Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks

Yulong Zou, *Senior Member, IEEE,* Xianbin Wang, *Senior Member, IEEE,* and Weiming Shen, *Fellow, IEEE*

Abstract—In this paper, we explore the physical-layer security in cooperative wireless networks with multiple relays where both amplify-and-forward (AF) and decode-and-forward (DF) protocols are considered. We propose the AF and DF based optimal relay selection (i.e., AF*b*ORS and DF*b*ORS) schemes to improve the wireless security against eavesdropping attack. For the purpose of comparison, we examine the traditional AF*b*ORS and DF*b*ORS schemes, denoted by T-AF*b*ORS and T-DF*b*ORS, respectively. We also investigate a so-called multiple relay combining (MRC) framework and present the traditional AF and DF based MRC schemes, called T-AF*b*MRC and T-DF*b*MRC, where multiple relays participate in forwarding the source signal to destination which then combines its received signals from the multiple relays. We derive closed-form intercept probability expressions of the proposed AF*b*ORS and DF*b*ORS (i.e., P-AF*b*ORS and P-DF*b*ORS) as well as the T-AF*b*ORS, T-DF*b*ORS, T-AF*b*MRC and T-DF*b*MRC schemes in the presence of eavesdropping attack. We further conduct an asymptotic intercept probability analysis to evaluate the diversity order performance of relay selection schemes and show that no matter which relaying protocol is considered (i.e., AF and DF), the traditional and proposed optimal relay selection approaches both achieve the diversity order M where M represents the number of relays. In addition, numerical results show that for both AF and DF protocols, the intercept probability performance of proposed optimal relay selection is strictly better than that of the traditional relay selection and multiple relay combining methods.

Index Terms—Relay selection, physical-layer security, intercept probability, diversity order, cooperative wireless networks.

I. INTRODUCTION

MULTIPLE-INPUT multiple-output (MIMO) [1], [2] has been widely recognized as an effective way to combat wireless fading and increase link throughput by exploiting multiple antennas at both the transmitter and receiver. However, it may be difficult to implement multiple antennas in some cases (e.g., handheld terminals, sensor nodes, etc.) due to the limitation in physical size and power consumption. As an alternative, user cooperation [3] is now emerging as

a promising paradigm to achieve the spatial diversity by enabling user terminals to share their antennas and form a virtual antenna array. Until recently, there has been extensive work on the user cooperation from different perspectives, e.g., cooperative resource allocation [4], performance analysis and optimization [5], [6], and cooperative medium access control (MAC) and routing design [7], [8].

User cooperation not only improves the reliability and throughput of wireless transmissions, but also has great potential to enhance the wireless security against eavesdropping attack. Differing from the conventional encryption techniques relying on secret keys, physical-layer security exploits the physical characteristics of wireless channels to prevent the eavesdropper from intercepting the signal transmission from source to its intended destination. It has been proven in [9] and [10] that in the presence of an eavesdropper, a so-called *secrecy capacity* is shown as the difference between the channel capacity from source to destination (called main link) and that from source to eavesdropper (called wiretap link). Moreover, if the secrecy capacity is negative, the eavesdropper will succeed in intercepting the source signal and an intercept event occurs in this case. Due to the fading effect, the secrecy capacity is severely limited in wireless communications. To that end, user cooperation as an emerging spatial diversity technique can effectively combat wireless fading and thus improves the secrecy capacity of wireless transmissions in the presence of eavesdropping attack.

At present, most of existing work on the user cooperation for wireless security is focused on developing the secrecy capacity from an information-theoretic perspective. In [11], the authors studied the secrecy capacity of wireless transmissions in the presence of an eavesdropper with a relay node, where the amplify-and-forward (AF), decode-and-forward (DF), and compress-and-forward (CF) relaying protocols are examined and compared with each other. The cooperative jamming was proposed in [12] and analyzed in terms of the achievable secrecy rate, where multiple users are allowed to cooperate with each other in preventing the eavesdropping attack. In [13], the cooperation strategy was further examined to enhance the physical-layer security and a so-called noise-forwarding scheme was proposed, where the relay node attempts to send codewords independent of the source message to confuse the eavesdropper. In [14] and [15], the authors studied the cooperative relays for enhancing physical-layer security and showed the security improvement by using cooperative relays. The physical-layer security was further examined in two-way relay networks in [16] and [17] where multiple two-way relays are exploited to improve the secrecy capacity

Y. Zou is with the Electrical and Computer Engineering Department, University of Western Ontario, London, ON N6A 5B9, Canada (e-mail: yulong.zou@gmail.com). He is also with the Institute of Signal Processing and Transmission, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

X. Wang is with the Electrical and Computer Engineering Department, University of Western Ontario, London, ON N6A 5B9, Canada.

W. Shen is with the College of Electronics and Information Engineering, Tongji University, Shanghai, China. He is also with the National Research Council, Canada.

against eavesdropping attack. In addition, [18] and [19] investigated the physical-layer security in MIMO relay networks and showed the significant improvement in terms of secrecy capacity through the use of MIMO relays.

In this paper, we consider a cooperative wireless network with multiple relays in the presence of an eavesdropper and examine the optimal relay selection to improve physical-layer security against eavesdropping attack. Differing from the traditional relay selection in [20]-[22] where only the channel state information (CSI) of two-hop relay links (i.e., source-relay and relay-destination) are considered, we here have to take into account additional CSI of the wiretap links, in addition to the two-hop relay links' CSI. The main contributions of this paper are summarized as follows. Firstly, considering AF and DF relaying protocols, we propose the AF and DF based optimal relay selection schemes which are denoted by P-AFbORS and P-DFbORS, respectively. We also examine the traditional AF and DF based optimal relay selection (i.e., T-AFbORS and T-DFbORS) and multiple relay combining (i.e., T-AFbMRC and T-DFbMRC) as benchmark schemes. Secondly, we derive closed-form expressions of intercept probability for the P-AFbORS and P-DFbORS as well as the T-AFbORS, T-DFbORS, T-AFbMRC and T-DFbMRC schemes in Rayleigh fading channels. It is shown that for both AF and DF protocols, the intercept probability of proposed optimal relay selection is always smaller than that of the traditional relay selection and multiple relay combining approaches, which shows the advantage of proposed optimal relay selection. Finally, we evaluate the diversity order performance of optimal relay selection schemes and show that no matter which relaying protocol is considered, the proposed and traditional optimal relay selection schemes both achieve the same diversity order M, where M represents the number of relays.

The remainder of this paper is organized as follows. Section II presents the system model and proposes the conventional direct transmission, T-AFbORS, T-DFbORS, T-AFbMRC, T-DFbMRC, P-AFbORS, and P-DFbORS schemes. In Section III, we derive closed-form intercept probability expressions of the direct transmission, T-AFbORS, T-DFbORS, T-AFbMRC, T-DFbMRC, P-AFbORS, and P-DFbORS schemes in the presence of eavesdropping attack. In Section IV, we analyze the diversity order performance of the traditional and proposed relay selection schemes. Next, in Section V, numerical evaluation is conducted to show the advantage of proposed optimal relay selection over traditional relay selection and multiple relay combining approaches in terms of the intercept probability. Finally, we make some concluding remarks in Section VI.

II. SYSTEM MODEL AND PROPOSED OPTIMAL RELAY SELECTION SCHEMES

A. System Model

Consider a cooperative wireless network consisting of one source, one destination, and M relays in the presence of an eavesdropper as shown in Fig. 1, where all nodes are equipped with single antenna and the solid and dash lines represent the main and wiretap links, respectively. The main and wiretap links both are modeled as Rayleigh fading channels and the thermal noise received at any node is modeled
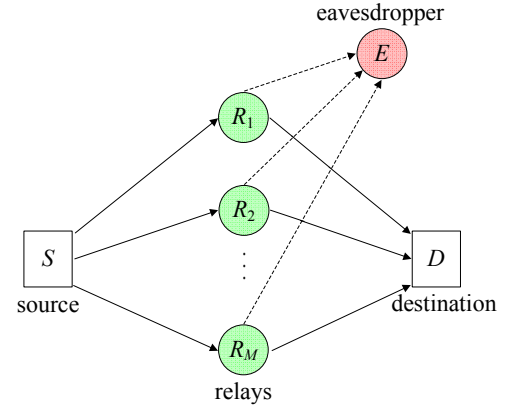

Fig. 1. A cooperative wireless network consisting of one source, one destination, and multiple relays in the presence of an eavesdropper.

as a complex Gaussian random variable with zero mean and variance σ_n^2, i.e., $\mathcal{CN}(0, \sigma_n^2)$. Following [14], we consider that M relays are exploited to assist the transmission from source to destination and the direct links from source to destination and eavesdropper are not available, e.g., the destination and eavesdropper both are out of the coverage area of source node. For notational convenience, M relays are denoted by $\mathcal{R} = \{R_i | i = 1, 2, \cdots, M\}$. We here consider the use of the optimal relay only to assist the signal transmission from source to destination. More specifically, the source node first broadcasts the message to cooperative relays among which only the best relay will be selected to forward its received signal to destination by using either the amplify-and-forward (AF) or decode-and-forward (DF) strategies. Meanwhile, the eavesdropper monitors the transmission from the optimal relay to destination and attempts to interpret the source message. Following the existing physical-layer security literature, we assume that the eavesdropper knows everything about the signal transmission from source via relay to destination, including the encoding scheme at source, forwarding protocol at relays, and decoding method at destination, except that the source signal is confidential.

It is pointed out that in order to effectively prevent the eavesdropper from intercepting, the optimal relay selection not only has to consider the CSI of main links to maximize the channel capacity from source to destination, but also needs to take into account the wiretap links' CSI to minimize the channel capacity from source to eavesdropper. This differs from the traditional relay selection in [20]-[22] where only the two-hop relay links' CSI is considered in performing the best relay selection. Similarly to [14] and [23], we here assume that the global CSI of both main and wiretap links is available, which is a common assumption in the physical-layer security literature. Moreover, if the eavesdropper's CSI is unknown, we can consider the use of traditional relay selection [20]-[22] which does not require the CSI of wiretap links. In the following, we first present the conventional direct transmission without relay as a benchmark scheme and then propose the AF and DF based optimal relay selection schemes to improve the physical-layer security against eavesdropping attack.

B. Direct Transmission

For comparison purpose, this subsection describes the conventional direct transmission without relay. Consider that the source transmits a signal s ($E(|s|^2) = 1$) with power P. Thus, the received signal at destination is expressed as

$$r_d = \sqrt{P}h_{sd}s + n_d, \tag{1}$$

where h_{sd} represents a fading coefficient of the channel from source to destination and $n_d \sim \mathcal{CN}(0, \sigma_n^2)$ represents additive white Gaussian noise (AWGN) at destination. Notice that the channel coefficient h_{sd} is modeled as Rayleigh fading which corresponds to an ideal OFDM subchannel [24] and [25]. Meanwhile, due to the broadcast nature of wireless transmissions, the eavesdropper also receives a copy of the source signal s and the corresponding received signal is written as

$$r_e = \sqrt{P}h_{se}s + n_e, \tag{2}$$

where h_{se} represents a fading coefficient of the channel from source to eavesdropper and $n_e \sim \mathcal{CN}(0, \sigma_n^2)$ represents AWGN at eavesdropper. Assuming the optimal Gaussian codebook used at source, the maximal achievable rate (also known as channel capacity) of the direct transmission from source to destination is obtained from Eq. (1) as

$$C_{sd}^{\text{direct}} = \log_2(1 + \frac{|h_{sd}|^2 P}{\sigma_n^2}), \tag{3}$$

where σ_n^2 is the noise variance. Similarly, from Eq. (2), the capacity of wiretap link from source to eavesdropper is easily given by

$$C_{se}^{\text{direct}} = \log_2(1 + \frac{|h_{se}|^2 P}{\sigma_n^2}). \tag{4}$$

It has been proven in [10] that the secrecy capacity is shown as the difference between the capacity of main link and that of wiretap link. Hence, the secrecy capacity of direct transmission is given by

$$C_s^{\text{direct}} = C_{sd}^{\text{direct}} - C_{se}^{\text{direct}}, \tag{5}$$

where C_{sd}^{direct} and C_{se}^{direct} are given in Eqs. (3) and (4), respectively. As discussed in [10], when the secrecy capacity is negative (i.e., the capacity of main link falls below the wiretap link's capacity), the eavesdropper will succeed in intercepting the source signal and an intercept event occurs. Thus, the probability that the eavesdropper successfully intercepts source signal, called *intercept probability*, is a key metric in evaluating the performance of physical-layer security. In this paper, we mainly focus on how to improve the intercept probability by exploiting cooperative relays for the physical-layer security enhancement. The following subsections propose the optimal relay selection by considering AF and DF protocols, respectively.

C. Amplify-and-Forward

In this subsection, we consider the AF relaying protocol in which the relay will forward a scaled version of its received source signal to destination without any sort of decoding. To be specific, the source node first broadcasts the signal s to M relays. Then, the optimal relay node will be selected to transmit a scaled version of its received signal. Notice that in the AF relaying process, the source signal s is transmitted twice from the source and relay. In order to make a fair comparison with the direct transmission, the total amount of transmit power at source and relay shall be limited to P. By using the equal-power allocation for simplicity, the transmit power at source and relay is given by $P/2$. Thus, considering that the source node transmits its signal s with power $P/2$, the received signal at relay R_i can be given by

$$r_i = \sqrt{\frac{P}{2}}h_{si}s + n_i, \tag{6}$$

where h_{si} represents a fading coefficient of the channel from source to R_i and $n_i \sim \mathcal{CN}(0, \sigma_n^2)$ represents AWGN at R_i. Without loss of generality, consider that R_i is selected as the optimal relay to forward its received signal to destination. Assuming that the CSI h_{si} is available, R_i first performs coherent detection by multiplying r_i with h_{si}^* and then normalizes $h_{si}^* r_i$ with a scaling factor $\frac{1}{|h_{si}|^2 \sqrt{P/2}}$. After that, R_i transmits the normalized $h_{si}^* r_i$ with power $P/2$ to destination, thus the received signal at destination is given by

$$\begin{aligned} r_d &= \sqrt{\frac{P}{2}}h_{id}\frac{h_{si}^* r_i}{|h_{si}|^2 \sqrt{P/2}} + n_d \\ &= \sqrt{\frac{P}{2}}h_{id}s + \frac{h_{id}h_{si}^*}{|h_{si}|^2}n_i + n_d, \end{aligned} \tag{7}$$

from which the capacity of AF relaying transmission from R_i to destination is given by

$$C_{id}^{\text{AF}} = \log_2\left(1 + \frac{|h_{si}|^2|h_{id}|^2 P}{2(|h_{si}|^2 + |h_{id}|^2)\sigma_n^2}\right). \tag{8}$$

Meanwhile, the received signal at eavesdropper from R_i is expressed as

$$r_e = \sqrt{\frac{P}{2}}h_{ie}s + \frac{h_{ie}h_{si}^*}{|h_{si}|^2}n_i + n_e. \tag{9}$$

Similarly to Eq. (8), we obtain the capacity of AF relaying transmission from R_i to eavesdropper as

$$C_{ie}^{\text{AF}} = \log_2\left(1 + \frac{|h_{si}|^2|h_{ie}|^2 P}{2(|h_{si}|^2 + |h_{ie}|^2)\sigma_n^2}\right). \tag{10}$$

Combining Eqs. (8) and (10), we can easily obtain the secrecy capacity of AF relaying transmission with R_i as

$$\begin{aligned} C_i^{\text{AF}} &= C_{id}^{\text{AF}} - C_{ie}^{\text{AF}} \\ &= \log_2\left(\frac{1 + \frac{|h_{si}|^2|h_{id}|^2 P}{2(|h_{si}|^2 + |h_{id}|^2)\sigma_n^2}}{1 + \frac{|h_{si}|^2|h_{ie}|^2 P}{2(|h_{si}|^2 + |h_{ie}|^2)\sigma_n^2}}\right). \end{aligned} \tag{11}$$

Next, we discuss how to determine the optimal relay and propose the AF based optimal relay selection scheme denoted by P-AF*b*ORS for notational convenience. For the comparison purpose, the traditional AF based optimal relay selection and multiple relay combining (i.e., T-AF*b*ORS and T-AF*b*MRC) are also presented.

1) P-AFbORS: Now, let us consider the P-AFbORS scheme in which the relay that maximizes the secrecy capacity of AF relaying transmission is viewed as the optimal relay. Thus, the AF based optimal relay selection criterion can be obtained from Eq. (11) as

$$
\begin{aligned}
\text{OptimalRelay} &= \arg\max_{i\in\mathcal{R}} C_i^{\text{AF}} \\
&= \arg\max_{i\in\mathcal{R}} \frac{1 + \dfrac{|h_{si}|^2|h_{id}|^2 P}{2(|h_{si}|^2+|h_{id}|^2)\sigma_n^2}}{1 + \dfrac{|h_{si}|^2|h_{ie}|^2 P}{2(|h_{si}|^2+|h_{ie}|^2)\sigma_n^2}},
\end{aligned} \quad (12)
$$

where $\mathcal{R}$ represents a set of M relays. One can observe from Eq. (12) that the P-AFbORS scheme takes into account not only the main links' CSI $|h_{si}|^2$ and $|h_{id}|^2$, but also the wiretap link's CSI $|h_{ie}|^2$. Notice that the transmit power P in Eq. (12) is a known parameter and the noise variance σ_n^2 is shown as $\sigma_n^2 = \kappa T B$ [26], where κ is Boltzmann constant (i.e., $\kappa = 1.38 \times 10^{-23}$), T is room temperature, and B is system bandwidth. Since the room temperature T and system bandwidth B both are predetermined, the noise variance σ_n^2 can be easily obtained. It is pointed out that using the proposed optimal relay selection criterion in Eq. (12), we can further develop a centralized or distributed relay selection algorithm. To be specific, for a centralized relay selection, the source node needs to maintain a table that consists of M relays and related CSI (i.e., $|h_{si}|^2$, $|h_{id}|^2$ and $|h_{ie}|^2$). In this way, the optimal relay can be easily determined by looking up the table using the proposed criterion in Eq. (12), which is referred to as centralized relay selection strategy. For a distributed relay selection, each relay maintains a timer and sets an initial value of the timer in inverse proportional to $[1 + \frac{|h_{si}|^2|h_{id}|^2 P}{2(|h_{si}|^2+|h_{id}|^2)\sigma_n^2}]/[1 + \frac{|h_{si}|^2|h_{ie}|^2 P}{2(|h_{si}|^2+|h_{ie}|^2)\sigma_n^2}]$, resulting in the optimal relay with the smallest initial value for its timer. As a consequence, the optimal relay exhausts its timer earliest compared with the other relays, and then broadcasts a control packet to notify the source node and other relays [21].

2) T-AFbORS: For the purpose of comparison, we here present the traditional AF based optimal relay selection (T-AFbORS) scheme. Since the wiretap link's CSI $|h_{ie}|^2$ is not considered in T-AFbORS scheme, a relay node with the largest C_{id}^{AF} (i.e., the capacity from R_i to destination) is selected as the optimal relay. Therefore, the traditional AF based optimal relay selection criterion is obtained from Eq. (8) as

$$
\begin{aligned}
\text{OptimalRelay} &= \arg\max_{i\in\mathcal{R}} C_{id}^{\text{AF}} \\
&= \arg\max_{i\in\mathcal{R}} \frac{|h_{si}|^2|h_{id}|^2}{|h_{si}|^2+|h_{id}|^2},
\end{aligned} \quad (13)
$$

which is the so-called harmonic mean policy as given by Eq. (2) in [20]. It is shown from Eq. (13) that only the main links' CSI $|h_{si}|^2$ and $|h_{id}|^2$ is taken into account in the T-AFbORS scheme, differing from the P-AFbORS scheme that requires the CSI of both main and wiretap links (i.e., $|h_{si}|^2$, $|h_{id}|^2$ and $|h_{ie}|^2$).

3) T-AFbMRC: This subsection presents the traditional AF based multiple relay combining (T-AFbMRC) scheme, where all AF relays participate in forwarding the source signal transmission to destination which combines its received signals

from the multiple AF relays. Notice that in the T-AFbMRC scheme, the total amount of transmit power consumed at the source and M relays should be constrained to a fixed value (i.e., P). With the equal-power allocation, the transmit power for each node (e.g., the source and relays) is given by $P/(M+1)$. Thus, the source node first transmits the signal s with power $P/(M+1)$ to M relays that will normalize their received signals with respective scaling factors $\frac{1}{|h_{si}|^2\sqrt{P/(M+1)}}$ wherein $i = 1, 2, \cdots, M$. Then, all relays forward their normalized signals to destination with power $P/(M+1)$. Hence, the received signal at destination from relay R_i can be expressed as

$$
r_d^i = \sqrt{\frac{P}{M+1}} h_{id}s + \frac{h_{id}h_{si}^*}{|h_{si}|^2}n_i + n_d^i, \quad (14)
$$

where n_i and n_d^i represent AWGN received at relay R_i and destination, respectively. The destination combines its received signals from multiple AF relays, where the combining coefficient $|h_{si}|^2 h_{id}^*$ is considered for the received signal r_d^i from relay R_i. Accordingly, the combined signal denoted by r_d at destination is given by

$$
\begin{aligned}
r_d = &\sum_{i=1}^{M} \sqrt{\frac{P}{M+1}} |h_{si}|^2|h_{id}|^2 s \\
&+ \sum_{i=1}^{M} \left(|h_{id}|^2 h_{si}^* n_i + |h_{si}|^2 h_{id}^* n_d^i \right),
\end{aligned} \quad (15)
$$

from which the transmission capacity from source to destination via M relays with the T-AFbMRC scheme is given by

$$
C_{sd}^{\text{AFbMRC}} = \log_2\left(1 + \frac{(\sum\limits_{i=1}^{M}|h_{si}|^2|h_{id}|^2)^2 P}{(M+1)\sum\limits_{i=1}^{M} H(h_{si},h_{id})\sigma_n^2} \right), \quad (16)
$$

where $H(h_{si},h_{id}) = |h_{si}|^2|h_{id}|^4 + |h_{si}|^4|h_{id}|^2$ and σ_n^2 represents the noise variance. Also, the transmission capacity from source to eavesdropper with the T-AFbMRC scheme is similarly obtained as

$$
C_{se}^{\text{AFbMRC}} = \log_2\left(1 + \frac{(\sum\limits_{i=1}^{M}|h_{si}|^2|h_{ie}|^2)^2 P}{(M+1)\sum\limits_{i=1}^{M} H(h_{si},h_{ie})\sigma_n^2} \right), \quad (17)
$$

where $H(h_{si},h_{ie}) = |h_{si}|^2|h_{ie}|^4 + |h_{si}|^4|h_{ie}|^2$. Hence, the secrecy capacity of T-AFbMRC scheme is shown as

$$
C_s^{\text{AFbMRC}} = C_{sd}^{\text{AFbMRC}} - C_{se}^{\text{AFbMRC}}, \quad (18)
$$

where C_{sd}^{AFbMRC} and C_{se}^{AFbMRC} are given by Eqs. (16) and (17), respectively.

D. Decode-and-Forward

This subsection mainly focuses on the DF relaying protocol in which the relay first decodes its received signal from source and then re-encodes and transmits its decoded outcome to the destination. More specifically, the source node first broadcasts the signal s to M relays that attempt to decode their received signals. Then, only the optimal relay is selected to re-encode

and transmit its decoded outcome to the destination. Similarly to AF relaying protocol, the total transmit power at source and relay with DF protocol is also limited to P in order to make a fair comparison with the direct transmission. Considering the equal-power allocation, we obtain the transmit power at source and relay as $P/2$. It has been shown in [2] that the capacity of DF relaying transmission is the minimum of the capacity from source to relay and that from relay to destination, since either source-relay or relay-destination links in failure will result in the two-hop DF transmission in failure. Hence, considering R_i as the optimal relay, we can obtain the capacity of DF transmission from source via R_i to destination as

$$C_{sid}^{\mathrm{DF}} = \min(C_{si}, C_{id}), \tag{19}$$

where C_{si} and C_{id}, respectively, represent the channel capacity from source to R_i and that from R_i to destination, which are given by

$$C_{si} = \log_2(1 + \frac{|h_{si}|^2 P}{2\sigma_n^2}), \tag{20}$$

and

$$C_{id} = \log_2(1 + \frac{|h_{id}|^2 P}{2\sigma_n^2}). \tag{21}$$

Meanwhile, the eavesdropper can overhear the transmission from R_i. Hence, the channel capacity from R_i to eavesdropper can be easily obtained as

$$C_{ie}^{\mathrm{DF}} = \log_2(1 + \frac{|h_{ie}|^2 P}{2\sigma_n^2}). \tag{22}$$

Combining Eqs. (19) and (22), the secrecy capacity of DF relaying transmission with R_i is given by

$$\begin{aligned} C_i^{\mathrm{DF}} &= C_{sid}^{\mathrm{DF}} - C_{ie}^{\mathrm{DF}} \\ &= \log_2\left(1 + \frac{\min(|h_{si}|^2, |h_{id}|^2)P}{2\sigma_n^2}\right) \\ &\quad - \log_2\left(1 + \frac{|h_{ie}|^2 P}{2\sigma_n^2}\right). \end{aligned} \tag{23}$$

In the following subsections, we present the P-DF*b*ORS and T-DF*b*ORS schemes, respectively. For the comparison purpose, the traditional DF based multiple relay combining (T-DF*b*MRC) scheme is also discussed.

1) P-DFbORS: Let us first consider P-DF*b*ORS scheme. Similarly to P-AF*b*ORS scheme, we consider the relay that maximizes the secrecy capacity of DF relaying transmission as the optimal relay. Thus, the DF based optimal relay selection criterion is easily obtained from Eq. (23) as

$$\begin{aligned} \mathrm{OptimalRelay} &= \arg\max_{i \in \mathcal{R}} C_i^{\mathrm{DF}} \\ &= \arg\max_{i \in \mathcal{R}} \frac{\min(|h_{si}|^2, |h_{id}|^2)P + 2\sigma_n^2}{|h_{ie}|^2 P + 2\sigma_n^2}, \end{aligned} \tag{24}$$

which shows that the global CSI of both main and wiretap links (i.e., $|h_{si}|^2$, $|h_{id}|^2$ and $|h_{ie}|^2$) is required in determining the optimal relay.

2) T-DFbORS: We now present the traditional DF based optimal relay selection (T-DF*b*ORS) scheme in which the relay that maximizes the capacity of DF relaying transmission C_{sid}^{DF} is selected as the optimal relay. Thus, the traditional DF based optimal relay selection criterion is obtained from Eq. (19) as

$$\begin{aligned} \mathrm{OptimalRelay} &= \arg\max_{i \in \mathcal{R}} C_{sid}^{\mathrm{DF}} \\ &= \arg\max_{i \in \mathcal{R}} \min(|h_{si}|^2, |h_{id}|^2), \end{aligned} \tag{25}$$

which is the traditional max-min relay selection criterion as given by Eq. (1) in [20]. As shown in Eq. (25), only the main links' CSI $|h_{si}|^2$ and $|h_{id}|^2$ is taken into account in T-DF*b*ORS scheme without considering the wiretap link's CSI $|h_{ie}|^2$.

3) T-DFbMRC: This subsection presents the T-DF*b*MRC scheme where multiple DF relays will assist the signal transmission from source to destination. To be specific, the source node first transmits its signal s with power $P/2$ to M relays which then attempt to decode their received signals. For notational convenience, these relays that succeed in decoding the source signal are represented by a set D, called *decoding set*, where the sample space of decoding set is given by $\Omega = \{\emptyset, \bigcup D_m, m = 1, 2, \cdots, 2^M - 1\}$, where $\cup$ denotes the union operation, $\emptyset$ denotes empty set, and D_m denotes a non-empty subcollection of M relays. If the decoding set is empty (i.e., all relays fail to decode the source signal), no relay will transmit and thus both the destination and eavesdropper cannot interpret the source signal. If the decoding set D is not empty (i.e., $D = D_m$), all relays in D_m are selected to forward their decoded outcomes to destination, where the total transmit power of multiple relays in the decoding set is constrained to $P/2$. With the equal-power allocation, the transmit power for each relay in decoding set D_m is given by $P/(2|D_m|)$, where $|D_m|$ represents the cardinality of set D_m (i.e., the number of elements in set D_m). Thus, considering that relay $R_i \in D_m$ transmits its decoded result s with power $P/(2|D_m|)$, the received signal at destination is given by

$$r_d^i = \sqrt{\frac{P}{2|D_m|}} h_{id}s + n_d^i. \tag{26}$$

Then, the destination combines its received signals from multiple DF relays in decoding set D_m with the maximal ratio combining. Thus, the combined signal denoted by r_d at destination can be written as

$$r_d = \sum_{i \in D_m} \sqrt{\frac{P}{2|D_m|}} |h_{id}|^2 s + \sum_{i \in D_m} h_{id}^* n_d^i, \tag{27}$$

from which the transmission capacity from source to destination with the T-DF*b*MRC scheme in the case of $D = D_m$ is given by

$$C_{sd}^{\mathrm{DFbMRC}}(D = D_m) = \log_2\left(1 + \sum_{i \in D_m} \frac{|h_{id}|^2 P}{2|D_m|\sigma_n^2}\right), \tag{28}$$

where σ_n^2 represents the noise variance. Similarly, the transmission capacity from source to eavesdropper with the T-DF*b*MRC scheme can be obtained as

$$C_{se}^{\mathrm{DFbMRC}}(D = D_m) = \log_2\left(1 + \sum_{i \in D_m} \frac{|h_{ie}|^2 P}{2|D_m|\sigma_n^2}\right). \tag{29}$$

Hence, combining Eqs. (28) and (29), the secrecy capacity of T-DFbMRC scheme in the case of $D = D_m$ is given by

$$
\begin{aligned}
C_s^{\text{DF}b\text{MRC}} (D = D_m) =& C_{sd}^{\text{DF}b\text{MRC}} (D = D_m) \\
& - C_{se}^{\text{DF}b\text{MRC}} (D = D_m),
\end{aligned}
\tag{30}
$$

which completes the signal modeling of T-DFbMRC scheme.

III. INTERCEPT PROBABILITY ANALYSIS OVER RAYLEIGH FADING CHANNELS

In this section, we derive closed-form intercept probability expressions of conventional direct transmission, P-AFbORS, P-DFbORS, T-AFbORS, T-DFbORS, T-AFbMRC, and T-DFbMRC schemes over Rayleigh fading channels.

A. Direct Transmission

Let us first analyze the intercept probability of direct transmission as a baseline for comparison purpose. As is discussed, an intercept event occurs when the secrecy capacity becomes negative. Thus, the intercept probability of direct transmission is obtained from Eq. (5) as

$$
\begin{aligned}
P_{\text{intercept}}^{\text{direct}} &= \Pr \left(C_{sd}^{\text{direct}} < C_{se}^{\text{direct}} \right) \\
&= \Pr \left(|h_{sd}|^2 < |h_{se}|^2 \right),
\end{aligned}
\tag{31}
$$

where the second equation is obtained by using Eqs. (3) and (4). Since the Rayleigh fading model is used throughout this paper, we can obtain that $|h_{sd}|^2$ and $|h_{se}|^2$ follow exponential distributions. Thus, a closed-form intercept probability expression of direct transmission is given by

$$
P_{\text{intercept}}^{\text{direct}} = \frac{\sigma_{se}^2}{\sigma_{se}^2 + \sigma_{sd}^2},
\tag{32}
$$

where $\sigma_{se}^2 = E(|h_{se}|^2)$ and $\sigma_{sd}^2 = E(|h_{sd}|^2)$. It is observed from Eq. (32) that the intercept probability of direct transmission is independent of the transmit power P, which implies that the wireless security performance cannot be improved by increasing the transmit power. This also motivates us to exploit cooperative relays to decrease the intercept probability and improve the physical-layer security.

B. P-AFbORS

In this subsection, we present the intercept probability analysis of P-AFbORS scheme. Considering the fact that an intercept event occurs when the secrecy capacity falls below zero, we can obtain the intercept probability of P-AFbORS scheme from Eq. (12) as

$$
\begin{aligned}
P_{\text{intercept}}^{\text{P-AF}b\text{ORS}} &= \Pr \left(\max_{i \in \mathcal{R}} C_i^{\text{AF}} < 0 \right) \\
&= \prod_{i=1}^{M} \Pr \left(|h_{ie}|^2 > |h_{id}|^2 \right),
\end{aligned}
\tag{33}
$$

where the second equation is obtained by using Eq. (11). Considering that $|h_{ie}|^2$ and $|h_{id}|^2$ are independent exponentially distributed random variables, we obtain

$$
P_{\text{intercept}}^{\text{P-AF}b\text{ORS}} = \prod_{i=1}^{M} \frac{\sigma_{ie}^2}{\sigma_{ie}^2 + \sigma_{id}^2},
\tag{34}
$$

where $\sigma_{ie}^2 = E(|h_{ie}|^2)$ and $\sigma_{id}^2 = E(|h_{id}|^2)$.

C. P-DFbORS

This subsection derives a closed-form intercept probability expression of P-DFbORS scheme. According to the definition of intercept event, an intercept probability of P-DFbORS scheme is obtained from Eq. (24) as

$$
\begin{aligned}
P_{\text{intercept}}^{\text{P-DF}b\text{ORS}} &= \Pr \left(\max_{i \in \mathcal{R}} C_i^{\text{DF}} < 0 \right) \\
&= \prod_{i=1}^{M} \Pr \left\{ \min(|h_{si}|^2, |h_{id}|^2) < |h_{ie}|^2 \right\},
\end{aligned}
\tag{35}
$$

where the second equation is obtained by using Eq. (23). Notice that random variables $|h_{si}|^2$, $|h_{id}|^2$ and $|h_{ie}|^2$ follow exponential distributions with means σ_{si}^2, σ_{id}^2 and σ_{ie}^2, respectively. Denoting $X = \min(|h_{si}|^2, |h_{id}|^2)$, we can easily obtain the cumulative density function (CDF) of X as

$$
P_X(X < x) = 1 - \exp(-\frac{x}{\sigma_{si}^2} - \frac{x}{\sigma_{id}^2}),
\tag{36}
$$

wherein $x \geq 0$. Using Eq. (36), we have

$$
\begin{aligned}
&\Pr \left\{ \min(|h_{si}|^2, |h_{id}|^2) < |h_{ie}|^2 \right\} \\
&= \int_0^\infty [1 - \exp(-\frac{x}{\sigma_{si}^2} - \frac{x}{\sigma_{id}^2})] \frac{1}{\sigma_{ie}^2} \exp(-\frac{x}{\sigma_{ie}^2}) dx \\
&= \frac{\sigma_{id}^2 \sigma_{ie}^2 + \sigma_{si}^2 \sigma_{ie}^2}{\sigma_{id}^2 \sigma_{ie}^2 + \sigma_{si}^2 \sigma_{ie}^2 + \sigma_{si}^2 \sigma_{id}^2}.
\end{aligned}
\tag{37}
$$

Substituting Eq. (37) into Eq. (35) gives

$$
P_{\text{intercept}}^{\text{P-DF}b\text{ORS}} = \prod_{i=1}^{M} \frac{\sigma_{id}^2 \sigma_{ie}^2 + \sigma_{si}^2 \sigma_{ie}^2}{\sigma_{id}^2 \sigma_{ie}^2 + \sigma_{si}^2 \sigma_{ie}^2 + \sigma_{si}^2 \sigma_{id}^2}.
\tag{38}
$$

In addition, we can easily prove $\frac{\sigma_{ie}^2}{\sigma_{ie}^2 + \sigma_{si}^2} < \frac{\sigma_{id}^2 \sigma_{ie}^2 + \sigma_{si}^2 \sigma_{ie}^2}{\sigma_{id}^2 \sigma_{ie}^2 + \sigma_{si}^2 \sigma_{ie}^2 + \sigma_{si}^2 \sigma_{id}^2}$. Considering $\frac{\sigma_{ie}^2}{\sigma_{ie}^2 + \sigma_{si}^2} > 0$ and $\frac{\sigma_{id}^2 \sigma_{ie}^2 + \sigma_{si}^2 \sigma_{ie}^2}{\sigma_{id}^2 \sigma_{ie}^2 + \sigma_{si}^2 \sigma_{ie}^2 + \sigma_{si}^2 \sigma_{id}^2} > 0$, we obtain

$$
\prod_{i=1}^{M} \frac{\sigma_{ie}^2}{\sigma_{ie}^2 + \sigma_{si}^2} < \prod_{i=1}^{M} \frac{\sigma_{id}^2 \sigma_{ie}^2 + \sigma_{si}^2 \sigma_{ie}^2}{\sigma_{id}^2 \sigma_{ie}^2 + \sigma_{si}^2 \sigma_{ie}^2 + \sigma_{si}^2 \sigma_{id}^2},
\tag{39}
$$

which theoretically shows that the intercept probability of P-AFbORS scheme is strictly less than that of P-DFbORS scheme, implying the advantage of AF relaying protocol over DF protocol from the physical-layer security perspective.

D. T-AFbORS

In this subsection, we present the intercept probability analysis of T-AFbORS scheme. From Eq. (13), we obtain an intercept probability of T-AFbORS scheme as

$$
P_{\text{intercept}}^{\text{T-AF}b\text{ORS}} = \Pr \left(\max_{i \in \mathcal{R}} C_{id}^{\text{AF}} < C_{oe}^{\text{AF}} \right),
\tag{40}
$$

where C_{oe}^{AF} denotes the channel capacity from the optimal relay to eavesdropper. It is pointed out that the T-AFbORS scheme does not consider the eavesdropper's CSI $|h_{ie}|^2$. This means that the traditional relay selection is independent of the eavesdropper's channel information. Using the law of total

probability, the intercept probability of T-AFbORS scheme is given by

$$P_{\text{intercept}}^{\text{T-AF}b\text{ORS}} = \sum_{m=1}^{M} \Pr\left(\text{OptimalRelay} = m\right) \times \Pr\left(\max_{i\in\mathcal{R}} C_{id}^{\text{AF}} < C_{me}^{\text{AF}}\right). \quad (41)$$

For simplicity, we here consider that fading coefficients h_{si} and h_{id} $(i = 1, \cdots, M)$ are identically and independently distributed, leading to $\Pr\left(\text{OptimalRelay} = m\right) = 1/M$. Substituting this result and Eq. (13) into Eq. (41) yields

$$P_{\text{intercept}}^{\text{T-AF}b\text{ORS}} = \sum_{m=1}^{M} \frac{1}{M} \Pr\left(\begin{array}{c} \max\limits_{i\in\mathcal{R}} \dfrac{|h_{si}|^2 |h_{id}|^2}{|h_{si}|^2 + |h_{id}|^2} \\ < \dfrac{|h_{sm}|^2 |h_{me}|^2}{|h_{sm}|^2 + |h_{me}|^2} \end{array} \right). \quad (42)$$

It is noted that obtaining a closed-form solution to Eq. (42) is challenging, however numerical intercept probability results of T-AFbORS scheme can be easily obtained through computer simulations.

E. T-DFbORS

This subsection analyzes the intercept probability of T-DFbORS scheme in Rayleigh fading channels. From Eq. (25), we obtain an intercept probability of T-DFbORS scheme as

$$P_{\text{intercept}}^{\text{T-DF}b\text{ORS}} = \Pr\left(\max_{i\in\mathcal{R}} C_{sid}^{\text{DF}} < C_{oe}^{\text{DF}}\right), \quad (43)$$

where C_{oe}^{DF} denotes the channel capacity from the optimal relay to eavesdropper with DF relaying protocol. Similarly, assuming that h_{si} and h_{id} $(i = 1, \cdots, M)$ are identically and independently distributed and using the law of total probability, the intercept probability of T-DFbORS scheme is given by

$$P_{\text{intercept}}^{\text{T-DF}b\text{ORS}} = \sum_{m=1}^{M} \frac{1}{M} \Pr\left(\begin{array}{c} \max\limits_{i\in\mathcal{R}} \min\left(|h_{si}|^2, |h_{id}|^2\right) \\ < |h_{me}|^2 \end{array} \right). \quad (44)$$

Notice that $|h_{si}|^2$, $|h_{id}|^2$ and $|h_{me}|^2$ follow exponential distributions with means σ_{si}^2, σ_{id}^2 and σ_{me}^2, respectively. Using Eq. (44) and letting $x = |h_{me}|^2$, we obtain Eq. (45) at the top of following page, where the second equation is obtained by using the binomial expansion, $\mathcal{A}_k$ represents the k-th non-empty sub-collection of M relays, and $|\mathcal{A}_k|$ represents the number of elements in set $\mathcal{A}_k$.

F. T-AFbMRC

This subsection presents the intercept probability analysis of T-AFbMRC scheme. From Eq. (18), an intercept probability of the T-AFbMRC scheme is obtained as

$$P_{\text{intercept}}^{\text{T-AF}b\text{MRC}} = \Pr\left(C_{sd}^{\text{AF}b\text{MRC}} < C_{se}^{\text{AF}b\text{MRC}}\right). \quad (46)$$

Substituting Eqs. (16) and (17) into Eq. (46) gives

$$P_{\text{intercept}}^{\text{T-AF}b\text{MRC}} = \Pr\left(\begin{array}{c} \dfrac{(\sum\limits_{i=1}^{M} |h_{si}|^2 |h_{id}|^2)^2}{\sum\limits_{i=1}^{M} H(h_{si}, h_{id})} \\[2ex] < \dfrac{(\sum\limits_{i=1}^{M} |h_{si}|^2 |h_{ie}|^2)^2}{\sum\limits_{i=1}^{M} H(h_{si}, h_{ie})} \end{array} \right), \quad (47)$$

where $H(h_{si}, h_{id}) = |h_{si}|^2 |h_{id}|^4 + |h_{si}|^4 |h_{id}|^2$ and $H(h_{si}, h_{ie}) = |h_{si}|^2 |h_{ie}|^4 + |h_{si}|^4 |h_{ie}|^2$. From Eq. (47), the numerical intercept probability results of T-AFbMRC scheme can be easily determined through computer simulations.

G. T-DFbMRC

In this subsection, the intercept probability analysis of T-DFbMRC scheme is presented. Using the law of total probability, we can obtain an intercept probability of the T-DFbMRC scheme from Eq. (30) as

$$P_{\text{intercept}}^{\text{T-DF}b\text{MRC}} = \sum_{m=1}^{2^M - 1} \Pr\left(D = D_m\right) \times \Pr\left(C_s^{\text{DF}b\text{MRC}}(D = D_m) < 0\right), \quad (48)$$

where $\Pr\left(D = D_m\right)$ represents the probability of occurrence of event $D = D_m$. Notice that if the decoding set is empty, all relays keep silent and nothing is transmitted, implying that the eavesdropper cannot intercept the source signal. Substituting Eqs. (28) and (29) into Eq. (48) yields

$$P_{\text{intercept}}^{\text{T-DF}b\text{MRC}} = \sum_{m=1}^{2^M - 1} \Pr\left(D = D_m\right) \times \Pr\left(\sum_{i\in D_m} |h_{id}|^2 < \sum_{i\in D_m} |h_{ie}|^2\right). \quad (49)$$

According to Shannon's channel coding theorem, relay R_i can succeed in decoding the source signal if no outage event occurs over the channel from source to relay R_i. Otherwise, relay R_i is deemed to fail to decode the source signal. Thus, the probability of occurrence of event $D = D_m$ can be given by

$$\Pr\left(D = D_m\right) = \prod_{i\in D_m} \left(1 - \text{Pout}_i\right) \prod_{i\in \bar{D}_m} \text{Pout}_i, \quad (50)$$

where $\bar{D}_m = \mathcal{R} - D_m$ represents the complementary set of D_m and Pout_i represents the probability of occurrence of outage event over the channel from source to relay R_i. So far, we have completed the intercept probability analysis of direct transmission, P-AFbORS, P-DFbORS, T-AFbORS, T-DFbORS, T-AFbMRC, and T-DFbMRC schemes.

IV. DIVERSITY ORDER ANALYSIS

In this section, we analyze the diversity order performance of the traditional and proposed optimal relay selection schemes

$$
\begin{aligned}
P_{\text{intercept}}^{\text{T-DF}b\text{ORS}} &= \sum_{m=1}^{M} \frac{1}{M} \int_0^{\infty} \prod_{i=1}^{M} [1 - \exp(-\frac{x}{\sigma_{si}^2} - \frac{x}{\sigma_{id}^2})] \frac{1}{\sigma_{me}^2} \exp(-\frac{x}{\sigma_{me}^2}) dx \\
&= \sum_{m=1}^{M} \frac{1}{M} \int_0^{\infty} \left(1 + \sum_{k=1}^{2^M-1} (-1)^{|\mathcal{A}_k|} \exp[-\sum_{i \in \mathcal{A}_k} (\frac{x}{\sigma_{si}^2} + \frac{x}{\sigma_{id}^2})] \right) \frac{1}{\sigma_{me}^2} \exp(-\frac{x}{\sigma_{me}^2}) dx \\
&= \sum_{m=1}^{M} \frac{1}{M} \left(1 + \sum_{k=1}^{2^M-1} (-1)^{|\mathcal{A}_k|} [1 + \sum_{i \in \mathcal{A}_k} (\frac{\sigma_{me}^2}{\sigma_{si}^2} + \frac{\sigma_{me}^2}{\sigma_{id}^2})]^{-1} \right)
\end{aligned}
\tag{45}
$$

including the T-AFbORS, T-DFbORS, P-AFbORS, and P-DFbORS. Let us first recall the traditional definition of diversity gain. As shown in [27], the traditional diversity gain is given by

$$
d = - \lim_{\text{SNR} \to \infty} \frac{\log P_e(\text{SNR})}{\log \text{SNR}},
\tag{51}
$$

where SNR denotes signal-to-noise ratio (SNR) and $P_e(\text{SNR})$ denotes bit error rate. One can observe from the preceding equation that the traditional diversity gain is defined as SNR $\to \infty$. However, the intercept probability expressions as shown in Eqs. (32), (34) and (38) are independent of SNR, leading to the fact that the traditional diversity gain definition is not applicable here. To that end, we propose a generalized diversity gain as follows

$$
d_{\text{generalized}} = - \lim_{\lambda_{de} \to \infty} \frac{\log(P_{\text{intercept}})}{\log(\lambda_{de})},
\tag{52}
$$

where $\lambda_{de} = \sigma_{sd}^2/\sigma_{se}^2$ is the ratio of average channel gain from source to destination to that from source to eavesdropper, which is referred to as the main-to-eavesdropper ratio (MER) throughout this paper.

A. Direct Transmission

Let us first analyze the diversity order of direct transmission as a baseline. From Eqs. (32) and (52), the diversity order of direct transmission is obtained as

$$
d_{\text{direct}} = - \lim_{\lambda_{de} \to \infty} \frac{\log(P_{\text{intercept}}^{\text{direct}})}{\log(\lambda_{de})} = 1,
\tag{53}
$$

which shows that the direct transmission achieves the diversity order of only one, i.e., the intercept probability of direct transmission scheme behaves as $\frac{1}{\lambda_{de}}$ in high main-to-eavesdropper ratio (MER) regions.

B. P-AFbORS

This subsection presents the diversity order analysis of P-AFbORS scheme. Similarly, the diversity order of P-AFbORS scheme is given by

$$
d_{\text{P-AF}b\text{ORS}} = - \lim_{\lambda_{de} \to \infty} \frac{\log(P_{\text{intercept}}^{\text{P-AF}b\text{ORS}})}{\log(\lambda_{de})},
\tag{54}
$$

where $P_{\text{intercept}}^{\text{P-AF}b\text{ORS}}$ is given in Eq. (34). Denoting $\sigma_{id}^2 = \alpha_{id}\sigma_{sd}^2$ and $\sigma_{ie}^2 = \alpha_{ie}\sigma_{se}^2$, we can rewrite $P_{\text{intercept}}^{\text{P-AF}b\text{ORS}}$ from Eq. (34) as

$$
P_{\text{intercept}}^{\text{P-AF}b\text{ORS}} = \prod_{i=1}^{M} \frac{\alpha_{ie}}{\alpha_{ie}\lambda_{de}^{-1} + \alpha_{id}} \cdot (\frac{1}{\lambda_{de}})^M,
\tag{55}
$$

where $\lambda_{de} = \sigma_{sd}^2/\sigma_{se}^2$. Substituting Eq. (55) into Eq. (54) gives

$$
d_{\text{P-AF}b\text{ORS}} = M,
\tag{56}
$$

which shows that the diversity order M is achieved by P-AFbORS scheme. One can see that as the number of relays M increases, the diversity order of P-AFbORS scheme increases accordingly, showing that increasing the number of relays can significantly improve the intercept probability performance.

C. P-DFbORS

In this subsection, we focus on the diversity order analysis of P-DFbORS scheme. Similarly to Eq. (54), the diversity order of P-DFbORS scheme is given by

$$
d_{\text{P-DF}b\text{ORS}} = - \lim_{\lambda_{de} \to \infty} \frac{\log(P_{\text{intercept}}^{\text{P-DF}b\text{ORS}})}{\log(\lambda_{de})},
\tag{57}
$$

where $P_{\text{intercept}}^{\text{P-DF}b\text{ORS}}$ is given in Eq. (38). Denoting $\sigma_{id}^2 = \alpha_{id}\sigma_{sd}^2$, $\sigma_{ie}^2 = \alpha_{ie}\sigma_{se}^2$ and $\sigma_{si}^2 = \alpha_{si}\sigma_{sd}^2$, we can rewrite $P_{\text{intercept}}^{\text{P-DF}b\text{ORS}}$ from Eq. (38) as

$$
\begin{aligned}
P_{\text{intercept}}^{\text{P-DF}b\text{ORS}} &= \prod_{i=1}^{M} \frac{\alpha_{id} + \alpha_{si}}{\alpha_{id}\lambda_{de}^{-1} + \alpha_{si}\lambda_{de}^{-1} + \alpha_{si}\alpha_{id}\alpha_{ie}^{-1}} \\
&\times (\frac{1}{\lambda_{de}})^M,
\end{aligned}
\tag{58}
$$

where $\lambda_{de} = \sigma_{sd}^2/\sigma_{se}^2$. Substituting Eq. (58) into Eq. (57) yields

$$
d_{\text{P-DF}b\text{ORS}} = M.
\tag{59}
$$

It is shown from Eq. (59) that the P-DFbORS scheme achieves the diversity order M, i.e., the intercept probability of P-DFbORS scheme behaves as $(\frac{1}{\lambda_{de}})^M$ for $\lambda_{de} \to \infty$.

D. T-AFbORS

We now examine the diversity order of T-AFbORS scheme. The diversity order of T-AFbORS scheme is given by

$$
d_{\text{T-AF}b\text{ORS}} = - \lim_{\lambda_{de} \to \infty} \frac{\log(P_{\text{intercept}}^{\text{T-AF}b\text{ORS}})}{\log(\lambda_{de})},
\tag{60}
$$

where $P_{\text{intercept}}^{\text{T-AF}b\text{ORS}}$ is given in Eq. (42). Denoting $X = |h_{sm}|^2$ and $Y = |h_{me}|^2$ and using the conditional probability, we obtain Eq. (61), where $f(x, y)$ represents a joint probability density function (PDF) of (X, Y). Considering that X and

$$P_{\text{intercept}}^{\text{T-AF}b\text{ORS}} = \sum_{m=1}^{M} \frac{1}{M} \int_0^\infty \int_0^\infty \prod_{i=1,i\neq m}^{M} \Pr\left(\frac{|h_{si}|^2|h_{id}|^2}{|h_{si}|^2 + |h_{id}|^2} < \frac{xy}{x+y}\right) \Pr\left(|h_{md}|^2 < y\right) f(x,y)dxdy \qquad (61)$$

Y are independent exponentially distributed, the joint PDF $f(x,y)$ is given by

$$f(x,y) = \frac{1}{\sigma_{sm}^2 \sigma_{me}^2} \exp(-\frac{x}{\sigma_{sm}^2} - \frac{y}{\sigma_{me}^2}), \qquad (62)$$

where $\sigma_{sm}^2 = E(|h_{sm}|^2)$ and $\sigma_{me}^2 = E(|h_{me}|^2)$. Using inequalities $\frac{1}{|h_{si}|^2} + \frac{1}{|h_{id}|^2} \geq \max(\frac{1}{|h_{si}|^2}, \frac{1}{|h_{id}|^2})$ and $\frac{1}{x} + \frac{1}{y} \leq 2\max(\frac{1}{x}, \frac{1}{y})$, we obtain

$$\begin{aligned}
&\Pr\left(\frac{|h_{si}|^2|h_{id}|^2}{|h_{si}|^2 + |h_{id}|^2} < \frac{xy}{x+y}\right) \\
&= \Pr\left(\frac{1}{|h_{si}|^2} + \frac{1}{|h_{id}|^2} > \frac{1}{x} + \frac{1}{y}\right) \\
&\geq \Pr\left(\max(\frac{1}{|h_{si}|^2}, \frac{1}{|h_{id}|^2}) > 2\max(\frac{1}{x}, \frac{1}{y})\right) \qquad (63) \\
&= \Pr\left(\min(|h_{si}|^2, |h_{id}|^2) < \frac{1}{2}\min(x,y)\right) \\
&= 1 - \exp[(-\frac{1}{2\sigma_{si}^2} - \frac{1}{2\sigma_{id}^2})\min(x,y)].
\end{aligned}$$

Substituting $\Pr\left(\frac{|h_{si}|^2|h_{id}|^2}{|h_{si}|^2+|h_{id}|^2} < \frac{xy}{x+y}\right) \geq 1 - \exp[(-\frac{1}{2\sigma_{si}^2} - \frac{1}{2\sigma_{id}^2})\min(x,y)]$ from Eq. (63) into Eq. (61), we can obtain a lower bound on the intercept probability of T-AFbORS scheme as

$$\begin{aligned}
P_{\text{intercept}}^{\text{T-AF}b\text{ORS}} \geq \sum_{m=1}^{M} \frac{1}{M} \int_0^\infty \int_0^\infty \prod_{i=1,i\neq m}^{M} g_i(x,y) \\
\times [1 - \exp(-\frac{y}{\sigma_{md}^2})] f(x,y)dxdy,
\end{aligned} \qquad (64)$$

where $g_i(x,y) = 1 - \exp[(-\frac{1}{2\sigma_{si}^2} - \frac{1}{2\sigma_{id}^2})\min(x,y)]$ and $f(x,y)$ is given by Eq. (62).

Proposition 1: *Given independent exponential random variables x and y with respective means σ_{sm}^2 and σ_{me}^2, the following equations hold,*

$$1-\exp[(-\frac{1}{2\sigma_{si}^2}-\frac{1}{2\sigma_{id}^2})\min(x,y)] = (\frac{1}{2\sigma_{si}^2}+\frac{1}{2\sigma_{id}^2})\min(x,y),$$

and

$$1 - \exp(-\frac{y}{\sigma_{md}^2}) = \frac{y}{\sigma_{md}^2},$$

for $\lambda_{de} \to \infty$, where $\lambda_{de} = \sigma_{sd}^2/\sigma_{se}^2$.

Proof: *See Appendix A for details.*

Using Proposition 1 and denoting $\sigma_{si}^2 = \alpha_{si}\sigma_{sd}^2$, $\sigma_{id}^2 = \alpha_{id}\sigma_{sd}^2$, $\sigma_{sm}^2 = \alpha_{sm}\sigma_{sd}^2$, $\sigma_{md}^2 = \alpha_{md}\sigma_{sd}^2$ and $\sigma_{me}^2 = \alpha_{me}\sigma_{se}^2$, we obtain from Eq. (64) as Eq. (65) with $\lambda_{de} \to \infty$ at the top of following page. Ignoring the higher-order terms in Eq. (65), we have

$$\begin{aligned}
P_{\text{intercept}}^{\text{T-AF}b\text{ORS}} \geq \sum_{m=1}^{M} \frac{1}{M} \prod_{i=1,i\neq m}^{M} (\frac{1}{2\alpha_{si}} + \frac{1}{2\alpha_{id}})\frac{M!\alpha_{me}^M}{\alpha_{md}} \\
\times (\frac{1}{\lambda_{de}})^M,
\end{aligned} \qquad (66)$$

Substituting Eq. (66) into Eq. (60) gives

$$d_{\text{T-AF}b\text{ORS}} \leq M. \qquad (67)$$

In addition, considering inequalities $\frac{1}{|h_{si}|^2} + \frac{1}{|h_{id}|^2} \leq 2\max(\frac{1}{|h_{si}|^2}, \frac{1}{|h_{id}|^2})$ and $\frac{1}{x} + \frac{1}{y} \geq \max(\frac{1}{x}, \frac{1}{y})$, we obtain an upper bound on the intercept probability of T-AFbORS scheme as

$$\begin{aligned}
P_{\text{intercept}}^{\text{T-AF}b\text{ORS}} \leq \sum_{m=1}^{M} \frac{1}{M} \int_0^\infty \int_0^\infty \prod_{i=1,i\neq m}^{M} h_i(x,y) \\
\times [1 - \exp(-\frac{y}{\sigma_{md}^2})] f(x,y)dxdy,
\end{aligned} \qquad (68)$$

where $h_i(x,y) = 1 - \exp[(-\frac{2}{\sigma_{si}^2} - \frac{2}{\sigma_{id}^2})\min(x,y)]$. Similarly to Eq. (66), we can obtain

$$\begin{aligned}
P_{\text{intercept}}^{\text{T-AF}b\text{ORS}} \leq \sum_{m=1}^{M} \frac{1}{M} \prod_{i=1,i\neq m}^{M} (\frac{2}{\alpha_{si}} + \frac{2}{\alpha_{id}})\frac{M!\alpha_{me}^M}{\alpha_{md}} \\
\times (\frac{1}{\lambda_{de}})^M,
\end{aligned} \qquad (69)$$

for $\lambda_{de} \to \infty$. Substituting Eq. (69) into Eq. (60) gives

$$d_{\text{T-AF}b\text{ORS}} \geq M. \qquad (70)$$

Therefore, by combining Eqs. (67) and (70), the diversity order of T-AFbORS scheme is readily obtained as

$$d_{\text{T-AF}b\text{ORS}} = M, \qquad (71)$$

which shows that the diversity order M is achieved by T-AFbORS scheme.

E. T-DFbORS

In this subsection, we present the diversity order analysis of T-DFbORS scheme. Using Eq. (52), we obtain the diversity order of T-DFbORS scheme as

$$d_{\text{T-DF}b\text{ORS}} = -\lim_{\lambda_{de}\to\infty} \frac{\log(P_{\text{intercept}}^{\text{T-DF}b\text{ORS}})}{\log(\lambda_{de})}, \qquad (72)$$

where $P_{\text{intercept}}^{\text{T-DF}b\text{ORS}}$ is given in Eq. (45). From Proposition 1, we can similarly obtain $1 - \exp(-\frac{x}{\sigma_{si}^2} - \frac{x}{\sigma_{id}^2}) = \frac{x}{\sigma_{si}^2} + \frac{x}{\sigma_{id}^2}$ for $\lambda_{de} \to \infty$ by using the Taylor series expansion and ignoring higher-order terms, from which $P_{\text{intercept}}^{\text{T-DF}b\text{ORS}}$ can be obtained as

$$\begin{aligned}
P_{\text{intercept}}^{\text{T-DF}b\text{ORS}} = \sum_{m=1}^{M} (M-1)! \prod_{i=1}^{M} (\frac{\alpha_{me}}{\alpha_{si}} + \frac{\alpha_{me}}{\alpha_{id}}) \\
\times (\frac{1}{\lambda_{de}})^M,
\end{aligned} \qquad (73)$$

where $\alpha_{si} = \sigma_{si}^2/\sigma_{sd}^2$, $\alpha_{id} = \sigma_{id}^2/\sigma_{sd}^2$, and $\alpha_{me} = \sigma_{me}^2/\sigma_{se}^2$. Substituting Eq. (73) into Eq. (72) yields

$$d_{\text{T-DF}b\text{ORS}} = M, \qquad (74)$$

which shows that the T-DFbORS scheme also achieves the diversity order M. As shown in Eqs. (56), (59), (71) and

$$P_{\text{intercept}}^{\text{T-AF}b\text{ORS}} \geq \sum_{m=1}^{M} \frac{1}{M} \prod_{i=1, i \neq m}^{M} \left(\frac{1}{2\sigma_{si}^2} + \frac{1}{2\sigma_{id}^2}\right) \int_0^\infty \int_0^\infty \frac{[\min(x,y)]^{M-1} y}{\sigma_{sm}^2 \sigma_{md}^2 \sigma_{me}^2} \exp\left(-\frac{x}{\sigma_{sm}^2} - \frac{y}{\sigma_{me}^2}\right) dx dy$$

$$= \sum_{m=1}^{M} \frac{1}{M} \prod_{i=1, i \neq m}^{M} \left(\frac{1}{2\sigma_{si}^2} + \frac{1}{2\sigma_{id}^2}\right) \frac{1}{\sigma_{md}^2} \int_0^\infty \frac{x^{M-1}}{\sigma_{sm}^2} \exp\left(-\frac{x}{\sigma_{sm}^2}\right) dx \int_x^\infty \frac{y}{\sigma_{me}^2} \exp\left(-\frac{y}{\sigma_{me}^2}\right) dy$$

$$+ \sum_{m=1}^{M} \frac{1}{M} \prod_{i=1, i \neq m}^{M} \left(\frac{1}{2\sigma_{si}^2} + \frac{1}{2\sigma_{id}^2}\right) \frac{1}{\sigma_{md}^2} \int_0^\infty \frac{y^M}{\sigma_{me}^2} \exp\left(-\frac{y}{\sigma_{me}^2}\right) dy \int_y^\infty \frac{1}{\sigma_{sm}^2} \exp\left(-\frac{x}{\sigma_{sm}^2}\right) dx \qquad (65)$$

$$= \sum_{m=1}^{M} \frac{1}{M} \prod_{i=1, i \neq m}^{M} \left(\frac{M+1}{2\alpha_{si}} + \frac{M+1}{2\alpha_{id}}\right) \frac{(M-1)! \alpha_{me}^{M+1}}{\alpha_{sm} \alpha_{md}} \cdot \left(\frac{1}{\lambda_{de}}\right)^{M+1}$$

$$+ \sum_{m=1}^{M} \frac{1}{M} \prod_{i=1, i \neq m}^{M} \left(\frac{1}{2\alpha_{si}} + \frac{1}{2\alpha_{id}}\right) \frac{M! \alpha_{me}^M}{\alpha_{md}} \cdot \left(\frac{1}{\lambda_{de}}\right)^M$$
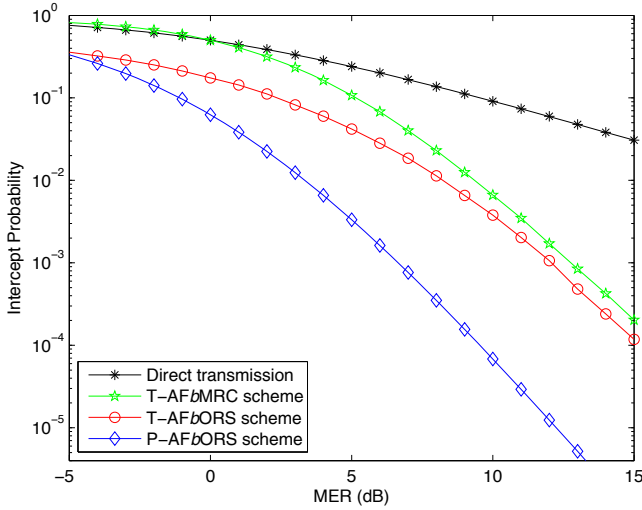

Fig. 2. Intercept probability versus main-to-eavesdropper ratio (MER) of the direct transmission, T-AFbORS, T-AFbMRC, and P-AFbORS schemes with $\alpha_{si} = \alpha_{id} = \alpha_{ie} = 1$.
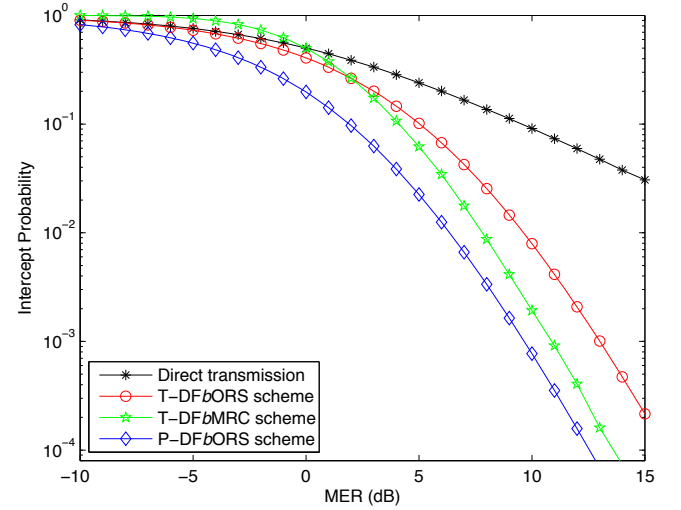

Fig. 3. Intercept probability versus main-to-eavesdropper ratio (MER) of the direct transmission, T-DFbORS, T-DFbMRC, and P-DFbORS schemes with $\text{Pout}_i = 10^{-3}$ and $\alpha_{si} = \alpha_{id} = \alpha_{ie} = 1$.

(74), the P-AFbORS, P-DFbORS, T-AFbORS and T-DFbORS schemes all achieve the same diversity order M. This implies that in high MER regions, the intercept probabilities of P-AFbORS, P-DFbORS, T-AFbORS and T-DFbORS schemes all behave as $(1/\lambda_{de})^M$ for $\lambda_{de} \to \infty$. Therefore, for $M > 1$, the intercept probabilities of P-AFbORS, P-DFbORS, T-AFbORS and T-DFbORS schemes are reduced much faster than that of direct transmission as $\lambda_{de} \to \infty$, showing the physical-layer security benefit of using the optimal relay selection.

V. NUMERICAL RESULTS AND DISCUSSIONS

This section presents the numerical intercept probability results of conventional direct transmission, T-AFbORS, T-DFbORS, T-AFbMRC, T-DFbMRC, P-AFbORS and P-DFbORS schemes. We show that for both AF and DF protocols, the proposed optimal relay selection outperforms the traditional relay selection and multiple relay combining approaches in terms of intercept probability. Moreover, nu-

merical results also illustrate that as the number of relays increases, the intercept probabilities of P-AFbORS and P-DFbORS schemes significantly decrease, showing the security improvement by exploiting cooperative relays.

Fig. 2 shows the intercept probability comparison among the direct transmission, P-AFbORS, T-AFbORS, and T-AFbMRC schemes by plotting Eqs. (32), (34), (42) and (47) as a function of MER. It is shown from Fig. 2 that the T-AFbORS, T-AFbMRC, and P-AFbORS schemes all perform better than the direct transmission in terms of intercept probability, implying the security benefits of exploiting cooperative relays to defend against eavesdropping attack. One can also see from Fig. 2 that the intercept probability performance of T-AFbMRC scheme is worse than that of the T-AFbORS scheme which performs worse than the P-AFbORS scheme, showing the advantage of proposed optimal relay selection over both the traditional relay selection and multiple relay combining approaches.

In Fig. 3, we show the numerical intercept probability results of various DF based optimal relay selection and multiple
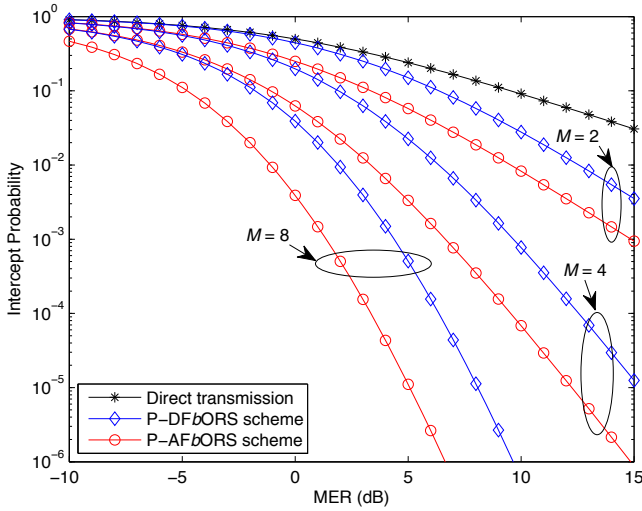
Fig. 4. Intercept probability versus main-to-eavesdropper ratio (MER) of the direct transmission, P-AF*b*ORS, and P-DF*b*ORS schemes with $\alpha_{si} = \alpha_{id} = \alpha_{ie} = 1$.

Fig. 5. Intercept probability versus the number of relays M of the P-AF*b*ORS and P-DF*b*ORS schemes with $\lambda_{de} = 3$dB and $\alpha_{si} = \alpha_{id} = \alpha_{ie} = 1$.

relay combining schemes, in which the intercept probability curves of direct transmission, P-DF*b*ORS, T-DF*b*ORS, and T-DF*b*MRC schemes are plotted by using Eqs. (32), (38), (45), and (49) with Pout$_i = 10^{-3}$ and $\alpha_{si} = \alpha_{id} = \alpha_{ie} = 1$. Fig. 3 shows that the intercept probability of P-DF*b*ORS scheme is always smaller than that of T-DF*b*MRC scheme which further outperforms the T-DF*b*ORS scheme in terms of intercept probability. In other words, the P-DF*b*ORS scheme achieves the best intercept probability performance, further confirming the advantage of proposed optimal relay selection over traditional relay selection and multiple relay combining. Therefore, no matter which relaying protocol (i.e., AF and DF) is considered, the proposed optimal relay selection always performs better than the traditional relay selection and multiple relay combining approaches in terms of intercept probability.

Fig. 4 depicts the intercept probability comparison between the P-AF*b*ORS and P-DF*b*ORS schemes with $\alpha_{si} = \alpha_{id} = \alpha_{ie} = 1$. One can see from Fig. 4 that for the cases of $M = 2$, $M = 4$, and $M = 8$, the direct transmission strictly performs worse than the P-AF*b*ORS and P-DF*b*ORS schemes in terms of intercept probability. Moreover, as the number of relays M increases from $M = 2$ to $M = 8$, the intercept probabilities of P-AF*b*ORS and P-DF*b*ORS schemes both decrease significantly. This means that increasing the number of cooperative relays can enhance the physical-layer security against eavesdropping attack. In addition, Fig. 4 also shows that for the cases of $M = 2$, $M = 4$, and $M = 8$, the P-AF*b*ORS scheme always outperforms the P-DF*b*ORS scheme, showing the advantage of AF relaying protocol over DF protocol.

Fig. 5 shows the intercept probability versus the number of relays M of the P-AF*b*ORS and P-DF*b*ORS schemes with $\lambda_{de} = 3$dB and $\alpha_{si} = \alpha_{id} = \alpha_{ie} = 1$. It is observed from Fig. 5 that the P-AF*b*ORS scheme strictly performs better the P-DF*b*ORS scheme in terms of intercept probability. One can
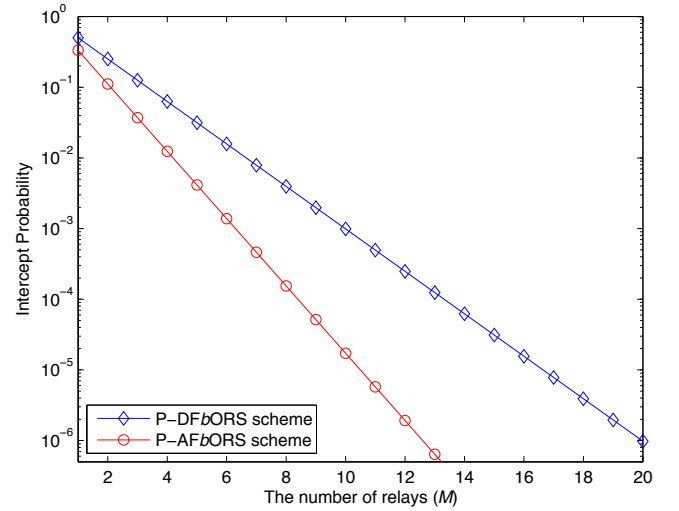
also see from Fig. 5 that as the number of relays M increases, the intercept probabilities of both P-AF*b*ORS and P-DF*b*ORS schemes significantly decrease, showing the wireless security improvement with an increasing number of relays. In addition, as shown in Fig. 5, the intercept probability improvement of P-AF*b*ORS over P-DF*b*ORS becomes more significant as the number of relays increases.

VI. CONCLUSION

In this paper, we explored the relay selection for improving physical-layer security in cooperative wireless networks and proposed the AF and DF based optimal relay selection schemes, i.e., P-AF*b*ORS and P-DF*b*ORS. For the purpose of comparison, we also examined the conventional direct transmission, T-AF*b*ORS, T-DF*b*ORS, T-AF*b*MRC, and T-DF*b*MRC schemes. We derived closed-form intercept probability expressions of the direct transmission, T-AF*b*ORS, T-DF*b*ORS, T-AF*b*MRC, T-DF*b*MRC, P-AF*b*ORS and P-DF*b*ORS schemes over Rayleigh fading channels. We further analyzed the diversity order performance of the traditional and proposed optimal relay selection schemes and showed that for both AF and DF protocols, the proposed and traditional relay selection schemes achieve the diversity order M, where M is the number of cooperative relays. Numerical results also illustrated that no matter which relaying protocol is considered (i.e., AF and DF), the proposed optimal relay selection strictly outperforms the traditional relay selection and multiple relay combining approaches in terms of intercept probability. In addition, as the number of relays increases, the intercept probability performance of both P-AF*b*ORS and P-DF*b*ORS significantly improves, implying the wireless security enhancement with an increasing number of cooperative relays.

It is worth mentioning that we only investigated the single-source and single-destination for cooperative relay networks in this paper. In future, we will extend the results of this paper to a general case with multiple-source and multiple-

destination, for which the opportunistic transmission scheduling may be exploited to defend against eavesdropping attack. More specifically, a source node with the highest secrecy capacity can be opportunistically scheduled to transmit to its destination. Once a source-destination pair is determined with the transmission scheduling policy, we can consider the use of optimal relay selection developed in this paper to assist the transmission between source and destination against the eavesdropping attack.

APPENDIX A
PROOF OF PROPOSITION 1

Denoting $z = (\frac{1}{2\sigma_{si}^2} + \frac{1}{2\sigma_{id}^2})\min(x,y)$ and using the joint PDF of (X,Y) in Eq. (62), we can obtain the mean of z as

$$
E(z) = (\frac{1}{2\alpha_{si}} + \frac{1}{2\alpha_{id}})\frac{\alpha_{sm}\alpha_{me}^2}{(\alpha_{sm} + \alpha_{me}\lambda_{de}^{-1})^2} \cdot \frac{1}{\lambda_{de}^2}
$$
$$
+ (\frac{1}{2\alpha_{si}} + \frac{1}{2\alpha_{id}})\frac{\alpha_{sm}^2\alpha_{me}}{(\alpha_{sm} + \alpha_{me}\lambda_{de}^{-1})^2} \cdot \frac{1}{\lambda_{de}}, \quad \text{(A.1)}
$$

where $\alpha_{si} = \sigma_{si}^2/\sigma_{sd}^2$, $\alpha_{id} = \sigma_{id}^2/\sigma_{sd}^2$, $\alpha_{sm} = \sigma_{sm}^2/\sigma_{sd}^2$, and $\alpha_{me} = \sigma_{me}^2/\sigma_{se}^2$. Considering $\lambda_{de} \to \infty$ and ignoring the higher-order term, we have

$$
E(z) = (\frac{\alpha_{me}}{2\alpha_{si}} + \frac{\alpha_{me}}{2\alpha_{id}}) \cdot \frac{1}{\lambda_{de}}, \quad \text{(A.2)}
$$

which shows that $E(z)$ converges to zero as $\lambda_{de} \to \infty$. Moreover, using Eq. (62) and letting $\lambda_{de} \to \infty$, we can obtain $E(z^2)$ as

$$
E(z^2) = (\frac{\alpha_{me}}{2\alpha_{si}} + \frac{\alpha_{me}}{2\alpha_{si}})^2 \cdot \frac{2}{\lambda_{de}^2}, \quad \text{(A.3)}
$$

where the third equation is obtained by ignoring higher-order terms. From Eqs. (A.2) and (A.3), the variance of z is given by

$$
Var(z) = E(z^2) - [E(z)]^2 = (\frac{\alpha_{me}}{2\alpha_{si}} + \frac{\alpha_{me}}{2\alpha_{si}})^2 \cdot \frac{1}{\lambda_{de}^2}, \quad \text{(A.4)}
$$

for $\lambda_{de} \to \infty$. It is shown from Eqs. (A.2) and (A.4) that both mean and variance of z approach to zero as $\lambda_{de} \to \infty$, implying that $z \to 0$ as $\lambda_{de} \to \infty$. Thus, considering $\lambda_{de} \to \infty$ and using Taylor series expansion, we obtain

$$
1 - \exp(-z) = z + O(z), \quad \text{(A.5)}
$$

where $O(z)$ represents higher-order infinitesimal. Substituting $z = (\frac{1}{2\sigma_{si}^2} + \frac{1}{2\sigma_{id}^2})\min(x,y)$ into Eq. (A.5) and ignoring higher-order infinitesimal, we have

$$
1 - \exp[(-\frac{1}{2\sigma_{si}^2} - \frac{1}{2\sigma_{id}^2})\min(x,y)]
$$
$$
= (\frac{1}{2\sigma_{si}^2} + \frac{1}{2\sigma_{id}^2})\min(x,y). \quad \text{(A.6)}
$$

In addition, denoting $t = \frac{y}{\sigma_{md}^2}$, we can easily obtain both mean and variance of t as

$$
E(t) = \int_0^\infty \frac{y}{\sigma_{md}^2\sigma_{me}^2}\exp(-\frac{y}{\sigma_{me}^2})dy = \frac{\alpha_{me}}{\alpha_{md}} \cdot \frac{1}{\lambda_{de}}, \quad \text{(A.7)}
$$

and

$$
Var(t) = E(t^2) - [E(t)]^2 = \frac{\alpha_{me}^2}{\alpha_{md}^2} \cdot \frac{1}{\lambda_{de}^2}. \quad \text{(A.8)}
$$

One can observe from Eqs. (A.7) and (A.8) that both mean and variance of t approach to zero as $\lambda_{de} \to \infty$, meaning that $t \to 0$ as $\lambda_{de} \to \infty$. Hence, considering $\lambda_{de} \to \infty$ and using Taylor series expansion, we obtain

$$
1 - \exp(-t) = t + O(t). \quad \text{(A.9)}
$$

Substituting $t = \frac{y}{\sigma_{md}^2}$ into Eq. (A.9) and ignoring the higher-order infinitesimal yield

$$
1 - \exp(-\frac{y}{\sigma_{md}^2}) = \frac{y}{\sigma_{md}^2}, \quad \text{(A.10)}
$$

which completes the proof of Proposition 1.

REFERENCES

[1] Y. Zhou and T.S. Ng, "Performance analysis on MIMO-OFCDM systems with Multi-code Transmission," *IEEE Trans. Wireless Commun.*, vol. 8, no. 9, pp. 4426-4433, Sept. 2009.

[2] Y. Zhou and T.S. Ng, "MIMO-OFCDM systems with joint iterative detection and optimal power allocation," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 5504-5516, Dec. 2008.

[3] J. N. Laneman, D. N. C. Tse, and G. W.Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, pp. 3062-3080, Dec. 2004.

[4] D. Gunduz and E. Erkip, "Opportunistic cooperation by dynamic resource allocation," *IEEE Trans. Wireless. Commun.*, vol. 6, no. 4, pp. 1446-1454, Apr. 2007.

[5] S. Ikki and M. H. Ahmed, "Performance analysis of cooperative diversity wireless networks over Nakagami-m fading channel," *IEEE Commun. Lett.*, vol. 11, no. 4, pp. 334-336, Apr. 2007.

[6] M. Safari and M. Uysal, "Cooperative diversity over log-normal fading channels: Performance analysis and optimization," *IEEE Trans. Wireless Commun.*, vol. 7, no. 5, pp. 1963-1972, May 2008.

[7] A. Azgin, Y. Altunbasak, and G. AlRegib, "Cooperative MAC and routing protocols for wireless ad hoc networks," in *Proc. GLOBECOM 2005*, pp. 2854-2859, 2005.

[8] T. Korakis, S. Narayanan, A. Bagri, and S. Panwar, "Implementing a cooperative MAC protocol for wireless LANs," in *Proc. ICC 2006*, pp. 4805-4810, 2006.

[9] A. D.Wyner, "The wire-tap channel," *Bell System Technical J.*, vol. 54, no. 8, pp. 1355-1387, 1975.

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

[11] M. Yuksel and E. Erkip, "Secure communication with a relay helping the wiretapper," in *Proc. 2007 IEEE Information Theory Workshop*, Lake Tahoe, CA, Sep. 2007.

[12] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735-2751, Jun. 2008.

[13] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005-4019, Sep. 2008.

[14] Y. Zou, X. Wang, and W. Shen, "Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack," in *Proc. 2013 IEEE Intern. Conf. Commun. (IEEE ICC 2013)*, pp. 1-5, Budapest, Hungary, Jun. 2013.

[15] Y. Zou, X. Wang, and W. Shen, "Eavesdropping attack in collaborative wireless Networks: Security protocols and intercept behavior," in *Proc. 2013 IEEE Intern. Conf. Comp. Supp. Cooper. Work in Design (IEEE CSCWD 2013)*, pp. 1-5, Whistler, Canada, Jun. 2013.

[16] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forens. Security*, vol. 7, no. 1, pp. 310-320, Feb. 2012.

[17] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693-3704, Oct. 2012.

[18] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871-4884, Oct. 2011.

[19] A. Mukherjee and A. L. Swindlehurst, "Securing multi-antenna two-way relay channels with analog network coding against eavesdroppers," in *Proc. IEEE 11th Intern. Workshop Signal Process. Adv. in Wireless Commun. (SPAWC 2010)*, pp. 1-5, Jun. 2010.

[20] A. Bletsas, H. Shin, M. Z. Win, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE J. Sel. Areas in Commun.*, vol. 24, no. 3, pp. 659-672, Mar. 2006.

[21] Y. Zou, J. Zhu, B. Zheng, and Y.-D. Yao, "An adaptive cooperation diversity scheme with best-relay selection in cognitive radio networks," *IEEE Trans. Signal Process.*, vol. 58, no. 10, pp. 5438-5445, Oct. 2010.

[22] S. Ikki and M. H. Ahmed, "Performance analysis of adaptive decode-and-forward cooperative diversity networks with best-relay selection," *IEEE Trans. Commun.*, vol. 58, no. 1, pp. 68-72, Jan. 2010.

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

[24] H. Zhu and J. Wang, "Chunk-based resource allocation in OFDMA systems - Part I: chunk allocation," *IEEE Trans. Commun.*, vol. 57, no. 9, pp. 2734-2744, Sept. 2009.

[25] H. Zhu and J. Wang, "Chunk-based resource allocation in OFDMA systems - Part II: joint chunk, power and bit allocation," *IEEE Trans. Commun.*, vol. 60, pp. 499-509, no. 2, Feb. 2012.

[26] A. F. Molisch, *Wireless Communications*, Wiley, New Jersey, USA, 2011.

[27] L. Zheng and D. Tse, "Diversity and multiplexing: A fundamental tradeoff in multiple antenna channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1073-1096, May 2003.

Yulong Zou received the B.Eng. degree in information engineering from the Nanjing University of Posts and Telecommunications (NUPT), Nanjing, China, in July 2006. Then, he was admitted to the Graduate School of NUPT to pursue his Ph.D. degree in September 2006. In May 2009, he was invited to serve as a visiting scholar at the Stevens Institute of Technology (Stevens Tech), New Jersey, United States. From September 2009, he joined a new Ph.D. program in electrical engineering at Stevens Tech under the full sponsorship of United States Department of Defense and started working toward his two Ph.D. degrees concurrently at NUPT and Stevens Tech, respectively. He received the first Ph.D. degree from the Stevens Institute of Technology in May 2012 and the second Ph.D. degree from the Nanjing University of Posts and Telecommunications in July 2012.

Dr. Zou is currently serving as an editor for the IEEE Communications Surveys & Tutorials, IEEE Communications Letters, EURASIP Journal on Advances in Signal Processing, and KSII Transactions on Internet and Information Systems. He is also serving as a lead guest editor for special issue on "Security Challenges and Issues in Cognitive Radio Networks" in the EURASIP Journal on Advances in Signal Processing. In addition, he has acted as symposium chairs, session chairs, and TPC members for a number of IEEE sponsored conferences including the IEEE Wireless Communications and Networking Conference (WCNC), IEEE Global Telecommunications Conference (GLOBECOM), IEEE International Conference on Communications (ICC), IEEE Vehicular Technology Conference (VTC), International Conference on Communications in China (ICCC), International Conference on Communications and Networking in China (ChinaCom), and so on.

His research interests span a wide range of topics in wireless communication and signal processing including the cooperative communications, cognitive radio, wireless security, and green communications. In these areas, he has published extensively in internationally renowned journals including the IEEE Transactions on Signal Processing, IEEE Transactions on Communications, IEEE Journal on Selected Areas in Communications, IEEE Transactions on Wireless Communications, and IEEE Communications Magazine.

Xianbin Wang (S'98-M'99-SM'06) is an Associate Professor at The University of Western Ontario and a Canada Research Chair in Wireless Communications. He received his Ph.D. degree in electrical and computer engineering from National University of Singapore in 2001.

Prior to joining Western, he was with Communications Research Centre Canada as Research Scientist/Senior Research Scientist between July 2002 and Dec. 2007. From Jan. 2001 to July 2002, he was a system designer at STMicroelectronics, where he was responsible for system design for DSL and Gigabit Ethernet chipsets. He was with Institute for Infocomm Research, Singapore (formerly known as Centre for Wireless Communications), as a Senior R & D engineer in 2000. His primary research area is wireless communications and related applications, including adaptive communications, wireless security, and wireless infrastructure based position location. Dr. Wang has over 150 peer-reviewed journal and conference papers on various communication system design issues, in addition to 23 granted and pending patents and several standard contributions.

Dr. Wang is an IEEE Distinguished Lecturer and a Senior Member of IEEE. He was the recipient of three IEEE Best Paper Awards. He currently serves as an Associate Editor for IEEE Wireless Communications Letters, IEEE Transactions on Vehicular Technology and IEEE Transactions on Broadcasting. He was also an editor for IEEE Transactions on Wireless Communications between 2007 and 2011. Dr. Wang was involved in a number of IEEE conferences including GLOBECOM, ICC, WCNC, VTC, and ICME, on different roles such as symposium chair, track chair, TPC and session chair.

Weiming Shen is a Senior Research Scientist at the National Research Council Canada and an Adjunct Professor at Tongji University, China, and University of Western Ontario, Canada. He is a Fellow of IEEE. He received his Bachelor and Masters degrees from Northern (Beijing) Jiaotong University, China and his PhD degree from the University of Technology of Compigne, France. His recent research interest includes agent-based collaboration technology and applications, wireless sensor networks. He has published several books and over 300 papers in scientific journals and international conferences in the related areas. His work has been cited over 6,000 times with an h-index of 37. He has been invited to provide over 60 invited lectures/seminars at different academic and research institutions over the world and keynote presentations / tutorials at various international conferences. He is a member of the Steering Committee for the IEEE Transactions on Affective Computing and an Associate Editor or Editorial Board Member of ten international journals (including IEEE Transactions on Automation Science and Engineering, Computers in Industry; Advanced Engineering Informatics; Service Oriented Computing and Applications) and served as guest editor for several other international journals.