doi:10.3772/j.issn.1006-6748.2018.03.005

Impacts of feedback delay and estimation error on secrecy performance of MISO single eavesdropper cognitive radio networks①

Lin Zhi(林 志)②, Wang Lei, Cai Yueming, Yang Weiwei, Yang Wendong
(College of Communications Engineering, Army Engineering University of PLA, Nanjing 210007, P. R. China)

Abstract

Due to the broadcast nature of wireless transmission medium, security threats may hinder propagation of cognitive radio systems for commercial and military data application. This paper sets a channel error analytical framework and studies the joint impact of estimation errors and feedback delay on secrecy performance in cognitive radio networks. Under the assumption that system applies beamforming and jamming scheme, a multi-antenna cognitive base station (CBS) sends confidential signals to a secondary user (SU) in the presence of M primary users (PUs) and an eavesdropper. Assuming only imperfect channel state information (CSI) about the receivers is available, secrecy rate, outage probability, secrecy throughput are deduced to obtain a closed-form expression. It is shown that while the transmit power increases, secrecy throughput would reach to a constant. Simulation results show that feedback delay adversely impacts on secrecy rate, connection outage probability and secrecy throughput, while estimation error causes more impact on secrecy outage probability. Furthermore, the secrecy rate could increase progressively with the transmit power only if there exists no feedback delay.

Key words: cognitive radio, physical layer security, channel uncertainty, outage probability, throughput.

0 Introduction

Due to tremendous increase in the usage of wireless devices, most of the frequency spectrum has been licensed to operators by government. However, it is reported that the spectrum efficiency is as low as 15%[1,2]. Recently, cognitive radio technology has been attracted much attention, as it can solve spectrum scarcity problem by allowing unlicensed users to share the same spectrum with licensed users[3-6]. To achieve it, cognitive networks usually adopt underlay, overlay or interweave approach[7,8]. For the underlay approach, the secondary user (SU) is permitted to utilize the spectrum of the primary user (PU) as long as the interference of SU is below a threshold which PU can tolerate.

Physical layer security (PLS) in cognitive networks has attracted increasing attention as it plays an important role in many communication areas, such as military and civil data transmission. In 1949, Wyner's pioneering work defined the wiretap channel model and explore the random channel and decoding as a basic frame work of PLS[9]. Their work proves that secure communication is guaranteed in the presence of eavesdropper without traditional key-based cryptographic approaches. Furthermore, the development of computer performance and new calculation appearance cause traditional key encryption more vulnerable. As a supplement on existing security technology, PLS approaches exploit time-varying property of wireless fading channels to achieve secure transmission at the physical layer.

To overcome unfavorable channel conditions, the legitimate channel condition has worse channel quality than eavesdropper's[10]. One feasible way to ensure positive secrecy rate is to use multiple antennas technology to get over channel fading, such as multiple-input single-output (MISO) networks[11,12]. Because multiple antennas at terminals can increase spatial degrees of freedom (DoF), which enables the nodes to adopt beamforming or artificial jamming strategy to enhance the receiving rate of legitimate while degrading the reception of eavesdropper[13,14]. Considering the outage constraint on legitimate user, Ref. [11] studied a secrecy rate maximization problem through artificial noise beamforming in MISO networks. Considering im-

① Supported by the National Natural Science Foundation of China (No. 61371122, 61471393), and the China Postdoctoral Science Foundation under a Special Financial Grant (No. 2013T60912).

② To whom correspondence should be addressed. E-mail: linzhi945@163.com

Received on July 24, 2017

pact of feedback delay and estimation errors, the secrecy throughput analysis in MISO wiretap networks is addressed in Ref. [12]. However, the above work is considered under perfect channel state information (CSI) to enable advanced encoding.

Practically, this assumption is not realistic and there exists many reasons for uncertainty of CSI, such as feedback delay, estimation error and quantization error[15]. The secure encoding based on above imperfect CSI would cause interference on signal receiving of legitimate user and heavily deteriorate the secrecy performance of networks. Thus, it is significant to analyze and distinguish the impact of various uncertain factors of CSI. Huang[16], et al. proposed a joint cooperative beamforming and jamming scheme to enhance the security of a cooperative relay network under unavailable ECSI. Considering the feedback delay, Ref. [17] adopted transmit antenna selection and analyzed secrecy performance of MISO wiretap channels. Joint jammer and relay selection strategy is adopted to enhance physical layer security in channel feedback delay condition[18]. Ma[19], et al. studied secure transmission where only outdated knowledge of the legitimate receiver's channel is available. Nevertheless, papers mentioned above only consider the influence of estimation error and feedback delay respectively.

In cognitive radio networks, how to analyze the joint impact of channel errors demonstrates extreme importance due to its characteristics. There is very few work considering channel feedback delay or estimation error conditions, especially in cognitive radio networks. Thus, impacts of channel errors on system secrecy performance actually remain unknown. Meanwhile, the outage probability and throughput performance under channel uncertainty are seldom analyzed in cognitive networks. In this paper, a scenario in which a multi-antenna CBS communicate with a secondary user in the presence of some PUs and an eavesdropper will be considered. The focus turns to analyze the joint impact of feedback delay and estimation errors in MISOSE cognitive radio networks. Focusing on the analysis of channel errors, it is assumed that CBS uses beamforming and jamming scheme as state-of-the-art security approaches. Specifically, the following contributions are summarized:

- A framework of channel errors analysis is set for PLS performance in cognitive networks, the conclusion could give rise to error analysis in other communication scene, such as heterogeneous and sensor networks. Furthermore, this framework is giving guidance to robust algorithm study on different channel uncertainties.
- Establish a joint channel error expression to study impact of estimation errors and feedback delay of legitimate user and eavesdropper CSI of SU. It is assumed the system employs beamforming and jamming strategies as state-of-the-art, where beamforming can enhance the receiving of private signals and jamming strategy can confuse eavesdropper and degrade the receiving of private signals.
- Deduce secrecy rate, outage probability, secrecy throughput and obtain closed-form expressions. Then, the impact of feedback delay and estimation errors are analyzed on above secrecy performance. Simulation results demonstrate that the channel feedback delay adversely impacts on secrecy performance.

In Section 1, the system model is described and a joint model of feedback delay and estimation errors is built. Section 2 addresses the secrecy performance analysis of secrecy rate, outage and secrecy throughput. Section 3 introduces theoretical and Monte Carlo simulation results. Section 4 gives the conclusion.

Notation: Bold uppercase and lowercase letters denote matrices and vectors, respectively. $(\cdot)^H$ stands for Hermitian transpose of a matrix or vector. $\boldsymbol{I}_N$ is the identity matrix of size $(N \times N)$. $\mathrm{tr}\{\cdot\}$ is the trace of a matrix. $CN(\tau,\sigma^2)$ denotes the circularly symmetric, complex Gaussian distribution with mean τ and variance σ^2.

1 System model

In this part, a MISOSE cognitive radio networks model is described and a joint error model is built which considers both feedback delay and estimation errors.

1.1 Model description

As shown in Fig. 1, consider an underlay cognitive network. The primary system consists of N-antennas cognitive base station (CBS) communicating to a single-antenna SU, M single-antenna PUs $P_m\{m \in 1, \cdots, M\}$ and a passive eavesdropper E, which attempt to wiretap the secondary messages. All the channels are assumed to be quasi-stationary and remain constant during one operation period. $\boldsymbol{h}_i(t) = [h_{i,1}(t), \cdots, h_{i,N_t}(t)]^T \sim CN(0,\sigma_i^2\boldsymbol{I}_{N_t})$, $i = \{D,E,P\}$ denote channel coefficients of CBS to SU, CBS to E and CBS to PUs at time t, respectively. It is assumed that receiving nodes adopt pilot symbol based linear minimum mean square (LMMSE) channel estimation[18].

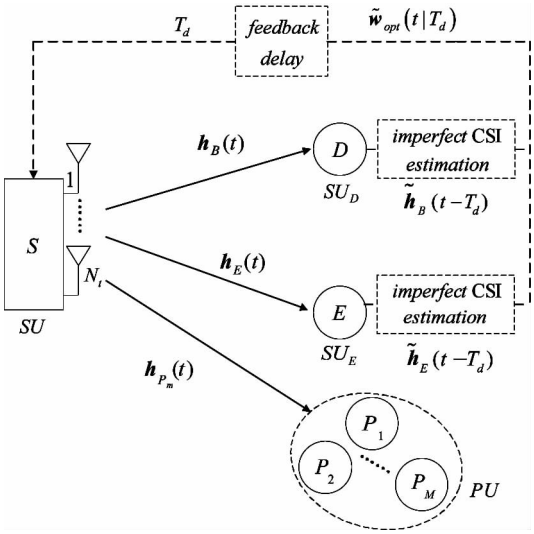

Fig. 1 Illustration of System Model

1.2 Joint error model

In traditional cognitive networks, it is key to achieve secure transmission only if perfect CSI could be obtained. However, it may not be possible to know the perfect CSI in practice because many imperfect factors would collectively prevent the acquisition of perfect CSI. Thus, how to evaluate the impact of imperfect CSI on performance appears extremely important. In this section, a joint channel error model is established, which considers both feedback delay and estimation errors.

1.2.1 Estimation errors

According to the CSI channel uncertainty model, while the CSI uncertainty is random and not bounded, such a model can be viewed as channel estimation error model. Pilot symbol based LMMSE channel estimation is employed and the channel impulse response is assumed to be constant during the pilot symbol feedback process[18].

Suppose that the private information $x(t)$ is inserted with pilot symbols periodically, where the interval is L. Then CBS transmitter estimates the corresponding CSI $h(t) \sim CN(0, \sigma_h^2)$ according to $N = N_1 + N_2$ pilot symbols, where N_1 symbol is inserted at the left and N_2 symbol is at the right sides of $x(t)$. And the received pilot signals to estimate CSI at CBS is

$$\boldsymbol{y}_{pilot} = diag(\boldsymbol{p}_{pilot})\boldsymbol{h}_{pilot}x(t) + \boldsymbol{n}_{pilot}$$

where $\boldsymbol{p}_{pilot} = [x(t-L(N_1-1)-l), \cdots, x(t-l), x(t+L-l), \cdots, x(t+L(N_2-1)-l)]^T$

$$\boldsymbol{h}_{pilot} = [h(t-L(N_1-1)-l), \cdots, h(t-l), h(t+L-l), \cdots, h(t+L(N_2-1)-l)]^T \quad (1)$$

where $\boldsymbol{y}_{pilot}$, $\boldsymbol{h}_{pilot}$, $\boldsymbol{n}_{pilot}$ denotes pilot symbol, CSI and noise, $l \in \{1,2,\cdots,l\}$. Thus, the estimation of channel can be written as

$$\hat{h}(t) = \boldsymbol{w}_{pilot}\boldsymbol{y}_{pilot} \quad (2)$$

where $\boldsymbol{w}_{pilot} = \boldsymbol{C}_{\boldsymbol{h}_{pilot}\boldsymbol{y}_{pilot}}\boldsymbol{R}_{y_{pilot}}^{-1}$ denotes weight of LMMSE estimation factor, while $\boldsymbol{C}_{\boldsymbol{h}_{pilot}\boldsymbol{y}_{pilot}} = E[h_{pilot}^*(n)\boldsymbol{y}_{pilot}]$ denotes correlation vector of $h_{pilot}(t)$, which is given as Eq. (3). $\boldsymbol{R}_{\boldsymbol{y}_{pilot}} = E[\boldsymbol{y}_{pilot}\boldsymbol{y}_{pilot}^H]$ represents autocorrelation matrix of $\boldsymbol{y}_{pilot}$ shown as Eq. (4).

$$\boldsymbol{C}_{\boldsymbol{y}_{pilot}} = [\sqrt{P_{pilot}}R_{h_{pilot}}(-(N_1-1)L-l), \cdots, \sqrt{P_{pilot}}R_{h_{pilot}}(L-l), \cdots, \sqrt{P_{pilot}}R_{h_{pilot}}((N_2-1)L-l)] \quad (3)$$

$$\boldsymbol{R}_{\boldsymbol{h}_{pilot}\boldsymbol{y}_{pilot}} = E[\boldsymbol{y}_{pilot}\boldsymbol{y}_{pilot}^H] = \begin{bmatrix} P_{pilot}R_{h_{pilot}}(0)+N_0 & P_{pilot}R_{h_{pilot}}(L) & \cdots & P_{pilot}R_{h_{pilot}}((N-1)L) \\ P_{pilot}R_{h_{pilot}}(L) & P_{pilot}R_{h_{pilot}}(0)+N_0 & \cdots & P_{pilot}R_{h_{pilot}}((N-2)L) \\ \vdots & \vdots & \vdots & \vdots \\ P_{pilot}R_{h_{pilot}}((N-1)L) & P_{pilot}R_{h_{pilot}}((N-2)L) & \cdots & P_{pilot}R_{h_{pilot}}(0)+N_0 \end{bmatrix} \quad (4)$$

The channel estimation error model can be written as[16]

$$h(t) = \hat{h}(t) + e(t) \quad (5)$$

The channel estimation $\hat{h}(t) \sim CN(0, \sigma_{\hat{h}}^2)$ and estimation error $e(t) \sim CN(0, \sigma_e^2)$ is independent, and they follow $\sigma_{\hat{h}}^2 = \boldsymbol{C}_{\boldsymbol{h}_{pilot}\boldsymbol{y}_{pilot}}(\boldsymbol{R}_{\boldsymbol{y}_{pilot}}^{-1})^H\boldsymbol{C}_{\boldsymbol{h}_{pilot}\boldsymbol{y}_{pilot}}^H$ and $\sigma_e^2 = \sigma_h^2 - \sigma_{\hat{h}}^2$.

To simplify the analysis, $N = 1$, $L = 2$ is defined. Thus $\sigma_{\hat{h}}^2$ can be simplified as $\sigma_{\hat{h}}^2 = P_{pilot}\sigma_h^4/(P_{pilot}\sigma_h^2 + N_0)$, channel estimation error can be written as

$$\sigma_e^2 = \frac{\sigma_h^2}{1+\sigma_h^2 P_{pilot}/N_0} = \frac{\sigma_h^2}{1+\delta\eta\sigma_h^2} \quad (6)$$

where P_{pilot} and N_0 denote pilot power and noise power, respectively. $\eta = P/N_0$ represents transmit SNR of useful information. $\delta = P_{pilot}/P$ the channel estimation quality.

Eq. (5) can be converted to another equivalent expression, which is expressed as

$$\hat{h}(t) = \rho_e h(t) + v(t) \quad (7)$$

Channel $h(t)$ and noise follow Gaussian distribution, $\rho_e = E[\hat{h}^*(t)h(t)]/\sigma_{\hat{h}}^2 = \delta\eta\sigma_{\hat{h}}^2/(1+\delta\eta\sigma_{\hat{h}}^2)$ is the normalized estimation error parameter.

1.2.2 Feedback delay

Due to time-variation of channel and time consuming of signal processing, there exist feedback delay between the estimated CSI and practical one, and T_d is defined as delay time and the mathematic relation between $h(t)$ and $h(t-T)$ through Markov process could be deduced:

$$h(t) = \rho_d h(t-T_d) + e_d(t) \quad (8)$$

where $\rho_d = E[\hat{h}^*(t)h(t-T_d)]/\sigma_{\hat{h}}^2$ denotes correlation coefficient of estimated channel, $e_d(t) \sim CN(0, (1-\rho_d^2)\sigma_{\hat{h}}^2)$ denotes feedback delay error. According to

Clark channel model in Ref. [20], ρ_d equals $J_0(2\pi f_d T_d)$, where $J_0(\cdot)$ is the first kind of zero Bessel function and f_d denotes maximum Doppler frequency. Define $X = |h(t)|^2$ and $Y = |h(t-T_d)|^2$, the joint probability density function of X and Y can be written as

$$f_{X,Y}(x,y) = \frac{e^{-\frac{x+y}{(1-\rho_d^2)\sigma_h^2}}}{(1-\rho_d^2)\sigma_h^2} I_0\left(\frac{2\sqrt{\rho_d^2 xy}}{(1-\rho_d^2)\sigma_h^2}\right) \quad (9)$$

where $I_0(\cdot)$ is the first kind of zero modified Bessel function of zero order.

1.2.3 Joint errors model

Eq. (3) and Eq. (8) are substituted into Eq. (7), a uniform model is built to demonstrate the relationship between practical CSI estimation at SU and time-delay CSI estimation, which can be expressed as

$$\begin{aligned}\hat{h}(t) &= \rho_e h(t) + v(t)\\ &= \rho_e[\rho_d h(t-T_d) + e_d(t)] + v(t)\\ &= \rho_e\rho_d\hat{h}(t-T_d) + \rho_e\rho_d e(t-T_d) + \rho_e e_d(t_d) + v(t)\\ &= \rho\hat{h}(t-T_d) + \varepsilon(t)\end{aligned} \quad (10)$$

where

$$\rho = \begin{cases}\rho_e\rho_d, & \rho_d < 1\\ 1, & \rho_d = 1\end{cases} \quad (11)$$

Obviously, if there exists feedback delay, $\rho = 1$. It is defined that $\varepsilon(t) = \rho_e\rho_d e(t) + \rho_e e_d(t-T_d) + v(t)$ is zero mean AWGN component and $\varepsilon(t) \sim CN(0, \sqrt{1-\rho^2}\sigma_h^2)$.

1.3 Transmission scheme based beamforming and jamming

In the MISOSE cognitive networks, it is assumed that CBS adopts hybrid beamforming and jamming scheme to enhance signal receiving at SU and confuse eavesdropper under the interference constraints at PUs. First, the interference constraints on PUs are analyzed. The probability that the CBS can transmit signals is derived as

$$\begin{aligned}&\Pr(\max\{IN_{P_m}\} \leqslant \gamma_{th})\\ &IN_{P_m} = P_S \|\boldsymbol{h}_{P_m}\|^2 + N_0 \quad m = 1,\cdots,M\end{aligned} \quad (12)$$

where IN_{P_m} is the interference power constraint at P_m from the CBS. γ_{th} denotes the interference tolerance at PUs. If interference power IN_{P_m} is beyond tolerance γ_{th}, CBS transmission would stay idle and occur outage. Otherwise, the CBS transmission would operate as usual.

Since the channel coefficients between single-antenna nodes are randomly generated as complex zero-mean Gaussian random vectors with unit covariance, the channel coefficient of CBS PUs link follows Gamma distribution $\|\boldsymbol{h}_{P_m}\|^2 \sim \Gamma\left(\frac{M}{2}, 2\right)$, the PDF of the coefficient is given by

$$f_{\|\boldsymbol{h}_{P_m}\|^2}(x) = \frac{x^{N_t/2-1}e^{-x/2}}{\Gamma(M/2)2^{N_t}} \quad (13)$$

Thus, the transmission probability under single PU condition is obtained as

$$\Pr(IN_{P_m} \leqslant \gamma_{th}) = 1 - \frac{\Gamma\left(\frac{N_t}{2}, \frac{\Gamma - N_0}{2P_S}\right)}{\Gamma\left(\frac{N_t}{2}/2\right)} \quad (14)$$

where $\Gamma(\cdot,\cdot)$ is the upper incomplete gamma function defined as $\Gamma(k,x) = \int_x^\infty e^{-t}t^{k-1}\mathrm{d}t$ and gamma function $\Gamma(z)$ equals $\int_0^\infty e^{-t}t^{z-1}\mathrm{d}t$. So Eq. (14) can be written as

$$\begin{aligned}\Pr(IN_{P_m} \leqslant \gamma_{th}) &= 1 - \frac{2^{-\frac{M}{2}}}{\Gamma\left(\frac{M}{2}\right)}\int_u^\infty x^{\frac{M}{2}-1}e^{-\frac{1}{2}x}\mathrm{d}x\\ &= 1 - \frac{\Gamma\left(\frac{M}{2}, \frac{u}{2}\right)}{\Gamma\left(\frac{M}{2}\right)}\\ &= 1 - \frac{2^{-M}e^{-\frac{u}{2}}}{\Gamma(M^*+1)}\sum_{k=0}^{M^*}\frac{M^*!(2\sigma^2\gamma_{th})^k}{k!P_A^k}\end{aligned} \quad (15)$$

where $u = \sigma^2\gamma_{th}/2P_A$, $M^* = [M/2] + 1$ and $[t]$ is defined as the integer part of t.

Note that there are M PUs, using order statistics, the probability of Eq. (12) can be obtained as

$$\begin{aligned}&\Pr(\max\{IN_{P_m}\} \leqslant \gamma_{th})\\ &= \left(1 - \frac{2^{-M}e^{-\frac{u}{2}}}{\Gamma(M^*+1)}\sum_{k=0}^{M^*}\frac{M^*!(2\sigma^2\gamma_{th})^k}{k!P_A^k}\right)^M\end{aligned} \quad (16)$$

Then, the beamforming weight of hybrid scheme can be written as

$$\hat{\boldsymbol{w}}_{opt}(t|T_d) = \arg\max_{\boldsymbol{w}} |\boldsymbol{w}^H\hat{\boldsymbol{h}}_D(t-T_d)|^2 \quad (17)$$

Meanwhile, random Gaussian noise with weight matrix $\boldsymbol{Q}(t) = \boldsymbol{N}_{\hat{\boldsymbol{w}}_{opt}(t|T_d)}$ is emitted, which is the null space of $\hat{\boldsymbol{w}}_{opt}(t|T_d)$. The transmit signals at CBS are given by

$$\boldsymbol{x}(t) = \boldsymbol{w}(t)s(t) + \boldsymbol{Q}(t)\boldsymbol{a}(t) \quad (18)$$

where $s(t)$ and $\boldsymbol{a}(t)$ denote private signal and jamming signal, respectively, and $\boldsymbol{E}[|s(t)|^2] = \sigma_s^2$, $\boldsymbol{a}(t) \sim CN(0, \sigma_a^2\boldsymbol{I}_{N_t-1})$. Power allocation coefficient between data signal and jamming signal is defined as $\lambda \in [0,1]$, which demands $\sigma_s^2 = \lambda P$ and $\sigma_a^2 = (1-\lambda)P/(N_t-1)$. Thus, received signals at CBS and eavesdropper can be written as

$$\begin{aligned} y_D(t) &= \hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)\boldsymbol{h}_D(t)s(t) + \boldsymbol{N}_{\hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)}\boldsymbol{a}(t)\boldsymbol{h}_D(t) \\ &\quad + n_D(t) \\ &= \hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)(\rho_D\hat{\boldsymbol{h}}_D(t-T_d) + \boldsymbol{\varepsilon}(t))s(t) \\ &\quad + \boldsymbol{N}_{\hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)}\boldsymbol{a}(t)(\rho_D\hat{\boldsymbol{h}}_D(t-T_d) + \boldsymbol{\varepsilon}(t)) + n_D(t) \\ &= \rho_D\hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)\hat{\boldsymbol{h}}_D(t-T_d)s(t) \\ &\quad + \boldsymbol{N}_{\hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)}\boldsymbol{a}(t)\boldsymbol{\varepsilon}(t) + \hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)\boldsymbol{\varepsilon}(t)s(t) \\ &\quad + n_D(t) \end{aligned} \tag{19}$$

$$\begin{aligned} y_E(t) &= \hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)\hat{\boldsymbol{h}}_E(t)s(t) + \boldsymbol{N}_{\hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)}\boldsymbol{a}(t)\hat{\boldsymbol{h}}_E(t) \\ &\quad + (\hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)s(t) + \boldsymbol{N}_{\hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)}\boldsymbol{a}(t))\boldsymbol{e}(t) \\ &\quad + n_E(t) \end{aligned} \tag{20}$$

It is assumed the system has full rate feedback and quantization error is not considered. The estimated CSI of $\boldsymbol{h}_B(t)$ and $\boldsymbol{h}_E(t)$ is modeled as Eq. (10), where the estimation error parameter is $\rho_{e_i} = \delta\eta\sigma_{h_i}^2/(1+\delta\eta\sigma_{h_i}^2)$.

The channel capacity at CBS and eavsesdropper can be written as

$$I_D = \log_2(1+\gamma_D) = \log_2\left(1 + \frac{\lambda P(\rho_D^2 \mid \hat{\mathbf{w}}_{\mathrm{opt}}^H(\mathrm{t} \mid \mathrm{T_d})\hat{\boldsymbol{h}}_D(t-T_d) \mid^2 + \mid \hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)\varepsilon(t) \mid^2)}{\frac{(1-\lambda)P}{N_t-1} \parallel N_{\hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)}\varepsilon(t) \parallel^2 + \lambda P(1-\rho_{e_D}^2)\sigma_D^2 + N_0}\right) \tag{21}$$

$$I_E = \log_2(1+\gamma_E) = \log_2\left(1 + \frac{\lambda P \mid \hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)\hat{\boldsymbol{h}}_E(t) \mid^2}{\frac{(1-\lambda)P}{N_t-1} \parallel \boldsymbol{N}_{\hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)}\hat{\boldsymbol{h}}_E(t) \parallel^2 + P(1-\rho_{e_E}^2)\sigma_E^2 + N_0}\right) \tag{22}$$

where $\mid \hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)\varepsilon(t) \mid^2$ and $\parallel \boldsymbol{N}_{\hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)}\varepsilon(t) \parallel^2$ denote beamforming excursion and artificial jamming leakage due to estimation errors and feedback delay. The received jamming signals at CBS and eavesdropper are $\parallel \boldsymbol{N}_{\hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)}\varepsilon(t) \parallel^2 \sim Gamma(N_t-1, (1-\rho_{e_D}^2)\sigma_D^2)$ and $\parallel \boldsymbol{N}_{\hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)}\hat{\boldsymbol{h}}_E(t) \parallel^2 \sim Gamma(N_t-1, \rho_{e_E}^2\sigma_E^2)$, respectively.

2 Performance analysis

In this part, first the receiving SNR at receivers is deduced and then the secrecy performance of average secrecy rate, outage probability and secrecy throughput are analyzed.

From Eq. (21), the receiving SNR at SU is given by

$$\begin{aligned} \gamma_D &= \frac{\lambda\rho_D^2 \mid \hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)\hat{\boldsymbol{h}}_b(t-T_d) \mid^2 + \mid \hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)\varepsilon(t) \mid^2}{\frac{(1-\lambda)}{N_t-1} \parallel \boldsymbol{N}_{\hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)}\varepsilon(t) \parallel^2 + \lambda(1-\rho_{e_D}^2)\sigma_D^2 + \eta^{-1}} \\ &= \frac{\lambda\rho_{e_D}^2\rho_d^2(\rho_{e_D}^{-2}-1)^{-1}\chi_{2N_t} + \chi_2}{\frac{(1-\lambda)}{N_t-1}\chi_{2N_t-2} + \lambda + (1-\rho_{e_D}^2)^{-1}\sigma_D^{-2}\eta^{-1}} \end{aligned} \tag{23}$$

The CDF of γ_D is obtained as

$$\begin{aligned} F_{\gamma_D}(x) &= 1 - \frac{e^{-a_3x}}{(1-a_1)^2}(a_2x+1)^{-1} \\ &\quad + \frac{e^{-a_3x/a_1}}{1-a_1}(a_2x+a_1)^{-1}\left[\frac{2-a_1}{1-a_1} + \frac{a_3x}{a_1} + \frac{a_2x}{a_1}\left(\frac{a_2x}{a_1}+1\right)^{-1}\right] \end{aligned} \tag{24}$$

where $a_1 = \lambda\rho_{e_D}^2\rho_d^2(\rho_{e_D}^{-2}-1)^{-1}$, $a_2 = (1-\lambda)/(N_t-1)$ and $a_3 = \lambda + (1-\rho_{e_D}^2)^{-1}\sigma_D^{-2}\eta^{-1}$.

The receiving SNR at eavesdropper can be written as

$$\begin{aligned} \gamma_E &= \frac{\lambda P \mid \hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)\hat{\boldsymbol{h}}_E(t) \mid^2}{\frac{(1-\lambda)P}{N_t-1} \parallel \boldsymbol{N}_{\hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)}\hat{\boldsymbol{h}}_E(t) \parallel^2 + P(1-\rho_{e_E}^2)\sigma_E^2 + N_0} \\ &= \frac{\lambda\chi_2}{\frac{1-\lambda}{N_t-1}\chi_{2N_t-2} + (\rho_{e_E}^{-2}-1) + \rho_{e_E}^{-2}\sigma_E^{-2}\eta^{-1}} \end{aligned} \tag{25}$$

The CDF of γ_E is obtained as

$$\begin{aligned} F_{\gamma_E}(x) &= 1 - \int_0^\infty e^{-\left(\frac{b_2}{b_1}y + \frac{b_3}{b_1}\right)x}\frac{y^{N_t-2}e^{-y}}{\Gamma(N_t-1)}\mathrm{d}y \\ &= e^{-\frac{b_3}{b_1}x}\left(1 + \frac{b_2}{b_1}x\right)^{1-N_t} \end{aligned} \tag{26}$$

where $b_1 = \lambda$, $b_2 = (1-\lambda)/(N_t-1)$, $b_3 = (\rho_{e_E}^{-2}-1) + \rho_{e_E}^{-2}\sigma_E^{-2}\eta^{-1}$.

While $\eta \to \infty$, channel estimation coefficient ρ_{e_i} tends to one. According to Eqs (23) and (25), in high SNR region, γ_D and γ_E can be written as

$$\lim_{\eta\to\infty}\gamma_D = \frac{N_t-1}{\lambda^{-1}-1}\frac{\rho_B^2 \parallel \hat{\boldsymbol{h}}_D(t-T_d) \parallel^2 + \mid \hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)\varepsilon(t) \mid^2}{\parallel \boldsymbol{N}_{\hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)}\varepsilon(t) \parallel^2} \tag{27}$$

$$\lim_{\eta\to\infty}\gamma_E = \frac{N_t-1}{\lambda^{-1}-1}\frac{\mid \hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)\hat{\boldsymbol{h}}_E(t) \mid^2}{\parallel \boldsymbol{N}_{\hat{\boldsymbol{w}}_{opt}^H(t \mid T_d)}\hat{\boldsymbol{h}}_E(t) \parallel^2} \tag{28}$$

From Eqs (27) and (28), one can find that the receiving SNR at SU and eavesdropper are some non-zero value in high SNR region, which is irrelevant to η.

2.1 Average secrecy rate

According to Wyner wiretap channel model, secrecy rate can be expressed as

$$C_S = \begin{cases} \log_2(1+\gamma_D) - \log_2(1+\gamma_E) & \gamma_D > \gamma_E \\ 0 & \text{otherwise} \end{cases} \tag{29}$$

where $\gamma_D = P \mid h_D \mid^2/\sigma_D^2$ and $\gamma_E = P \mid h_E \mid^2/\sigma_E^2$ denote the instantaneous SNR at Bob and Eve. P is transmit power, γ_D and γ_E are channel gains at Bob and Eve, σ_D^2 and σ_E^2 denote corresponding noise variance.

While the CSI of main channel and eavesdropping channel is imperfect, then fixed encoding rates (R_0,

R_s) would be adopted, where R_0 and R_s are the coding rate and secrecy rate, respectively. It often uses average secrecy rate to judge the performance, which is written as

$$\bar{C}_S = [I_D - I_E]^+ \tag{30}$$

Secrecy rate criterion is suitable for delay tolerant networks, such as email. In this paper, SU is assumed to employ fixed encoding rates (R_0, R_s), the average secrecy rate is given as

$$\begin{aligned}\bar{C}_s &= [C_D - C_E]^+ \Pr(\max\{IN_{P_m}\} \leqslant \gamma_{th}) \\ &= (E_{\boldsymbol{h}_D}[\log_2(1+\gamma_D)] - E_{\boldsymbol{h}_D,\boldsymbol{h}_E}[\log_2(1+\gamma_E)])^+ \\ &\quad \Pr(\max\{IN_{P_m}\} \leqslant \gamma_{th})\end{aligned} \tag{31}$$

From the CDF expression of γ_B and γ_E, it can be obtained that the average mutual information of main channel and eavesdropper channel as Eqs(32) and (33). Substitute Eq. (32) and Eq. (33) into Eq. (31), one can obatin the average secrecy rate.

While there exist feedback delay and $\eta \to \infty$, the average secrecy rate tends to a certain non-zero value. However when there is no feedback delay or $\gamma_D \to \infty$, average secrecy rate also tends to ∞, which means that any secrecy rate through increasing transmit power could be got.

$$\begin{aligned}C_D &= \frac{1}{\ln 2}\int_0^\infty \frac{1-f_{\gamma_D}(x)}{1+x}\mathrm{d}x \\ &= \frac{(1-a_1)^{-2}a_2^{-1}}{\ln 2}\Big[\Big(\frac{e^{a_3a_2^{-1}}}{1-a_2^{-1}} - \frac{(2-a_1)e^{a_3a_2^{-1}}}{1-a_1a_2^{-1}}\Big)Ei(a_3a_2^{-1}) + \frac{e^{a_3}Ei(a_3)}{(1-a_2^{-1})^2} - \frac{(2-a_1)e^{a_3a_2^{-1}}Ei(a_3a_1^{-1})}{(1-a_1a_2^{-1})^2}\Big] \\ &\quad - \frac{1}{\ln 2}\frac{a_1}{1-a_1}\Big[\frac{a_3e^{a_3a_1^{-1}}}{a_2}Ei(a_3a_1^{-1}) + \frac{a_1}{a_2}(1-a_3a_2^{-1})\Big(\frac{e^{a_3a_2^{-1}}Ei(a_3a_2^{-1})}{(1-a_1a_2^{-1})} + \frac{e^{a_3a_1^{-1}}Ei(a_3a_1^{-1})}{(1-a_1a_2^{-1})^2}\Big) \\ &\quad - \frac{a_1^2}{a_2^2}\Big(\frac{a_2a_1^{-1}-a_3a_1^{-1}e^{a_3a_2^{-1}}}{(1-a_1a_2^{-1})} - \frac{e^{a_3a_2^{-1}}+e^{a_3a_1^{-1}}}{(1-a_1a_2^{-1})^2}\Big)Ei(a_3a_2^{-1})\Big]\end{aligned} \tag{32}$$

$$\begin{aligned}C_E &= \frac{1}{\ln 2}\int_0^\infty \frac{e^{-\frac{b_3}{b_1}x}}{1+x}\Big(1+\frac{b_2}{b_1}x\Big)^{1-N_t}\mathrm{d}x \\ &= \frac{1}{\ln 2}\int_0^\infty e^{-\frac{b_3}{b_1}x}\Big[\Big(1+\frac{b_2}{b_1}\Big)^{1-N_t}\frac{1}{x+1} + \sum_{k=1}^{N-1}\binom{N_t-1}{k}\Big(1+\frac{b_2}{b_1}\Big)^{-k}\Big(\frac{b_2}{b_1}\Big)^{N_t-1-k}\Big(x+\frac{b_1}{b_2}\Big)^{k+1-N_t}\Big]\mathrm{d}x \\ &= \frac{1}{\ln 2}\Big[\Big(1+\frac{b_2}{b_1}\Big)^{1-N_t}e^{\frac{b_3}{b_1}}Ei\Big(\frac{b_3}{b_1}\Big) + \sum_{k=1}^{N-1}\binom{N_t-1}{k}\Big(1+\frac{b_2}{b_1}\Big)^{-k}\Big(\frac{b_2}{b_1}\Big)^{N_t-1-k}e^{\frac{b_3}{b_2}}\Gamma\Big(k+1-N,\frac{b_3}{b_2}\Big)\Big]\end{aligned} \tag{33}$$

2.2 Outage probability and secrecy throughput

Average secrecy rate criterion is suitable to measure non-real-time transmission. However, for systems with stringent delay constraints, perfect secret can not be achieved especially for the imperfect CSI, outage probability criterion is more appropriate to measure the secrecy performance.

Connection outage probability (COP) is defined to measure transmission reliability while secrecy outage probability (SOP) is put forward to stand for the security of communications[21], which uses fixed secrecy rate encoding rates (R_0, R_s), If $R_0 > I_D$, it shows that connection between transmitter and legitimate receiver can not be achieved and connection outage occurs, if $R_S > R_0 - I_E$, it indicates that eavesdropper could obtain some private signals and secrecy outage occurs. Outage probabilities can be expressed as

$$\begin{aligned}P_{co} &= \Pr(I_D < R_0)\Pr(\max\{IN_{P_m}\} \leqslant \gamma_{th}) \\ &\quad + \Pr(\max\{IN_{P_m}\} > \Gamma) \\ &= F_{\gamma_D}(2^{R_0}-1)\Pr(\max\{IN_{P_m}\} \leqslant \gamma_{th}) \\ &\quad + \Pr(\max\{IN_{P_m}\} > \gamma_{th})\end{aligned} \tag{34}$$

$$\begin{aligned}P_{so} &= \Pr(I_E > R_0 - R_s)\Pr(\max\{IN_{P_m}\} \leqslant \gamma_{th}) \\ &\quad + \Pr(\max\{IN_{P_m}\} > \gamma_{th}) \\ &= (1 - F_{\gamma_E}(2^{R_0-R_s}-1))\Pr(\max\{IN_{P_m}\} \\ &\quad \leqslant \gamma_{th}) + \Pr(\max\{IN_{P_m}\} > \gamma_{th})\end{aligned} \tag{35}$$

From Eqs(34) and (35), it is observed that COP and SOP tend to some certain non-zero value in high SNR region.

Moreover, the secrecy throughput performance is analyzed. Compared with traditional throughput concept, it only considers reliability of transmission[22]. In the cognitive MISOSE networks, a modified secrecy throughput criterion is defined to measure both the transmission security and reliability, which is based on COP and SOP.

$$\begin{aligned}\zeta &= R_s \cdot \Pr\{I_D > R_0,\ I_E < R_0 - R_s\} \\ &\quad \Pr(\max\{IN_{P_m}\} \leqslant \gamma_{th}) \\ &= R_s(1-P_{co})(1-P_{so})\Pr(\max\{IN_{P_m}\} \leqslant \gamma_{th}) \\ &= R_sF_{\gamma_D}(2^{R_0}-1)(1-F_{\gamma_E}(2^{R_0-R_s}-1))\end{aligned}$$

$$\Pr(\max\{IN_{P_m}\} \leqslant \gamma_{th}) \tag{36}$$

According to Eq. (36), while transmit SNR $\eta \to \infty$, secrecy throughput would reach to a certain non-zero value.

3 Numerical analysis results

In this part, Monte Carlo and analytical simulation results are presented to verify the performance analysis in Section 2. The number of simulation times is 50000, and the system is assumed to only consider the impact of feedback delay and estimation errors without quantization errors. Except Fig. 5, the power allocation of beamforming and jamming is $\lambda = 0.5$ and antenna number of CBS is 3. Solid and dotted lines denote theoretical simulation, marks (such as circle) denote Monte Carlo simulation.

- NFD, $\delta = 1$: Estimation error $\delta = 1$ without feedback delay;
- $f_dT_d = 0.1$, $\delta = 1$: Feedback delay $f_dT_d = 0.1$, estimation error $\delta = 1$.
- $f_dT_d = 0.1$, PE: Feedback delay $f_dT_d = 0.1$ with perfect estimation.
- NFD, PE: No feedback delay and perfect estimation.

In Fig. 2, the secrecy rate comparison against transmit SNR of different channel error conditions is presented. In general, it can be seen that the feedback delay ($f_dT_d = 0.1$) cause much more performace degradation than estimation error ($\delta = 1$). While feedback delay exists (f_dT_d is much more than 0.1), the secrecy rate would reach to an upper floor with increasing of transmit power. If the estimation errors exists, NFD condition performance is much better than feedback delay condition, and secrecy rate would increase progressively with the transmit power.

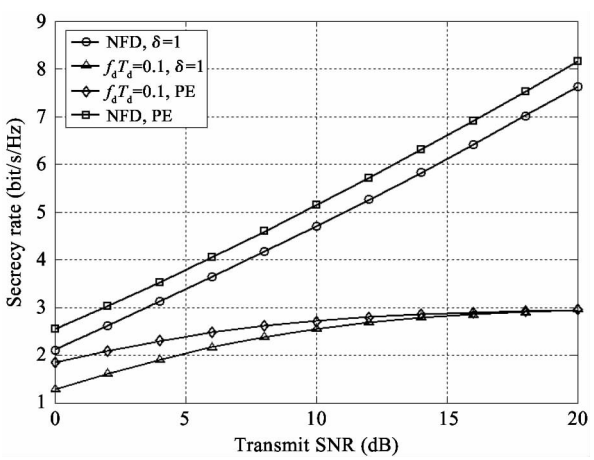

Fig. 2 Secrecy rate versus transmit SNR

Fig. 3 presents the outage probability of different channel error conditions versus transmit SNR. As seen in Fig. 3, feedback delay almost has no impact on the secrecy outage performance and secrecy outage of different channel error conditions would rise to a same threshold as transmit SNR increases. Conversely, connection outage is more sensitive to feedback delay but estimation errors have little influence on it. If there exists feedback delay, connection outage is almost not impacted by estimation errors and it would fall to a lower bound while transmit SNR increases. If system holds estimation errors, connection outage would decrease as the increasing of transmit SNR.

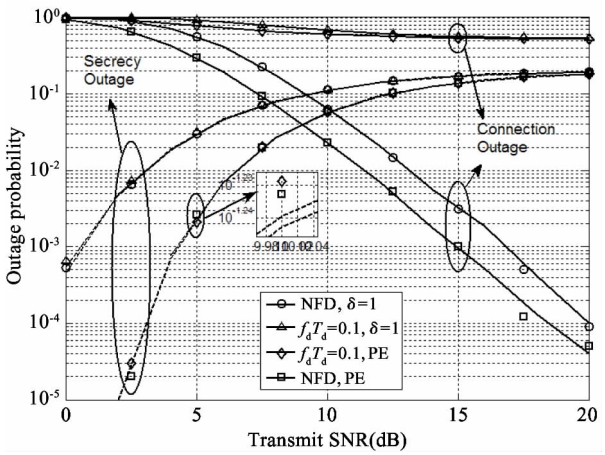

Fig. 3 Outage probability versus transmit SNR

Figs4 – 6 depict the results for the secrecy throughput against transmit SNR, power allocation factor and channel error parameters, respectively. From Fig. 4 and Fig. 5, it can be observed that the secrecy throughput is deeply affected by feedback delay, while the influence of estimation error becomes much less as transmit SNR increases. Under equal power allocation of beamforming and jamming, if it is NFD condition, there exists

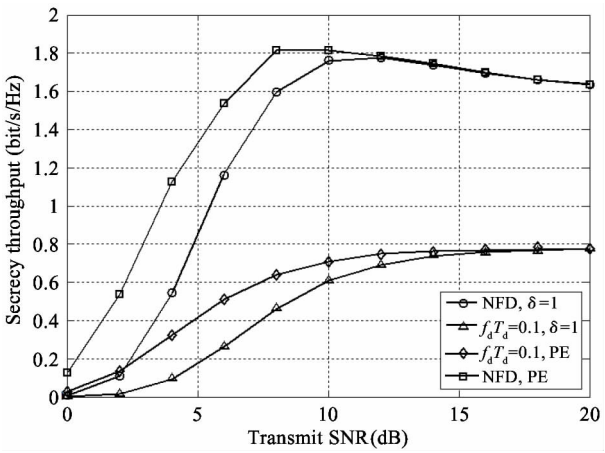

Fig. 4 Secrecy throughput versus transmit SNR

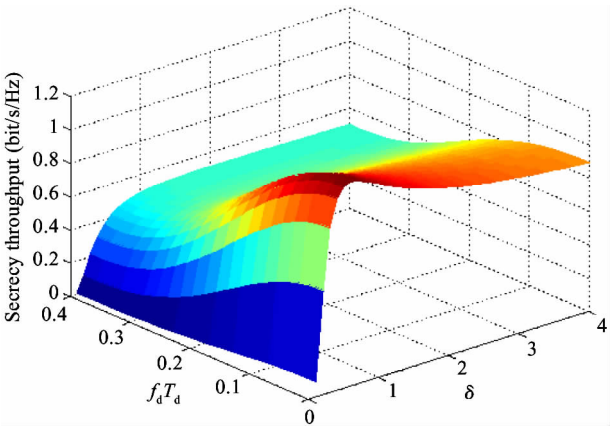

Fig. 5 Throughput versus channel error

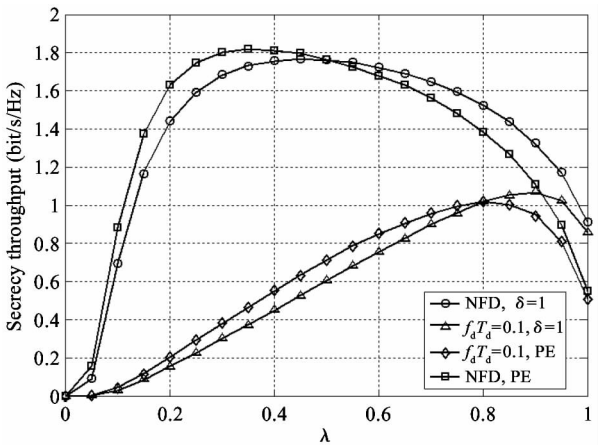

Fig. 6 Secrecy throughput versus power allocation coefficient

optimal transmit SNR to maximize the secrecy throughput. Because with the increasing of transmit SNR, the information leakage would increase at eavesdraopper, thus increasing transmit SNR is not an efficient way for performance improvement. From Fig. 6, while there is no feedback delay, it should apply more power to beamforming signals. On the contrary, it should better apply more power to jamming signals if there is feedback.

4 Conclusion

This paper has investigated the joint impact of estimation errors and feedback delay on the secrecy performance of secondary user in MISOSE cognitive radio networks. Taking the joint channel error model into account, secrecy rate, outage probability, secrecy throughput are deduced and the closed-form expression is obtained. When the transmit power increases, secrecy throughput would reach to some constant. Simulation results show that feedback delay adversely impacts on secrecy rate, connection outage probability and secrecy throughput, while estimation error causes more impact on secrecy outage probability. Furthermore, the secrecy rate could increase progressively with the transmit power only if there exists no feedback delay. In general, this framework is giving guidance to robust algorithm study on different channel uncertainties.

However, one should mention some worthwhile work in the future. Here the analysis for the case of single antenna eavesdropper has limitation. It would be more practical to consider multi-antenna eavesdropper and the interference to SU from PUs. Moreover, robust design and relay channel of SU in cognitive radio networks should be taken into account.

-References

[1] Federal Communication Commission. Spectrum policy task force report [R]. FCC Document ET Docket, 2002

[2] Federal Communication Commission. Notice of proposed rulemaking on cognitive radio [R]. FCC Document ET Docket, 2003

[3] Kolodzy P J. Interfence temperature: a metric for dynamic spectrum utilization [J]. *International Journal of Network Management*, 2006, 16(2): 103-113

[4] Sakran H, Shokair M. Proposed relay selection scheme for physical layer security in cognitive radio networks [J]. *IET Commununications*, 2012, 6(16): 2676-2687

[5] Lee J, Wang H, Andrews J G, et al. Outage probability of cognitive relay networks with interference constraints [J]. *IEEE Transaction on Wireless Communnications*, 2011, 10(2): 390-395

[6] Zou Y, Yao Y D, Zheng B. Cognitive transmissions with mutiple relays in cognitive radio networks [J]. *IEEE Transaction on Wireless Communnications*, 2011, 10(2): 648-659

[7] Goldsmith A, Jafer S A, Maric I, et al. Breaking spectrum gridlock with cognitive radio: An information theoretic perspective [J]. *Proceedings of IEEE*, 2009, 59(5): 894-914

[8] An K, Lin M, Ouyang J, et al. Secure transmission in cognitive satellite terrestrial networks [J]. *IEEE Journal on Selected Areas in Communications*, 2016, 34(11): 3025-3037

[9] Wyner A D. The wire-tap channel [J]. *The Bell System Technical Journal*, 1975, 54(8): 1355-1387

[10] Leung-Yan-Cheong S K, Hellman M E. The Gaussian wiretap channel [J]. *IEEE Transactions on Information Theory*, 1978, 24(4): 451-456

[11] Wang B, Mu P, Li Z. Secrecy rate maximization with artificial-noise-aided beaforming for MISO wiretap channels under secrecy outage constraint [J]. *IEEE Communnications Letters*, 2015, 19(1): 18-21

[12] Wang C ,Wang H M. On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels [J]. *IEEE Transactions on Information Forensics and Security*, 2014, 9(11): 1814-1827

[13] Winters J H. On the capacity of radio communication systems with diversity in Rayleigh fading environment [J]. *IEEE Journal on Selected Areas in Communications*,

1987, 5(5): 871-878
[14] Lin M, Ouyang J, Zhu W P. Joint beamforming and power control for device-to-device communications underlaying cellular networks [J]. *IEEE Journal on Selected Areas in Communications*, 2016, 34(1): 138-150
[15] Li M, Lin M, Zhu W P. Performance analysis of MIMO MRC systems with feedback delay and channel estimation error [J]. *IEEE Transactions on Vehicular Technology*, 2016, 65(2): 707-717
[16] Huang J, Swindlehurst A L. Robust secure transmission in MISO channels based on worst-case optimization [J]. *IEEE Transaction on Signal Processing*, 2012, 60(4): 1696-1707
[17] Ferdinand N S, Costa D B, Latva M. Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection [J]. *IEEE Communnications Letters*, 2013, 17(5): 864-867
[18] Han S, Ahn S, Oh E, et al. Effect of channel-estimation errors on BER performance in cooperative transmission [J]. *IEEE Transactions on Vehicular Technology*, 2009, 58(10): 2083-2088
[19] Ma Y, Schober R, Pasupathy S. Effect of channel estimation errors on M-QAM with MRC and EGC in Nakagami fading channels [J]. *IEEE Transactions on Vehicular Technology*, 2007, 56(10): 1239-1250
[20] Tan C C, Beaulieu N C. On first-order Markov modeling for the Rayleigh fading channel [J]. *IEEE Transaction on Communnications*, 2000, 48(12): 2032-2040
[21] Tang X, Liu R, Spasojevic P, et al. On the throughput of secure hybrid-ARQ Protocols for Gaussian block-fading channels [J]. *IEEE Transactions on Information Theory*, 2009, 55(4): 1575-1591
[22] Zhou X, McKay M R. Rething the secrecy outage formulation: A secure transmission design perspective [J]. *IEEE Communnications Letters*, 2011, 15(3): 302-304

Lin Zhi, born in 1992. He is currently pursuing the Ph. D degree at the Amy Engineering University, Nanjing. He received the B. S. degree and the M. S. degree in communications engineering from the PLA University of Science and Technology, Nanjing, China, in 2013 and 2016. His research interests include satellite communication, cognitive radio, physical layer security, and convex optimization.