Secrecy Analysis of Amplify-and-Forward Relay Networks with Beamforming

Pu Chen[1], Jian Ouyang[1] and Wei-Ping Zhu[2,1]
[1] College of Telecommunications and Information Engineering
Nanjing University of Posts and Telecommunications, Nanjing, China
[e-mail: chenpu8828@163.com, ouyangjian@njupt.edu.cn]
[2] Department of Electrical and Computer Engineering
Concordia University, Montreal, QC, Canada
[e-mail: weiping@ece.concordia.ca]
*Corresponding author: Jian Ouyang

Received March 17, 2016; revised July 3, 2016; accepted August 4, 2016; published October 31, 2016

Abstract

This paper analyzes the secrecy performance of an amplify-and-forward (AF) relay network, where a multi-antenna eavesdropper attempts to overhear the transmitted message from a multi-antenna source to a multi-antenna destination with a single antenna relay. Firstly, we derive the approximate analytical expressions for the secrecy outage probability (SOP) and average secrecy rate (ASR) of the relay network. Then, asymptotic expressions of SOP and ASR at high main-to-eavesdropper ratio (MER) are also provided to reveal the diversity gain of the secure communication. Finally, numerical results are given to verify the theoretical analysis and show the effect of the number of antennas in the considered relay network.

Keywords: Physical layer security, relay network, secrecy outage probability, average secrecy rate, beamforming

This work was supposed by National Natural Science Foundation of China under grant 61372122, the China Postdoctoral Science Foundation under grant 2015M571784, the Natural Science Foundation of Jiangsu Province under grant BK20160911, the Natural Science Foundation of Jiangsu Higher Education Institutions of China under grant 16KJB510027, and the NUPTSF under grants NY215135 and NY214140.

http://dx.doi.org/10.3837/tiis.2016.10.022 **ISSN : 1976-7277**

1. Introduction

Relay communication has been considered as a promising means to enhance the throughput and the power efficiency of wireless networks[1]. It also improves performance gain and reduces transmission loss as compared with direct transmission. In addition, relay systems show advantages in overcoming the shadowed fading. In relay communication systems, relay nodes are capable of employing various relaying protocols to assist information transmission from a source to its destination. Among the existing relaying protocols, amplify-and-forward (AF) and decode-and-forward (DF) are two most popular ones [2], [3]. The authors in [4] derived a closed-form bit error rate (BER) expression for their proposed scheme over Rayleigh fading channels, showing that the full diversity can be achieved by the new scheme. Also, the BER performance of the known coded cooperation is provided in [4] for the purpose of comparison. In [5], the authors studied the opportunistic cooperation with an AF relay transmission and proposed an opportunistic AF scheme where the relay transmission mode is adopted only when the source to relay channel is in a relatively good condition. It was shown that the reliability of wireless transmission can be significantly improved by using cooperative relay techniques.

On the other hand, some multi-antenna techniques, such as maximal ratio combining (MRC), transmit antennas selection (TAS), transmit beamforming, have also been proposed in literature to enhance the overall system performance [6], [7]. In [6], the authors investigated the impact of multi-antenna relay on the end-to-end error performance with the threshold-based MRC and the threshold-based selection combining (SC) at the relay. In [7], the authors considered the optimal signal-to-noise ratio (SNR)-based TAS at the source and the relay with AF protocol. Additionally, the maximal-ratio transmission (MRT) at the relay as well as the partial relay selection were also considered for performance analysis.

Recently, secure communication over the wireless medium at the physical layer (PHY) has achieved considerable attention. Compared with the traditional encryption method in secure communication, physical layer security communication with multi-antenna techniques have the advantages of stronger anti-eavesdrop ability. The security performance for cooperative systems in the presence of multiple eavesdroppers was investigated in [8], [9]. Specifically, the authors in [8] introduced the relay-eavesdropper channel and offered an outer-bound on the rate-equivocation region over several cooperation strategies. Moreover, the optimal relay weights to maximize the achievable secrecy rate for the multiple relays with several relay protocols were studied in [9]. In [10], the authors analyzed the performance of the external eavesdropper, and proposed two anti-eavesdropping schemes for IA-based networks. When the channel state information (CSI) of the eavesdropper is available, zero-forcing scheme can be utilized. Furthermore, a more generalized artificial noise (AN) scheme is proposed for IA-based networks without the knowledge of eavesdropper's CSI. In [11], the authors investigated the secure relay beamforming problems for the AFrelay network, where the transmitter sends information to the receiver with the help of a multiple-antenna relay in the presence of an eavesdropper. The authors in [12] proposed an anti-jamming scheme by aligning the jamming signal together with interference among users cooperation when an adversarial jammer exists. Then an AN scheme is proposed, in which the external eavesdropping is disrupted by AN without introducing any additional interference to the legitimate network. To further analyze the potential threat, a collusive eavesdropping scheme by some hostile IA users in the network is also proposed. The secrecy outage probability (SOP) of a dual hop AF relay system was evaluated in [13], showing that the SOP decreases with an increase in the number of relays and increases with an increase in the required secrecy rate. In [14], the authors discussed the secrecy rate of a two-hop multi-antenna relay network in the presence of an eveasdropper. However, to the best of our knowledge, the impact of multi-antenna transmission and reception with a single antenna relay while a multi-antenna eavesdropper exists has not been studied sufficiently.

In this paper, we consider an AF relay network in the presence of an eavesdropper. First of all, we derive approximate expressions of secrecy outage probability and average secrecy rate of the considered network in the Rayleigh fading environment. Then, the asymptotic analysis at high main-to-eavesdropper ratio (MER) is presented to reveal the diversity order and array gain of the relay network. Next, we verify our analytical results by comparing with Monto Carlo simulation results. It is shown that the secrecy outage probability reduces with the increase of antennas in destination, at the same time the average secrecy rate increases with the number of destination antennas.

Notation: Bold letters denote the vectors, $|\cdot|$ represents the absolute value, $E[\cdot]$ the expectation, $CN(\mu,\sigma^2)$ the complex Gaussian distribution with mean μ and variance σ^2, $(\cdot)^H$ denotes the conjugate transpose operator, $[a]^+$ denotes $\max(a,0)$, $K_v(\cdot)$ stands for the $v-th$ modified Bessel function of the second kind, ${}_2F_1(a,b;c;d)$ the hypergeometric function, and $E_i(x)=\int_{-\infty}^{x} e^t/t dt$.

2. System Model

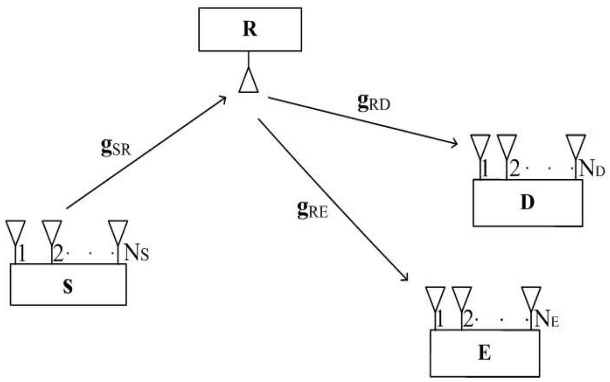

Fig. 1. Diagram of the System model

As illustrated in **Fig. 1**, we consider a relay network consisting of a source (S), a destination (D), a relay (R), and an eavesdropper (E) who attempts to overheat the confidential message between S and D. The S, D and E are equipped with N_S, N_D and N_E antennas, respectively, whereas R has a single antenna. We assume that E is close to D, and the direct link between S and D and that between S and E are unavailable due to heavy shadowing. All the communication links are assumed to undergo Rayleigh fading. In the considered relay network, the AF protocol is adopted at R, and the overall communication occurs during two time slots. In the first time slot, S performs transmit beamforming with the weight vector $\boldsymbol{\omega}_S$ and then sends its confidential signal x with $E\left[|x|^2\right]=1$ to R. As such, the received signal at R is given by

$$y=\sqrt{P_S}\mathbf{g}_{SR}^H\boldsymbol{\omega}_S x+n_R \tag{1}$$

where P_S is the transmit power at S, $\mathbf{g}_{SR}$ is the $N_S\times 1$ channel vector of the S-R link, $n_R\in CN(0,\sigma_R^2)$ is the additive white Gaussian noise (AWGN) with zero mean and variance σ_R^2. By adopting the MRT, the transmit beamformer $\boldsymbol{\omega}_S$ is chosen as $\boldsymbol{\omega}_S=\mathbf{g}_{SR}/\|\mathbf{g}_{SR}\|_F$. In the second time slot, R amplifies the received signal y with a variable gain G as $G=1/\sqrt{P_S}\left|\mathbf{g}_{SR}^H\boldsymbol{\omega}_S\right|$ [16] and then broadcasts the signal to D. The signal received at D can be expressed as

$$z_D=\boldsymbol{\omega}_D^H(\sqrt{P_R}Gy\mathbf{g}_{RD}+\mathbf{n}_D)=\sqrt{P_SP_R}G\boldsymbol{\omega}_D^H\mathbf{g}_{RD}\mathbf{g}_{SR}^H\boldsymbol{\omega}_S x+\sqrt{P_R}G\boldsymbol{\omega}_D^H\mathbf{g}_{RD}n_R+\boldsymbol{\omega}_D^H\mathbf{n}_D \tag{2}$$

where P_R denotes the transmit power at R, $\mathbf{g}_{RD}$ the channel vector of the R-D link, $\mathbf{n}_D\in CN(0,\sigma_D^2\mathbf{I}_{N_D})$ the AWGN at D. To maximize the received SNR, MRC is used at D, and the receive beamformer $\boldsymbol{\omega}_D$ is defined as $\boldsymbol{\omega}_D=\mathbf{g}_{RD}/\|\mathbf{g}_{RD}\|_F$. Meanwhile, due to the broadcast nature of the wireless communication, the signal overheard by E can be written as

$$z_E=\boldsymbol{\omega}_E^H(\sqrt{P_R}Gy\mathbf{g}_{RE}+\mathbf{n}_E)=\sqrt{P_SP_R}G\boldsymbol{\omega}_E^H\mathbf{g}_{RE}\mathbf{g}_{SR}^H\boldsymbol{\omega}_S x+\sqrt{P_R}G\boldsymbol{\omega}_E^H\mathbf{g}_{RE}n_R+\boldsymbol{\omega}_E^H\mathbf{n}_E \tag{3}$$

where $\mathbf{g}_{ER}$ is an $N_E\times 1$ channel vector of the R-E link, $\boldsymbol{\omega}_E=\mathbf{g}_{RE}/\|\mathbf{g}_{RE}\|_F$ is the receive beamformer of the MRC at E and $\mathbf{n}_E\sim CN(0,\sigma_E^2\mathbf{I}_{N_E})$ is the AWGN at E. After some algebraic manipulations, the instantaneous received SNRs at D and E can be, respectively, obtained as

$$\gamma_D=\frac{G^2P_SP_R|\boldsymbol{\omega}_D^H\mathbf{g}_{RD}|^2|\mathbf{g}_{SR}^H\boldsymbol{\omega}_S|^2}{G^2P_R\sigma_R^2|\boldsymbol{\omega}_D^H\mathbf{g}_{RD}|^2+\sigma_D^2}=\frac{\gamma_{SR}\gamma_{RD}}{\gamma_{SR}+\gamma_{RD}+1} \tag{4}$$

$$\gamma_E=\frac{G^2P_SP_R|\boldsymbol{\omega}_E^H\mathbf{g}_{RE}|^2|\mathbf{g}_{SR}^H\boldsymbol{\omega}_S|^2}{G^2P_R\sigma_R^2|\boldsymbol{\omega}_E^H\mathbf{g}_{RE}|^2+\sigma_E^2}=\frac{\gamma_{SR}\gamma_{RE}}{\gamma_{SR}+\gamma_{RE}+1} \tag{5}$$

where $\gamma_{SR}=P_S|\mathbf{g}_{SR}^H\boldsymbol{\omega}_S|^2/\sigma_R^2$, $\gamma_{RD}=P_R|\boldsymbol{\omega}_D^H\mathbf{g}_{RD}|^2/\sigma_D^2$, and $\gamma_{RE}=P_R|\boldsymbol{\omega}_E^H\mathbf{g}_{RE}|^2/\sigma_E^2$.

According to the definition of physical layer secure communication [2], the achievable secrecy rate is formulated as the difference of the capacities between the main channel and the wiretap channel, i.e.,

$$C_S=\begin{cases}\frac{1}{2}\log_2(1+\gamma_D)-\frac{1}{2}\log_2(1+\gamma_E) & \gamma_D\ge\gamma_E\\ 0 & \gamma_D<\gamma_E\end{cases} \tag{6}$$

where the coefficient $1/2$ denotes that two time slots are required to complete the transmission process. In the following, we will analyze two important secrecy performance metrics of the considered relay network, namely SOP and ASR, and further derive the asymptotic SOP and

ASR expressions at high MER to provide insights into the diversity order and array gain.

3. Performance Analysis

3.1 Preliminaries

To analyze the secrecy performance of the considered relay network, we need to know the statistical properties of each link. Suppose that the S-R, R-D and R-E links are subject to Rayleigh fading, the probability density function (PDF) of $\gamma_{\alpha\beta}$, $\alpha \in \{S,R\}, \beta \in \{R,E,D\}$ is given by [16]

$$f_{\gamma_{\alpha\beta}}(x) = \frac{1}{\Gamma(N_j)\bar{\gamma}_{\alpha\beta}^{N_j}} x^{N_j-1} \exp\left(-\frac{x}{\bar{\gamma}_{\alpha\beta}}\right) \tag{7}$$

where $j \in \{S,D,E\}$ and $\bar{\gamma}_{\alpha\beta} = P_\alpha / \sigma_\beta^2$ represents the average received SNR of each link. By using (7), the corresponding cumulative distribution function (CDF) of $\gamma_{\alpha\beta}$ can be obtained as

$$F_{\gamma_{\alpha\beta}}(x) = 1 - \exp\left(-\frac{x}{\bar{\gamma}_{\alpha\beta}}\right)\sum_{k=0}^{N_j-1}\frac{1}{\Gamma(k+1)}\left(\frac{x}{\bar{\gamma}_{\alpha\beta}}\right)^k \tag{8}$$

3.2 Secrecy Outage Probability

According to [13], SOP is defined as the probability that the achievable secrecy rate C_S is below the target secrecy rate $R_S \geq 0$, namely,

$$\mathrm{P}_{SOP} = \Pr(C_S \leq R_S) \tag{9}$$

By substituting (6) into (9), one can obtain

$$\mathrm{P}_{SOP} = \Pr(C_S < R_S \mid \gamma_D \geq \gamma_E)\Pr(\gamma_D \geq \gamma_E) + \Pr(C_S < R_S \mid \gamma_D < \gamma_E)\Pr(\gamma_D < \gamma_E)\,. \tag{10}$$

Note that, $C_S = 0$ when $\gamma_D < \gamma_E$. Hence, we can obtain $P_r(C_S < R_S \mid \gamma_D < \gamma_E) = 1$, and further simplify (10) as

$$\mathrm{P}_{SOP} = \Pr(C_S < R_S \mid \gamma_D \geq \gamma_E)\Pr(\gamma_D \geq \gamma_E) + \Pr(\gamma_D < \gamma_E) \tag{11}$$

Since deriving the exact expression of the term $\Pr(C_S < R_S \mid \gamma_D \geq \gamma_E)$ is mathematically intractable, analogous to [17], we make the following approximations,

$$\gamma_\tau \approx \frac{\gamma_{SR}\gamma_{R\tau}}{\gamma_{SR}+\gamma_{R\tau}} \quad \tau \in \{D,E\} \tag{12}$$

$$\frac{1+\gamma_D}{1+\gamma_E} \approx \left(\frac{\gamma_{SR}\gamma_{RD}}{\gamma_{SR}+\gamma_{RD}}\right) \Big/ \left(\frac{\gamma_{SR}\gamma_{RE}}{\gamma_{SR}+\gamma_{RE}}\right) \tag{13}$$

and obtain

$$\begin{aligned}\Pr(C_S \le R_S \mid \gamma_D \ge \gamma_E) &\approx \frac{1}{\Pr(\gamma_D \ge \gamma_E)}\left(\Pr\left(\gamma_{RD} \le L\gamma_{RE}\right)+\Pr\left(\gamma_{SR} < \frac{(L-1)\gamma_{RD}\gamma_{RE}}{\gamma_{RD}-L\gamma_{RE}}, \gamma_{RD} > L\gamma_{RE}\right)\right)\\ &= \frac{1}{\Pr(\gamma_D \ge \gamma_E)}\left(\int_0^\infty\int_0^{L\gamma_{RE}} f_{\gamma_{RD}}(y) f_{\gamma_{RE}}(z)dydz + \int_0^\infty\int_{L\gamma_{RE}}^\infty\int_0^{Q(L,y,z)} f_{\gamma_{SR}}(x) f_{\gamma_{RD}}(y) f_{\gamma_{RE}}(z)dxdydz\right)\\ &= \frac{1}{\Pr(\gamma_D \ge \gamma_E)}\left(1-\underbrace{\int_0^\infty\int_{L\gamma_{RE}}^\infty \exp\left(\frac{Q(L,y,z)}{\overline{\gamma}_{SR}}\right)\sum_{i=0}^{N_S-1}\frac{1}{i!}\left(\frac{Q(L,y,z)}{\overline{\gamma}_{SR}}\right)^i f_{\gamma_{RD}}(y) f_{\gamma_{RE}}(z)dydz}_{I_1}\right)\end{aligned} \quad (14)$$

where $L = 2^{2R_S}$ and $Q(L,y,z) = (L-1)yz/(y-Lz)$.

By employing the PDFs of γ_{RD} and γ_{RE} as given in (7), I_1 in (14) can be rewritten as

$$I_1 = \frac{1}{\Gamma(N_D)\Gamma(N_E)}\sum_{i=0}^{N_S-1}\int_0^\infty\int_{L\gamma_{RE}}^\infty \frac{1}{i!}\frac{Q(L,y,z)^i y^{N_D-1} z^{N_E-1}}{\overline{\gamma}_{SR}^i\overline{\gamma}_{RD}^{N_D}\overline{\gamma}_{RE}^{N_E}}\exp\left(-\left(\frac{Q(L,y,z)}{\overline{\gamma}_{SR}}+\frac{y}{\overline{\gamma}_{RD}}+\frac{z}{\overline{\gamma}_{RE}}\right)\right)dydz \quad (15)$$

By using variable replacement $t = y - Lz$ and the binomial theorem, one can obtain

$$\begin{aligned} I_1 = &\frac{1}{\overline{\gamma}_{RD}^{N_D}\overline{\gamma}_{RE}^{N_E}\Gamma(N_D)\Gamma(N_E)}\sum_{i=0}^{N_S-1}\sum_{j=0}^{i}\sum_{k=0}^{N_D-1}\int_0^\infty \frac{1}{i!}\left(\binom{i}{j}\binom{N_D-1}{k}\left(\frac{(L-1)z}{\overline{\gamma}_{SR}}\right)^i \exp\left(-\frac{(L-1)z}{\overline{\gamma}_{SR}}-\frac{Lz}{\overline{\gamma}_{RD}}\right)\right.\\ &\left.\times(Lz)^{N_D+j-1-k}\int_0^\infty t^{k-j}\exp\left(-\frac{L(L-1)z^2}{\overline{\gamma}_{SR}t}-\frac{t}{\overline{\gamma}_{RD}}\right)dt\right) f_{\gamma_{RE}}(z)dz \end{aligned} \quad (16)$$

With the help of the following identifies [19, eq. 28], [17, eq. 24]

$$\int_0^\infty x^{v-1}\exp\left(-\frac{\beta}{x}-\gamma x\right)dx = 2\left(\frac{\rho}{\gamma}\right)^{\frac{v}{2}} K_v\left(2\sqrt{\rho\gamma}\right) \quad (17)$$

$$\int_0^\infty x^{\kappa-1}e^{-px}K_v(cx)dx = \frac{\sqrt{\pi}p^{v-\kappa}c^{-v}\Gamma(\kappa-v)\Gamma(\kappa+v)}{2^\alpha\Gamma(\kappa+1/2)}\,{}_2F_1\left(\frac{\kappa-v}{2},\frac{\kappa-v+1}{2};\kappa+\frac{1}{2};1-\frac{c^2}{p^2}\right) \quad (18)$$

I_1 can be further expressed as

$$\begin{aligned} I_1 = &\frac{2}{\overline{\gamma}_{RD}^{N_D}\overline{\gamma}_{RE}^{N_E}\Gamma(N_D)\Gamma(N_E)}\sum_{i=0}^{N_S-1}\sum_{j=0}^{i}\sum_{k=0}^{N_D-1}\frac{1}{i!}\binom{i}{j}\binom{N_D-1}{k}\left(\frac{L}{\overline{\gamma}_{RD}}\right)^{\frac{j-k+2N_D-1}{2}}\\ &\times\overline{\gamma}_{SR}^{-2i+j-k-1}(L-1)^{\frac{2i-j+k+1}{2}}\int_0^\infty z^{N_D+N_E+i-1}\cdot\exp(-\alpha z)\cdot K_{k-j+1}(2\beta z)dz \end{aligned}$$

$$
\begin{aligned}
&= \frac{\sqrt{\pi}L^{N_D}}{\overline{\gamma}_{RD}^{N_D}\overline{\gamma}_{RE}^{N_E}\Gamma(N_D)\Gamma(N_E)}\sum_{i=0}^{N_S-1}\sum_{j=0}^{i}\sum_{K=0}^{N_D-1}\frac{1}{i!}\binom{i}{j}\binom{N_D-1}{k}\left(\frac{L-1}{\overline{\gamma}_{SR}}\right)^{\mu+i} \\
&\times\frac{\Gamma(\lambda+\mu)\Gamma(\lambda-\mu)}{\Gamma(\lambda+1/2)}\frac{2^{2\mu+1}}{(\alpha+\beta)^{\lambda+\mu}}\,{}_2F_1\left(\lambda+\mu,\mu+\frac{1}{2};\lambda+\frac{1}{2};\frac{\alpha-\beta}{\alpha+\beta}\right)
\end{aligned} \tag{19}
$$

where $\lambda = N_D + N_E + i$, $\mu = k - j + 1$, $\alpha = (L-1)/\overline{\gamma}_{SR} + L/\overline{\gamma}_{RD} + 1/\overline{\gamma}_{RE}$, $\beta = 2\sqrt{(L-1)L/\overline{\gamma}_{SR}\overline{\gamma}_{RD}}$. By substituting (19) into (14), one can obtain

$$
\begin{aligned}
\Pr(C_S \le R_S \mid \gamma_D \ge \gamma_E) \approx \frac{1}{\Pr(\gamma_D \ge \gamma_E)}\Bigg[1 - &\frac{\sqrt{\pi}L^{N_D}}{\overline{\gamma}_{RD}^{N_D}\overline{\gamma}_{RE}^{N_E}\Gamma(N_D)\Gamma(N_E)}\sum_{i=0}^{N_S-1}\sum_{j=0}^{i}\sum_{K=0}^{N_D-1}\frac{1}{i!}\binom{i}{j}\binom{N_D-1}{k}\left(\frac{L-1}{\overline{\gamma}_{SR}}\right)^{\mu+i} \\
&\times\frac{\Gamma(\lambda+\mu)\Gamma(\lambda-\mu)}{\Gamma(\lambda+1/2)}\frac{2^{2\mu+1}}{(\alpha+\beta)^{\lambda+\mu}}\,{}_2F_1\left(\lambda+\mu,\mu+\frac{1}{2};\lambda+\frac{1}{2};\frac{\alpha-\beta}{\alpha+\beta}\right)\Bigg]
\end{aligned} \tag{20}
$$

Next, we derive the expression of $\Pr(\gamma_{RD} < \gamma_{RE})$. By applying the PDFs of γ_{RD} and γ_{RE} in (7)**,** one can obtain,

$$
\begin{aligned}
\Pr(\gamma_{RD} < \gamma_{RE}) &= \int_0^\infty\int_0^{\gamma_{RE}} f_{\gamma_{RD}}(y) f_{\gamma_{RE}}(z)\,dydz \\
&= 1 - \frac{1}{\overline{\gamma}_{RE}^{N_E}\Gamma(N_E)}\sum_{m=0}^{N_D-1}\frac{\Gamma(N_E+m)}{\Gamma(m-1)}\left(\frac{1}{\overline{\gamma}_{RD}}\right)^m\left(\frac{1}{\overline{\gamma}_{RD}}+\frac{1}{\overline{\gamma}_{RE}}\right)^{-N_E-m}
\end{aligned} \tag{21}
$$

By substituting (20) and (21) into (11), we can eventually obtain the approximate expression of SOP as

$$
\begin{aligned}
\Pr(C_S \le R_S) \approx 1 - \frac{1}{\overline{\gamma}_{RE}^{N_E}\Gamma(N_E)}\Bigg(&\frac{\sqrt{\pi}L^{N_D}}{\overline{\gamma}_{RD}^{N_D}\Gamma(N_D)}\sum_{i=0}^{N_S-1}\sum_{j=0}^{i}\sum_{k=0}^{N_D-1}\frac{1}{i!}\binom{i}{j}\binom{N_D-1}{k}\frac{\Gamma(\lambda+\mu)\Gamma(\lambda-\mu)}{\Gamma(\lambda+1/2)} \\
&\times\frac{2^{2\mu+1}}{(\alpha+\beta)^{\lambda+\mu}}\left(\frac{L-1}{\overline{\gamma}_{SR}}\right)^{\mu+i}\,{}_2F_1\left(\lambda+\mu,k-j+\frac{3}{2};\lambda+\frac{1}{2};\frac{\alpha-\beta}{\alpha+\beta}\right) \\
&-\sum_{m=0}^{N_D-1}\frac{\Gamma(N_E+m)}{\Gamma(m-1)}\left(\frac{1}{\overline{\gamma}_{RD}}\right)^m\left(\frac{1}{\overline{\gamma}_{RD}}+\frac{1}{\overline{\gamma}_{RE}}\right)^{-N_E-m}\Bigg)
\end{aligned} \tag{22}
$$

3.3 Average Secrecy Rate

ASR is another fundamental performance metric for secure communications [22], which is defined as the average of the secrecy rate C_S as given by

$$
\overline{C}_S = E[C_S] \tag{23}
$$

By substituting (6) into (23), we have

$$\begin{aligned}\overline{C}_S &= \frac{1}{2}E\left[\left(\log_2\left(1+\gamma_D\right)-\log_2\left(1+\gamma_E\right)\right)^+\right]\\ &= \frac{1}{2}\iint_{\gamma_D \geq \gamma_E} \log_2\left(1+x\right)-\log_2\left(1+y\right) f_{\gamma_D}\left(x\right) f_{\gamma_E}\left(y\right)dxdy\\ &= \frac{1}{2}\int_0^\infty \underbrace{\int_0^{\gamma_D}\left(\log_2\left(1+x\right)-\log_2\left(1+y\right)\right) f_{\gamma_E}\left(y\right)dy}_{I_2} f_{\gamma_D}\left(x\right)dx\end{aligned} \tag{24}$$

By using the integration by parts, I_2 can be rewritten as

$$\begin{aligned}I_2 &= \int_0^{\gamma_D}\log_2\left(1+x\right)f_{\gamma_E}\left(y\right)dy-\int_0^{\gamma_D}\log_2\left(1+y\right)f_{\gamma_E}\left(y\right)dy\\ &= \log_2\left(1+x\right)\int_0^{\gamma_D} f_{\gamma_E}\left(y\right)dy-\int_0^{\gamma_D}\log_2\left(1+y\right)f_{\gamma_E}\left(y\right)dy\\ &= \frac{1}{\ln 2}\int_0^{\gamma_D}\frac{F_{\gamma_E}\left(y\right)}{1+y}dy\ .\end{aligned} \tag{25}$$

Substituting (25) into (24) yields

$$\overline{C}_S = \frac{1}{2\ln 2}\int_0^\infty\int_0^{\gamma_D}\frac{F_{\gamma_E}\left(y\right)}{1+y} f_{\gamma_D}\left(x\right)dydx = \frac{1}{2\ln 2}\int_0^\infty\frac{F_{\gamma_E}\left(x\right)}{1+x}\left[1-F_{\gamma_D}\left(x\right)\right]dx \tag{26}$$

To derive the CDFs of γ_D and γ_E, we use the approximate formula (12) and obtain

$$\begin{aligned}F_{\gamma_D}\left(s\right) &\approx \Pr\left(\gamma_D < s\right)\\ &= \int_0^s \Pr\left(y > \frac{sx}{x-s}\right)f_{\gamma_{SR}}\left(x\right)dx + \int_s^\infty \Pr\left(y < \frac{sx}{x-s}\right) f_{\gamma_{SR}}\left(x\right)dx\\ &= 1-\int_0^\infty\left(1-F_{\gamma_{RD}}\left(\frac{sx}{x-s}\right) f_{\gamma_{SR}}\left(x\right)\right)dx\end{aligned} \tag{27}$$

where $F_{\gamma_{RD}}\left(y\right)$ is the CDF of γ_{RD}. By substituting (7) into (27), one can obtain

$$\begin{aligned}F_{\gamma_D}\left(s\right) &= 1-\frac{1}{\overline{\gamma}_{SR}^{N_S}\Gamma\left(N_S\right)}\sum_{k=0}^{N_D-1}\frac{1}{k!}\frac{s^k}{\overline{\gamma}_{RD}^k}\int_s^\infty\frac{x^{N_S+k-1}}{\left(x-s\right)^k}\exp\left(-\left(\frac{s}{x-s}-1\right)\frac{x}{\overline{\gamma}_{RD}}\right)dx\\ &= 1-\sum_{i=0}^{N_D-1}\left(-s\right)^i\frac{\left(\overline{\gamma}_{RD}\right)^{N_S-\frac{1}{2}}\Gamma\left(N_S+i\right)}{\sqrt{\pi}\Gamma\left(N_S\right)\Gamma\left(i+1\right)}\exp\left(-\frac{\overline{\gamma}_{SR}s^2+\overline{\gamma}_{RD}s}{2\overline{\gamma}_{SR}\overline{\gamma}_{RD}}\right)\\ &\quad\times\left(\frac{s\overline{\gamma}_{SR}}{s\overline{\gamma}_{SR}+\overline{\gamma}_{RD}}\right)^{N_S+i-\frac{1}{2}}K_{N_S+i-\frac{1}{2}}\left(\frac{\overline{\gamma}_{SR}s^2+\overline{\gamma}_{RD}s}{2\overline{\gamma}_{SR}\overline{\gamma}_{RD}}\right).\end{aligned} \tag{28}$$

In a similar manner, the CDF of γ_E can be expressed as

$$F_{\gamma_E}(s)=1-\sum_{j=0}^{N_E-1}(-s)^j\frac{(\overline{\gamma}_{RE})^{N_S-\frac{1}{2}}\Gamma(N_S+j)}{\sqrt{\pi}\Gamma(N_S)\Gamma(j+1)}\exp\left(-\frac{\overline{\gamma}_{SR}s^2+\overline{\gamma}_{RE}s}{2\overline{\gamma}_{SR}\overline{\gamma}_{RE}}\right)$$
$$\times\left(\frac{s\overline{\gamma}_{SR}}{s\overline{\gamma}_{SR}+\overline{\gamma}_{RE}}\right)^{N_S+j-\frac{1}{2}}K_{N_S+j-\frac{1}{2}}\left(\frac{\overline{\gamma}_{SR}s^2+\overline{\gamma}_{RE}s}{2\overline{\gamma}_{SR}\overline{\gamma}_{RE}}\right). \tag{29}$$

Substituting (28) and (29) into (26) and employing (18), we can rewrite the ASR as

$$\overline{C}_S=\frac{1}{\sqrt{2\pi}\ln 2}\sum_{i=0}^{N_D-1}\sum_{j=0}^{N_E-1}(-1)^i\frac{\overline{\gamma}_{RD}^{N_S-i}}{2^{N_S+2i+1}}\frac{\Gamma(N_S+i)\Gamma(2N_S+3i)}{\Gamma(N_S)\Gamma(N_S+2i+1)}\left(\frac{\overline{\gamma}_{SR}\overline{\gamma}_{RD}}{\overline{\gamma}_{SR}+\overline{\gamma}_{RD}}\right)^{N_S+3i}$$
$$\times\,{}_2F_1\left(\varphi_1,\varphi_1+\frac{1}{2};\varphi_2;1-\frac{\overline{\gamma}_{SR}+\overline{\gamma}_{RD}}{\overline{\gamma}_{SR}\overline{\gamma}_{RD}}\right)\left(1-\frac{(-1)^j}{2\sqrt{\pi}\ln 2}\frac{\overline{\gamma}_{SR}^{-N_S-1}\overline{\gamma}_{RE}^{-j-1}}{2^{2N_S+4j+1}}\left(\frac{\overline{\gamma}_{SR}\overline{\gamma}_{RE}}{\overline{\gamma}_{SR}+\overline{\gamma}_{RE}}\right)^{2N_S+3j+1}\right.$$
$$\left.\times\frac{\Gamma(N_S+j)\Gamma(2N_S+3j)}{\Gamma(N_S+2j+1)}\,{}_2F_1\left(\phi_1,\phi_1+\frac{1}{2};\phi_2;1-\frac{\overline{\gamma}_{SR}+\overline{\gamma}_{RE}}{\overline{\gamma}_{SR}\overline{\gamma}_{RE}}\right)\right) \tag{30}$$

where $\varphi_1=\frac{i+1}{2}$, $\varphi_2=N_S+2i+1$, and $\phi_1=\frac{j+1}{2}$, $\phi_2=N_S+2j+1$.

5. Asymptotic Analysis

To provide further insights into diversity order and array gain, we drive the asymptotic SOP expression at high MER of the considered relay network, where MER defined as the ratio of average channel from the relay to destination to that from the relay to the eavesdropper. Letting $\theta=\overline{\gamma}_{RD}/\overline{\gamma}_{RE}$ and using the following asymptotic relations for ${}_2F_1(a,b;c;d)$, $x\to 1$ [18]

$${}_2F_1(a,b;c;x)=\begin{cases}\frac{B(c,a+b-c)}{B(a+b)}(1-x)^{c-a-b} & a+b>c\\ \frac{2\Psi(1)-\Psi(a)-\Psi(b)-\ln(1-x)}{B(a,b)} & a+b=c\\ \frac{\Gamma(c)\Gamma(c-a-b)}{\Gamma(c-a)\Gamma(c-b)} & a+b<c\end{cases} \tag{31}$$

where $B(a,b)=\Gamma(a)\Gamma(b)/\Gamma(a+b)$ and $\Psi(x)$ is the digamma function, the asymptotic expression of SOP at high MER can be written as

$$P_r^\infty(C_S<R_S)=(G_a\theta)^{-G_d}+O(\theta^{-G_d}) \tag{32}$$

where $O(\bullet)$ represents the higher order terms, and the diversity order G_d and array gain G_a are respectively given by

$$G_d=N_D \tag{33}$$

and

$$G_a = \left[\frac{\sqrt{\pi} L^{N_D+1/2}}{\overline{\gamma}_{RE}^{N_D+N_E} \Gamma(N_D)\Gamma(N_E)} \sum_{i=1}^{N_S-1} \sum_{j=0}^{i} \sum_{k=0}^{N_D-1} \binom{i}{j} \binom{N_D-1}{k} \frac{\Gamma(\lambda+\mu)\Gamma(2\mu)}{\Gamma(i+1)\Gamma(k-j+3/2)} \right.$$
$$\left. \times \frac{4^{k-j+2}(L-1)^{\mu+i+3/2}}{\overline{\gamma}_{SR}^{\mu+i+1/2}\left((L+1)/\overline{\gamma}_{RD}+1/\overline{\gamma}_{RE}\right)^{\lambda+\mu+1}} + \sum_{m=0}^{N_D-1} \frac{B(N_E-1,m)}{2} \right]^{-\frac{1}{N_D}}. \tag{34}$$

Substituting (31) into (30), we finally obtain the asymptotic expression of ASR as

$$\overline{C}_S^{\infty} = \sum_{i=0}^{N_D-1} \sum_{j=1}^{i} (-1)^{i-j} \frac{\Gamma(j)}{\Gamma(i+1)} + \sum_{i=0}^{N_D-1} (-1)^{i-1} (\theta \overline{\gamma}_{RE})^{-i} \frac{1}{\Gamma(i+1)}$$
$$- \sum_{i=0}^{N_D-1} \sum_{n=0}^{N_E-1} \frac{(-1)^{i+n-1}\theta^i}{\Gamma(i+1)\Gamma(n+1)} \left(\frac{1}{\overline{\gamma}_{RE}}\right)^{n+i} e^{\frac{1}{\overline{\gamma}_{RE}}} E_i\left(-\frac{1}{\overline{\gamma}_{RE}}\right)$$
$$- \sum_{i=0}^{N_D-1} \sum_{n=0}^{N_E-1} \sum_{k=1}^{i+n} \frac{(-1)^{i-1}}{\Gamma(i+1)\Gamma(n+1)} \left(\frac{1}{\theta \overline{\gamma}_{RE}}\right)^{i} \tag{35}$$

6. Numerical Results

As the first example, **Fig. 2** plots the approximate and asymptotic SOP versus MER for different values of N_D and N_E . In this example, we assume $R_S = 0.5 bits/s/Hz$, $N_S = 2$, $\overline{\gamma}_{SR} = 30$ dB, and $\overline{\gamma}_{RE} = 10$ dB. The approximate curves are obtained from (22), and the asymptotic curves are calculated by (32). As observed from the figure despite the use of approximation (12), the approximate curves match well with the Monte Carlo simulation results. It is also observed that the SOP increases with N_E and decreases with N_D. This is because the increase of N_D improve the gain of the main channel, while the decrease of N_E makes the main channel better quality than the wiretap channel. In addition, the diversity order and the array gain reflected from the asymptotic curves are consistent with the theoretical analysis results. Coincidentally, the secrecy diversity order is equal with N_D .

Fig. 3 depicts the ASR versus MER for different values of N_D with $\overline{\gamma}_{SR} = 30$ dB, $\overline{\gamma}_{RE} = 10$ dB, $N_S = 2$ and $N_E = 2$. The approximate and asymptotic ASR curves are obtained from (30) and (35), respectively. As observed from the figure, regardless of the approximation, the approximate curves match well with Monte Carlo simulations, and the asymptotic result converges to the approximate value at high MER. It is also observed that the ASR increases with increasing N_D, which can be explained by the fact that increasing N_D improves the diversity order of the considered system. Moreover, the ASR increases with increasing MER. This is due to the fact that the increasing N_D makes the main channel have better quality than the wiretap channel.

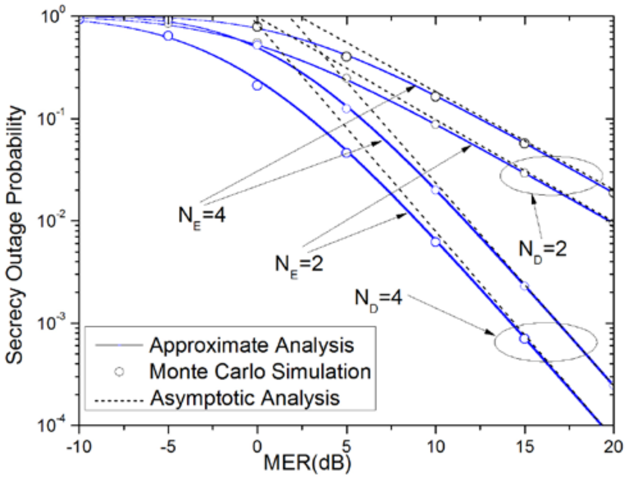

Fig. 2. Secrecy outage probability with different N_D and N_E

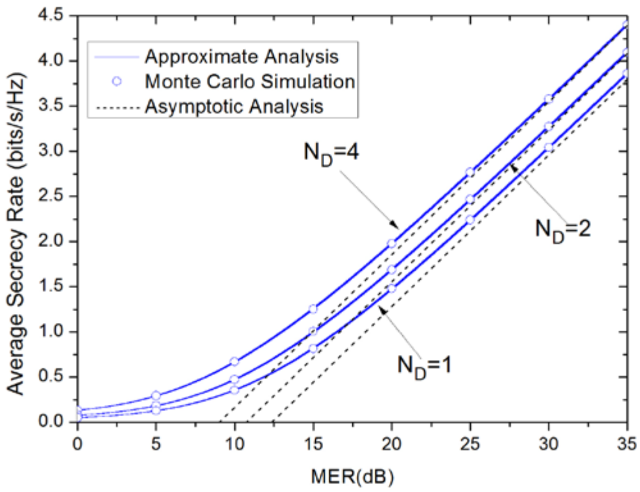

Fig. 3. Average secrecy rate versus the MER for different N_D

7. Conclusion

In this paper, we have investigated the secrecy performance of the AF relay network with MRT/MRC in Rayleigh fading channels. Firstly, we have derived the SNRs of the main link and the wiretap link, respectively. Then, we have presented the approximate expressions for the SOP and ASR of the considered relay network. To further investigate the diversity gain and array gain, the asymptotic expressions of SOP and ASR at high MER have been derived. Finally, Monte Carlo simulation has been conducted to demonstrate the validity of the analytical results.

References

[1] V. A. Aalo, and G. P. Efthymoglou, "Performance analysis of multi-hop amplify-and-forward relaying systems in rayleigh fading channels with a poisson interference field," *IEEE Trans. Wireless Commun*., vol. 13, no. 1, pp. 24-35, Jan 2014. Article (CrossRef Link)

[2] M. Elsaadany and W. Hamouda, "Performance analysis of non-orthogonal AF relaying in Cognitive radio networks," *IEEE Wireless Commun. Lett.*, vol. 4, no. 4, pp. 373-376, Aug. 2015. Article (CrossRef Link)

[3] M. S. Alam and F. Labeau, "Performance analysis of DF cooperative relaying over bursty impulsive noise channel," *IEEE Tran. Commun.*, vol. 64, no. 7, Jul. 2011.Article (CrossRef Link)

[4] Y. Zou, B. Zheng, and W. P. Zhu, "An opportunistic cooperation scheme and its BER analysis," *IEEE Trans. Wireless Commun.*, vol. 8, no. 9, pp. 4492-2297, Sept. 2009. Article (CrossRef Link)

[5] Y. Zou, B. Zheng, and J. Zhu, "Outage analysis of opportunistic cooperation over Rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 6, pp. 3077-3085, Jun. 2009. Article (CrossRef Link)

[6] A. Adinoyi and H. Yanikomeroglu, "Cooperative relaying in multi-antenna fixed relay networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 2, pp. 533-544, Feb. 2007. Article (CrossRef Link)

[7] S. W. Peters and J. R. W. Heath, "Non-regenerative MIMO relaying with optimal transmit antenna selection," *IEEE Signal Process. Lett.*, vol. 15, pp. 421-424, Aug. 2008. Article (CrossRef Link)

[8] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory.*, vol. 54, no. 9, pp. 4005-4019, Sept. 2008. Article (CrossRef Link)

[9] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875-1888, Mar. 2010. Article (CrossRef Link)

[10] N. Zhao , F. R. Yu and M. Li, "Anti-eavesdropping schemes for interference alignment (IA)-based wireless networks," *IEEE Trans. Wireless Commun.*, 2016. Article (CrossRef Link)

[11] X. Y. Wang, and Z. S. Zhang, "Secure beamforming for multiple-antenna amplify-and-forward relay networks," *IEEE Trans. Signal Process.*, vol. 64, no. 6, pp: 1477 - 1492, Mar. 2016. Article (CrossRef Link)

[12] N. Zhao and F. R. Yu, "Physical layer security issues in interference alignment (IA)-based wireless networks," *IEEE Commun. Mag.*, pp. 162-168, Aug. 2016. Article (CrossRef Link)

[13] A. Jindal and C. Kundu, "Secrecy outage of dual-hop AF relay system with relay selection without eavesdropper's CSI," *IEEE Commun. Lett.*, vol. 18, no. 10, pp: 1759 – 176, Oct. 2014. Article (CrossRef Link)

[14] M. Mirzaee and S. Akhlaghi, "Achievable secrecy rate of wiretap channels incorporating multi-input–multi-output amplify and forward relaying," *IET Commum.*, vol. 10, no. 3, pp: 300 - 308, Mar. 2016. Article (CrossRef Link)

[15] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory.*, vol. 54, no. 6,pp. 2515–2534, Sept. 2008. Article (CrossRef Link)

[16] M. Li and M. Lin, "Optimal beamformer design for dual-hop MIMO AF relay networks over rayleigh fading channels," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1402-1414, Sep. 2012. Article (CrossRef Link)

[17] P. L. Yeoh and M. Elkashlan, "Selection relaying with transmit beamforming: a comparison of fixed and variable gain relay," *IEEE Trans. Commun.*, vol. 59, no. 6, pp. 1720-1729, Apr. 2011. Article (CrossRef Link)

[18] M. Lin and J. Ouyang, "On the performance of hybrid satellite-terrestrial cooperative networks with Interferences," in *Proc. of IEEE Asilomar Conf. Signals Syst. Comput.*, pp. 1796-1800, Nov. 2014. Article (CrossRef Link)

[19] K. S. Hwang and M. C. Ju, "Secrecy outage probability of amplify-and-forward transmission with multi-antenna relay in presence of eavesdropper," in *Proc. of IEEE Int. Conf. Commun.*, pp. 5408-5412, Jun. 2014. Article (CrossRef Link)

[20] N. Yang and P. L. Yeoh, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144-153, Jan. 2013. Article (CrossRef Link)

[21] C. Kundu, and S. Ghose, "Secrecy outage of dual-hop regenerative multi-relay system with relay selection," *IEEE Trans. Wireless Commun.*, vol.14, no.8, pp. 4614-4625, Aug. 2015. Article (CrossRef Link)

[22] N. Yang and P. L. Yeoh, "MIMO wiretap channels: secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1754-1757, Sep. 2013. Article (CrossRef Link)

[23] J. H. Fan and C. W. Yuan, "Outage Performance for DF Two-Way Relaying with Co-Channel Interference over Nakagami-m Fading," *KSII Trans. Internet Inf. Syst.*, vol. 9, no. 11, pp. 4469-4482, Nov. 2015. Article (CrossRef Link)

[24] L. Fan, and X. F. Lei, "Secure multiuser multiple amplify-and-forward relay networks in presence of multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 8, no.6, pp.4120-4125, Oct. 2014. Article (CrossRef Link)

[25] P. S. Pan and B. Y. Zheng, "Outage probability of two-hop relay networks with related interference," in *Proc. of KSII Trans. Internet Inf. Syst.*, vol. 7, no. 8, pp. 1786-1803, Aug. 2013. Article (CrossRef Link)

Pu Chen received the B.S. degree from Nanjing University of Posts and Telecommunications, Nanjing, China, in 2013. He is currently pursuing for his M.S. degree in Signal and Information Processing at the college of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing, China. His research interest is performance analysis of communication systems.

Jian Ouyang received the B.S., M.S. and Ph.D. degrees from Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2007, 2010 and 2014, respectively. From 2015 to 2016, he was a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada. Since July 2014, he has been a full-time faculty member with the College of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests are signal processing in wireless communications, optimization and performance analysis of communication systems and machine learning algorithms.

Wei-Ping Zhu (SM'97) received the B.E. and M.E. degrees from Nanjing University of Posts and Telecommunications, and the Ph.D. degree from Southeast University, Nanjing, China, in 1982, 1985, and 1991, respectively, all in electrical engineering. He was a Postdoctoral Fellow from 1991 to 1992 and a Research Associate from 1996 to 1998 with the Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada. During 1993–1996, he was an Associate Professor with the Department of Information Engineering, Nanjing University of Posts and Telecommunications. From 1998 to 2001, he worked with hi-tech companies in Ottawa, Canada, including Nortel Networks and SR Telecom Inc. Since July 2001, he has been with Concordia's Electrical and Computer Engineering Department as a full-time faculty member, where he is presently a Full Professor. Since 2008, he has been an Adjunct Professor at Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests include digital signal processing fundamentals, speech and statistical signal processing, and signal processing for wireless communication with a particular focus on MIMO systems and cooperative communication. Dr. Zhu served as an Associate Editor for the IEEE Transactions on Circuits and Systems Part I: Fundamental Theory and Applications during 2001-2003, an Associate Editor for Circuits, Systems and Signal Processing during 2006-2009, and an Associate Editor for the IEEE Transactions on Circuits and Systems Part II: Transactions Briefs during 2011-2015. He was also a Guest Editor for the IEEE Journal on Selected Areas in Communications for the special issues of: Broadband Wireless Communications for High Speed Vehicles, and Virtual MIMO during 2011-2013. Currently, he is an Associate Editor of Journal of The Franklin Institute. Dr. Zhu was the Secretary of Digital Signal Processing Technical Committee (DSPTC) of the IEEE Circuits and System Society during June 2012-May 2014, and the Chair of the DSPTC during June 2014-May 2016.