Multiple Eavesdropper-Based Physical Layer Security in SIMO System With Antenna Correlation

Gangcan Sun[1*] , Mengge Liu[2] , Zhuo Han[2] , Chuanyong Zhao[2]
[1] School of Information Engineering and Industrial Technology Research Institute, Zhengzhou University
Zhengzhou，450001 – CHINA
[e-mail: iegcsun@zzu.edu.cn]
[2] School of Information Engineering, Zhengzhou University
[e-mail: liumenggezs@163.com]
*Corresponding author: Gangcan Sun

Received February 12, 2018; revised January 29, 2019; accepted August 4, 2019; published January 31, 2020

Abstract

In this paper, we investigate the impact of antenna correlation on secure transmission in a multi-eavesdropper single-input multiple-output (SIMO) system, where the receiver and eavesdroppers are equipped with correlated antennas. Based on the practical passive eavesdropping system, the new closed-form expressions of secrecy outage probability (SOP) and non-zero secrecy capacity probability are derived to explore the effect of antenna correlation on the system with multiple eavesdroppers. To further analyze the secrecy performance of the investigated system, we theoretically derive the expression of asymptotic SOP to clearly show the diversity order and array gain. Finally, Monte Carlo simulations verify the effectiveness of our theoretical results.

Keywords: physical layer security, secrecy outage probability, antenna correlation, Rayleigh fading

http://doi.org/10.3837/tiis.2020.01.023 **ISSN : 1976-7277**

1. Introduction

With the increasing demand for the transmission performance of the communication system, how to ensure the information security has become an urgent aporia. At present, wireless communication has been diffusely used in many fields, since the broadcasting feature of the wireless communication, it is essential to impede eavesdroppers stealing information during the information transmission. In general, the secrecy measures are carried out at the upper layer of the wireless network formerly [1]. However, they are all based on the error-free link at the physical level. In fact, because of the broadcast characteristics of the wireless transmission environment, the transmitting data is easy to be eavesdropped. Therefore, it is challenging to guarantee the transmission information security at the physical layer.

Shannon [2] and Wyner [3] have provided a solid foundation for the basic research on the secrecy transmission theory and model construction in wireless communication. The author in [4] studied the physical layer security based on multicasting scheme with multiple receivers and eavesdroppers both having multiple antennas, and indicated that increasing eavesdroppers and antennas own by each of them would decrease the transmission security. Based on these explorations, [5] probed the secrecy outage probability (SOP) of information transmission in the eavesdropping system especially. The author in [6] indicated that SOP increases with the number of receivers in a wireless multicasting system, where there is a single eavesdropper equipped with a single antenna. In [7], the author stated that secrecy capacity and SOP can be improved by optimizing the transmission power and diversity order in SIMO wiretap channels with maximal ratio combining (MRC) scheme in Rayleigh fading environment. The studies in [4-7] focused on the research of SIMO wiretap system. There are also some work involved MIMO eavesdropping channels. To heighten the physical layer security of wireless networks, [8] proposed a guide to several general techniques. In [9], the secrecy capacity of secure transmission system was investigated under eavesdropping and external interference. To explore the secrecy performance of a multiple-input multiple-output (MIMO) wiretap system with transmitting antenna selection and generalized selection combining (TAS/GSC), the maximum secrecy diversity gain was obtained in [10]. In [11], the MRC scheme and the selection combining (SC) scheme were compared, and the research results demonstrated that the security of the system with Nakagami-m fading channels can be effectively improved by using MRC at receiver and SC at eavesdropper. The authors in [12, 13] investigated the impact of the imperfect feedback at the transmitter on the performance of system security with MIMO wiretap channels, and what is different is that the general-order transmit antenna selection technique was adopted in [13] while the optimal TAS technique was applied in [12]. Recently, secure transmission in massive MIMO, a new communication technology in 5G wireless networks, is analyzed in [14, 15]. To sum up, the research of secure transmission in wireless system is very important.

In practice, antenna correlation exists in many cases, such as mobile phones and laptops communications. It results from the close space between the different antenna branches in the antenna array [16]. Therefore, the effect of antenna correlation on secure transmission performance of the communication system must be considered. However, only a few works about the analysis of the secrecy performance in physical layer communication system with antenna correlation are reported. Currently, some literatures have studied the secrecy performance of antenna correlation in SIMO system. [17] pointed out that the antenna correlation is gainful to system secrecy performance when the average signal-to-noise ratio (SNR) of receiver is at low level but is harmful to system secrecy performance when the

average SNR of receiver is at medium and high level. The author in [18] demonstrated the impact of antenna correlation on secrecy performance increases with the increasing transmission rate when the receiver and the eavesdropper are both equipped with correlated antennas in Rayleigh fading channels. In addition, researchers studied the influence of antenna correlation in MIMO systems. In [19, 20], the closed expressions of SOP, non-zero secrecy capacity probability (NZSC) and asymptotic SOP were achieved for MIMO wiretap channels with arbitrary antenna correlation at receiver and eavesdropper. Furthermore, the difference between the above two systems is that Rayleigh fading was utilized in [19] while Nakagami-*m* fading was applied in [20].

However, the above work only considered the single eavesdropper in the system. In fact, the information between legal parties can be wiretapped by multiple potential eavesdroppers at the same time. Therefore, it is necessary to investigate the impact of antenna correlation on physical layer security in communication system with multiple eavesdroppers. In this paper, the main contributions are summarized as follows:

1) The new closed-form expressions (CFEs) of SOP and NZSC, which apply to arbitrary antenna correlation, are derived in the system with respective antenna correlation at the receiver and multiple eavesdroppers. Meanwhile, diversity order and array gain of the system are also analyzed when the average SNR of the receiver is high.
2) For this scenario, where the average SNR of the main channel is much higher than that of eavesdroppers' channels, a new compact expression of the asymptotic SOP is provided, which consequently gives the system diversity order and array gain.
3) In particular, the uniform antenna correlation model is analyzed, and the simulation results are discussed and summarized in detail.

We arrange the structure of this paper as follows. The considered system model is demonstrated in Section 2. Section 3 presents the proposed new expressions of the SOP and NZSC. And the asymptotic SOP is provided to show the diversity order and array gain. The numerical results are investigated and the simulation results are discussed in Section 4. Finally, Section 5 summarizes the findings of this paper and provides solutions to some problems.

2. System Model

The considered system model is shown in **Fig. 1**, which comprises a transmitter called Alice, a receiver called Bob and L_E eavesdroppers called Eve L_E. We assume that the transmitter equips with a single antenna, where the receiver and each eavesdropper equip N_B and N_E antennas, respectively. The impact of uniform antenna correlation at receiver and each eavesdropper in the SIMO communication system has been investigated in [21], where multiple eavesdroppers are independent. Alice only knows the channel state information (CSI) of the main channel. However, neither Alice nor Bob knows the CSI of the eavesdroppers' channels, i.e., passive eavesdropping. We assume that the MRC scheme is adopted [17] by receiver and each eavesdropper for the independent and identically distributed (i.i.d.) Rayleigh fading channel [22]. Previous system models either considered the existence of a single eavesdropper [20] or ignored the antenna correlation [5] in multi-antenna systems. To the authors' knowledge, the effect of the correlation between antennas in the multi-eavesdropper SIMO system on the secrecy performance has not been considered. Therefore, the system model makes a good improvement.

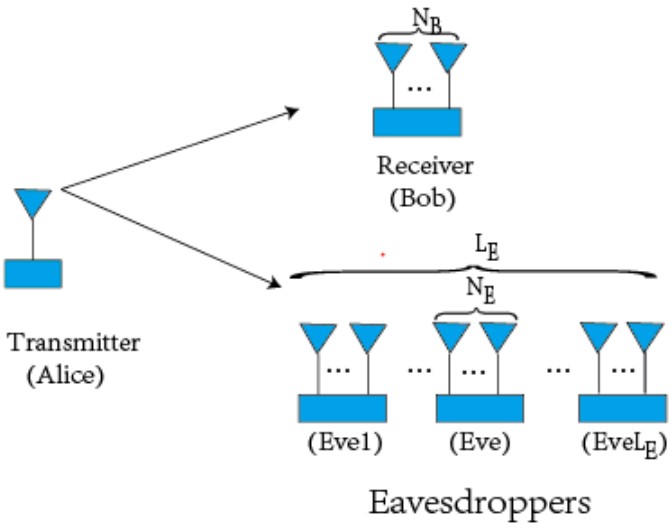

Fig. 1. The model of the system with a transmitter, a receiver and L_E eavesdroppers

To maximize the security risks caused by multiple eavesdroppers on the legitimate communication between Alice and Bob, each eavesdropper should be considered independently. When the eavesdropper with the largest SNR cannot decode the transmitted information, the information will be secure and reliable. For convenience, we refer to the eavesdropper with the largest SNR as Eve. Therefore, on the premise of perfect secrecy [23], the achievable secure transmission rate C_s in the model is given as

$$C_s = \begin{cases} C_B - C_E, & \gamma_B > \gamma_E \\ 0, & \gamma_B \le \gamma_E \end{cases} \tag{1}$$

where γ_B and $\gamma_E = \max\limits_{1\le i\le L_E} \gamma_{E_i}$ denote the instantaneous SNRs of Bob and Eve, respectively. $C_B = \log_2(1+\gamma_B)$ and $C_E = \log_2(1+\gamma_E)$ represent the instantaneous capacity in the main channel (Alice-Bob channel) and eavesdropping channel (Alice-Eve channel), respectively.

According to the feedback CSI from Bob, Alice selects an appropriate coding mode [13] and encodes the transmission information into the code word $\mathbf{x} = [x(1), \cdots x(q), \cdots x(Q)]$ with a given coding rate R_s for secure transmission. The code word is exposed to $\sum_{q=1}^{Q} E\left[\left|x(q)\right|^2\right] \Big/ Q \le P$, where P denotes the maximum transmitted signal power. The information can be transmitted securely only when $R_s < C_s$ [23].

At time q, the received signal vector at Bob can be written as

$$\mathbf{y}(q) = \mathbf{\Phi}_B^{\frac{1}{2}} \mathbf{h}_B x(q) + \mathbf{n}_B \tag{2}$$

Where $\mathbf{\Phi}_B$ denotes $N_B \times N_B$ dimensional antenna correlation matrix of receiver Bob. The b eigenvalues are denoted as $\lambda_1, \lambda_2, \cdots \lambda_b$, respectively, with multiplicities $\delta_1, \delta_2 \cdots \delta_b$, where $\sum_{i=1}^{b} \delta_i = N_B$. $\mathbf{h}_B = \left[h_{1,} \cdots h_{N_b,} \cdots h_{N_B} \right]^T$ and $\mathbf{n}_B$ indicate $N_B \times 1$ dimensional main channel vector and the additive white Gaussian noise (AWGN) with the mean value zero and the variance α_B^2, respectively. The output signal at Bob with MRC scheme can be represented as

$$y(q) = \left\| \mathbf{\Phi}_B^{\frac{1}{2}} \mathbf{h}_B \right\| x(q) + (\mathbf{w}_B)^{\dagger} \mathbf{n}_B \tag{3}$$

where $\mathbf{w}_B = \mathbf{\Phi}_B^{\frac{1}{2}} \mathbf{h}_B \Big/ \left\| \mathbf{\Phi}_B^{\frac{1}{2}} \mathbf{h}_B \right\|$ denotes the weight vector of each branch, and $(\cdot)^{\dagger}$ signifies matrix conjugate transpose. Therefore, the instantaneous SNR at Bob is provided as $\gamma_B = \left\| \mathbf{\Phi}_B^{\frac{1}{2}} \mathbf{h}_B \right\|^2 P \Big/ \alpha_B^2$.

Similar with Bob, at time q, the received signal vector at Eve can be given as

$$z(q) = \left\| \mathbf{\Phi}_E^{\frac{1}{2}} \mathbf{h}_E \right\| x(q) + (\mathbf{w}_E)^{\dagger} \mathbf{n}_E \tag{4}$$

Where $\mathbf{\Phi}_E$ denotes $N_E \times N_E$ dimensional antenna correlation matrix at eavesdropper Eve. The a eigenvalues $\varphi_1, \varphi_2, \cdots \varphi_a$, respectively, with multiplicities $\mu_1, \mu_2 \cdots \mu_a$, where $\sum_{i=1}^{a} \mu_i = N_E$. $\mathbf{h}_E = \left[h_{1,} \cdots h_{m,} \cdots h_{N_E} \right]^T$ and $\mathbf{n}_E$ indicate $N_E \times 1$ dimensional main channel vector and the AWGN with the mean value zero and the variance α_E^2, respectively. $\mathbf{w}_E = \mathbf{\Phi}_E^{\frac{1}{2}} \mathbf{h}_E \Big/ \left\| \mathbf{\Phi}_E^{\frac{1}{2}} \mathbf{h}_E \right\|$ is the weight vector of each branch, and $(\cdot)^{\dagger}$ signifies matrix conjugate transpose. Thus, the instantaneous SNR at Eve is provided by $\gamma_E = \left\| \mathbf{\Phi}_E^{\frac{1}{2}} \mathbf{h}_E \right\|^2 P \Big/ \alpha_E^2$.

3. Secrecy Performance

3.1 SNR Distribution

To accurately study how antenna correlation would affect the secure transmission in SIMO communication system with multiple eavesdroppers, three key secrecy performance

indicators for this system are derived, i.e., the SOP, NZSC and the asymptotic SOP. The cumulative distribution function (CDF) of γ_B can be obtained from [24], which is shown as

$$F_{\gamma_B}(\gamma)=1-\sum_{i=1}^{b}\sum_{j=1}^{\sigma_i}\sum_{k=0}^{j-1}\frac{D_{i,j}}{k!}\left(\frac{\gamma_B}{\lambda_i\bar{\gamma}_B}\right)^k e^{-\frac{\gamma_B}{\lambda_i\bar{\gamma}_B}} \tag{5}$$

where

$$D_{i,j}=\frac{1}{(\sigma_i-j)!}\left(\frac{1}{\lambda_i\bar{\gamma}_B}\right)^{\sigma_i-j}\frac{d^{\sigma_i-j}}{ds^{\sigma_i-j}}\left(\prod_{i'=1,i'\neq i}^{b}(1+s\bar{\gamma}_B\lambda_{i'})^{-\sigma_{i'}}\right)\Bigg|_{s=-\frac{1}{\bar{\gamma}_B\lambda_i}} \tag{6}$$

and $\bar{\gamma}_B=P/\alpha_B^2$.

Since the channels of each eavesdropper obey i.i.d. fading, the probability density function (PDF) of the instantaneous SNR at any eavesdropper can be expressed as [4] [24]

$$f_{\gamma_E}(\gamma)=\sum_{n=1}^{a}\sum_{l=1}^{\mu_n}\frac{A_{n,l}}{\Gamma(l)}\left(\frac{1}{\varphi_n\bar{\gamma}_E}\right)^l\gamma_E{}^{l-1}e^{-\frac{\gamma_E}{\varphi_n\bar{\gamma}_E}} \tag{7}$$

where

$$A_{n,l}=\frac{1}{(\mu_n-l)!}\left(\frac{1}{\varphi_n\bar{\gamma}_E}\right)^{\mu_n-l}\frac{d^{\mu_n-l}}{ds^{\mu_n-l}}\left(\prod_{n'=1,n'\neq n}^{a}(1+s\bar{\gamma}_E\varphi_{n'})^{-\mu_{n'}}\right)\Bigg|_{s=-\frac{1}{\bar{\gamma}_E\varphi_n}} \tag{8}$$

and $\bar{\gamma}_E=P/\alpha_E^2$.

According to [25], the CDF of γ_E at any eavesdropper is achieved as

$$F_{\gamma_E}(\gamma)=1-\sum_{n=1}^{a}\sum_{l=1}^{\mu_n}\sum_{k=0}^{l-1}\frac{A_{n,l}}{k!}\left(\frac{\gamma_E}{\varphi_n\bar{\gamma}_E}\right)^k e^{-\frac{\gamma_E}{\varphi_n\bar{\gamma}_E}} \tag{9}$$

Based on [26], the CDF of γ_E at eavesdropper Eve, the one with the highest instantaneous SNR among all the eavesdroppers, is represented as

$$\hat{F}_{\gamma_E}(\gamma)=[F_{\gamma_E}(\gamma)]^{L_E} \tag{10}$$

Then, the PDF of γ_E at eavesdropper Eve is formulated as

$$\begin{aligned}\hat{f}_{\gamma_E}(\gamma) &= L_E F_{\gamma_E}^{L_E-1} f_{\gamma_E} \\ &= L_E\left[1-\sum_{q=1}^{L_E-1}\binom{L_E-1}{q}(-1)^{q-1}\sum_{n=1}^{a}\sum_{l=1}^{\mu_n}\sum_{k=0}^{l-1}\sum_{S_t\in\mathbf{S}}\frac{q!}{\prod_{t=1}^{J}s_t!}\right. \\ &\left.\times\prod_{1\le t\le J}\left(\frac{A_{n,l}}{k!}\right)^{s_t}\left(\frac{\gamma_E}{\varphi_n\bar{\gamma}_E}\right)^{ks_t}e^{-\frac{\gamma_E s_t}{\varphi_n\bar{\gamma}_E}}\right] \\ &\times\sum_{n=1}^{a}\sum_{l=1}^{\mu_n}\frac{A_{n,l}}{\Gamma(l)}\left(\frac{1}{\varphi_n\bar{\gamma}_E}\right)^{l}\gamma_E{}^{l-1}e^{-\frac{\gamma_E}{\varphi_n\bar{\gamma}_E}}\end{aligned} \tag{11}$$

where $J=\sum_{n=1}^{a}\sum_{l=1}^{\mu_n}l$ and $S=\left\{\mathbf{S}_t\,|\,\sum_{t=1}^{J}\mathbf{s}_t=q\right\}$.

3.2 Secrecy performance

According to [19] [20], the SOP of the typical wiretap system is defined as

$$\begin{aligned}P_{out}(R_S) &= P_r(C_S<R_S\,|\,\gamma_B>\gamma_E)+P_r(\gamma_B<\gamma_E) \\ &= \int_0^{\infty}\int_{\gamma_E}^{2^{R_S(1+\gamma_E)}-1} f_{\gamma_E}(\gamma_E)\,f_{\gamma_B}(\gamma_B)d_{\gamma_B}d_{\gamma_E} \\ &+\int_0^{\infty}\int_0^{\gamma_E} f_{\gamma_E}(\gamma_E)\,f_{\gamma_B}(\gamma_B)d_{\gamma_B}d_{\gamma_E} \\ &= \int_0^{\infty} f_{\gamma_E}(\gamma_E)F_{\gamma_B}(2^{R_S}(1+\gamma_E)-1)d_{\gamma_E}\end{aligned} \tag{12}$$

where $R_s>0$. Therefore, the SOP of our system discussed can be rewritten by replacing (12) as

$$P_{out}\left(R_s\right)=\int_0^{\infty}\hat{f}_{\gamma_E}F_{\gamma_B}\left(2^{R_s}\left(1+\gamma_E\right)-1\right)d\gamma_E \tag{13}$$

Substituting (5) and (11) into (13) and making some basic mathematical operations, the new closed-form expression of the SOP is formulated as (14)

$$
\begin{aligned}
P_{out}(R_s) = L_E \Bigg\{ & 1 - \sum_{i=1}^{b} \sum_{j=1}^{\sigma_i} \sum_{k=0}^{j-1} \frac{D_{i,j}}{k!} \left(\frac{1}{\bar{\lambda}_i \bar{\gamma}_B} \right)^k e^{-\frac{2^{R_s}-1}{\bar{\lambda}_i \bar{\gamma}_B}} \sum_{p=0}^{k} \binom{k}{p} (2^{R_s}-1)^{k-p} 2^{R_s p} \\
& \times \sum_{n=1}^{a} \sum_{l=1}^{\mu_n} \frac{A_{n,l}}{\Gamma(l)} \left(\frac{1}{\bar{\varphi}_n \bar{\gamma}_E} \right)^l \Gamma(p+l) \left(\frac{2^{R_s}}{\bar{\lambda}_i \bar{\gamma}_B} + \frac{1}{\bar{\varphi}_n \bar{\gamma}_E} \right)^{-(p+l)} \\
& - \sum_{q=1}^{L_E-1} \binom{L_E-1}{q} (-1)^{q-1} \sum_{n=1}^{a} \sum_{l=1}^{\mu_n} \sum_{k=0}^{l-1} \sum_{S_t \in \mathbf{S}} \frac{q!}{\prod_{t=1}^{J} s_t!} \\
& \times \prod_{1 \le t \le J} \left(\frac{A_{n,l}}{k!} \right)^{s_t} \left(\frac{1}{\bar{\varphi}_n \bar{\gamma}_E} \right)^{k s_t} \Bigg[\sum_{u=1}^{e} \sum_{v=1}^{\varepsilon_u} \frac{A_{u,v}}{\Gamma(v)} \left(\frac{1}{\bar{\phi}_u \bar{\gamma}_E} \right)^v \\
& \times \Gamma(k s_t + v) \left(\frac{s_t}{\bar{\varphi}_n \bar{\gamma}_E} + \frac{1}{\bar{\phi}_u \bar{\gamma}_E} \right)^{-(k s_t + v)} - \sum_{u=1}^{e} \sum_{v=1}^{\varepsilon_u} \frac{A_{u,v}}{\Gamma(v)} \left(\frac{1}{\bar{\phi}_u \bar{\gamma}_E} \right)^v \\
& \times \sum_{i=1}^{b} \sum_{j=1}^{\sigma_i} \sum_{f=0}^{j-1} \frac{D_{i,j}}{f!} \left(\frac{1}{\bar{\lambda}_i \bar{\gamma}_B} \right)^f e^{-\frac{2^{R_s}-1}{\bar{\lambda}_i \bar{\gamma}_B}} \sum_{p=0}^{f} \binom{f}{p} (2^{R_s}-1)^{f-p} 2^{R_s p} \\
& \times \Gamma(k s_t + v + p) \left(\frac{s_t}{\bar{\varphi}_n \bar{\gamma}_E} + \frac{1}{\bar{\phi}_u \bar{\gamma}_E} + \frac{2^{R_s}}{\bar{\lambda}_i \bar{\gamma}_B} \right)^{-(k s_t + v + p)} \Bigg] \Bigg\}
\end{aligned} \tag{14}
$$

where $e = a$, $u = n = 1, \cdots, a$, $\varepsilon_u = \mu_n$, $v = l = 1, \cdots, \mu_n$, $\phi_u = \varphi_n$, and $A_{u,v} = A_{n,l}$. By definition, the closed-form expression of NZSC is obtained by $1 - P_{out}(R_s = 0)$. For our system, a new closed-form expression of NZSC can be achieved as

$$
\begin{aligned}
P_r\left(C_s > 0\right) = 1 - P_{out}(0) = 1 - L_E \Bigg\{ & 1 - \sum_{i=1}^{b} \sum_{j=1}^{\sigma_i} \sum_{k=0}^{j-1} \frac{D_{i,j}}{k!} \left(\frac{1}{\bar{\lambda}_i \bar{\gamma}_B} \right)^k \\
& \times \sum_{n=1}^{a} \sum_{l=1}^{\mu_n} \frac{A_{n,l}}{\Gamma(l)} \left(\frac{1}{\bar{\varphi}_n \bar{\gamma}_E} \right)^l \Gamma(k+l) \left(\frac{1}{\bar{\lambda}_i \bar{\gamma}_B} + \frac{1}{\bar{\varphi}_n \bar{\gamma}_E} \right)^{-(k+l)} \\
& - \sum_{q=1}^{L_E-1} \binom{L_E-1}{q} (-1)^{q-1} \sum_{n=1}^{a} \sum_{l=1}^{\mu_n} \sum_{k=0}^{l-1} \sum_{S_t \in \mathbf{S}} \frac{q!}{\prod_{t=1}^{J} s_t!} \prod_{1 \le t \le J} \left(\frac{A_{n,l}}{k!} \right)^{s_t} \left(\frac{1}{\bar{\varphi}_n \bar{\gamma}_E} \right)^{k s_t} \\
& \times \Bigg[\sum_{u=1}^{e} \sum_{v=1}^{\varepsilon_u} \frac{A_{u,v}}{\Gamma(v)} \left(\frac{1}{\bar{\phi}_u \bar{\gamma}_E} \right)^v \Gamma(k s_t + v) \left(\frac{s_t}{\bar{\varphi}_n \bar{\gamma}_E} + \frac{1}{\bar{\phi}_u \bar{\gamma}_E} \right)^{-(k s_t + v)} \\
& - \sum_{u=1}^{e} \sum_{v=1}^{\varepsilon_u} \frac{A_{u,v}}{\Gamma(v)} \left(\frac{1}{\bar{\phi}_u \bar{\gamma}_E} \right)^v \sum_{i=1}^{b} \sum_{j=1}^{\sigma_i} \sum_{f=0}^{j-1} \frac{D_{i,j}}{f!} \left(\frac{1}{\bar{\lambda}_i \bar{\gamma}_B} \right)^f \\
& \times \Gamma(k s_t + v + f) \left(\frac{s_t}{\bar{\varphi}_n \bar{\gamma}_E} + \frac{1}{\bar{\phi}_u \bar{\gamma}_E} + \frac{1}{\bar{\lambda}_i \bar{\gamma}_B} \right)^{-(k s_t + v + f)} \Bigg] \Bigg\}
\end{aligned} \tag{15}
$$

To practically explore the impact of sufficiently high SNR in the main channel on the system, it is essential to analyze the asymptotic SOP which contributes to inspect the diversity order and array gain. With the aid of [25, Eq. (1.211.1)], the first nonzero order extension of $F_{\gamma_B}(\gamma)$ is formulated as

$$F_{\gamma_B}^{\infty}(\gamma)=\left(\sum_{i=1}^{b}\sum_{j=1}^{\sigma_i}\sum_{k=0}^{j-1}\frac{(-1)^{N_B-k+1}D_{i,j}}{(N_B-k)!k!\lambda_i^{N_B}}\right)\left(\frac{\gamma_B}{\bar{\gamma}_B}\right)^{N_B}+o\left(\bar{\gamma}_B^{-N_B}\right) \tag{16}$$

Substituting (11) and (16) into (13), according to combining [25. Eq. (3.326.2)], $P_{out}^{\infty}(R_s)$ is derived as

$$P_{out}^{\infty}(R_s)=(G_a\bar{\gamma}_B)^{-G_d}+o(\bar{\gamma}_B^{-G_d}) \tag{17}$$

where $G_d=N_B$ denotes the diversity order, and G_a as shown in (18) denotes the array gain.

$$\begin{aligned}G_a=\frac{1}{(2^{R_S}-1)}\Bigg[&L_E\sum_{i=1}^{b}\sum_{j=1}^{\sigma_i}\sum_{k=0}^{j-1}\frac{(-1)^{N_B-k+1}D_{i,j}}{(N_B-k)!k!\lambda_i^{N_B}}\times\sum_{n=1}^{a}\sum_{l=1}^{\mu_n}\frac{A_{n,l}}{\Gamma(l)}\left(\frac{1}{\varphi_n\bar{\gamma}_E}\right)^{l}\\&\times\sum_{p=0}^{N_B}\binom{N_B}{p}\left(\frac{2^{R_s}}{2^{R_s}-1}\right)^{p}\left(\Gamma(p+l)\left(\frac{1}{\varphi_n\bar{\gamma}_E}\right)^{-(p+l)}-\sum_{q=1}^{L_E-1}\binom{L_E-1}{q}(-1)^{q-1}\right.\\&\left.\times\sum_{u=1}^{a}\sum_{v=1}^{\varepsilon_u}\sum_{f=0}^{v-1}\sum_{S_t\in\mathbf{S}}\frac{q!}{\prod_{t=1}^{J}s_t!}\prod_{1\le t\le J}\left(\frac{A_{u,v}}{f!}\right)^{s_t}\left(\frac{1}{\phi_u\bar{\gamma}_E}\right)^{ks_t}\Gamma(fs_t+l+p)\right.\\&\left.\times\left(\frac{s_t}{\phi_u\bar{\gamma}_E}+\frac{1}{\varphi_n\bar{\gamma}_E}\right)^{-(fs_t+l+p)}\right)\Bigg]^{-\frac{1}{N_B}}\end{aligned} \tag{18}$$

Note that our new CFEs of the SOP in (14), NZSC in (15) and the asymptotic SOP in (17) apply to arbitrary number of antennas at receiver and each eavesdropper, arbitrary average SNR, arbitrary numbers of eavesdroppers and arbitrary antenna correlation. After analysis, we find that the correlation coefficient at Bob and Eve as well as the total number of eavesdroppers have no effect on diversity order but affect array gain. What's more, the larger correlation coefficient or the more number of eavesdroppers lead to the smaller array gain and the higher SOP when average SNR in main channel is sufficiently high.

3.3 Uniform Antenna Correlation

Due to the limited physical size at terminal device, uniform antenna correlation caused by close arrangement exists in many practical environments [27, 28]. Resorting to [21], the uniform correlation matrix $\mathbf{\Phi}_B=(1-\rho_B)\mathbf{E}+\rho_B\mathbf{I}$ at Bob has two real eigenvalues, i.e., $\lambda_1=1+\rho_B(N_B-1)$ and $\lambda_2=1-\rho_B$ with multiplicities $\delta_1=1$ and $\delta_2=N_B-1$, respectively. As such, the uniform correlation matrix $\mathbf{\Phi}_E=(1-\rho_E)\mathbf{E}+\rho_E\mathbf{I}$ at Eve has two real eigenvalues, i.e., $\varphi_1=1+\rho_E(N_E-1)$ and $\varphi_2=1-\rho_E$ with multiplicities $\mu_1=1$

and $\mu_2 = N_E - 1$, respectively, where both $\mathbf{I}$ and $\mathbf{E}$ denote a matrix with its all elements equally to be 1, namely identity matrix. ρ_B and ρ_E denote antenna correlation coefficient at Bob and Eve, respectively. Therefore, the expressions in (6) and (8) can be respectively simplified as

$$D_{i,j} = \frac{1}{(\sigma_i - j)!}\left(\frac{1}{\lambda_i \bar{\gamma}_B}\right)^{\sigma_i - j} \frac{d^{\sigma_i - j}}{ds^{\sigma_i - j}}\left(1 + s\bar{\gamma}_B \lambda_{i'}\right)^{-\sigma_{i'}}\Big|_{s=-\frac{1}{\bar{\gamma}_B \lambda_i}} \tag{19}$$

and

$$A_{n,l} = \frac{1}{(\mu_n - l)!}\left(\frac{1}{\varphi_n \bar{\gamma}_E}\right)^{\mu_n - l} \frac{d^{\mu_n - l}}{ds^{\mu_n - l}}\left(1 + s\bar{\gamma}_E \varphi_{n'}\right)^{-\mu_{n'}}\Big|_{s=-\frac{1}{\bar{\gamma}_E \varphi_n}} \tag{20}$$

Substituting (19) and (20) into (14), (15) and (17), the new CFZs of the SOP, NZSC and the asymptotic SOP with uniform antenna correlation and multiple eavesdroppers can be obtained.

4. Numerical Results and Analysis

In this section, Monte Carlo simulations and numerical results related to our obtained theoretical expressions are demonstrated to verify the impact of antenna correlation and the number of eavesdroppers on the system secrecy performance.

4.1 The impact of N_B, L_E and ρ on the SOP and the asymptotic SOP

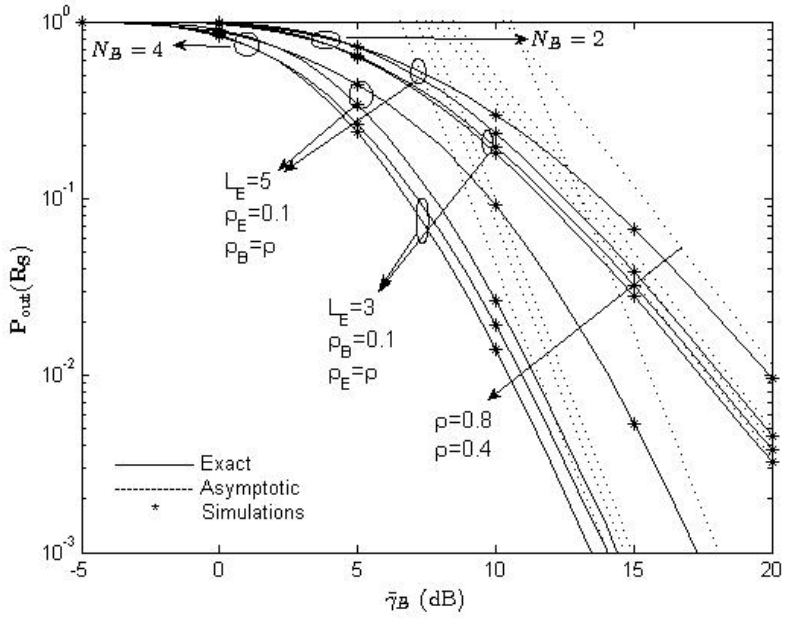

Fig. 2. The SOP and the asymptotic SOP versus $\bar{\gamma}_B$ for different N_B and L_E with uniform correlation

Fig. 2 illustrates the SOP and asymptotic SOP versus $\bar{\gamma}_B$ under $N_A = 1$, $\bar{\gamma}_E = 0\text{dB}$, $N_E = 2$, and $R_s = 1$ for different N_B, L_E and antenna correlation coefficient ρ. The exact numerical results can be obtained from the formula (14) and (17). It is clear that higher N_B or lower L_E consequently leads to lower SOP. This result is consistent with the conclusion of [13]. Moreover, the phenomenon that more eavesdroppers will lead to greater potential threat is verified. We also observe that the slope of the asymptotic curve increases with increasing N_B while it is not affected by L_E and ρ, which indicates that the diversity order has no relationship with ρ but is related to N_B, and this conclusion corresponds to that in [20]. However, the finding that the diversity order is independent of L_E has not been involved in previous literatures. Furthermore, we find that increasing N_B can obviously reduce the SOP, which shows that increasing diversity order at receiver can effectively improve the secrecy performance of the system. In addition, the correlation coefficient of the receiver and eavesdroppers can weaken the secrecy performance of the system when $\bar{\gamma}_B$ is in the high region. However, the stronger antenna correlation at receiver leads to a greater risk to the system.

4.2 The impact of $\bar{\gamma}_E$, N_E and ρ on the SOP and the asymptotic SOP

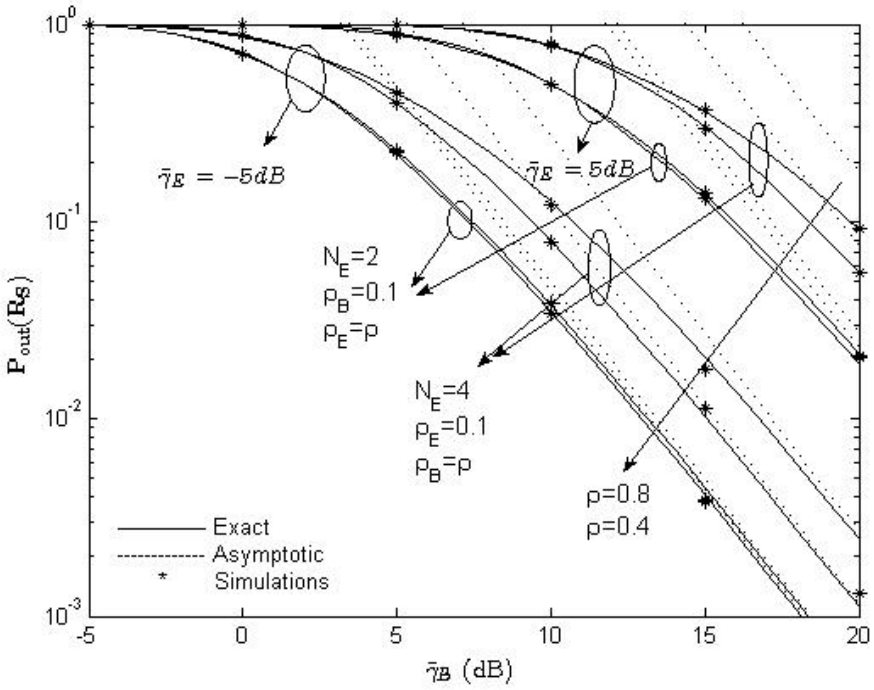

Fig. 3. The SOP and the asymptotic SOP versus $\bar{\gamma}_B$ for different N_E and $\bar{\gamma}_E$ with uniform correlation

Fig. 3 presents the impact of different $\bar{\gamma}_E$, N_E and antenna correlation coefficient ρ on the secrecy performance when $N_A = 1, N_B = 2$, $R_s = 1$ and $L_E = 2$. We can evidently note that the numerical results are in good agreement with the Monte Carlo simulation. We also observe that the outage probability increases with increasing $\bar{\gamma}_E$ and N_E. This conclusion is consistent with [15], i.e., a growing number of N_E does not help improve system security in massive MIMO systems for 5G wireless technology. Notably, the asymptotic curves are parallel, which indicates that the diversity order has nothing to do with $\bar{\gamma}_E$, N_E and ρ while the array gain is related to each of them. For example, a gain at $\rho = 0.4$ is about $2.5dB$ larger than that at $\rho = 0.8$ for $P_{out}(R_s) = 10^{-2}$ with $\bar{\gamma}_E = -5dB$ and $N_E = 4$.

4.3 The impact of L_E and ρ on NZSC

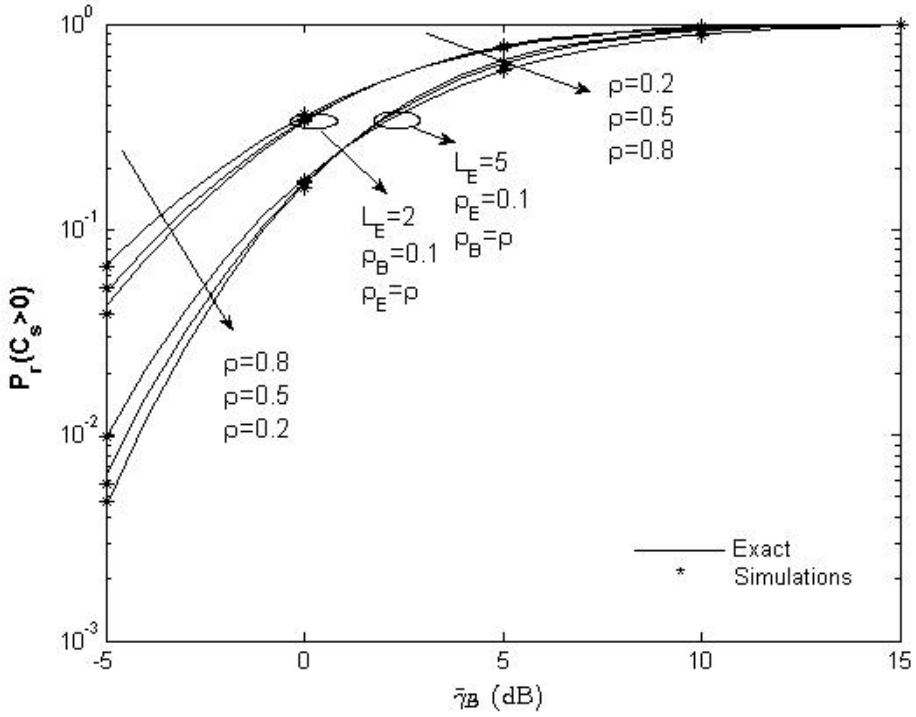

Fig. 4. NZSC versus $\bar{\gamma}_B$ for different L_E and ρ with uniform correlation

As we can see in **Fig. 4**, NZSC decreases with increasing L_E under the condition of $\bar{\gamma}_E = 0dB$, $N_A = 1$, $N_B = N_E = 2$ and $R_s = 0$. In addition, we can observe that NZSC decreases with increasing ρ when $\bar{\gamma}_B$ is in a higher SNR region compared with $\bar{\gamma}_E = 0dB$, which indicates that the antenna correlation at receiver and eavesdroppers is harmful to the secrecy performance of the system in such a case. However, NZSC increases

with increasing ρ when the SNR of $\overline{\gamma}_B$ is low, which indicates that the antenna correlation at receiver and eavesdroppers is beneficial to the secrecy performance of the system in such a case. This case can be explained as that when $\overline{\gamma}_B$ is smaller, the increase of correlation coefficient reduces the effective dimension of the antenna array, so that Bob's power is more concentrated. At this time, the effective dimension of Eve plays a major role, leading the quality of the main channel increases while that of the eavesdropping channel decreases. When $\overline{\gamma}_B$ is larger, the increase of correlation coefficient reduces the effective dimension of antenna and makes Eve's power more concentrated. At this time, the effective dimension of Bob plays a major role, so the quality of eavesdropping channel increases and that of main channel decreases.

5. Conclusion

We evaluated the impact of antenna correlation on the secure transmission performance in the SIMO communication system with multiple eavesdroppers, and the new CFEs of the SOP and NZSC were derived, which can be applied to arbitrary number of antennas at receiver and each eavesdropper, arbitrary average SNR, arbitrary number of eavesdroppers and arbitrary antenna correlation. Based on the high SN in many practical communication scenarios, the new CFE of asymptotic SOP was achieved to show the diversity order and array gain of the investigated system. Moreover, the uniform antenna correlation is analyzed as a special case. The analysis result of the derived theoretical expressions show that more eavesdroppers, more antennas at each eavesdropper, and higher average SNR of the eavesdropping channel will lead to a greater detriment to the secrecy performance. However, mroe antennas at receiver can reduce the defect. In particular, the asymptotic SOP illustrates that the diversity order is N_B, which is independent of ρ, L_E, N_E and $\overline{\gamma}_E$ while all of them affect the array gain. In addition, the larger antenna correlation coefficient at receiver and eavesdropper is more detrimental to the system when $\overline{\gamma}_B$ is at high level and more beneficial to the system when $\overline{\gamma}_B$ is at low level. Therefore, the antenna correlation at the receiver can be adjusted to improve the secrecy performance of the system in the practical passive eavesdropping communication scenario. For example, the antenna correlation at receiver can be increased when $\overline{\gamma}_B$ is small, and the antenna correlation at receiver can be reduced when $\overline{\gamma}_B$ is high.

References

[1] H. V. Poor, “Information and inference in the wireless physical layer,” *IEEE Wireless Communications*, vol. 19, no. 1, pp. 40-47, February 2012. Article (CrossRef Link).

[2] C. E. Shannon, “Communication theory of secrecy systems,” *Bell Syst.Techn. J*, vol. 28, no. 4, pp. 656-715, 1949. Article (CrossRef Link).

[3] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J*, vol. 54, no. 8, pp.1355-1387, Oct. 1975. Article (CrossRef Link).

[4] A. P. Shrestha, J. Jung and K. S. Kwak, "Secure wireless multicasting in presence of multiple eavesdroppers," in *Proc. of 2013 13th International Symposium on Communications and Information Technologies (ISCIT)*, Surat Thani, pp. 814-817, 2013. Article (CrossRef Link).

[5] J. Zhu, Y. Chen, Y. Nakamura, X. Jiang, O. Takahashi and N. Shiratori, "Outage performance of secure multicasting in the presence of multiple eavesdroppers," in *Proc. of 2015 Eighth International Conference on Mobile Computing and Ubiquitous Networking (ICMU), Hakodate*, pp. 138-142, 2015. Article (CrossRef Link).
[6] M. Z. I. Sarkar and T. Ratnarajah, "Information-theoretic security in wireless multicasting," *International Conference on Electrical & Computer Engineering (ICECE 2010), Dhaka*, 2010, pp. 53-56. Article (CrossRef Link).
[7] F. He, H. Man and W. Wang, "Maximal Ratio Diversity Combining Enhanced Security," *IEEE Communications Letters*, vol. 15, no. 5, pp. 509-511, May 2011. Article (CrossRef Link).
[8] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang and H. H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66-74, April 2011. Article (CrossRef Link).
[9] G. Prema and R. Sowmini, "Secrecy rate evaluation of wireless channel in the presence of eavesdroppers," in *Proc. of 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore*, pp. 1-5, 2015. Article (CrossRef Link).
[10] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober and J. Yuan, "MIMO Wiretap Channels: Secure Transmission Using Transmit Antenna Selection and Receive Generalized Selection Combining," *IEEE Communications Letters*, vol. 17, no. 9, pp. 1754-1757, September 2013. Article (CrossRef Link).
[11] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober and I. B. Collings, "Transmit Antenna Selection for Security Enhancement in MIMO Wiretap Channels," *IEEE Transactions on Communications*, vol. 61, no. 1, pp. 144-154, January 2013. Article (CrossRef Link).
[12] J. Xiong, Y. Tang, D. Ma, P. Xiao and K. K. Wong, "Secrecy Performance Analysis for TAS-MRC System With Imperfect Feedback," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1617-1629, Aug. 2015. Article (CrossRef Link).
[13] Y. Huang, F. S. Al-Qahtani, T. Q. Duong and J. Wang, "Secure Transmission in MIMO Wiretap Channels Using General-Order Transmit Antenna Selection With Outdated CSI," *IEEE Transactions on Communications*, vol. 63, no. 8, pp. 2959-2971, Aug. 2015. Article (CrossRef Link).
[14] T. Yang, R. Zhang, X. Cheng and L. Yang, "Secure Massive MIMO Under Imperfect CSI: Performance Analysis and Channel Prediction," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1610-1623, 2019. Article (CrossRef Link).
[15] D. Hu, W. Zhang, L. He and J. Wu, "Secure Transmission in Multi-cell Multi-user Massive MIMO Systems with an Active Eavesdropper," *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 85-88, 2019. Article (CrossRef Link).
[16] R. H. Y. Louie, Y. Li, H. A. Suraweera and B. Vucetic, "Performance analysis of beamforming in two hop amplify and forward relay networks with antenna correlation," *IEEE Transactions on Wireless Communications*, vol. 8, no. 6, pp. 3132-3141, June 2009. Article (CrossRef Link).
[17] J. Jiao, G. Sun, Z. Han and Z. Wang, "Exact Physical Layer Security in SIMO Wiretap Channels with Antenna Correlation," in *Proc. of 2015 11th International Conference on Computational Intelligence and Security (CIS), Shenzhen*, pp. 416-419, 2015. Article (CrossRef Link).
[18] M. Z. I. Sarkar and T. Ratnarajah, "Enhancing Security in Correlated Channel With Maximal Ratio Combining Diversity," *IEEE Transactions on Signal Processing*, vol. 60, no. 12, pp. 6745-6751, Dec. 2012. Article (CrossRef Link).
[19] N. Yang, H. A. Suraweera, I. B. Collings and C. Yuen, "Physical Layer Security of TAS/MRC With Antenna Correlation," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 254-259, Jan. 2013. Article (CrossRef Link).
[20] G. Sun, Z. Han, J. Jiao, Z. Wang and D. Wang, "Physical layer security in MIMO wiretap channels with antenna correlation," *China Communications*, vol. 14, no. 8, pp. 149-156, Aug. 2017. Article (CrossRef Link).
[21] R. K. Mallik, "The Uniform Correlation Matrix and its Application to Diversity," *IEEE Transactions on Wireless Communications*, vol. 6, no. 5, pp. 1619-1625, May 2007. Article (CrossRef Link).

[22] M. K. Simon , M.-S. Alouini, *Digital Communication over Fading Channels, 2nd ed*, Wiley, New York, 2005. Article (CrossRef Link).
[23] M. Bloch, J. Barros, M. R. D. Rodrigues and S. W. McLaughlin, "Wireless Information-Theoretic Security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515-2534, June 2008. Article (CrossRef Link).
[24] P. Lombardo, G. Fedele and M. M. Rao, "MRC performance for binary signals in Nakagami fading with general branch correlation," *IEEE Transactions on Communications*, vol. 47, no. 1, pp. 44-52, Jan 1999. Article (CrossRef Link).
[25] I. S. Gradshteyn, I. M. Ryzhik, *Table of Integrals, Series and Products, 7th ed.*, Academic, San Diego, CA, USA, 2007.
[26] H. A. David and H. N. Nagaraja, *Order Statistics, 3rd ed. Hoboken*, John Wiley and Sons, Inc., New Jersey, 2005.
[27] M. S. Alouini, A. Abdi and M. Kaveh, "Sum of gamma variates and performance of wireless communication systems over Nakagami-fading channels," *IEEE Transactions on Vehicular Technology*, vol. 50, no. 6, pp. 1471-1480, Nov 2001. Article (CrossRef Link).
[28] H. Bolcskei, M. Borgmann and A. J. Paulraj, "Impact of the propagation environment on the performance of space-frequency coded MIMO-OFDM," *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 3, pp. 427-439, Apr 2003. Article (CrossRef Link)

Gangcan Sun received his Ph.D. degree in Communication and Information System from Beijing Institute of Technology, China, in 2009. He was promoted to an associate professor in School of Information Engineering, Zhengzhou University, China, in 2013. His current research interests include communication signal processing, communication modulation recognition and blind estimation of key parameters of communication signals.

Mengge Liu received the Bachelor's degree in North China University of Water Resources and Electric Power, Henan, China, in 2016. Since 2017, she has been pursuing towards the Master's degree in Information and Communication Engineering, Industrial Technology Research Institute, Zhengzhou University.

Zhuo Han received the Master's degree in Information and Communication Engineering, from Zhengzhou University, Henan, China, in 2017. Since 2018, she has been pursuing towards the Ph.D. degree in Information and Communication Engineering, Industrial Technology Research Institute, Zhengzhou University.

Chuanyong Zhao received the Bachelor's degree in Qingdao University of Technology, Shandong, China, in 2017. Since 2018, he has been pursuing towards the Master's degree in Information and Communication Engineering, Industrial Technology Research Institute, Zhengzhou University.