doi:10.3772/j.issn.1006-6748.2014.04.008

Secrecy rate analysis of dual-hop AF relay wiretap channel①

Ding Fei (丁 飞)[*,***], Song Aiguo②[**], Li Jianqing[**], Wu Zhenyang[*]
([*] School of Information Science and Engineering, Southeast University, Nanjing 210096, P. R. China)
([**] School of Instrument Science and Engineering, Southeast University, Nanjing 210096, P. R. China)
([***] Research and Development Center, China Mobile Group Jiangsu Co., Ltd, Nanjing 210029, P. R. China)

Abstract

An amplify-and-forward (AF) dual-hop relay is proposed for secure communication within Wyner's wiretap channel. Based on an information-theoretic formulation, the average secrecy rate is characterized when two legitimate partners communicate over a quasi-static fading channel. Theoretical analysis and simulation results show that both cooperative strategies of average power scaling (APS) and instantaneous power scaling (IPS) are proved to be able to achieve information-theoretic security, and eavesdropper is unable to decode any information.

Key words: secrecy rate, information-theoretic security, amplify-and-forward (AF), dual-hop, relay, wiretap channel

0 Introduction

Due to the broadcast nature of transmission medium, wireless communications are susceptible to eavesdropping. Traditional security mechanisms mainly rely on cryptographic protocols assuming that there is an error-free channel available to users before secret key generation. In contrast to this paradigm, the idea of physical layer security is that exploiting the randomness of wireless channels can significantly strengthen the security of wireless communications. Information theoretic literature has supported the potential benefits of deriving secure information from physical layer.

The basic principle of information-theoretic security is widely accepted as the strictest notion of security that guarantees sent messages can not be decoded by a malicious eavesdropper[1-9]. Wyner introduced a wiretap channel model to evaluate secure transmission at the physical layer[1]. In the wiretap channel model, two legitimate users communicate over a main channel, meanwhile, an eavesdropping channel is a degraded one of the user's channel. Csiszar and Leung-Yan-Cheong generalized it to broadcast channel and basic Gaussian channel, respectively[2]. Barros generalized the Gaussian wiretap channel model[2] to wireless quasi-static fading channel[3]. Recently, some works have been proposed to enhance the security by taking advantage of multiple antenna systems[4,5]. However, due to cost and size limitations, multiple antennas may not be available at nodes. Motivated by emerging wireless applications, there is growing interest in exploiting the benefits of relay or cooperative strategies to make sure secure transmission[6-9]. Lai shows that secure communications can take place via an untrusty relay node which jams an eavesdropper[6]. Recently, physical layer secure protocols based on decode-and-forward (DF) and amplify-and-forward (AF) strategies are proposed in Refs[7-9] and trusty relay nodes are employed.

The AF dual-hop relay are investigated for secure communication within Wyner's wiretap channel. In contrast to fixed channel conditions[7-9], we consider the impact of fading on the secrecy capacity of AF relay with average power scaling (APS) and instantaneous power scaling (IPS) constraints[10-14]. Based on an information-theoretic formulation of secure communication over wireless channels[3], we characterize the secrecy of AF relay in terms of average secure communication rates. Theoretical analysis shows that both AF-APS and AF-IPS can achieve secure communication.

1 System model

Fig. 1 shows the half-duplex relay system considered in this paper, the Source (S) transmits confidential information to the Destination (D) using the trusty

① Supported by the National Natural Science Foundation of China (No. 61325018, 61272379), the National High Technology Research and Development Program of China (No. 2006AA04Z246) and the Ministry of Education Science and Technology Innovation Engineering Major Cultivation Project of China (No. 107053).

② To whom correspondence should be addressed. E-mail: a.g.song@seu.edu.cn

Received on Sep. 26, 2013

relay (R). A third party (Eve) is able to eavesdrop on relay's transmissions. All terminals use single antenna to transmit and receive signals.

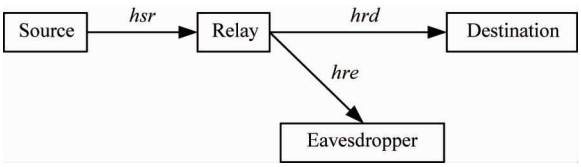

Fig. 1 Dual-hop relay wiretap channel model

In the first transmission interval, S communicates with R. The received signal at the relay is

$$Y_r = \sqrt{E_{sr}} h_{sr} X + N_r \tag{1}$$

During the next signalling interval, R transmits a scaled replica of Y_r towards the destination. D observes the output of a discrete-time Rayleigh-fading channel (the main channel). The output can be written as

$$Y_d = \sqrt{E_{rd}} h_{rd} G Y_r + N_d \tag{2}$$

Eve observes the output of an independent discrete-time Rayleigh-fading channel (the eavesdropper's channel). The output is given by

$$Y_e = \sqrt{E_{re}} h_{re} G Y_r + N_e \tag{3}$$

In Eqs (1)-(3), h_{sr}, h_{rd} and h_{re} are circularly symmetric complex Gaussian random variables (RV) with unit-variance; N_r, N_d and N_e denote zero-mean circularly symmetric complex Gaussian noise RVs with unit-variance. From the point of view of user location, the received power is $E_{ij} = P/d_{ij}^{\phi}$, where P corresponds to the transmit power, d_{ij} is the distance between node i and node j, and ϕ is the pathloss exponent ($i \in \{s,r\}$, $j \in \{r,d,e\}$). The power scaling factor is $G^2 = 1/(E_{sr} + 1)$ for APS and $G^2 = 1/(E_{sr} |h_{sr}|^2 + 1)$ for IPS. It is assumed that the channel fading coefficient h and noise N are both independent. It is assumed that all nodes have perfect channel side information (CSI).

For APS, the instantaneous signal-to-noise ratio (SNR)[2] is

$$\gamma_d = \frac{E_{sr}E_{rd}|h_{sr}|^2|h_{rd}|^2}{1 + E_{sr} + E_{rd}|h_{rd}|^2} = \frac{E_{sr}\mu\alpha}{1 + E_{sr} + \alpha},$$
$$\gamma_e = \frac{E_{sr}E_{re}|h_{sr}|^2|h_{re}|^2}{1 + E_{sr} + E_{re}|h_{re}|^2} = \frac{E_{sr}\mu\beta}{1 + E_{sr} + \beta} \tag{4}$$

For IPS, the instantaneous SNR is

$$\gamma_d = \frac{E_{sr}E_{rd}|h_{sr}|^2|h_{rd}|^2}{1 + E_{sr}|h_{sr}|^2 + E_{rd}|h_{rd}|^2} = \frac{E_{sr}\mu + \alpha}{1 + E_{sr}\mu + \alpha},$$
$$\gamma_e = \frac{E_{sr}E_{re}|h_{sr}|^2|h_{re}|^2}{1 + E_{sr}|h_{sr}|^2 + E_{re}|h_{re}|^2} = \frac{E_{sr}\mu\beta}{1 + E_{sr}\mu + \beta} \tag{5}$$

where γ_d is the instantaneous SNR of main channel, γ_e denotes instantaneous SNR of eavesdropper's channel, and $\mu = |h_{sr}|^2$, $\alpha = E_{rd}|h_{rd}|^2$ and $\beta = E_{re}|h_{re}|^2$. Hence, it is considered that the probability density function (PDF) is μ, α and β. Assuming the channel fading coefficients h_{rd} and h_{re} are zero-mean complex Gaussian RVs, α and β are exponentially distributed, specifically

$$f(\alpha) = \frac{1}{E_{rd}}\exp\left(-\frac{\alpha}{E_{rd}}\right), f(\beta) = \frac{1}{E_{re}}\exp\left(-\frac{\beta}{E_{re}}\right) \tag{6}$$

2 Secrecy rate of dual-hop relay wire-tap channel

This section characterizes the secrecy rate of a dual-hop relay wiretap channel in terms of average secure communication rates. First, the secrecy rate for the fixed realization of h_{sr} is computed. Then, the secrecy rate in the fading case is evaluated, assuming sufficiently high SNR for the S-R link, i.e. $E_{sr} > E_{rd}, E_{re}$.

- Preliminaries

Recalling the results of Ref. [3] for the Rayleigh fading wiretap channel, the secrecy rate for one realization can be evaluated as

$$C_s(\gamma_d,\gamma_e) = \begin{cases} \ln(1+\gamma_d) - \ln(1+\gamma_e), & \text{if } \gamma_d > \gamma_e \\ 0, & \text{if } \gamma_d \leqslant \gamma_e \end{cases} \tag{7}$$

where $\ln(1+\gamma_d)$ is the capacity of main channel, while $\ln(1+\gamma_e)$ denotes the capacity of eavesdropper's channel. For Gaussian dual-hop wiretap channel, the secrecy rate is given by

$$C_s(E_{rd},E_{re}) = \begin{cases} \ln\left(1 + \frac{E_{rd}E_{sr}}{1 + E_{rd} + E_{sr}}\right) - \ln\left(1 + \frac{E_{re}E_{sr}}{1 + E_{re} + E_{sr}}\right), & \text{if } E_{rd} > E_{re} \\ 0, & \text{if } E_{rd} < E_{re} \end{cases}$$

where $\gamma_d = \frac{E_{rd}E_{sr}}{1 + E_{rd} + E_{sr}}$, $\gamma_e \frac{E_{re}E_{sr}}{1 + E_{re} + E_{sr}}$.

From Eq. (7), it follows that secrecy rate is positive when $\gamma_d > \gamma_e$. In other words, a non-zero secrecy rate exists only when $\alpha > \beta$. Invoking independent between h_{rd} and h_{re}, the probability of existence of a non-zero secrecy rate can be evaluated as

$$P_0 = P_r(C_s(\gamma_d,\gamma_e) > 0) = P_r(\gamma_d > \gamma_e)$$
$$= P_r(\alpha > \beta)$$
$$= \int_0^{\infty}\int_0^{\alpha} f(\alpha)f(\beta)\,\mathrm{d}\alpha\mathrm{d}\beta = \frac{E_{rd}}{E_{rd} + E_{re}} \tag{8}$$

The probability of existence of a non-zero secrecy rate is not dependent on the SNR of S-R link E_{sr}, but E_{sr} will affect the values of average secrecy rate.

In order to compute average secrecy rate, a Lem-

ma is proposed in Ref. [15]

Lemma:

$$\int_0^\infty ve^{-vx}\log(1+ux)\,\mathrm{d}x = \exp(v/u)E_1(v/u) = F_e(v/u) \quad (9)$$

$$\int_0^\infty x^{m-1}\exp\left(-mx-\frac{\nu}{x}\right)\mathrm{d}x = 2(\nu/m)^{\frac{m}{2}}K_m(2\sqrt{m\nu}) \quad (10)$$

where $E_1(x) = \int_1^\infty \frac{e^{-xt}}{t}\mathrm{d}t$ is the exponential-integral function and $K_m(x)$ is the m-order modified Bessel function of the second kind. When $x \to 0$, $K_m(x) \to \frac{(m-1)!}{2}\left(\frac{x}{2}\right)^{-m}$.

- Average secrecy rate

The average secrecy rate for the fixed realization of h_{sr} can be evaluated. α and β are independent and exponentially distributed with PDF given by Eq. (6). When h_{sr} is fixed, the secrecy capacity of APS is

$$\begin{aligned}\bar{C}_{APS}(\mu) &= \int_0^\infty\int_0^\infty C_s(\gamma_d,\gamma_e)f(\alpha)f(\beta)\,\mathrm{d}\alpha\mathrm{d}\beta \\ &= \int_0^\infty\int_0^\alpha \log\left(1+\frac{E_{sr}\alpha\mu}{1+E_{sr}+\alpha}\right)f(\alpha)f(\beta)\,\mathrm{d}\alpha\mathrm{d}\beta \\ &\quad - \int_0^\infty\int_\beta^\infty \log\left(1+\frac{E_{sr}\beta\mu}{1+E_{sr}+\beta}\right)f(\alpha)f(\beta)\,\mathrm{d}\alpha\mathrm{d}\beta \\ &= \left[F_e\left(\frac{1}{\varphi_1 E_{rd}}\right)-F_e\left(\frac{1}{\varphi_1 E_{re}P_0}\right)\right] \\ &\quad - \left[F_e\left(\frac{\varphi}{E_{rd}}\right)-F_e\left(\frac{\varphi}{E_{re}P_0}\right)\right] \end{aligned} \quad (11)$$

where $\varphi_1 = (1+E_{sr}\mu)/(1+E_{sr})$, $\varphi = 1+E_{sr}$. Similarly, the secrecy rate of IPS is

$$\begin{aligned}\bar{C}_{IPS}(\mu) &= \left[F_e\left(\frac{1}{E_{rd}}\right)-F_e\left(\frac{1}{E_{re}P_0}\right)\right] \\ &\quad - \left[F_e\left(\frac{1+E_{sr}\mu}{E_{rd}}\right)-F_e\left(\frac{1+E_{sr}\mu}{E_{re}P_0}\right)\right] \end{aligned} \quad (12)$$

The average secrecy rate for APS can be shown as

$$\bar{C}_{APS} = \int_0^\infty \bar{C}_{APS}(\mu)f(\mu)\,\mathrm{d}\mu \quad (13)$$

The average secrecy rate for IPS is evaluated by

$$\begin{aligned}\bar{C}_{IPS} &= \int_0^\infty \bar{C}_{IPS}(\mu)f(\mu)\,\mathrm{d}\mu \\ &= \frac{E_{sr}}{E_{sr}-E_{rd}}F_e\left(\frac{1}{E_{rd}}\right)-\frac{E_{sr}}{E_{sr}-E_{re}P_0}F_e\left(\frac{1}{E_{re}P_0}\right) \\ &\quad + \frac{E_{sr}(E_{re}P_0-E_{rd})}{(E_{sr}-E_{rd})(E_{sr}-E_{re}P_0)}F_e\left(\frac{1}{E_{sr}}\right) \end{aligned} \quad (14)$$

The asymptotic behaviour of the average secrecy rate for the fixed realization of h_{sr} is evaluated as follows, and the asymptotic results followed by bounding the exponential-integral function as $E_1(x) \leqslant e^{-x}/x$[15]. Assuming $E_{sr} \to \infty$

$$F_e\left(\frac{1}{\varphi_1 E_{rd}}\right)\to F_e\left(\frac{1}{\mu E_{rd}}\right),\ F_e\left(\frac{\varphi_1}{E_{re}P_0}\right)\to F_e\left(\frac{1}{E_{re}P_0\mu}\right)$$

$$F_e\left(\frac{\varphi}{E_{rd}}\right)\leqslant \frac{E_{rd}}{1+E_{sr}}\to 0,\ F_e\left(\frac{\varphi}{E_{re}P_0}\right)\to 0$$

$$F_e\left(\frac{1+E_{sr}\mu}{E_{rd}}\right)\to 0,\ F_e\left(\frac{1+E_{sr}\mu}{E_{re}P_0}\right)\to 0$$

Then, the asymptotic average secrecy rate is evaluated by

$$\bar{C}_{IPS} \approx F_e\left(\frac{1}{E_{rd}}\right)-F_e\left(\frac{1}{E_{re}P_0}\right) \quad (15)$$

$$\begin{aligned}\bar{C}_{APS} &\approx \int_0^\infty\left[F_e\left(\frac{1}{E_{rd}\mu}\right)-F_e\left(\frac{1}{E_{re}P_0\mu}\right)\right]f(\mu)\,\mathrm{d}\mu \\ &= 4(\sqrt{a})S_{-2,1}(\sqrt{a})-4(\sqrt{b})S_{-2,1}(\sqrt{b}) \end{aligned} \quad (16)$$

where $a = 4/E_{rd}$, $b = 4/E_{re}/P_0$ and $S_{\mu,\nu}(\cdot)$ is the Lommel function[15].

For IPS, we can prove that the secrecy capacity is improved when the value E_{sr} increases (see the proof in Appendix). So, Eq. (15) is the maximum value of the average secrecy capacity $\bar{C}_{IPS}$. For APS, computer simulation results also show that the higher E_{sr}, the larger average secrecy capacity $\bar{C}_{APS}$.

3 Simulation results

In this section, the average secure communication rates and outage probability of dual-hop AF relay under APS and IPS constraint is evaluated. It shows that the secrecy capacity exits under a fading scenario when the average SNR of main channel is equal to the average SNR of eavesdropper's channel, and we set $E_{rd} = E_{re}$. In this situation of Gaussian wiretap channel, the secrecy rate will be zero.

Fig. 2 shows the average secrecy capacity versus E_{rd} for different values of E_{sr}. In contrast with the Gaussian wiretap channel, it is observed that the average secrecy rate is positive and improved when the values of E_{sr} increase. When E_{sr} is less than E_{rd}, for example, $E_{sr} = E_{rd} - 10\text{dB}$, the secrecy rates of AF-APS and AF-IPS are lower. So, the higher E_{sr} is, the larger average secrecy capacity will be. In the moderate E_{sr} regions, the secrecy rates of AF-APS outperform the secrecy rates of AF-IPS. But if E_{sr} is sufficiently high, i.e., $E_{sr} = E_{rd} + 20\text{dB}$, the secrecy rates of AF-IPS are superior to the secrecy rates of AF-APS.

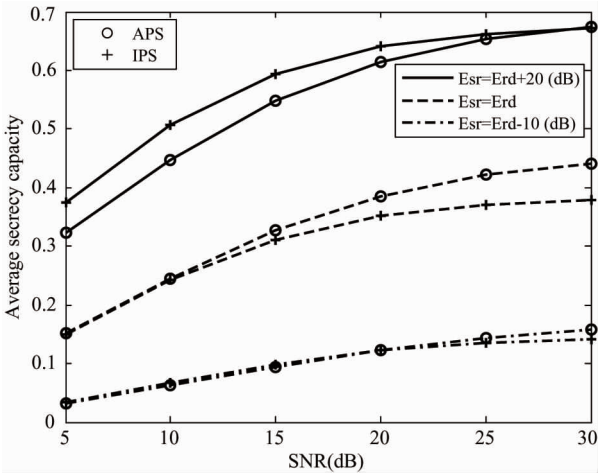

Fig. 2 The average secrecy rate versus E_{rd} for selected values of E_{sr}

Fig. 3 depicts the approximate average secrecy capacity versus E_{rd} assuming SNR is sufficiently high for the S-R link. This assumption has been used to compute the BER performance of dual-hop AF relay in Ref. [12]. To compare with the approximate results, we also show the exact results in Fig. 3. The approximate results of IPS match well only when the SNR E_{sr} is very high (i. e., $E_{sr} = E_{rd} + 30$dB). However, the approximate results of APS match well when the SNR E_{sr} is relative low (i. e., $E_{sr} = E_{rd} + 10$dB). Thereby, the approximate results of APS are more robust.

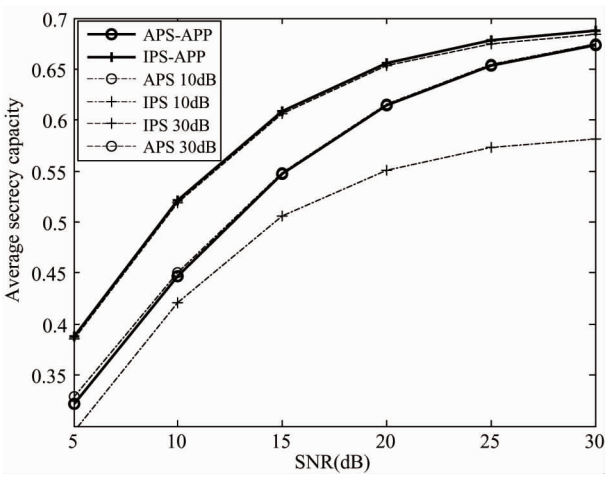

Fig. 3 The approximate average secrecy rate for higher values of E_{sr}

In one word, comparison with APS, the performance of IPS is better when SNR is sufficiently high for the S-R link and worse in the moderate SNR regime for the S-R link.

4 Conclusions

This paper investigates the AF dual-hop relay for secure communication within the Wyner's wiretap channel and characterizes the average secrecy capacity and outage probability when two legitimates partners communicate over a quasi-static fading channel. Both APS and IPS cooperative strategies are proved theoretically to be able to achieve information-theoretic security. Simulation results show that the performance of IPS is better than that of APS assuming that SNR is sufficiently high for the S-R link. However, the performance of APS outperforms IPS in the moderate SNR regime for the S-R link.

Appendix A

$F(x)$ is rewritten as

$$F(x) = \int_0^\infty \frac{\exp(-tx)}{t+1}\mathrm{d}t \qquad (a.1)$$

So, we show

$$\begin{aligned}\bar{F}(\lambda) &= \int_0^\infty F\left(\frac{1}{\lambda x}\right) f(x)\,\mathrm{d}x \\ &= \int_0^\infty \int_0^\infty \exp\left(-x - \frac{t}{\lambda x}\right)\frac{1}{t+1}\mathrm{d}x\mathrm{d}t \end{aligned} \qquad (a.2)$$

Using the integrals given in Eq. (10), Eq. (a.2) is given by

$$\bar{F}(\lambda) = \int_0^\infty \frac{2}{t+1}\left(\frac{t}{\lambda}\right)^{1/2} K_1\left(2\sqrt{\frac{t}{\lambda}}\right)\mathrm{d}t \qquad (a.3)$$

which can be evaluated by using Ref. [15],

$$\int_0^\infty x^{1+\nu}(x^2+a^2)^\mu K_\nu(bx)\,\mathrm{d}x = 2^\nu \Gamma(1+\nu) a^{\nu+\mu+1} b^{-1-\mu} S_{\mu-\nu,\mu+\nu+1}(ab) \qquad (a.4)$$

Then, Eq. (a.3) can be re-expressed as

$$\bar{F}(\lambda) = \frac{4}{2\Gamma(1)}\int_0^\infty \frac{x^2 K_1(x)}{x^2+a^2}\mathrm{d}x = 4aS_{-2,1}(a) \qquad (a.5)$$

where $a = 2\sqrt{1/\lambda}$.

Appendix B

For the fixed realization of μ, the secrecy rate of IPS is rewritten as

$$\begin{aligned}\bar{C}_{IPS}(E_{sr}) &= \left[F\left(\frac{1}{E_{rd}}\right) - F\left(\frac{1}{E_{re}P_0}\right)\right] \\ &\quad - \left[F\left(\frac{1+E_{sr}\mu}{E_{rd}}\right) - F\left(\frac{1+E_{sr}\mu}{E_{re}P_0}\right)\right] \\ &= C - C(E_{sr}) \end{aligned} \qquad (b.1)$$

where $F(x) = \int_0^\infty \frac{e^{-xt}}{t+1}\mathrm{d}t$. It can be shown as

$$F'(x) = -\int_0^\infty \frac{te^{-xt}}{t+1}\mathrm{d}t < 0$$

$$F''(x) = \int_0^\infty \frac{t^2e^{-xt}}{t+1}\mathrm{d}t > 0. \quad (b.2)$$

So, $F'(x)$ is the increasing function about SNR x. We have

$$C'(E_{sr}) = \mu\left[\frac{1}{E_{rd}}F'\left(\frac{1+E_{sr}\mu}{E_{rd}}\right) - \frac{1}{\lambda}F'\left(\frac{1+E_{sr}\mu}{\lambda}\right)\right]$$

where $\lambda = E_{re}P_0 = \frac{E_{rd}E_{re}}{E_{re}+E_{rd}}(\lambda < E_{rd})$. Since $F'(x)$ is a increasing function about SNR x, it is obviously

$$\frac{1}{E_{rd}}F'\left(\frac{1+E_{sr}\mu}{E_{rd}}\right) < \frac{1}{\lambda}F'\left(\frac{1+E_{sr}\mu}{\lambda}\right)$$

Then, $C'(E_{sr}) < 0$. Therefore, $C(E_{sr})$ is the decreasing function about SNR E_{sr}. Conversely, $\bar{C}_{IPS}(E_{sr})$ is the increasing function about SNR E_{sr} and the maximum secrecy capacity is Eq. (15).

References

[1] Wyner D. The wire-tap channel. Bell Syst. Tech. J., 1975, 54(8): 1355-1376

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

[3] Bloch M, Barros J, Miguel R D. Wireless Information-Theoretic Security. *IEEE Transactions Information Theory*, 2008, 54(6): 2515-2534

[4] He F, Man H, Wang W. Maximal ratio diversity combining enhanced security. *IEEE Commun. Lett*, 2011, 15(5): 509-511

[5] Sun X, Liu X, Jiang M, et al. Probabilistic Constrained Power Allocation for MISO Wiretap Channel Based on Statistical CSI-E. *IEICE Transactions on Communications* 2011, 94(11): 3175-3178

[6] Lai L, Gamal H. The relay-eavesdropper channel: cooperation for secrecy. *IEEE Transactions Information Theory*, 2008, 54(9): 4005-4019

[7] Dong Z, Han A, Petropulu H V P. Secure wireless communications via cooperation. *Signal Process*, 2010, 58(3): 1875-1888

[8] Dong Z, Han A, Petropulu H V P. Amplify-and-forward based cooperation for secure wireless communications. In: Proceedings of the IEEE International Conference on Acoustics, Speech & Signal Processing, Taipei, China, 2009. 2613-2616

[9] Zhang P Y, Yuan J, Chen J S, et al. Analyzing amplify-and-forward and decode-and-forward cooperative strategies in Wyner's channel model. In: Proceedings of the 2009 IEEE International Conference on Wireless Communications and Networking, Budapest, Hungary, 2009. 1-5

[10] Xu W, Dong X, Lu W. MIMO relaying broadcast channels with linear precoding and quantized channel state information feedback. *Signal. Process*, 2010, 58(10): 5233-5245

[11] Xu W, Dong X, Lu W. Joint precoding optimization for multiuser multiantenna relaying downlinks using quadratic programming. *IEEE Transactions on Communications*, 2011, 59(5): 1228-1235

[12] Himal A, Suraweera J A. Performance of OFDM-Based Dual-Hop Amplify-and-Forward Relaying. *IEEE Commun. Lett*, 2006, 11(9): 726-728

[13] Suraweera H A, Louie R H Y, Li Y H, et al. Two hop amplify-and-forward transmission in mixed rayleigh and rician fading channels. *IEEE Communications Letter*, 2009, 13(10): 227-229

[14] Suraweera H, Karagiannidis G, Smith P. Performance analysis of the dual-hop asymmetric fading channel. *IEEE Trans. Wireless. Commun*, 2009, 8(6): 2783-2788

[15] Gradshteyn S, Ryzhik I M. Table of Integrals, Series, and Products, 6th ed. Singapore: Elsevier, 2004

Ding Fei, born in 1981. He received his Ph. D. degrees in Instrument Science and Technology, Southeast University, Nanjing, China, in 2010. His research interests include wireless sensor networks, mobile communication system and applications of embedded systems.