On Secrecy Performance of Antenna-Selection-Aided MIMO Systems Against Eavesdropping

Jia Zhu, Yulong Zou, *Senior Member, IEEE*, Gongpu Wang, Yu-Dong Yao, *Fellow, IEEE*, and George K. Karagiannidis, *Fellow, IEEE*

Abstract—In this paper, we consider a multiple-input–multiple-output (MIMO) system consisting of one source, one destination, and one eavesdropper, where each node is equipped with an arbitrary number of antennas. To improve the security of source–destination transmissions, we investigate the antenna selection at the source and propose the optimal antenna selection (OAS) and suboptimal antenna selection (SAS) schemes, depending on whether the source node has the global channel state information (CSI) of both the main link (from source to destination) and the wiretap link (from source to eavesdropper). Moreover, the traditional space–time transmission (STT) is studied as a benchmark. We evaluate the secrecy performance of STT, SAS, and OAS schemes in terms of the probability of zero secrecy capacity. Furthermore, we examine the generalized secrecy diversity of the STT, SAS, and OAS schemes through an asymptotic analysis of the probability of zero secrecy capacity as the ratio between the average gains of the main and wiretap channels tends to infinity. This is different from the conventional secrecy diversity that assumes an infinite signal-to-noise ratio (SNR) received at the destination under the condition that the eavesdropper has a finite received SNR. It is shown that the generalized secrecy diversity orders of the STT, SAS, and OAS schemes are the product of the number of antennas at source and destination. Additionally, numerical results show that the proposed OAS scheme strictly outperforms both the STT and the SAS schemes in terms of the probability of zero secrecy capacity.

Index Terms—Antenna selection, eavesdropping attack, multiple-input multiple-output (MIMO), secrecy diversity, space–time code.

I. INTRODUCTION

DUE to the broadcast nature of wireless medium, the radio signal of a source node can be overheard by any unauthorized user within its transmit coverage, which makes the wireless communications vulnerable to eavesdropping attacks. To achieve secure wireless transmissions, cryptographic techniques have been widely used to ensure that the confidential information can be decoded by the legitimate receiver only while preventing an eavesdropper from the interception. In addition to the conventional cryptographic techniques, physical-layer security is now emerging as a new secure communication paradigm by exploiting the physical characteristics of wireless channels to prevent the eavesdropper from intercepting the information exchange between legitimate users.

The study on physical-layer security was pioneered by Shannon [1] and later extended by Wyner [2], where an information-theoretic framework has been established by developing achievable secrecy rates for a classical three-node scenario consisting of a source, a destination, and an eavesdropper. More specifically, Wyner showed that when the main channel spanning from a source to a destination has a better conditional than the wiretap channel from a source to an eavesdropper, there exists a positive rate at which the source and destination can communicate reliably and securely. In [3], Wyner's results were further extended to the Gaussian wiretap channel, where the secrecy capacity is shown as the difference between the capacity of the main channel and that of the wiretap channel.

A. Related Literature

It is known that the wireless capacity is severely degraded due to the channel fading effect. To this end, multiple-input–multiple-output (MIMO) was proposed as an effective means to combat wireless fading and improve channel capacity [4], [5], which also has great potential to increase the secrecy capacity of wireless transmissions and enhance the wireless physical-layer security. In [6] and [7], the secrecy capacity of multiple-input–single-output (MISO) wiretap channel was examined and characterized in terms of generalized eigenvalues. In [8], Khisti *et al.* studied the maximal achievable rates of MIMO wiretap channel and proposed a generalized singular

J. Zhu and Y. Zou are with the School of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing, 210003, China (e-mail: jiazhu@njupt.edu.cn; yulong.zou@njupt.edu.cn).

G. Wang is with the School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China (e-mail: gpwang@bjtu.edu.cn).

Y.-D. Yao is with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ 07030-5991 USA (e-mail: yyao@stevens.edu).

G. K. Karagiannidis is with the Department Electrical and Computer Engineering, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece, and also with Khalifa University, Abu Dhabi, United Arab Emirates (e-mail: geokarag@auth.gr).

value decomposition (GSVD) scheme to achieve the secrecy capacity. In [9], the MIMO broadcast wiretap channel was investigated from an information-theoretic perspective in terms of the secrecy capacity. Furthermore, in [10]–[12], the secrecy capacity of wiretap channel in wireless fading environments was examined and evaluated by using optimal power and rate allocation strategies. In addition, user cooperation [13]–[15] as virtual MIMO by allowing users to share each other's antennas was shown in [16] and [17] to improve the wireless secrecy capacity. For example, in [18], we studied cooperative relay selection for securing wireless communications and demonstrated that the wireless physical-layer security significantly improves with an increasing number of relays. In [19] and [20], multiuser scheduling was shown as a promising approach to protect cognitive radio networks against eavesdropping.

Recently, extensive efforts have been devoted to the research of transmit antenna selection for the wireless physical-layer security. In [21], Alves *et al.* explored the transmit antenna selection for a MISO communication system consisting of a multiple-antenna transmitter and a single-antenna receiver in the presence of a multiple-antenna eavesdropper. It was shown in [21] that the transmit antenna selection considerably enhances the wireless security in terms of secrecy outage probability. Later on, the antenna selection work of [21] was further extended in [22] and [23] to a MIMO communication system comprised of a source, a destination, and an eavesdropper, each equipped with multiple antennas. Closed-form expressions of the secrecy outage probability were derived in [22] and [23] for the transmit-antenna-selection-assisted MIMO communications in fading environments. In [24], the impact of outdated channel state information (CSI) on the transmit antenna selection was examined for a MISO system, showing that the secrecy outage performance expectedly degrades when the CSI obtained at the transmitter is outdated due to the CSI feedback delay.

It is worth mentioning that all the aforementioned studies [21]–[24] assume only the CSI of the main channel available at the transmitter without knowing the eavesdropper's CSI knowledge. The transmit antenna selection with the global CSI of both the main channel and the wiretap channel was analyzed in [25], which, however, is limited to the performance evaluation of a simple MISO system only in terms of the average secrecy rate. The performance of optimal antenna selection (OAS) with the global CSI knowledge remains unknown for MIMO communication systems, which will provide a theoretical upper bound as a guide for developing new approaches to defend against eavesdropping attacks. Additionally, in existing literature (e.g., [22], [23], [26], and [28]), the secrecy diversity was established and analyzed by assuming that the average received signal-to-noise ratio (SNR) at the destination tends to infinity, whereas the eavesdropper's received SNR is finite. As an alternative, we presented a generalized secrecy diversity definition in [18]–[20] for characterizing an asymptotic behavior on the secrecy performance as the ratio between the average gains of the main channel and the eavesdropper's wiretap channel approaches infinity, i.e., the main-to-eavesdropper (MER) ratio. To the best of our knowledge, it is still an open issue to examine our generalized secrecy diversity for the transmit-

antenna-selection-assisted MIMO communications in the face of an eavesdropper.

B. Motivation and Contribution

As stated previously, no previous work addresses the OAS with the global CSI knowledge of both the main channel and the wiretap channel for MIMO communication systems, where the source, destination, and eavesdropper are equipped with an arbitrary number of antennas. It has been shown in [3] and [9] that the secrecy capacity of MIMO communications is given by the difference between the capacity of the main channel and that of the wiretap channel. To be specific, when the main channel has a better quality than the wiretap channel, a positive secrecy capacity is achieved, and the source can transmit at a nonzero rate to the destination reliably and securely. However, if the main channel is a degraded version of the wiretap channel, then the secrecy capacity becomes zero, and an event of zero secrecy capacity occurs. In this case, the source and destination cannot transmit reliably and securely, which is referred to as an intercept event in [18]. This paper is focused on deriving analytical expressions of the probability of zero secrecy capacity for transmit-antenna-selection-aided MIMO communications in Rayleigh fading environments. Moreover, we examine the generalized secrecy diversity [18]–[20] for MIMO communications through an asymptotic analysis of the probability of zero secrecy capacity in the high MER region, which provides a useful insight into the effect of the number of antennas on wireless security against eavesdropping. The main contributions of this paper are summarized as follows.

- We explore the transmit antenna selection for physical-layer security of a MIMO system consisting of one source and one destination in the presence of an eavesdropper, where each node is equipped with an arbitrary number of antennas. The OAS and SAS schemes are proposed to improve the security of source–destination transmissions against the eavesdropper. Specifically, in the OAS scheme, the source is assumed to have the global CSI knowledge of the main channel and the wiretap channel, whereas only the main channel's CSI is known in the SAS scheme without requiring the eavesdropper's CSI. As discussed in the following, the existing antenna selection work (see, e.g., [21]–[24]) considers that only the main channel's CSI is available at the source node; moreover, the source–destination with the global CSI knowledge studied in [25] is constrained to a MISO scenario without considering a more general MIMO system. For comparison purposes, we also consider the conventional space–time transmission (STT) as a benchmark.
- We consider the probability of zero secrecy capacity as a metric to evaluate the security performance of STT, SAS, and OAS schemes. To be specific, an event of the zero secrecy capacity occurs when the capacity of the main channel spanning from the source to the destination falls below the capacity of the wiretap channel from the source to the eavesdropper. In this case, the eavesdropper would be able to succeed in intercepting

the source–destination transmission. The probability of zero secrecy capacity is thus to evaluate the probability that the physical-layer security cannot be achieved. We derive analytical expressions of the probability of zero secrecy capacity for the STT, SAS, and OAS schemes. It is shown that the probabilities of zero secrecy capacity for the STT, SAS, and OAS schemes are independent of the SNR, implying that increasing the transmit power cannot improve the wireless security in terms of the probability of zero secrecy capacity.

- We examine the use of our generalized secrecy diversity [18]–[20] to characterize an asymptotic behavior on the probability of zero secrecy capacity, as the MER tends to infinity. It needs to be pointed out that, as aforementioned, the probability of zero secrecy capacity is independent of the SNR, which makes the conventional SNR-based secrecy diversity (e.g., in [22], [23], [26], and [28]) not applicable here. By contrast, our generalized secrecy diversity attempts to show an asymptotic probability of zero secrecy capacity in the high-MER region, which is motivated by the fact that the probability of zero secrecy capacity is mainly determined by the average gains of main and wiretap channels. Using our generalized secrecy diversity definition, we obtain that the STT, SAS, and OAS schemes achieve the full diversity order of MN_d, where M and N_d represent the number of antennas at the source and destination, respectively. This coincidentally matches the conventional secrecy diversity result of [22]. It is also implied that the secrecy diversity performance of STT, SAS, and OAS schemes is independent of the number of eavesdropper's antennas.

C. Organization and Structure

The remainder of this paper is organized as follows. Section II describes the system model and presents the STT, SAS, and OAS schemes. Next, we conduct the performance analysis of the STT, SAS, and OAS schemes in terms of the probability of zero secrecy capacity and the secrecy diversity in Section III, followed by Section IV, where numerical results are evaluated to show the security advantage of the proposed antenna selection over the conventional space–time coding. Finally, we make some concluding remarks in Section V.

II. SYSTEM MODEL AND PROBLEM FORMULATION

As shown in Fig. 1, we consider a wireless MIMO system consisting of a source s and a destination d in the presence of an eavesdropper e, in which the solid and dash lines represent the main channel (from source to destination) and the wiretap link (from source to eavesdropper), respectively. In Fig. 1, each network node is equipped with an arbitrary number of antennas, where M, N_d, and N_e represent the number of antennas at the source, destination, and eavesdropper, respectively. Moreover, the sets of antennas at the source, destination, and eavesdropper are denoted by $\mathcal{S}$, $\mathcal{D}$, and $\mathcal{E}$, respectively. Additionally, both the main and wiretap channels are modeled as the Rayleigh fading and the thermal noise received at any node is modeled
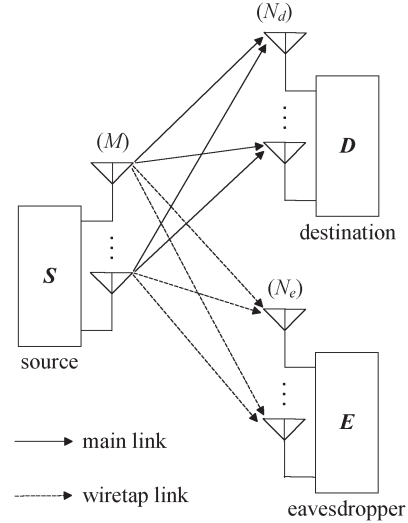

Fig. 1. MIMO system consisting of one source s and one destination d in the presence of an eavesdropper e.

as a zero-mean complex Gaussian random variable (RV) with a variance of σ_n^2, i.e., $\mathcal{CN}(0, \sigma_n^2)$. Although only the Rayleigh fading model is considered in this paper, similar performance analysis and results could be obtained for other fading models e.g., Nakagami fading.

In MIMO communications systems, space–time coding [29] has been widely recognized as an effective means to improve the performance of wireless transmissions. In what follows, we first consider the STT as a benchmark and then examine the transmit antenna selection to improve the physical-layer security for MIMO systems. We present two antenna selection schemes, namely the OAS and SAS, which operate depending on whether the global CSI of both the main and wiretap channels is available at the source. To be specific, in the OAS scheme, the global CSI is known at the source, whereas only the main channel's CSI is assumed in the SAS scheme without knowing the eavesdropper's CSI.

A. STT Scheme

In the STT scheme, the source signal is first encoded by using space–time coding [29]. Then, all M transmit antennas participate in sending the encoded signal to the destination, where the total amount of transmit power across M antennas is constrained to a fixed value, i.e., P. For simplicity, we here consider an equal-power allocation method, leading to the transmit power of P/M for each transmit antenna. Assuming that the destination has the perfect CSI of the main channel for space–time decoding [29], the receive SNR at the destination relying on the STT scheme can be given by

$$\gamma_d^{\text{STT}} = \sum_{i=1}^{M} \sum_{j=1}^{N_d} \frac{P|h_{id_j}|^2}{M\sigma_n^2} \tag{1}$$

where h_{id_j} is a fading coefficient of the main channel from transmit antenna i of the source to receive antenna j of the destination. Thus, according to (1), the maximal achievable rate

of the source-to-destination transmission relying on the STT scheme is expressed as

$$R_{sd}^{\text{STT}} = \log_2 \left(1 + \gamma_d^{\text{STT}} \right). \tag{2}$$

Similarly, the maximal achievable rate at the eavesdropper with the STT scheme can be given by

$$R_{se}^{\text{STT}} = \log_2 \left(1 + \gamma_e^{\text{STT}} \right) \tag{3}$$

where γ_e^{STT} represents the receive SNR at the eavesdropper as given by

$$\gamma_e^{\text{STT}} = \sum_{i=1}^{M} \sum_{j=1}^{N_e} \frac{P \left| h_{ie_j} \right|^2}{M \sigma_n^2} \tag{4}$$

where h_{ie_j} is a fading coefficient of the wiretap channel from transmit antenna i to receive antenna j of the eavesdropper.

B. OAS Scheme

In the OAS scheme, only the "best" transmit antenna will be selected and used for transmitting the source signal to the destination. We here assume that the source node has the global CSI of both the main and wiretap channels, where the CSI of the wiretap channel may be estimated and obtained by monitoring the eavesdropper's transmissions [12], [17]. Notice that the eavesdropper could be a legitimate user who is interested in tapping other users' signals, which may be active in the network. It is pointed out that, in the following, this scenario will be addressed, where the wiretap channel's CSI is unavailable at the source. Without loss of generality, let us consider that the transmit antenna i is selected as the "best" antenna to transmit the source signal with power P. Considering the use of maximal ratio combining (MRC) at the destination, we can obtain the maximal achievable rate of the transmission from transmit antenna i to the destination as

$$R_{id} = \log_2 \left(1 + \sum_{j=1}^{N_d} \frac{P \left| h_{id_j} \right|^2}{\sigma_n^2} \right). \tag{5}$$

Similarly, the maximal achievable rate obtained at the eavesdropper is given by

$$R_{ie} = \log_2 \left(1 + \sum_{j=1}^{N_e} \frac{P \left| h_{ie_j} \right|^2}{\sigma_n^2} \right). \tag{6}$$

Obviously, the transmit antenna that maximizes the secrecy capacity can be viewed as the "best" antenna. As discussed in [3] and [9], the secrecy capacity is given by the difference between the capacity of the main channel and that of the wiretap channel. Thus, the OAS criterion can be given by

$$b = \arg \max_{i \in \mathcal{S}} (R_{id} - R_{ie}) = \arg \max_{i \in \mathcal{S}} \frac{1 + \sum_{j=1}^{N_d} \frac{P \left| h_{id_j} \right|^2}{\sigma_n^2}}{1 + \sum_{j=1}^{N_e} \frac{P \left| h_{ie_j} \right|^2}{\sigma_n^2}} \tag{7}$$

where b denotes the "best" antenna, and $\mathcal{S}$ represents a set of M transmit antennas at the source node. Note that the transmit power P in (7) is known at the source. Moreover, the thermal noise variance σ_n^2 is shown as $\sigma_n^2 = \kappa T B$ [32], where κ is the Boltzmann constant (i.e., $\kappa = 1.38 \times 10^{-23}$ J/K), T is the room temperature in Kelvin, and B is the system bandwidth in Hertz. Since both the room temperature T and system bandwidth B are predetermined, the noise variance σ_n^2 can be easily obtained at the source. Therefore, once the global CSI of the main and wiretap channels $\left| h_{id_j} \right|^2$ and $\left| h_{ie_j} \right|^2$ are available, the "best" antenna could be determined at the source by using (7).

C. SAS Scheme

As stated previously, the OAS scheme requires that the global CSI of both the main and wiretap channels is available at the source node. However, in some cases, where the eavesdropper's CSI is unavailable, the OAS scheme cannot work properly. To this end, here, a so-called SAS scheme is presented, in which the "best" transmit antenna would be the one that maximizes the channel capacity of the source–destination transmission, instead of maximizing the secrecy capacity. Therefore, the antenna selection criterion in the SAS scheme is expressed as

$$b = \arg \max_{i \in \mathcal{S}} R_{id} = \arg \max_{i \in \mathcal{S}} \sum_{j=1}^{N_d} \left| h_{id_j} \right|^2 \tag{8}$$

where b denotes the selected "best" transmit antenna. Meanwhile, considering the SAS scheme, the maximal achievable rate at the eavesdropper is given by

$$R_{be}^{\text{SAS}} = \log_2 \left(1 + \sum_{j=1}^{N_e} \frac{P \left| h_{be_j} \right|^2}{\sigma_n^2} \right). \tag{9}$$

We now complete the signal modeling of the STT, OAS, and SAS schemes.

III. PERFORMANCE ANALYSIS

Here, we carry out performance analysis for the STT, OAS, and SAS schemes over Rayleigh fading channels. We first derive closed-form expressions of the probability of zero secrecy capacity for these three schemes. Next, the generalized secrecy diversity analysis is conducted for the sake of providing an insight into the impact of the number of antennas on the probability of zero secrecy capacity in the high-MER region.

A. Probability of Zero Secrecy Capacity

As discussed earlier, if the capacity of the main channel falls below that of the wiretap channel, the secrecy capacity becomes zero; thus, an event of zero secrecy capacity happens. Accordingly, the probability of zero secrecy capacity is defined as follows.

Definition 1: Letting R_m and R_w, respectively, denote the achievable rates of the main channel and wiretap channel, then the probability of zero secrecy capacity is obtained as

$$P_{\text{zeroSC}} = \Pr \{ R_m < R_w \}. \tag{10}$$

1) STT Scheme: Let us first analyze the probability of zero secrecy capacity for the STT scheme. By using (2) and (3), the probability of zero secrecy capacity for the STT scheme is given by

$$P_{\text{zeroSC}}^{\text{STT}} = \Pr\left\{R_{sd}^{\text{STT}} < R_{se}^{\text{STT}}\right\}$$

$$= \Pr\left\{\sum_{i=1}^{M}\left[\sum_{j=1}^{N_d}\left|h_{id_j}\right|^2 - \sum_{j=1}^{N_e}\left|h_{ie_j}\right|^2\right] < 0\right\}. \quad (11)$$

For simplicity, we consider the case, where the fading coefficients of all main links $\left|h_{id_j}\right|^2$ ($i \in \mathcal{S}, j \in \mathcal{D}$) are independent and identically distributed (i.i.d.) RVs with the same average channel gain denoted by $\sigma_{sd}^2 = E(|h_{id_j}|^2)$. Moreover, the fading coefficients of all wiretap links $\left|h_{ie_j}\right|^2$ ($i \in \mathcal{S}, j \in \mathcal{E}$) are also assumed i.i.d. RVs with an average channel gain denoted by $\sigma_{se}^2 = E(|h_{ie_j}|^2)$. For notational convenience, let λ_{de} denote the ratio of σ_{sd}^2 to σ_{se}^2, i.e., $\lambda_{de} = \sigma_{sd}^2/\sigma_{se}^2$ that is referred to as the MER throughout this paper. Since $\left|h_{id_j}\right|^2$ and $\left|h_{ie_j}\right|^2$ are assumed i.i.d. with exponential distribution, then $\sum_{i=1}^{M}\sum_{j=1}^{N_d}\left|h_{id_j}\right|^2$ and $\sum_{i=1}^{M}\sum_{j=1}^{N_e}\left|h_{ie_j}\right|^2$ are two independent gamma RVs. Using [31], a closed-form solution to (11) is obtained as

$$P_{\text{zeroSC}}^{\text{STT}} = (1 + \lambda_{de})^{1-MN_d-MN_e}$$

$$\times \sum_{k=0}^{MN_e-1}\left(\begin{array}{c}MN_d + MN_e - 1 \\ k\end{array}\right)\lambda_{de}^k. \quad (12)$$

In addition, considering $\sum_{i=1}^{M}\left[\sum_{j=1}^{N_d}\left|h_{id_j}\right|^2 - \sum_{j=1}^{N_e}\left|h_{ie_j}\right|^2\right] \leq M \cdot \max_{i \in \mathcal{S}}\left[\sum_{j=1}^{N_d}\left|h_{id_j}\right|^2 - \sum_{j=1}^{N_e}\left|h_{ie_j}\right|^2\right]$, we obtain a lower bound on the probability of zero secrecy capacity of (11) as given by

$$P_{\text{zeroSC}}^{\text{STT}} \geq \Pr\left\{M \max_{i \in \mathcal{S}}\left[\sum_{j=1}^{N_d}\left|h_{id_j}\right|^2 - \sum_{j=1}^{N_e}\left|h_{ie_j}\right|^2\right] < 0\right\}$$

$$= \prod_{i=1}^{M}\Pr\left\{\sum_{j=1}^{N_d}\left|h_{id_j}\right|^2 < \sum_{j=1}^{N_e}\left|h_{ie_j}\right|^2\right\}. \quad (13)$$

It is worth mentioning that the lower bound as given in (13) is an exact probability of zero secrecy capacity for the OAS scheme, as will be shown in the following. This theoretically shows that the probability of zero secrecy capacity for the proposed OAS scheme is strictly lower than that of the conventional STT scheme, showing the security benefit of using the OAS scheme.

2) OAS Scheme: Here, we analyze the probability of zero secrecy capacity for the proposed OAS scheme. Denoting the maximal achievable rates of the transmission from the "best" transmit antenna to the destination and to the eavesdropper by R_{bd}^{OAS} and R_{be}^{OAS}, respectively, we can express the probability of zero secrecy capacity for the OAS scheme as

$$P_{\text{zeroSC}}^{\text{OAS}} = \Pr\left\{R_{bd}^{\text{OAS}} < R_{be}^{\text{OAS}}\right\} \quad (14)$$

where R_{bd}^{OAS} and R_{be}^{OAS} are given by

$$R_{bd}^{\text{OAS}} = \log_2\left(1 + \sum_{j=1}^{N_d}\frac{\left|h_{bd_j}\right|^2 P}{\sigma_n^2}\right), \quad (15)$$

$$R_{be}^{\text{OAS}} = \log_2\left(1 + \sum_{j=1}^{N_e}\frac{\left|h_{be_j}\right|^2 P}{\sigma_n^2}\right). \quad (16)$$

Substituting R_{bd}^{OAS} and R_{be}^{OAS} from (15) and (16) into (14) yields

$$P_{\text{zeroSC}}^{\text{OAS}} = \Pr\left\{\frac{1 + \sum_{j=1}^{N_d}\frac{\left|h_{bd_j}\right|^2 P}{\sigma_n^2}}{1 + \sum_{j=1}^{N_e}\frac{\left|h_{be_j}\right|^2 P}{\sigma_n^2}} < 1\right\}. \quad (17)$$

Combining (7) and (17) gives

$$P_{\text{zeroSC}}^{\text{OAS}} = \Pr\left\{\max_{i \in \mathcal{S}}\left(\frac{1 + \sum_{j=1}^{N_d}\frac{\left|h_{id_j}\right|^2 P}{\sigma_n^2}}{1 + \sum_{j=1}^{N_e}\frac{\left|h_{ie_j}\right|^2 P}{\sigma_n^2}}\right) < 1\right\} \quad (18)$$

which can be further obtained as

$$P_{\text{zeroSC}}^{\text{OAS}} = \prod_{i=1}^{M}\Pr\left\{\frac{1 + \sum_{j=1}^{N_d}\frac{\left|h_{id_j}\right|^2 P}{\sigma_n^2}}{1 + \sum_{j=1}^{N_e}\frac{\left|h_{ie_j}\right|^2 P}{\sigma_n^2}} < 1\right\}$$

$$= \prod_{i=1}^{M}\Pr\left\{\sum_{j=1}^{N_d}\left|h_{id_j}\right|^2 < \sum_{j=1}^{N_e}\left|h_{ie_j}\right|^2\right\} \quad (19)$$

which is exactly the same as the STT scheme's lower bound on the probability of zero secrecy capacity, as given by (13), confirming the security advantage of the OAS scheme over the STT scheme. Assume that the fading coefficients $\left|h_{id_j}\right|^2$ and $\left|h_{ie_j}\right|^2$ are i.i.d. exponential RVs with respective average channel gains σ_{sd}^2 and σ_{se}^2. Following [31], we obtain a closed-form expression of (19) as

$$P_{\text{zeroSC}}^{\text{OAS}} = (1 + \lambda_{de})^{M(1-N_d-N_e)}$$

$$\times \left[\sum_{k=0}^{N_e-1}\left(\begin{array}{c}N_d + N_e - 1 \\ k\end{array}\right)\lambda_{de}^k\right]^M. \quad (20)$$

3) SAS Scheme: Here, the probability of zero secrecy capacity analysis of the SAS scheme is presented. As shown in (8), the SAS scheme attempts to maximize the capacity of the main channel spanning from source to destination. Hence, using (8)

and (9), we obtain the probability of zero secrecy capacity for the SAS scheme as

$$P_{\text{zeroSC}}^{\text{SAS}} = \Pr\left\{R_{bd}^{\text{SAS}} < R_{be}^{\text{SAS}}\right\}$$

$$= \Pr\left\{\sum_{j=1}^{N_d}|h_{bd_j}|^2 < \sum_{j=1}^{N_e}|h_{be_j}|^2\right\}$$

$$= \sum_{m=1}^{M}\Pr\left\{\sum_{j=1}^{N_d}|h_{md_j}|^2 < \sum_{j=1}^{N_e}|h_{me_j}|^2, b = m\right\} \tag{21}$$

where b denotes the "best" antenna determined by (8), and the last equation is obtained by using the law of total probability. From (8), an event $b = m$ means

$$\sum_{j=1}^{N_d}|h_{md_j}|^2 > \max_{i\in\mathcal{S},i\neq m}\sum_{j=1}^{N_d}|h_{id_j}|^2 \tag{22}$$

and substituting this into (21) gives

$$P_{\text{zeroSC}}^{\text{SAS}} = \sum_{m=1}^{M}\Pr\left\{\begin{array}{c}\sum_{j=1}^{N_e}|h_{me_j}|^2 > \sum_{j=1}^{N_d}|h_{md_j}|^2 \\ \max_{i\in\mathcal{S},i\neq m}\sum_{j=1}^{N_d}|h_{id_j}|^2 < \sum_{j=1}^{N_d}|h_{md_j}|^2\end{array}\right\}. \tag{23}$$

For simplicity, we consider that the fading coefficients $h_{ie_j}(i\in\mathcal{S}, j\in\mathcal{E})$ of wiretap links from M transmit antennas (at source) to N_e receive antennas (at eavesdropper) are i.i.d. In this way, RV $\sum_{j=1}^{N_e}|h_{me_j}|^2$ follows the same distribution for different transmit antenna m ($1\leq m\leq M$). Thus, (23) can be further simplified to

$$P_{\text{zeroSC}}^{\text{SAS}} = \Pr\left\{\max_{i\in\mathcal{S}}\sum_{j=1}^{N_d}|h_{id_j}|^2 < \sum_{j=1}^{N_e}|h_{me_j}|^2\right\} \tag{24}$$

which can be used to numerically calculate the probability of zero secrecy capacity for the SAS scheme. As shown in (11), (19), and (23), the probabilities of zero secrecy capacity for the STT, OAS, and SAS schemes are only related to the main channel $|h_{id_j}|^2$ and wiretap channel $|h_{ie_j}|^2$, which has nothing to do with the SNR. This means that increasing the transmit power cannot improve the wireless security in terms of the probability of zero secrecy capacity.

B. Generalized Secrecy Diversity

In what follows, we are focused on the secrecy diversity analysis for characterizing an asymptotic behavior on the probability of zero secrecy capacity in the high-MER region. In [22] and [23], the conventional secrecy diversity is defined as

$$d = -\lim_{\text{SNR}_d\to\infty}\frac{\log P_{\text{out}}(\text{SNR}_d)}{\log \text{SNR}_d} \tag{25}$$

where SNR_d represents the received SNR at the destination, and $P_{\text{out}}(\text{SNR}_d)$ represents the secrecy outage probability. One can observe that the conventional SNR-based secrecy diversity definition is not applicable here since the probability of zero secrecy capacity is independent of the SNR and only relates to the main and wiretap channels, as shown in (11), (19), and (23). To this end, we consider the use of our generalized secrecy diversity [18]–[20] to characterize an asymptotic behavior on the probability of zero secrecy capacity in the high-MER region. In our generalized secrecy diversity, an asymptotic probability of zero secrecy capacity is characterized as the ratio between the average gains of the main channel and the eavesdropper's wiretap channel (i.e., MER) tends to infinity. Therefore, our generalized secrecy diversity is defined as follows.

Definition 2: Denoting $\lambda_{de} = \sigma_{sd}^2/\sigma_{se}^2$, the generalized secrecy diversity is given by the asymptotic ratio of the probability of zero secrecy capacity to MER λ_{de}, yielding

$$d = -\lim_{\lambda_{de}\to\infty}\frac{\log(P_{\text{zeroSC}})}{\log(\lambda_{de})}. \tag{26}$$

It is pointed out that the MER λ_{de} possibly approaches infinity by mitigating the eavesdropper's received signal using an advanced signal processing technique, such as beamforming. To be specific, when the beamforming is adopted, the source node could transmit its signal in a particular direction to the destination; therefore, the main channel experiences constructive interference, whereas destructive interference is encountered in the wiretap channel, resulting in a high MER.

1) STT Scheme: Here, the secrecy diversity analysis of the STT scheme is presented. Using (26), the secrecy diversity of STT scheme is given by

$$d_{\text{STT}} = -\lim_{\lambda_{de}\to\infty}\frac{\log(P_{\text{zeroSC}}^{\text{STT}})}{\log(\lambda_{de})} \tag{27}$$

where $P_{\text{zeroSC}}^{\text{STT}}$ is given by (11). Using the inequalities of $\sum_{i=1}^{M}\sum_{j=1}^{N_d}|h_{id_j}|^2 \leq MN_d\max_{i\in\mathcal{S},j\in\mathcal{D}}|h_{id_j}|^2$ and $\sum_{i=1}^{M}\sum_{j=1}^{N_e}|h_{ie_j}|^2 \geq \max_{i\in\mathcal{S},j\in\mathcal{E}}|h_{ie_j}|^2$, we can obtain a lower bound on the probability of zero secrecy capacity of the STT scheme as

$$P_{\text{zeroSC}}^{\text{STT}} \geq \Pr\left\{MN_d\max_{i\in\mathcal{S},j\in\mathcal{D}}|h_{id_j}|^2 < \max_{i\in\mathcal{S},j\in\mathcal{E}}|h_{ie_j}|^2\right\} \tag{28}$$

where $\mathcal{D}$ and $\mathcal{E}$ represent the sets of antennas at the destination and eavesdropper, respectively. Denoting $X_e = \max_{i\in\mathcal{S},j\in\mathcal{E}}|h_{ie_j}|^2$ and considering that $|h_{ie_j}|^2$ follows exponential distribution with mean $\sigma_{ie_j}^2$, we can obtain the cumulative distribution function (cdf) of X_e as

$$P_{X_e}(x) = 1 + \sum_{k=1}^{2^{MN_e}-1}(-1)^{|\mathcal{A}_k|}\exp\left(-\sum_{i,j\in\mathcal{A}_k}\frac{x}{\sigma_{ie_j}^2}\right) \tag{29}$$

for $x \geq 0$; otherwise, $P_{X_e}(x) = 0$ for $x < 0$, where $\mathcal{A}_k$ represents the kth nonempty subcollection of MN_e elements of term $\exp(-(x/\sigma_{ie_j}^2))$ for $(i\in\mathcal{S}, j\in\mathcal{E})$, and $|\mathcal{A}_k|$ is the number of

the elements in $\mathcal{A}_k$. From (29), the probability density function (pdf) of X_e can be derived as

$$p_{X_e}(x) = \sum_{k=1}^{2^{MN_e}-1} \sum_{i,j\in\mathcal{A}_k} \frac{(-1)^{|\mathcal{A}_k|+1}}{\sigma_{ie_j}^2} \exp\left(-\sum_{i,j\in\mathcal{A}_k} \frac{x}{\sigma_{ie_j}^2}\right) \tag{30}$$

for $x \geq 0$. Using (28) and (30), we have

$$P_{\text{zeroSC}}^{\text{STT}} \geq \int_{-\infty}^{\infty} \prod_{i\in\mathcal{S},j\in\mathcal{D}} \left[1 - \exp\left(-\frac{x}{MN_d\sigma_{id_j}^2}\right)\right] p_{X_e}(x)dx \tag{31}$$

where $p_{X_e}(x)$ is given in (30).

Theorem 1: Considering an RV x with a pdf given by (30), then the following equation holds for $\lambda_{de} \to \infty$

$$1 - \exp\left(-\frac{x}{MN_d\sigma_{id_j}^2}\right) \stackrel{1}{=} \frac{x}{MN_d\sigma_{id_j}^2}$$

where $\stackrel{1}{=}$ represents an equality with probability 1.

Proof: See the Appendix.

Substituting (30) into (31) and using Theorem 1, we obtain

$$P_{\text{zeroSC}}^{\text{STT}} \geq \sum_{k=1}^{2^{MN_e}-1} \left(\frac{1}{MN_d}\right)^{MN_d} \prod_{i\in\mathcal{S},j\in\mathcal{D}} \frac{1}{\sigma_{id_j}^2}$$
$$\times \int_0^{\infty} \sum_{i,j\in\mathcal{A}_k} \frac{(-1)^{|\mathcal{A}_k|+1}x^{MN_d}}{\sigma_{ie_j}^2} \exp\left(-\sum_{i,j\in\mathcal{A}_k}\frac{x}{\sigma_{ie_j}^2}\right)dx$$
$$= \sum_{k=1}^{2^{MN_e}-1} (-1)^{|\mathcal{A}_k|+1} \frac{(MN_d)! \prod_{i\in\mathcal{S},j\in\mathcal{D}}\frac{1}{\sigma_{id_j}^2}}{\left(\sum_{i,j\in\mathcal{A}_k}\frac{MN_d}{\sigma_{ie_j}^2}\right)^{MN_d}} \tag{32}$$

for $\lambda_{de} \to \infty$. By denoting $\sigma_{id_j}^2 = \alpha_{id_j}\sigma_{sd}^2$ and $\sigma_{ie_j}^2 = \alpha_{ie_j}\sigma_{se}^2$, (32) can be rewritten as

$$P_{\text{zeroSC}}^{\text{STT}} \geq \sum_{k=1}^{2^{MN_e}-1} \frac{(-1)^{|\mathcal{A}_k|+1}(MN_d)!}{\left(\sum_{i,j\in\mathcal{A}_k}\frac{MN_d}{\alpha_{ie_j}}\right)^{MN_d} \prod_{i\in\mathcal{S},j\in\mathcal{D}}\alpha_{id_j}} \left(\frac{1}{\lambda_{de}}\right)^{MN_d} \tag{33}$$

where $\lambda_{de} = \sigma_{sd}^2/\sigma_{se}^2$. Thus, substituting (33) into (27) gives

$$d_{\text{STT}} \leq MN_d. \tag{34}$$

In addition, considering $\sum_{i=1}^{M}\sum_{j=1}^{N_d}|h_{id_j}|^2 \geq \max_{i\in\mathcal{S},j\in\mathcal{D}}|h_{id_j}|^2$ and $\sum_{i=1}^{M}\sum_{j=1}^{N_e}|h_{ie_j}|^2 \leq MN_e\max_{i\in\mathcal{S},j\in\mathcal{E}}|h_{ie_j}|^2$, we obtain an upper bound on the probability of zero secrecy capacity of the STT scheme as

$$P_{\text{zeroSC}}^{\text{STT}} \leq \Pr\left\{\max_{i\in\mathcal{S},j\in\mathcal{D}}|h_{id_j}|^2 < MN_e\max_{i\in\mathcal{S},j\in\mathcal{E}}|h_{ie_j}|^2\right\}. \tag{35}$$

Using (30) and letting $\lambda_{de} \to \infty$, (35) can be further obtained and expressed in closed form as

$$P_{\text{zeroSC}}^{\text{STT}} \leq \int_{-\infty}^{\infty} \prod_{i\in\mathcal{S},j\in\mathcal{D}} \left[1 - \exp\left(-\frac{MN_e x}{\sigma_{id_j}^2}\right)\right] p_{X_e}(x)dx$$
$$= \sum_{k=1}^{2^{MN_e}-1} (-1)^{|\mathcal{A}_k|+1} \frac{(MN_e)^{MN_d}(MN_d)!}{\left(\sum_{i,j\in\mathcal{A}_k}\frac{1}{\alpha_{ie_j}}\right)^{MN_d} \prod_{i\in\mathcal{S},j\in\mathcal{D}}\alpha_{id_j}}$$
$$\times \left(\frac{1}{\lambda_{de}}\right)^{MN_d} \tag{36}$$

where the second equation is obtained by using $1 - \exp(-(MN_e x/\sigma_{id_j}^2)) \stackrel{1}{=} (MN_e x/\sigma_{id_j}^2)$ with $\lambda_{de} \to \infty$. Substituting (36) into (27) gives

$$d_{\text{STT}} \geq MN_d. \tag{37}$$

Therefore, by combining (34) and (37), the secrecy diversity of the STT scheme is readily obtained as

$$d_{\text{STT}} = MN_d. \tag{38}$$

One can observe from (38) that the secrecy diversity of the STT scheme is the product of the number of transmit antennas M and that of receive antennas at the destination N_d, which is independent of the number of eavesdropper's antennas N_e. This implies that the secrecy diversity of the STT scheme is insusceptible to the eavesdropper. More specifically, although increasing the number of eavesdropper's antennas would definitely degrade the probability of zero secrecy capacity, it will not affect the speed at which the probability of zero secrecy capacity decreases as $\lambda_{de} \to \infty$. Moreover, as M and N_d increase, the secrecy diversity MN_d of the STT scheme increases accordingly, meaning that increasing the number of antennas at the source and destination can significantly improve the speed at which the probability of zero secrecy capacity decreases as $\lambda_{de} \to \infty$.

2) OAS Scheme: Here, we present the secrecy diversity analysis of the proposed OAS scheme. Similarly to (27), the secrecy diversity of the OAS scheme is given by

$$d_{\text{OAS}} = -\lim_{\lambda_{de}\to\infty} \frac{\log\left(P_{\text{zeroSC}}^{\text{OAS}}\right)}{\log(\lambda_{de})} \tag{39}$$

where $P_{\text{zeroSC}}^{\text{OAS}}$ is given by (19). Considering inequalities $\sum_{j=1}^{N_d}|h_{id_j}|^2 \leq N_d\max_{j\in\mathcal{D}}|h_{id_j}|^2$ and $\sum_{j=1}^{N_e}|h_{ie_j}|^2 \geq \max_{j\in\mathcal{E}}|h_{ie_j}|^2$, a lower bound on the probability of the zero secrecy capacity of the OAS scheme is obtained as

$$P_{\text{zeroSC}}^{\text{OAS}} \geq \prod_{i=1}^{M} \Pr\left\{N_d\max_{j\in\mathcal{D}}|h_{id_j}|^2 < \max_{j\in\mathcal{E}}|h_{ie_j}|^2\right\}. \tag{40}$$

Denoting $Y_e = \max_{j \in \mathcal{E}} |h_{ie_j}|^2$, we can easily derive the pdf of Y_e as

$$p_{Y_e}(y) = \sum_{k=1}^{2^{N_e}-1} \sum_{j \in \mathcal{B}_k} \frac{(-1)^{|\mathcal{B}_k|+1}}{\sigma_{ie_j}^2} \exp\left(-\sum_{j \in \mathcal{B}_k} \frac{y}{\sigma_{ie_j}^2}\right) \quad (41)$$

for $y \geq 0$; otherwise $p_{Y_e}(y) = 0$ for $y < 0$, where $\mathcal{B}_k$ is the kth nonempty subset of N_e receive antennas at eavesdropper and $|\mathcal{B}_k|$ is the number of elements of set $\mathcal{B}_k$. Using (40) and (41), we have

$$P_{\text{zeroSC}}^{\text{OAS}} \geq \prod_{i=1}^{M} \int_0^\infty \prod_{j=1}^{N_d} \left[1 - \exp\left(-\frac{y}{N_d \sigma_{id_j}^2}\right)\right]$$
$$\times \sum_{k=1}^{2^{N_e}-1} \sum_{j \in \mathcal{B}_k} \frac{(-1)^{|\mathcal{B}_k|+1}}{\sigma_{ie_j}^2} \exp\left(-\sum_{j \in \mathcal{B}_k} \frac{y}{\sigma_{ie_j}^2}\right) dy. \quad (42)$$

Considering $\lambda_{de} \to \infty$, we have $1 - \exp(-(y/N_d\sigma_{id_j}^2)) \doteq (y/N_d\sigma_{id_j}^2)$ by using Theorem 1. Substituting this result into (42) yields

$$P_{\text{zeroSC}}^{\text{OAS}} \geq \prod_{i=1}^{M} \sum_{k=1}^{2^{N_e}-1} \left(\frac{1}{N_d}\right)^{N_d} \prod_{j=1}^{N_d} \frac{1}{\sigma_{id_j}^2}$$
$$\times \int_0^\infty \sum_{j \in \mathcal{B}_k} \frac{(-1)^{|\mathcal{B}_k|+1} y^{N_d}}{\sigma_{ie_j}^2} \exp\left(-\sum_{j \in \mathcal{B}_k} \frac{y}{\sigma_{ie_j}^2}\right) dy$$
$$= \prod_{i=1}^{M} \left[\sum_{k=1}^{2^{N_e}-1} (-1)^{|\mathcal{B}_k|+1} \frac{N_d! \prod_{j=1}^{N_d} \frac{1}{\alpha_{id_j}}}{\left(\sum_{j \in \mathcal{B}_k} \frac{N_d}{\alpha_{ie_j}}\right)^{N_d}}\right] \left(\frac{1}{\lambda_{de}}\right)^{MN_d}$$
$$\tag{43}$$

for $\lambda_{de} \to \infty$. Thus, substituting (43) into (39) gives

$$d_{\text{OAS}} \leq MN_d. \quad (44)$$

In addition, by using inequalities $\sum_{j=1}^{N_d} |h_{id_j}|^2 \geq \max_{j \in \mathcal{D}} |h_{id_j}|^2$ and $\sum_{j=1}^{N_e} |h_{ie_j}|^2 \leq N_e \max_{j \in \mathcal{E}} |h_{ie_j}|^2$, an upper bound on the probability of zero secrecy capacity of the OAS scheme is given by

$$P_{\text{zeroSC}}^{\text{OAS}} \leq \prod_{i=1}^{M} \Pr\left\{\max_{j \in \mathcal{D}} |h_{id_j}|^2 < N_e \max_{j \in \mathcal{E}} |h_{ie_j}|^2\right\} \quad (45)$$

which can be further expressed as (46), shown at the bottom of the page, for $\lambda_{de} \to \infty$. Substituting (46) into (39) gives

$$d_{\text{OAS}} \geq MN_d. \quad (47)$$

Using (44) and (47), we can easily obtain the secrecy diversity of OAS scheme with the squeeze theorem as

$$d_{\text{OAS}} = MN_d \quad (48)$$

which shows that the OAS scheme achieves the same secrecy diversity as the STT scheme. It is pointed out that the same secrecy diversity order achieved by both the OAS and STT schemes only means that the probabilities of the zero secrecy capacity of the two schemes are reduced at the same speed as $\lambda_{de} \to \infty$.

3) SAS Scheme: Here, the secrecy diversity of the SAS scheme is examined. Similarly, the secrecy diversity of the SAS scheme can be defined as

$$d_{\text{SAS}} = -\lim_{\lambda_{de} \to \infty} \frac{\log\left(P_{\text{zeroSC}}^{\text{SAS}}\right)}{\log(\lambda_{de})} \quad (49)$$

where $P_{\text{zeroSC}}^{\text{SAS}}$ is given by (24). Using inequalities $\max_{i \in \mathcal{S}} \sum_{j=1}^{N_d} |h_{id_j}|^2 \leq N_d \max_{i \in \mathcal{S}, j \in \mathcal{D}} |h_{id_j}|^2$ and $\sum_{j=1}^{N_e} |h_{me_j}|^2 \geq \max_{j \in \mathcal{E}} |h_{me_j}|^2$, we obtain a lower bound on the probability of the zero secrecy capacity of the SAS scheme as

$$P_{\text{zeroSC}}^{\text{SAS}} \geq \Pr\left\{N_d \max_{i \in \mathcal{S}, j \in \mathcal{D}} |h_{id_j}|^2 < \max_{j \in \mathcal{E}} |h_{me_j}|^2\right\}. \quad (50)$$

$$P_{\text{zeroSC}}^{\text{OAS}} \leq \prod_{i=1}^{M} \Pr\left\{\max_{j \in \mathcal{D}} |h_{id_j}|^2 < N_e \max_{j \in \mathcal{E}} |h_{ie_j}|^2\right\}$$
$$= \prod_{i=1}^{M} \int_0^\infty \prod_{j=1}^{N_d} \left[1 - \exp\left(-\frac{N_e y}{\sigma_{id_j}^2}\right)\right] \sum_{k=1}^{2^{N_e}-1} \sum_{j \in \mathcal{B}_k} \frac{(-1)^{|\mathcal{B}_k|+1}}{\sigma_{ie_j}^2} \exp\left(-\sum_{j \in \mathcal{B}_k} \frac{y}{\sigma_{ie_j}^2}\right) dy$$
$$= \prod_{i=1}^{M} \sum_{k=1}^{2^{N_e}-1} (N_e)^{N_d} \prod_{j=1}^{N_d} \frac{1}{\sigma_{id_j}^2} \int_0^\infty \sum_{j \in \mathcal{B}_k} \frac{(-1)^{|\mathcal{B}_k|+1} y^{N_d}}{\sigma_{ie_j}^2} \exp\left(-\sum_{j \in \mathcal{B}_k} \frac{y}{\sigma_{ie_j}^2}\right) dy$$
$$= \prod_{i=1}^{M} \left[\sum_{k=1}^{2^{N_e}-1} (-1)^{|\mathcal{B}_k|+1} (N_e)^{N_d} \frac{N_d! \prod_{j=1}^{N_d} \frac{1}{\alpha_{id_j}}}{\left(\sum_{j \in \mathcal{B}_k} \frac{1}{\alpha_{ie_j}}\right)^{N_d}}\right] \left(\frac{1}{\lambda_{de}}\right)^{MN_d} \quad (46)$$

Letting $\lambda_{de} \to \infty$ and using (41), the preceding equation can be further calculated as

$$
\begin{aligned}
P_{\text{zeroSC}}^{\text{SAS}} &\geq \Pr\left\{ N_d \max_{i\in\mathcal{S},j\in\mathcal{D}} \left|h_{id_j}\right|^2 < \max_{j\in\mathcal{E}} \left|h_{me_j}\right|^2 \right\} \\
&= \int_0^\infty \prod_{i\in\mathcal{S},j\in\mathcal{D}} \left[1 - \exp\left(-\frac{y}{N_d\sigma_{id_j}^2} \right) \right] \\
&\quad \times \sum_{k=1}^{2^{N_e}-1} \sum_{j\in\mathcal{B}_k} \frac{(-1)^{|\mathcal{B}_k|+1}}{\sigma_{me_j}^2} \exp\left(-\sum_{j\in\mathcal{B}_k} \frac{y}{\sigma_{me_j}^2} \right) dy \\
&= \sum_{k=1}^{2^{N_e}-1} (-1)^{|\mathcal{B}_k|+1} \frac{(MN_d)! \prod_{i\in\mathcal{S},j\in\mathcal{D}} \left(\frac{1}{\alpha_{id_j}}\right)}{\left(\sum_{j\in\mathcal{B}_k} \frac{N_d}{\alpha_{me_j}} \right)^{MN_d}} \left(\frac{1}{\lambda_{de}} \right)^{MN_d}
\end{aligned}
$$
(51)

where the third equation is obtained by using $1 - \exp(-(y/N_d\sigma_{id_j}^2)) \stackrel{1}{=} (y/N_d\sigma_{id_j}^2)$ with $\lambda_{de} \to \infty$. Substituting (51) into (49) yields

$$
d_{\text{SAS}} \leq MN_d. \tag{52}
$$

In addition, considering $\max_{i\in\mathcal{S}} \sum_{j=1}^{N_d} |h_{id_j}|^2 \geq \max_{i\in\mathcal{S},j\in\mathcal{D}} |h_{id_j}|^2$ and $\sum_{j=1}^{N_e} |h_{me_j}|^2 \leq N_e \max_{j\in\mathcal{E}} |h_{me_j}|^2$, an upper bound on the probability of the zero secrecy capacity of the SAS scheme is given by

$$
\begin{aligned}
P_{\text{zeroSC}}^{\text{SAS}} &\leq \Pr\left\{ \max_{i\in\mathcal{S},j\in\mathcal{D}} \left|h_{id_j}\right|^2 < N_e \max_{j\in\mathcal{E}} \left|h_{me_j}\right|^2 \right\} \\
&= \int_0^\infty \prod_{i\in\mathcal{S},j\in\mathcal{D}} \left[1 - \exp\left(-\frac{N_e y}{\sigma_{id_j}^2} \right) \right] \\
&\quad \times \sum_{k=1}^{2^{N_e}-1} \sum_{j\in\mathcal{B}_k} \frac{(-1)^{|\mathcal{B}_k|+1}}{\sigma_{me_j}^2} \exp\left(-\sum_{j\in\mathcal{B}_k} \frac{y}{\sigma_{me_j}^2} \right) dy \\
&= \sum_{k=1}^{2^{N_e}-1} \frac{(-1)^{|\mathcal{B}_k|+1}(N_e)^{MN_d}(MN_d)!}{\left(\sum_{j\in\mathcal{B}_k} \frac{1}{\alpha_{me_j}} \right)^{MN_d} \prod_{i\in\mathcal{S},j\in\mathcal{D}} (\alpha_{id_j})} \left(\frac{1}{\lambda_{de}} \right)^{MN_d}
\end{aligned}
$$
(53)

for $\lambda_{de} \to \infty$. Using (49) and (53), we have

$$
d_{\text{SAS}} \geq MN_d. \tag{54}
$$

Therefore, we obtain the secrecy diversity of the SAS scheme from (52) and (54) as

$$
d_{\text{SAS}} = MN_d \tag{55}
$$

which shows that the proposed SAS scheme achieves the same secrecy diversity as the STT and OAS schemes. This means that in the high-MER region, the probabilities of zero secrecy capacity of the STT, OAS, and SAS schemes all behave as $(1/\lambda_{de})^{MN_d}$ as $\lambda_{de} \to \infty$.
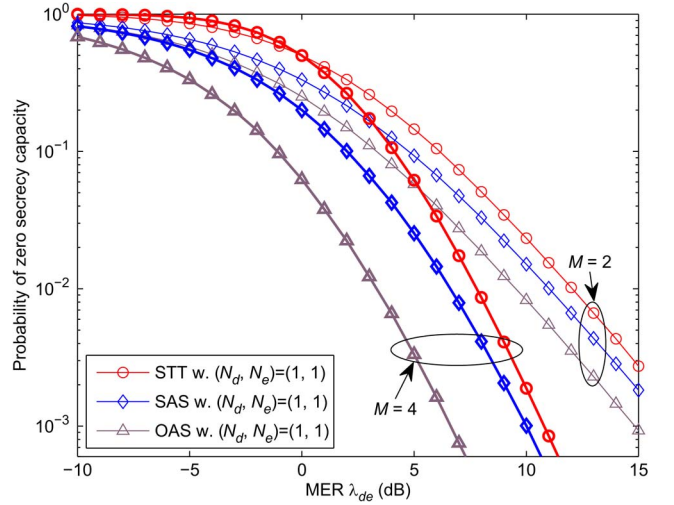

Fig. 2. Probability of zero secrecy capacity versus MER of the STT, SAS, and OAS schemes with $\alpha_{id_j} = \alpha_{ie_j} = 1$.

IV. NUMERICAL RESULTS AND DISCUSSIONS

Here, we present numerical performance results of the STT, SAS, and OAS schemes in terms of the probability of zero secrecy capacity. Fig. 2 shows the probability of zero secrecy capacity versus MER of the STT, SAS, and OAS schemes with $N_d = N_e = 1$ and $\alpha_{id_j} = \alpha_{ie_j} = 1$. In Fig. 2, one can see that, as the number of transmit antennas M increases from $M = 2$ to 4, the probabilities of zero secrecy capacity of the STT, SAS, and OAS schemes decrease significantly, showing the security benefits of exploiting multiple transmit antennas at the source node. Fig. 2 shows that, for both the cases of $M = 2$ and $M = 4$, the OAS scheme achieves the best security performance; moreover, the SAS scheme performs better than the STT scheme in terms of the probability of zero secrecy capacity.

Fig. 3 shows the probability of zero secrecy capacity versus the number of transmit antennas M of the STT, SAS, and OAS schemes with $N_d = N_e = 1$, $\lambda_{de} = 3$ dB, and $\alpha_{id_j} = \alpha_{ie_j} = 1$. It is shown in Fig. 3 that the OAS scheme outperforms both the SAS and STT schemes in terms of its probability of zero secrecy capacity. Moreover, as the number of transmit antennas M increases, the security advantage of the OAS scheme over the SAS and STT approaches become much more significant. One can also observe in Fig. 3 that the conventional STT scheme performs worse than both the SAS and OAS schemes, showing the security benefits of using the transmit antenna selection.

In Figs. 2 and 3, only the source node is assumed with multiple antennas to show the performance improvement through using multiple transmit antennas. Next, we consider that the destination and eavesdroppers are also equipped with multiple antennas in evaluating the probability of zero secrecy capacity. Fig. 4 shows the probability of zero secrecy capacity versus MER of the STT, SAS, and OAS schemes with $M = 4$ and $\alpha_{id_j} = \alpha_{ie_j} = 1$. It is shown in Fig. 4 that, for both the cases of $(M, N_d, N_e) = (4, 1, 1)$ and $(M, N_d, N_e) = (4, 4, 4)$, the OAS scheme strictly achieves a better secrecy performance than both the SAS and STT schemes. However, for
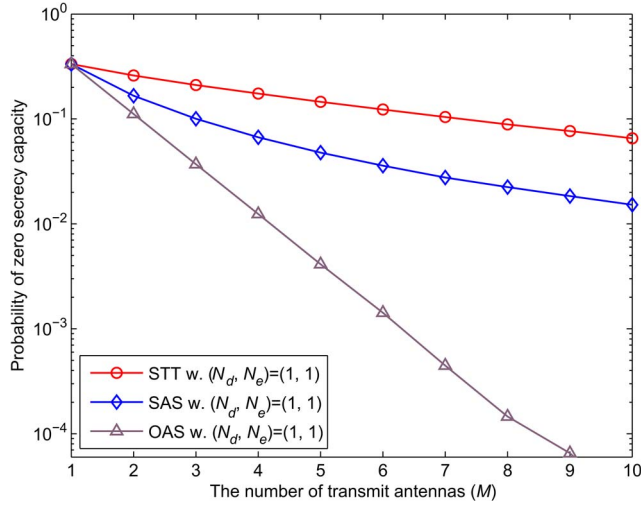
Fig. 3. Probability of zero secrecy capacity versus the number of transmit antennas M of the STT, SAS, and OAS schemes with $N_d = N_e = 1$, $\lambda_{de} = 3$ dB, and $\alpha_{id_j} = \alpha_{ie_j} = 1$.
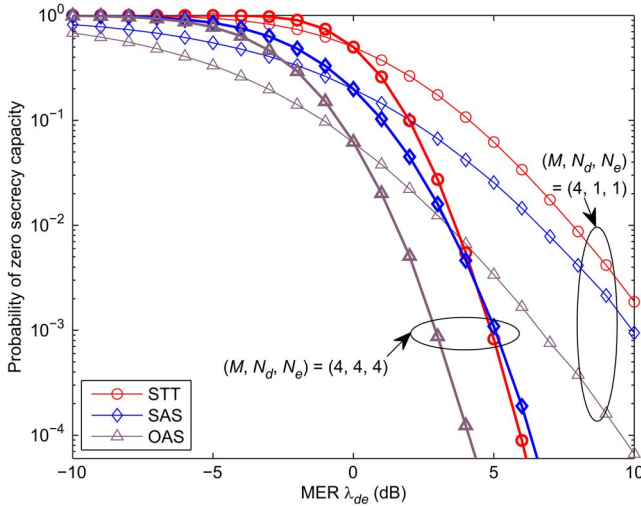

Fig. 4. Probability of zero secrecy capacity versus MER of the STT, SAS, and OAS schemes with $M = 4$, $N_d = N_e$, and $\alpha_{id_j} = \alpha_{ie_j} = 1$.

$(M, N_d, N_e) = (4, 4, 4)$, as the MER increases from -10 to 10 dB, the SAS scheme initially outperforms the STT scheme and eventually performs worse than the STT scheme in terms of probability of zero secrecy capacity.

Fig. 5 shows the asymptotic and exact results on the probability of zero secrecy capacity for the proposed OAS scheme by plotting (20), (43), and (46) as a function of MER λ_{de}. Specifically, the exact probability of zero secrecy capacity for the OAS scheme is obtained using (20), whereas the corresponding lower and upper bounds are plotted from (43) and (46), respectively. As shown in Fig. 5, upon increasing the MER, the exact probability of zero secrecy capacity falls between the lower and upper bounds. Notice that the lower and upper bounds are based on Theorem 1, which is valid for high MER only. Additionally, one can observe in Fig. 5 that in the high-MER region, the slopes of these three performance curves are the same, which confirms the correctness of the secrecy diversity analysis based on the squeeze theorem.
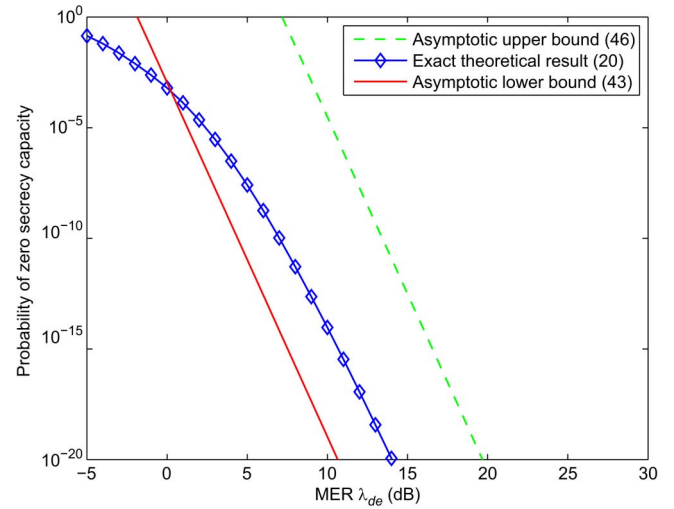

Fig. 5. Asymptotic and exact results on the probability of zero secrecy capacity for the proposed OAS scheme with $M = N_d = 4$, $N_e = 2$, and $\alpha_{id_j} = \alpha_{ie_j} = 1$.

V. CONCLUSION

In this paper, we explored the physical-layer security of a MIMO system comprised of one source and one destination in the presence of an eavesdropper, where each node is equipped with multiple antennas. We proposed two transmit antenna selection schemes, namely the OAS and SAS, which operate depending on whether the global CSI knowledge of both the main and wiretap channels is available at the source. For the purpose of performance comparison, we also considered the conventional STT scheme as a benchmark. We derived closed-form expressions of the probability of zero secrecy capacity for the STT, OAS, and SAS schemes in Rayleigh fading environments. We further examined the generalized secrecy diversity of STT, SAS, and OAS schemes through an asymptotic analysis of the probability of zero secrecy capacity in the high-MER region. It was shown that the generalized secrecy diversity orders of STT, SAS, and OAS schemes are the product of the number of antennas at the source and destination. Additionally, numerical results demonstrated that the OAS scheme outperforms both the SAS and STT schemes in terms of its probability of zero secrecy capacity, confirming the security benefits of using the optimal antenna selection against eavesdropping.

APPENDIX
PROOF OF THEOREM 1

Letting $z = (x / MN_d \sigma_{id_j}^2)$ and using (30), we obtain the expected value of RV z as

$$
\begin{aligned}
E(z) &= \int_0^\infty \sum_{k=1}^{2^{MN_e}-1} \sum_{i,j \in A_k} \frac{(-1)^{|A_k|+1} x}{MN_d \sigma_{id_j}^2 \sigma_{ie_j}^2} \\
&\quad \times \exp\left(-\sum_{i,j \in A_k} \frac{x}{\sigma_{ie_j}^2} \right) dx \\
&= \sum_{k=1}^{2^{MN_e}-1} \frac{(-1)^{|A_k|+1} \left(\sum_{i,j \in A_k} \sigma_{ie_j}^{-2} \right)^{-1}}{MN_d \sigma_{id_j}^2}.
\end{aligned} \tag{A.1}
$$

Denoting $\sigma_{id_j}^2 = \alpha_{id_j}\sigma_{sd}^2$ and $\sigma_{ie_j}^2 = \alpha_{ie_j}\sigma_{se}^2$ and letting $\lambda_{de} \to \infty$, we have

$$E(z) = \sum_{k=1}^{2^{MN_e}-1} \frac{(-1)^{|A_k|+1}\left(\sum_{i,j\in A_k}\alpha_{ie_j}^{-2}\right)^{-1}}{MN_d\alpha_{id_j}}\frac{1}{\lambda_{de}} \quad (A.2)$$

which shows that $E(z)$ tends to zero as $\lambda_{de} \to \infty$. Meanwhile, we can obtain the expected value of z^2 as

$$E(z^2) = \sum_{k=1}^{2^{MN_e}-1} \frac{2(-1)^{|A_k|+1}\left(\sum_{i,j\in A_k}\alpha_{ie_j}^{-2}\right)^{-2}}{\left(MN_d\alpha_{id_j}^2\right)^2}\left(\frac{1}{\lambda_{de}}\right)^2. \quad (A.3)$$

From (A.3), one can see that $E(z^2)$ tends to zero as $\lambda_{de} \to \infty$. Thus, the variance of z given by $\text{Var}(z) = E(z^2) - [E(z)]^2$ also converges to zero for $\lambda_{de} \to \infty$, since both $E(z)$ and $E(z^2)$ approach zero as shown in (A.2) and (A.3). Considering the fact that both mean and variance of z converge to zero as $\lambda_{de} \to \infty$, one can conclude that RV z approaches zero with probability 1 for $\lambda_{de} \to \infty$. Here, we use a symbol $\overset{1}{=}$ to denote an equality with probability 1 as $\lambda_{de} \to \infty$, i.e., we write $z \overset{1}{=} 0$ to represent

$$\Pr\left(\lim_{\lambda_{de}\to\infty} z = 0\right) = 1. \quad (A.4)$$

In addition, using the Maclaurin series expansion and Cauchy's mean value theorem, we can easily obtain

$$1 - \exp(-z) = z + \frac{z^2}{2}\exp(-\theta) \quad (A.5)$$

where $0 < \theta < z$. From (A.5), we have

$$\lim_{\lambda_{de}\to\infty} 1 - \exp(-z) - z = \lim_{\lambda_{de}\to\infty} \frac{z^2}{2}\exp(-\theta). \quad (A.6)$$

Similar to (A.2) and (A.3), we can prove that both mean and variance of z^2 converge to zero as $\lambda_{de} \to \infty$, i.e., $z^2 \overset{1}{=} 0$. Meanwhile, considering $0 < \exp(-\theta) < 1$ due to $0 < \theta < z$, we obtain $\lim_{\lambda_{de}\to\infty}(z^2/2)\exp(-\theta) = 0$. Substituting this result into (A.6) yields

$$1 - \exp(-z) - z \overset{1}{=} 0. \quad (A.7)$$

Using $z = (x/MN_d\sigma_{id_j}^2)$ and (A.7), we obtain

$$1 - \exp\left(-\frac{x}{MN_d\sigma_{id_j}^2}\right) \overset{1}{=} \frac{x}{MN_d\sigma_{id_j}^2} \quad (A.8)$$

for $\lambda_{de} \to \infty$. This completes the proof of Theorem 1.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, pp. 451–456, Jul. 1978.

[4] G. J. Foschini and M. J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," *Wireless Pers. Commun.*, vol. 6, no. 3, pp. 311–335, Mar. 1998.

[5] A. J. Paulraj, D. A. Gore, R. U. Nabar, and H. Bolcskei, "An overview of MIMO communications - A key to gigabit wireless," *Proc. IEEE*, vol. 92, no. 2, pp. 198–218, Feb. 2004.

[6] Y. Pei, Y.-C. Liang, K. C. Teh, and K. Li, "Secure communication in multiantenna cognitive radio networks with imperfect channel state information," *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1683–1693, Apr. 2011.

[7] H.-M. Wang, T. Zheng, and X.-G. Xia, "Secure MISO wiretap channels with multi-antenna passive eavesdropper: Artificial noise vs. artificial fast fading," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 94–106, Jan. 2015.

[8] A. Khisti, G. Womell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 2007, pp. 2471–2475.

[9] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[10] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, USA, Jul. 2006, pp. 356– 360.

[11] H.-M. Wang, F. Liu, and M. Yang, "Joint cooperative beamforming, jamming and power allocation to secure AF relay systems," *IEEE Trans. Veh. Technol.*, vol. 64, no. 10, pp. 4893–4898, Oct. 2015.

[12] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[13] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity—Part I: System description," *IEEE Trans. Commun.*, vol. 51, no. 11, pp. 1927–1938, Nov. 2003.

[14] 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.

[15] Y. Zou, Y.-D. Yao, and B. Zheng, "Opportunistic distributed space-time coding for decode-and-forward cooperation systems," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1766–1781, Apr. 2012.

[16] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532–3545, Jul. 2012.

[17] Y. Zou, J. Zhu, X. Wang, and V. Leung, "Improving physical-layer security in wireless communications through diversity techniques," *IEEE Netw.*, vol. 29, no. 1, pp. 42–48, Jan. 2015.

[18] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[19] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5103–5113, Dec. 2013.

[20] Y. Zou, X. Li, and Y.-C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2222–2236, Nov. 2014.

[21] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.

[22] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[23] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 254–259, Jan. 2013.

[24] N. S. Ferdinand, D. B. da Costa, and M. Latva-Aho, "Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection," *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 864–867, May 2013.

[25] N. Sadeque, I. Land, and R. Subramanian, "Average secrecy rate under transmit antenna selection for the multiple-antenna wiretap channel," in *Proc. IEEE PIMRC*, London, U.K., Sep. 2013, pp. 238– 242.

[26] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1656–1667, Mar. 2014.

[27] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 509–511, May 2011.

[28] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 247–258, Feb. 2014.

[29] A. F. Molisch, *Wireless Communications*. Hoboken, NJ, USA: Wiley, 2011.

[30] M. K. Simon and M.-S. Alouini, "On the difference of two chi-square variates with application to outage probability computation," *IEEE Trans. Commun.*, vol. 49, no. 11, pp. 1946–1954, Nov. 2001.

[31] M. K. Simon and M.-S. Alouini , "Corrections to "On the difference of two chi-square variates with application to outage probability computation"," *IEEE Trans. Commun.*, vol. 54, no. 7, pp. 1346–1347, Jul. 2006.

[32] Y. Zou, J. Zhu, and R. Zhang, "Exploiting network cooperation in green wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 3, pp. 999–1010, Mar. 2013.

Jia Zhu received the B.Eng. degree in computer science and technology from Hohai University, Nanjing, China, in July 2005 and the Ph.D. degree in signal and information processing from Nanjing University of Posts and Telecommunications (NUPT) in April 2010.

She is currently an Associate Professor with NUPT. From June 2010 to June 2012, she was a Postdoctoral Research Fellow with Stevens Institute of Technology, Hoboken, NJ, USA. Since November 2012, she has been a full-time faculty member with the School of Telecommunication and Information, NUPT. Her main research interests include the cognitive radio, physical-layer security, and communications theory.

Yulong Zou (S'07–M'12–SM'13) received the B.Eng. degree in information engineering from Nanjing University of Posts and Telecommunications (NUPT), Nanjing, China, in July 2006; the Ph.D. degree in electrical engineering from Stevens Institute of Technology, Hoboken, NJ, USA, in May 2012; and the Ph.D. degree in signal and information processing from NUPT in July 2012.

He is currently a Full Professor with NUPT. His research interests include topics in wireless communications and signal processing, such as cooperative communications, cognitive radio, wireless security, and energy-efficient communications.

Dr. Zou has acted as a Symposium Chair, as a Session Chair, and as a Technical Program Committee member for a number of IEEE sponsored conferences, including the IEEE Wireless Communications and Networking Conference, the IEEE Global Communications Conference, the IEEE International Conference on Communications, the IEEE Vehicular Technology Conference, and the International Conference on Communications in China. He is currently serving as an Editor for the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, IEEE COMMUNICATIONS LETTERS, the *EURASIP Journal on Advances in Signal Processing*, and the *KSII Transactions on Internet and Information Systems*. He served as the Lead Guest Editor for a special issue on security challenges and issues in cognitive radio networks in the *EURASIP Journal on Advances in Signal Processing*. He is also serving as the Lead Guest Editor for a special issue on security and reliability challenges in industrial wireless sensor networks for the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS.

Gongpu Wang received the B.Eng. degree in communication engineering from Anhui University, Hefei, China, in 2001; the M.Sc. degree from Beijing University of Posts and Telecommunications, Beijing, China, in 2004; and the Ph.D. degree from the University of Alberta, Edmonton, AB, Canada, in 2011.

From 2004 to 2007, he was an Assistant Professor with the School of Network Education, Beijing University of Posts and Telecommunications. He is currently an Associate Professor with the School of Computer and Information Technology, Beijing Jiaotong University. His research interests include wireless communication theory and signal processing technologies.

Yu-Dong Yao (S'88–M'88–SM'94–F'11) received the B.Eng. and M.Eng. degrees from Nanjing University of Posts and Telecommunications, Nanjing, China, in 1982 and 1985, respectively, and the Ph.D. degree from Southeast University, Nanjing, in 1988, all in electrical engineering.

In 1987 and 1988, he was a Visiting Student with Carleton University, Ottawa, ON, Canada. From 1989 to 2000, he was with Carleton University, Spar Aerospace Ltd., Montreal, QC, Canada, and Qualcomm Inc., San Diego, CA, USA. Since 2000, he has been with Stevens Institute of Technology, Hoboken, NJ, USA, where he is currently a Professor and the Department Director of Electrical and Computer Engineering. He is also the Director of Stevens' Wireless Information Systems Engineering Laboratory (WISELAB). He is a holder of one Chinese patent and 13 U.S. patents. His research interests include wireless communications and networking, spread spectrum and code-division multiple access, and cognitive radio.

Dr. Yao has been active in the nonprofit organization WOCC, Inc., which promotes wireless and optical communications research and technical exchange. He served as WOCC President from 2008 to 2010 and as the Chair of the board of trustees from 2010 to 2012. He was an Associate Editor for the IEEE COMMUNICATIONS LETTERS from 2000 to 2008 and for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY from 2001 to 2006, as well as the Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2001 to 2005. He received the Advancement of Invention Award from the New Jersey Inventors Hall of Fame. He is a Distinguished Lecturer of the IEEE Communication Society for 2015–2016.

George K. Karagiannidis (M'96–SM'03–F'14) was born in Pithagorion, Samos Island, Greece. He received the University Diploma (five years) and the Ph.D. degree in electrical and computer engineering from the University of Patras, Patras, Greece, in 1987 and 1999, respectively.

From 2000 to 2004, he was a Senior Researcher with the Institute for Space Applications and Remote Sensing, National Observatory of Athens, Athens, Greece. Since June 2004, he has been with Aristotle University of Thessaloniki, Thessaloniki, Greece, where he is currently a Professor with the Department Electrical and Computer Engineering and the Director of the Digital Telecommunications Systems and Networks Laboratory. Since January 2014, he has been with Khalifa University, Abu Dhabi, United Arab Emirates, where he is currently a Professor with the Department of Electrical and Computer Engineering and the Coordinator of the ICT Cluster. He is the author or coauthor of more than 250 technical papers published in scientific journals and presented at international conferences. He is also the author of the Greek edition of a book on telecommunications systems and a coauthor of *Advanced Optical Wireless Communications Systems* (Cambridge, 2012). His research interests include digital communications systems with emphasis on communications theory, energy-efficient multiple-input–multiple-output and cooperative communications, satellite communications, cognitive radio, smart grid, and optical wireless communications.

Dr. Karagiannidis has served as a member of technical program committees for several IEEE conferences, such as the IEEE International Conference on Communications, the IEEE Global Communications Conference, and the IEEE Vehicular Technology Conference. He coreceived the Best Paper Award at the Wireless Communications Symposium in the IEEE International Conference on Communications in 2007, held in Glasgow, U.K. He served as an Editor on fading channels and diversity for the IEEE TRANSACTIONS ON COMMUNICATIONS, as a Senior Editor for IEEE COMMUNICATIONS LETTERS, as an Editor for the *EURASIP Journal of Wireless Communications & Networks*, as a Lead Guest Editor of the special issue on optical wireless communications, and as a Guest Editor of the special issue on large-scale multiple-antenna wireless systems for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He has been the Editor-in-Chief of IEEE COMMUNICATIONS LETTERS since January 2012.