R_{m1}}\frac{h_r{}^H Q_s h_r}{t_1}t_2 + t_2(2^{-R_{m1}}-1)] \leq 0\} \geq 1-\rho \tag{3.12}$$

The above constraint can be formulated based on $e_{e1} = C_{e1}{}^{\frac{1}{2}} v_{e1}$ and $v_{e1} \sim N(0, I)$ as follows

$$Pr\left\{v_{e1}{}^H C_{e1}{}^{\frac{1}{2}} Q_s C_{e1}{}^{\frac{1}{2}} v_{e1} + 2\Re\left\{v_{e1}{}^H C_{e1}{}^{\frac{1}{2}} Q_s \widetilde{h_e}\right\} + \widetilde{h_e}{}^H Q_s \widetilde{h_e} - \left[2^{-R_{m1}}\frac{h_r{}^H Q_s h_r}{t_1}t_2 + t_2(2^{-R_{m1}}-1)\right] \leq 0\right\} \geq 1-\rho \tag{3.13}$$

Setting $A_r = -C_{e1}{}^{\frac{1}{2}} Q_s C_{e1}{}^{\frac{1}{2}}$, $u_r = -C_{e1}{}^{\frac{1}{2}} Q_s \widetilde{h_e}$ and $c_r = -\widetilde{h_e}{}^H Q_s \widetilde{h_e} + 2^{-R_{m1}}\frac{h_r{}^H Q_s h_r}{t_1}t_2 + t_2(2^{-R_{m1}}-1)$, the constraint in (3.13) can be modified as

$$Pr\{v_{e1}{}^H A_r v_{e1} + 2\Re\{v_{e1}{}^H u_r\} + c_r \geq 0\} \geq 1-\rho \tag{3.14}$$

$Pr\{v_{e1}{}^H v_{e1} \leq \gamma_{e1}{}^2\} \geq 1-\rho$ holds with $\gamma_r = \sqrt{\frac{P^{-1}(1-\rho)}{2}}$.

By using S-Procedure, the constraint in (3.13) and (3.14) can be modified as follows

$$\begin{bmatrix} A_r+\lambda_r I & u_r \\ u_r{}^H & c_r-\lambda_r\gamma_r{}^2 \end{bmatrix} \geq 0, \lambda_r \geq 0. \tag{3.15}$$

In the same way, the constraint in (3.9) can be modified. And P3 can be modified as an easily solvable problem:

$$P^*(t) = \min_{Q_s \geq 0} Tr(Q_s)$$

$$s.t. \begin{bmatrix} A_r+\lambda_r I & u_r \\ u_r{}^H & c_r-\lambda_r\gamma_r{}^2 \end{bmatrix} \geq 0, \lambda_r \geq 0 \tag{3.16}$$

$$k^2 Tr\left(H_b{}^H Q_s H_b\right) \leq \frac{p_t\|h_t\|^2}{2^t-1} - \sigma_t{}^2 \tag{3.17}$$

$$\begin{bmatrix} A_k+\lambda_k I & u_k \\ u_k{}^H & c_k-\lambda_k\gamma_k{}^2 \end{bmatrix} \geq 0, \lambda_k \geq 0$$

$$rank(Q_s) = 1$$

Where, $A_k = C_{e2}{}^{\frac{1}{2}} Q_s C_{e2}{}^{\frac{1}{2}}$, $u_k = C_{e2}{}^{\frac{1}{2}} Q_s \widetilde{h_e}$, $c_k = \widetilde{h_e}{}^H Q_s \widetilde{h_e} + 1 - \frac{p_t\|g_e\|^2}{2^{t-R_{m2}}-1}$.

Constant t is a fixed value in the inner level problem and the external optimization problem can be written as:

$$\text{Outer problem: } \min_t P^*(t)$$

$$s.t. \ \ R_{m2} < t \leq R$$

The R can be determined by the constraints in (3.16). It can be seen that there is no solution when $\frac{p_t\|h_t\|^2}{2^t-1} - \partial_t{}^2 \leq 0$. That optimal problem is infeasible when $t \geq log_2(\frac{p_t\|h_t\|^2}{\partial_t{}^2}+1)$.

Fig. 3 shows that the feasible interval of $P^*(t)$ is small and limited. We can use a one dimensional search method to find the minimal solution in the solvable range. The iterations of this method are approximately 20 times. It falls within the scope of general search method and it can be received by general study.

By solving the inner and outer problem, we can find the optimal matrix of the beam forming vector w^*. It ensures the secure communication of uplink and downlink in BS with minimal transmission power of BS and does not require the interference of the assistance of jamming nodes at the same time. The method increases the transmission efficiency of the base station because the transmission power of the base station is fully utilized to transmit useful signals.

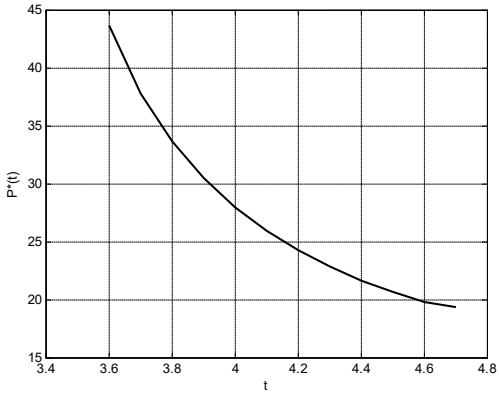

Fig. 3. Relationship between t and $P^*(t)$

IV. SIMULATION RESULTS

It is assumed that BS is equipped with 2 transmitting antennas and 3 receiving antennas（M=3，N=2. All of the channels are Gaussian channels, and the white Gaussian noise power of the channel is 1($\partial_t^2=\partial_{e2}=\partial_e=\partial_r=1$). In this paper, the method does not need to use artificial noise, hence we use NO AN to express this method in the simulation figures.

First, we use a series of simulation results to validate our theoretical results in the situation where self-interference of BS has been completely eliminated.

Fig. 4 shows the comparison of our proposed method with the traditional artificial noise method when the self-interference of BS is completely eliminated. The simulation results show that our method can save more transmission power compared to the traditional artificial noise method[18]. (In this figure, a denotes the percentage of artificial noise. a= Transmission power of artificial noise/ Transmission power of base station).

Fig. 5 shows the comparison of the required minimum transmission power of the base station corresponding to the situation of perfect CSI of Eve ($\varepsilon_{e1}=\varepsilon_{e2}=0$) and imperfect CSI of Eve ($\varepsilon_{e1}=\varepsilon_{e2}=0.01$). The required minimum transmission power of the base station in imperfect CSI of Eve is larger than that in perfect CSI of Eve. Additionally, more transmission power is required as the CSI becomes worse. The difference between these two approaches becomes larger as the required secrecy rate increases.

Fig. 6 shows the required minimum transmission power of the base station, corresponding to different required secrecy rates in different outage probabilities. Assuming that the outage probability of safety rate is 0.05 and 0.1($\rho = 0.05$ and $\rho = 0.1$) respectively, we can see that the smaller the outage probability is, the greater the optimal transmission power of base station needs. It's due to the fact that the requirement for the safety rate of system is higher when the outage probability is smaller. Thus, the optimal transmission power is larger.

Next, we validate our theoretical results in the situation of residual self-interference. Fig. 7 shows the optimal power of BS with different self-interference eliminations. As we expect, when the value of k is larger, the optimal power of BS is larger. The more residual self-interference is, the more interference the base station receives, and in order to improve the legal channel capacity, more transmission power is required. At the same time, in our simulation we find that there is no solution to the optimization problem when the value of k is greater than 0.2. After analysis, we find that the left inequality in constraints (3.16) increases as the value of k increases. It is difficult to meet the constraint conditions of inequality. Therefore, the optimization problem has no solution. Consequently, under the condition of channel in our simulation, the beamforming methods require that the system has a good performance of interference elimination. Our method doesn't work when the system has a bad performance of interference elimination. This is a defect of our method and will be improved in our future studies.

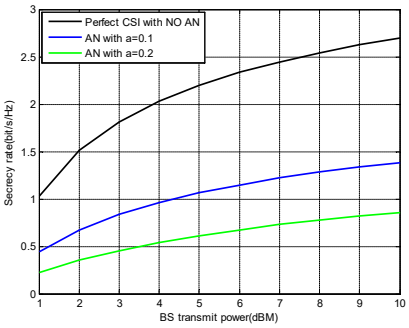

Fig. 4 Secrecy rates with different BS transmit powers

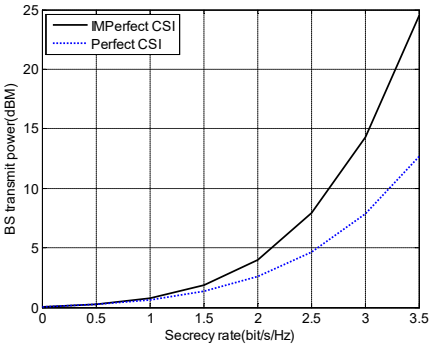

Fig. 5 BS transmit powers with different CSI

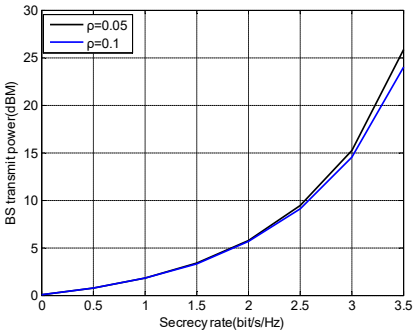

Fig. 6 BS transmit powers with different ρ

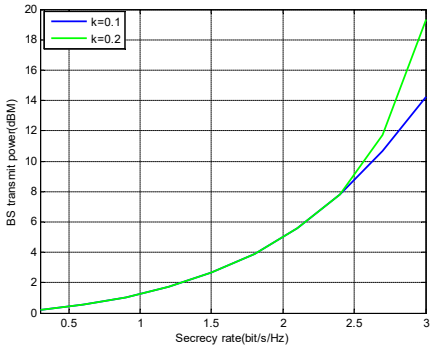

Fig. 7 BS transmit powers with different k

CONCLUSION

This paper proposes a beamforming method in full duplex wireless communications and ensures a secure transmission with the minimal transmission power of BS. We consider different solutions in different situations including completely eliminating self-interference and residual self-interference. In the latter situation, a two-level optimization method is proposed. The method can solve the power optimization problem under residual self-interference with an acceptable range of iterations. It can flexibly set the target safety rates without the fixed SNR of every point. Due to the safety rate constraints of uplink, the optimization problem has no solution when the value of k is too large. Therefore, this method requires a good interference elimination performance and it still needs to be improved.

REFERENCES

[1] J.Barros and M.R.D.Rodrigues,"Secrecy Capacity of Wireless Channels," to appear in Proc. ISIT 2006,July 2006

[2] Tan C C, Wang H, Zhong S, et al. Body sensor network security: an identity-based cryptography approach[C]//Proceedings of the first ACM conference on Wireless network security. ACM, 2008: 148-153.

[3] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," IEEE Commun. Mag., vol. 18, no. 5, pp. 66–74, Apr. 2011.

[4] A. D. Wyner, "The wire-tap channel," Bell System Technical Journal, vol. 54,no.8, pp. 1355-1387,Jan. 1975.

[5] Shannon C E. Coummunication Theory of Secrecy Systems [J]. Bell System Technical Journal, 1949, 28(4): 656-715.

[6] Liang Y., Kramer G., Poor H. V., et al. Compound wiretap channels[J]. EURASIP Journal on Wireless Communications and Networking, 2009, 5: 1-12

[7] G. Zheng, K.-K. Wong, A. Paulraj, and B. Ottersten, "Robust collaborative-relay beamforming," IEEE Trans. Signal Process., vol. 57, no. 8, pp. 3130–3143, Aug,2009.

[8] S. Hong,J. Brand, J. L Choi,M. Jain, J. Mehlman, K. Networks, S. Katti, P. Levis, and Stanford University, "Applications of Self-Interference Cancellation in 5G and Beyond,," in IEEE Communication Magzine, February 2014,pp.114-121.

[9] Michael E. Knox. Single Antenna Full Duplex Communications using a Common Carrier . Wireless and Microwave Technology Conference(WAMICON), 2012 IEEE 13th Annual. 2012,1-6

[10] YE Xia, ZHU Fengchao, GAO Feifei. A beam forming method for secure communications of full duplex physical layer [J]. JOURNAL OF XI'AN JIAOTONG UNIVERSITY,2015,08.

[11] ZHOU Y, XIANG Z Z, ZHU Y, et al. Application of full-duplex wireless technique into secure MIMO communication: achievable secrecy rate based optimization[J]. IEEE Signal Processing letters, 2014, 21(7): 804-808

[12] Jong-Ho,Lee, Full-Duplex relay for enhancing physical layer security in Multi-Hop Relaying Systems, IEEE COMMUNICATIONS LETTERS, 2015,19(4):525-528.

[13] Fengchao Zhu, Feifei Gao, Tao Zhang, Ke Sun and Minli Yao, "Physical-Layer Security for Full Duplex Communications With Self-Interference Mitigation," in IEEE Transactions on Wireless Communications, vol. 15, no. 1, pp. 329-340, Jan. 2016.

[14] Sahai A, Patel G, and Sabharwal A. Pushing the limits of full-duplex: design and real-time implementation[R]. The Computing Research Repository (CoRR), 2011.

[15] M.Grant and S.Boyd, "CVX: Matlab software for disciplined convex programming(web page and software) http://cvxr.com/cvx/," Jun.2009.

[16] S. Boyd and L. Vandenberghe, Convex Optimization. Cambridge,UK: Cambridge University Press, 2004.

[17] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian Wire-Tap Channel,IEEE Trans. Inf. Theory, vol. 24,pp. 451456,July 1978.

[18] Zhao Jiajie. Research on the physical layer security transmission algorithm of the MIMO system [D].PLA information engineering university,2012.