Security Performance Analysis of DF Cooperative Relay Networks over Nakagami-m Fading Channels

Huan Zhang[1], **Hongjiang Lei**[1*], **Imran Shafique Ansari**[2], **Gaofeng Pan**[3], **and Khalid A. Qaraqe**[2]
[1] Chongqing Key Lab of Mobile Communications Technology
Chongqing University of Posts and Telecommunications, Chongqing, China
[e-mail: cquptzh@gmail.com, leihj@cqupt.edu.cn]
[2] Department of Electrical and Computer Engineering, Texas A&M University at Qatar
Education City, Doha, Qatar
[e-mail: {imran.ansari@qatar.tamu.edu, khalid.qaraqe@qatar.tamu.edu]
[3] Chongqing Key Laboratory of Nonlinear Circuits and Intelligent Information Processing
Southwest University, Chongqing, China
[e-mail: gfpan@swu.edu.cn]
*Corresponding author: Hongjiang Lei

Received November 9, 2016; revised February 27, 2017; accepted March 5, 2017;
published May 31, 2017

Abstract

In this paper, we investigate the security performance for cooperative networks over Nakagami-*m* fading channels. Based on whether the channel state information (CSI) of wiretap link is available or not, optimal relay selection (ORS) and suboptimal relay selection (SRS) schemes are considered. Also, multiple relays combining (MRC) scheme is considered for comparison purpose. The exact and asymptotic closed-form expressions for secrecy outage probability (SOP) are derived and simulations are presented to validate the accuracy of our proposed analytical results. The numerical results illustrate that the ORS is the best scheme and SRS scheme is better than MRC scheme in some special scenarios such as when the destination is far away from the relays. Furthermore, through asymptotic analysis, we obtain the closed-form expressions for the secrecy diversity order and secrecy array gain for the three different selection schemes. The secrecy diversity order is closely related to the number of relays and fading parameter between relay and destination.

Keywords: Secrecy outage performance, cooperative communications, relay selection, decode-and-forward, Nakagami-*m* fading

---

This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant 61471076, 61401372, the Program for Changjiang Scholars and Innovative Research Team in University under Grant IRT_16R72, the special fund for Key Lab of Chongqing Municipal Education Commission, the Project of Fundamental and Frontier Research Plan of Chongqing under Grant cstc2015jcyjBX0085, the Scientific and Technological Research Program of Chongqing Municipal Education Commission under Grant KJ1600413, and Chongqing Postgraduate Scientific Research and Innovation Projects under Grant CYS16162. Parts of this publication were made possible by PDRA (PostDoctoral Research Award) grant # PDRA1-1227-13029 from the Qatar National Research Fund (QNRF) (a member of Qatar Foundation (QF)). The statements made herein are solely the responsibility of the authors.

https://doi.org/10.3837/tiis.2017.05.006 **ISSN : 1976-7277**

1. Introduction

1.1 Background

Wireless communication faced many severe issues of security due to the broadcast nature. The physical layer security (PLS) has emerged and received much attention as a key technique to prevent wiretap. In [1], the PLS was first introduced by Wyner to study the secrecy rate. Different from conventional cryptographic approaches used to address wireless security issues, the PLS utilizes channel coding and signal processing techniques to communicate secret messages between the source and the destination while maintaining confidentiality against the eavesdropper [2].

Multiple antennas technique is considered as an effective method to improve the security performance of wireless wiretap channels [3], [4]. The conclusion in [5] has shown that the transmit antenna selection can considerably enhance the system security. In [6] and [7], the authors have analyzed transmit antenna selection in a multiple-input-multiple-output (MIMO) system to enhance the system security and obtained the exact and asymptotic closed-form expressions for secrecy outage probability (SOP). But in some scenarios, it is difficult to implement multiple antennas due to the limitation in physical size and power consumption, such as hand-held terminals, sensor nodes, etc. Cooperative diversity has emerged as a key technique to achieve the spatial diversity without the need for multiple antennas implemented at the terminals [8].

1.2 Related works

Recently, the PLS in cooperative networks has attracted considerable attention, due to the fact that cooperative relaying can improve the reliability and throughput of next-generation wireless communication networks [9]-[13]. In [14], the authors analyzed the security capacity of the wireless transmissions in the presence of an eavesdropper with one relay node, where the amplify-and-forward (AF), decode-and-forward (DF), and compress-and-forward (CF) relaying protocols were examined and compared with each other. Besides, DF can be further specified as fixed DF and selective DF [15]. Refs. [16] and [17] studied the opportunistic relay selection in cooperative networks with secrecy constraints and obtained the closed-form expressions for SOP. In [18], the authors investigated the secrecy performance of DF strategy and derived the optimal power allocation. In [19], the authors proposed the AF and DF based optimal relay selection schemes to improve the wireless security against eavesdropping attack. In [20], the authors proposed a generalized multi-relay selection scheme to improve the security in the cooperative relay network. The authors in [21] presented two physical layer secure transmission schemes for multi-user multi-relay networks and derived a tight lower bound and asymptotic expressions for SOP. Cooperative Jamming (CJ) is another kind of cooperative scheme that the relay can transmit the jamming signal to confound the eavesdropper. In [22] and [23], the authors proposed several selection policies for secure communication with CJ relay. The secure resource allocations of the wireless sensor network with and without CJ were considered in [24]. Ref. [25] presented a comprehensive review of PLS issues in interference-alignment-based wireless networks.

While all of the aforementioned works ([16]-[24]) substantially provide a good understanding of cooperative communications. However, all of them assumed Rayleigh fading channels, which are typical in realistic wireless relay applications. Compared with Rayleigh fading, Nakagami-m fading model provides a good match to various empirically obtained measurement data and is widely used for modeling wireless fading channels, including Rayleigh ($m=1$) and one-sided Gaussian distribution ($m = 0.5$) as special cases [26].

In [27], the authors analyzed the symbol-error-rate (SNR) performance of DF cooperative communications. The outage performance of dual-hop cooperative spectrum sharing systems over Nakagami-m fading channels have been investigated in [28] and [29]. In [30], the authors presented performance analysis for underlay cognitive DF relay networks with the N th best relay selection scheme over Nakagami-m fading channels. Ref. [31] investigated the performance of DF relaying over Nakagami-m fading channel and obtained the closed-form expression for outage probability.

1.2 Motivation and Contributions

So far, to the best of the authors' knowledge based on the open literature, there is an absence of investigation on the security performance of the cooperative networks over Nakagami-m fading channels with relay selection. In this paper, we investigate the security performance of DF relay networks over Nakagami-m fading channels, our main contributions are as follows:

- The secrecy performance with optimal relay selection (ORS) and suboptimal relay selection (SRS) schemes are analyzed and compared with multiple relays combining (MRC) scheme. The exact closed-form expressions for the SOP of the three different selection schemes are derived, which build the relationship between the secrecy performance and the parameters of the related system and are verified via simulations.
- The asymptotic closed-form expressions for the SOP of the three different selection schemes are derived, and the secrecy diversity order and secrecy array gain are also obtained. An interesting observation is achieved that the three different selection schemes achieve the same secrecy diversity order and the impact of the wiretap channels is only reflected in the secrecy array gain.
- Relative to [19], wherein the intercept probability (IP) of the three different selection schemes over Rayleigh fading channels were derived, which is a special case of SOP when a predefined target secrecy rate is zero. Besides, the DF protocol in [19] is unfair where the ORS and SRS schemes used fixed DF, and MRC schemes used selective DF. In the following, we used DF to denote selective DF if not specified.

1.4 Motivation and Contributions

The rest of the paper is organized as follows. In Section 2, the system model considered in our work is described and the ORS, SRS, and MRC schemes are presented. The exact and asymptotic closed-form expressions for the SOP of the three different relay selection schemes are derived in Section 3 and 4. In Section 5, we present and discuss the numerical results and the Monte-Carlo simulations. Finally, Section 6 concludes the paper.

2. System Model

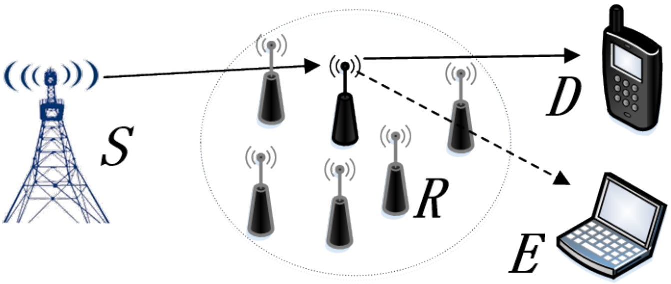

Fig. 1. System Model demonstrating a source (*S*), a collection of relays (*R*), a desired destination (*D*), and an undesired eavesdropper (*E*).

In this paper, we consider a cooperative network as shown in **Fig. 1**, which includes a source (*S*), N DF cooperative relays $R_i\left(i=1,\cdots,N\right)$, a destination(*D*), and an eavesdropper (*E*). All nodes are equipped with a single antenna and operate in half-duplex mode. Following [19] and [32], we assume that the direct link between *S* and *D*/*E* is unavailable due to severe shadowing and path loss, and the communication from *S* to *D* can be established only via relays. In the first phase, *S* broadcasts messages to relays, and each relay tries to decode the received signal. In the second phase, the best relay will be selected from the successful decoding relay set and forwards the decoded outcome to *D*, and *E* may overhear messages from the selected relay. Moreover, the link between each node can be classified into three groups, $S\to R_i$, $R_i\to D$, and $R_i\to E$. All the channels of each group in the DF relay system of **Fig. 1** are considered to be characterized as independent and identically-distributed (i.i.d.) quasi-static Nakagami-m fading as [30] with fading parameter m_j, the average channel fading gains of each group is Ω_j, where $j\in\left\{SR,RD,RE\right\}$. The transmitting power at *S* and relay is P_S and P_R, respectively. The thermal noise at each receiver is modeled as additive white Gaussian noise (AWGN) with variance σ^2.

The probability density function (PDF) and the cumulative distribution function (CDF) of each channel gain can be written as

$$f_{Y_j}\left(y\right)=\frac{\lambda_j^{m_j}}{\Gamma\left(m_j\right)}y^{m_j-1}\exp\left(-\lambda_j y\right), \tag{1}$$

$$F_{Y_j}\left(y\right)=1-\exp\left(-\lambda_j y\right)\sum_{n=0}^{m_j-1}\frac{\left(\lambda_j y\right)^n}{n!}, \tag{2}$$

where $Y_j=\left|h_j\right|^2$, h_j is the instantaneous channel fading coefficient of each link, and $\lambda_j=m_j/\Omega_j$.

In the first time phase, the channel capacity between *S* and the i th relay can be expressed as

$$C_{SR_i} = \frac{1}{2}\log_2\left(1+\alpha Y_{SR_i}\right), \tag{3}$$

where $\alpha = P_S / \sigma^2$ and $1 \le i \le N$.

Based on [30] and [32], the i th relay can successfully decode the received signal when C_{SR_i} is larger than the target data rate $R_d > 0$. Otherwise, the relays are unable to recover the signal from *S*. So the probability of the i th relay can successful decoding is

$$\begin{aligned} P_{suc}^{i} &= \Pr\left(C_{SR_i} \ge R_d\right) \\ &= \Pr\left(Y_{SR_i} \ge \theta\right) \end{aligned}, \tag{4}$$

where $\theta = \left(2^{2R_d} - 1\right)/\alpha$.

In the second time phase, we denote the successful decoding set as Φ and the number of relays in Φ is $L = |\Phi|, \left(0 \le L \le N\right)$. The channel capacity between the k th relay of Φ and *D*/*E* is expressed as

$$C_{R_k D} = \frac{1}{2}\log_2\left(1+\beta Y_{R_k D}\right), \tag{5}$$

$$C_{R_k E} = \frac{1}{2}\log_2\left(1+\beta Y_{R_k E}\right), \tag{6}$$

where $\beta = P_R / \sigma^2$ and $k \in \Phi$.

Next, we will introduce and analyze the three different relay selection schemes for the transmitting signal to *D* as follows.

2.1 The Optimal Relay Selection Scheme

In this subsection, we consider that the full CSI of both the main and wiretap channels is available at relays, which is called active eavesdropping [33]. We can select an optimal relay that maximizes the secrecy capacity as [19]. The relay selection criterion for ORS scheme can be expressed as

$$\begin{aligned} b &= \arg\max_{k\in\Phi}\left[C_{R_k D} - C_{R_k E}\right]^{+} \\ &= \arg\max_{k\in\Phi}\frac{1+\beta Y_{R_k D}}{1+\beta Y_{R_k E}} \end{aligned}, \tag{7}$$

where b signifies the selected relay and $[x]^{+} = \max(x,0)$.

Then the instantaneous secrecy capacity of ORS scheme can be written as

$$\begin{aligned} C_S^{\mathrm{ORS}} &= \max_{k\in\Phi}\left[C_{R_k D} - C_{R_k E}\right]^{+} \\ &= \max_{k\in\Phi}\left[\frac{1}{2}\log_2\left(1+\beta Y_{R_k D}\right) - \frac{1}{2}\log_2\left(1+\beta Y_{R_k E}\right)\right]^{+} \end{aligned}. \tag{8}$$

2.2 The Suboptimal Relay Selection Scheme

In this subsection, we concentrate on passive eavesdropping scenario, where the CSI of wiretap channel is unavailable at relays. We can select an optimal relay that maximizes the main channel capacity [32]. The selection criterion for SRS scheme can be expressed as

$$\begin{aligned} b &= \arg\max_{k\in\Phi}\left[C_{R_kD}\right]^{+} \\ &= \arg\max_{k\in\Phi} \beta Y_{R_kD} \end{aligned} . \tag{9}$$

Then the instantaneous secrecy capacity of ORS scheme can be written as

$$\begin{aligned} C_S^{\mathrm{SRS}} &= \left[C_{R_bD} - C_{R_bE}\right]^{+} \\ &= \left[\frac{1}{2}\log_2\left(1+\beta Y_{\mathrm{SRS}}\right) - \frac{1}{2}\log_2\left(1+\beta Y_{R_bE}\right)\right]^{+} \end{aligned} , \tag{10}$$

where C_{R_bD} and C_{R_bE} is the channel capacity between the selected relay b and D/E, $Y_{\mathrm{SRS}} = \max_{k\in\Phi} Y_{R_kD}$.

Because the fading channel $R_k \to D$ is i.i.d., utilizing the multinomial theorem [34], the CDF of Y_{SRS} can be written as

$$\begin{aligned} F_{Y_{\mathrm{SRS}}}(y) &= \prod_{k\in\Phi} F_{Y_{R_kD}}(y) \\ &= \left(1-\exp\left(-\lambda_{RD}y\right)\sum_{n=0}^{m_{RD}-1}\frac{\left(\lambda_{RD}y\right)^n}{n!}\right)^{L} \\ &= \sum_{SS} A\exp\left(-By\right)y^{C} \end{aligned} , \tag{11}$$

where SS denotes a set of $\left(m_{RD}+1\right)$ tuples satisfying the condition: $SS = \left\{\left(p_1,\cdots,p_{m_{RD}+1}\right)\middle|\sum_{n=1}^{m_{RD}+1} p_n = L\right\}$, $A = \frac{L!}{\prod_{n}^{m_{RD}+1} p_n!}\prod_{n=1}^{m_{RD}}\left(-\frac{\lambda_{RD}{}^{n-1}}{(n-1)!}\right)^{p_n}$, $B = \lambda_{RD}\left(L - p_{m_{RD}+1}\right)$, and $C = \sum_{n=1}^{m_{RD}}\left(n-1\right)p_n$.

2.3 The Multiple Relays Combining Scheme

In this subsection, we assume all relays in Φ participate in forwarding the signal to D for comparison purpose. Maximal ratio combining scheme is employed both at D and E. With the equal power allocation, the transmitting power at each successful decoding relay in the set Φ is P_R / L .

Then the instantaneous secrecy capacity of MRC scheme can be written as

$$\begin{aligned} C_S^{\mathrm{MRC}} &= \left[C_D^{\mathrm{MRC}} - C_E^{\mathrm{MRC}}\right]^{+} \\ &= \left[\frac{1}{2}\log_2\left(1+\frac{\beta}{L}Y_D\right) - \frac{1}{2}\log_2\left(1+\frac{\beta}{L}Y_E\right)\right]^{+} \end{aligned} , \tag{12}$$

where $Y_D = \sum_{k\in\Phi} Y_{R_kD}$ and $Y_E = \sum_{k\in\Phi} Y_{R_kE}$.

Based on [35], the CDF of Y_D and PDF of Y_E are given as

$$F_{Y_D}(y) = \frac{\Upsilon\left(m_{RD}L, \lambda_{RD}y\right)}{\Gamma\left(m_{RD}L\right)} , \tag{13}$$

$$f_{Y_E}(y) = \frac{\lambda_{RE}^{\,m_{RE}L}}{\Gamma(m_{RE}L)} y^{m_{RE}L-1} \exp(-\lambda_{RE}y), \tag{14}$$

where $\Upsilon(a,x) = \int_0^x t^{a-1}\exp(-t)\,dt$ is the lower incomplete gamma function as eq. (8.350.1) of [36].

3. Exact Secrecy Outage Probability Analysis

We evaluate the secrecy performance of the three different selection schemes by deriving the exact closed-form expressions for SOP in this section. SOP is defined as the probability that the instantaneous secrecy capacity is less than the desired secrecy rate $R_S > 0$ [2].

According to the law of total probability, the SOP of this system can be expressed as

$$\begin{aligned} P_{out} &= \Pr(C_S \le R_S) \\ &= \sum_{L=0}^{N} \binom{N}{L} \Pr(C_S \le R_S, |\Phi| = L) \\ &= \sum_{L=0}^{N} \binom{N}{L} \Pr(|\Phi| = L) \underbrace{\Pr(C_S \le R_S \,\|\Phi| = L)}_{P_{out}^{L}} \end{aligned} , \tag{15}$$

where $\binom{N}{L} = \frac{N!}{L!(N-L)!}$, $\Pr(|\Phi| = L)$ represents the probability that the number of successful decoding relay is L, and P_{out}^{L} represents the conditional SOP on $|\Phi| = L$. In the event of $|\Phi| = 0$, no relay can be selected to forward the messages, as a result of $C_S = 0$.

According to the definition of Φ, the probability of $|\Phi| = L$ is given as

$$\begin{aligned} \Pr(|\Phi| = L) &= \Pr\left(\bigcap_{i\in\Phi} C_{SR_i} \ge R_d, \bigcap_{k\notin\Phi} C_{SR_k} < R_d \right) \\ &= \left[\Pr(Y_{SR} \ge \theta)\right]^{L} \left[\Pr(Y_{SR} < \theta)\right]^{N-L} \\ &= \left[\exp(-\lambda_{SR}\theta) \sum_{n=0}^{m_{SR}-1} \frac{(\lambda_{SR}\theta)^n}{n!} \right]^{L} \left[1 - \exp(-\lambda_{SR}\theta) \sum_{n=0}^{m_{SR}-1} \frac{(\lambda_{SR}\theta)^n}{n!} \right]^{N-L} \end{aligned} , \tag{16}$$

Next, we will derive the conditional probability P_{out}^{L} of the three different schemes, respectively.

3.1 The Optimal Relay Selection Scheme

Because the fading channel of each group is i.i.d., using eq. (8), P_{out}^{L} of ORS scheme can be written as

$$\begin{aligned} P_{out}^{L,\mathrm{ORS}} &= \Pr\left(C_S^{\mathrm{ORS}} \le R_S\right) \\ &= \prod_{k\in\Phi} \Pr\left(C_{R_kD} - C_{R_kE} \le R_S\right), \\ &= \left(P_{ORS}\right)^{L} \end{aligned} \tag{17}$$

where $P_{ORS} = \Pr\left(C_{R_k D} - C_{R_k E} \le R_S\right)$.

Substituting eqs. (1), (2), and (8) into P_{ORS}, and using eq. (3.326.2) of [36], we obtain

$$\begin{aligned}
P_{ORS} &= \Pr\left(Y_{RD} \le \Theta Y_{RE} + \frac{\Theta-1}{\beta}\right) \\
&= \int_0^\infty F_{Y_{RD}}\left(\Theta y + \frac{\Theta-1}{\beta}\right) f_{Y_{RE}}(y)\,dy \\
&= 1 - \exp\left(-\frac{\lambda_{RD}(\Theta-1)}{\beta}\right) \sum_{n=0}^{m_{RD}-1} \sum_{l=0}^{n} \frac{{\lambda_{RD}}^{n}}{n!} \binom{n}{l} \Theta^{l} \left(\frac{\Theta-1}{\beta}\right)^{n-l} \frac{{\lambda_{RE}}^{m_{RE}}}{\Gamma(m_{RE})} \\
&\quad \times \int_0^\infty y^{m_{RE}+l-1} \exp\left(-\left(\lambda_{RD}\Theta + \lambda_{RE}\right) y\right) dy \\
&= 1 - \exp\left(-\frac{\lambda_{RD}(\Theta-1)}{\beta}\right) \frac{{\lambda_{RE}}^{m_{RE}}}{\Gamma(m_{RE})} \sum_{n=0}^{m_{RD}-1} \sum_{l=0}^{n} \left(\binom{n}{l} \frac{\Theta^{l}}{n! {\lambda_{RD}}^{-n}} \right. \\
&\quad \left. \times \left(\frac{\Theta-1}{\beta}\right)^{n-l} \frac{\Gamma(m_{RE}+l)}{\left(\lambda_{RD}\Theta + \lambda_{RE}\right)^{m_{RE}+l}} \right)
\end{aligned} \quad . \tag{18}$$

Finally, the SOP with the ORS scheme is obtained by substituting eq. (16) and eq. (18) into eq. (15).

3.2 The Suboptimal Relay Selection Scheme

Using eq. (10), P_{out}^{L} of SRS scheme can be written as

$$\begin{aligned}
P_{out}^{L,\mathrm{SRS}} &= \Pr\left(C_S^{\mathrm{SRS}} \le R_S\right) \\
&= \Pr\left(Y_{\mathrm{SRS}} \le \Theta Y_{RE} + \frac{\Theta-1}{\beta}\right) \\
&= \int_0^\infty F_{Y_{\mathrm{SRS}}}\left(\Theta y + \frac{\Theta-1}{\beta}\right) f_{Y_{RE}}(y)\,dy
\end{aligned} \quad . \tag{19}$$

Substituting eq. (1) and eq. (11) into eq. (19), and using eq. (3.326.2) of [36], we obtain

$$\begin{aligned}
P_{out}^{L,\mathrm{SRS}} &= \frac{\exp\left(-\frac{B(\Theta-1)}{\beta}\right)}{{\lambda_{RE}}^{-m_{RE}} \Gamma(m_{RE})} \sum_{SS} \sum_{l=0}^{C} \binom{C}{l} \Theta^{l} \left(\frac{\Theta-1}{\beta}\right)^{C-l} \\
&\quad \times \int_0^\infty y^{m_{RE}+l-1} \exp\left(-\left(B\Theta + \lambda_{RE}\right) y\right) dy \\
&= \frac{\exp\left(-\frac{B(\Theta-1)}{\beta}\right)}{{\lambda_{RE}}^{-m_{RE}} \Gamma(m_{RE})} \sum_{SS_1} \sum_{l=0}^{C_1} \binom{C}{l} \Theta^{l} \left(\frac{\Theta-1}{\beta}\right)^{C-l} \frac{\Gamma(m_{RE}+l)}{\left(B\Theta + \lambda_{RE}\right)^{m_{RE}+l}}
\end{aligned} \quad . \tag{20}$$

Finally, the SOP with the SRS scheme is obtained by substituting eq. (16) and eq. (20) into eq. (15).

3.3 The Multiple Relays Combining Scheme

Using eq. (12), P_{out}^{L} of MRC scheme can be written as

$$\begin{aligned} P_{out}^{L,\mathrm{MRC}} &= \Pr\left(C_S^{\mathrm{MRC}} \le R_S\right) \\ &= \Pr\left(Y_D \le \Theta Y_E + \frac{L(\Theta-1)}{\beta}\right) \\ &= \int_0^\infty F_{Y_D}\left(\Theta y + \frac{L(\Theta-1)}{\beta}\right) f_{Y_E}(y)\,dy \end{aligned} . \tag{21}$$

Substituting eqs. (13) and (14) into eq. (21), and using eqs. (3.326.2) and (8.352.1) of [36], we obtain

$$\begin{aligned} P_{out}^{L,\mathrm{MRC}} &= 1-\exp\left(-\frac{\lambda_{RD}L(\Theta-1)}{\beta}\right)\sum_{n=0}^{m_{RD}L-1}\sum_{l=0}^{n}\frac{\binom{n}{l}\lambda_{RE}{}^{m_{RE}L}\lambda_{RD}{}^{n}}{\Theta^{-l}\Gamma(m_{RE}L)n!}\left(\frac{L(\Theta-1)}{\beta}\right)^{n-l} \\ &\quad \times\int_0^\infty y^{m_{RE}L-1}\exp\left(-(\lambda_{RD}\Theta+\lambda_{RE})y\right)dy \\ &= 1-\exp\left(-\frac{\lambda_{RD}L(\Theta-1)}{\beta}\right)\sum_{n=0}^{m_{RD}L-1}\sum_{l=0}^{n}\left(\frac{\binom{n}{l}\lambda_{RD}{}^{n}\Theta^{l}}{\Gamma(m_{RE}L)n!}\right. \\ &\quad \left.\times\left(\frac{L(\Theta-1)}{\beta}\right)^{n-l}\frac{\lambda_{RE}{}^{m_{RE}L}\Gamma(m_{RE}L+l)}{(\lambda_{RD}\Theta+\lambda_{RE})^{m_{RE}L+l}}\right) \end{aligned} . \tag{22}$$

Finally, the SOP with the MRC scheme is obtained by substituting eqs. (16) and (22) into eq. (15).

4. Asymptotic Secrecy Outage Probability

In this section, we consider a special scenario that the received SNR at R and D in the high regime to derive the closed-form expressions for asymptotic SOP with the three different selection schemes. The asymptotic expressions can help us analyzing the secrecy diversity order G_d and the secrecy array gain G_a. Mathematically, we describe this scenario as $\Omega_{SR} = \Omega_{RD} = \Omega_D \to \infty$.

Based on eq. (4), when $\Omega_{SR} \to \infty$ all relays can correctly decode received signal. then the probability of $\lim\limits_{\Omega_{SR}\to\infty} \Pr\left(|\Phi| = N\right) = 1$ and eq. (15) can be simplified as

$$P_{out}^{\infty} = \Pr\left(C_S \le R_S \,\middle\|\, \Phi| = N\right). \tag{23}$$

According to refs. [6] and [7], the asymptotic SOP also can be written as

$$P_{out}^{\infty} = \left(G_a\Omega_D\right)^{-G_d} + \mathcal{O}\left(\Omega_D{}^{-G_d}\right), \tag{24}$$

where G_d determines the slope of the asymptotic SOP curve, G_a characterizes the SNR advantage of the asymptotic SOP relative to the reference curve $\Omega_D{}^{-G_d}$, and $\mathcal{O}(\cdot)$ denotes higher order terms.

4.1 The Optimal Relay Selection Scheme

Applying the Taylor series expansion given by $\exp(x)=\sum_{n=0}^{\infty}\frac{x^n}{n!}$, we obtain

$$\sum_{n=0}^{m_{RD}-1}\frac{(\lambda_{RD}y)^n}{n!}=\exp(\lambda_{RD}y)-\frac{(\lambda_{RD}y)^{m_{RD}}}{m_{RD}!}+\mathcal{O}\left(y^{m_{RD}}\right). \tag{25}$$

Substituting eq. (25) into eq. (2), the asymptotic CDF of Y_{RD} can be written as

$$F_{Y_{RD}}^{\infty}=\frac{(\lambda_{RD}y)^{m_{RD}}}{m_{RD}!}+\mathcal{O}\left(y^{m_{RD}}\right). \tag{26}$$

Substituting eqs. (2) and (26) into eq. (18) and using eq. (3.326.2) of [36], we obtain

$$\begin{aligned} P_{out}^{\infty,\mathrm{ORS}} &= \left(P_{ORS}^{\infty}\right)^N \\ &= \left[\int_0^{\infty}F_{Y_{RD}}^{\infty}\left(\Theta y+\frac{\Theta-1}{\beta}\right)f_{Y_{RE}}(y)\,dy\right]^N \\ &= \frac{1}{\Omega_{RD}{}^{m_{RD}N}}\left[\frac{m_{RD}{}^{m_{RD}}}{\Gamma(m_{RE})m_{RD}!}\sum_{n=0}^{m_{RD}}\binom{m_{RD}}{n}\left(\frac{\Theta-1}{\beta}\right)^{m_{RD}-n}\frac{\Gamma(m_{RE}+n)}{\Theta^{-n}m_{RE}{}^{n}}\Omega_{RE}{}^{n}\right]^N \end{aligned}. \tag{27}$$

Henceforth, using eqs. (23) and (27), the secrecy diversity order and the secrecy array gain for the ORS scheme are obtained as

$$G_d^{\mathrm{ORS}}=Nm_{RD}, \tag{28}$$

$$G_a^{\mathrm{ORS}}=\left[\frac{m_{RD}{}^{m_{RD}}}{\Gamma(m_{RE})m_{RD}!}\sum_{n=0}^{m_{RD}}\binom{m_{RD}}{n}\left(\frac{\Theta-1}{\beta}\right)^{m_{RD}-n}\frac{\Theta^n\Gamma(m_{RE}+n)}{\lambda_{RE}{}^{n}}\right]^{-\frac{1}{m_{RD}}}. \tag{29}$$

4.2 The Suboptimal Relay Selection Scheme

Substituting eq. (25) into eq. (11), the asymptotic CDF of Y_{SRS} can be written as

$$F_{Y_{\mathrm{SRS}}}^{\infty}(y)=\frac{(\lambda_{RD}y)^{Nm_{RD}}}{(m_{RD}!)^N}+\mathcal{O}\left(y^{Nm_{RD}}\right). \tag{30}$$

Substituting eqs. (1) and (30) into eq. (19), and using eq. (3.326.2) of [36], we obtain

$$\begin{aligned} P_{out}^{\infty,\mathrm{SRS}} &= \int_0^{\infty}F_{Y_{\mathrm{SRS}}}^{\infty}\left(\Theta y+\frac{\Theta-1}{\beta}\right)f_{Y_{RE}}(y)\,dy \\ &= \frac{\Omega_{RD}{}^{-Nm_{RD}}m_{RD}{}^{Nm_{RD}}}{\Gamma(m_{RE})(m_{RD}!)^N}\sum_{n=0}^{Nm_{RD}}\Omega_{RE}{}^{n}\binom{Nm_{RD}}{n}\left(\frac{\Theta-1}{\beta}\right)^{Nm_{RD}-n}\frac{\Gamma(m_{RE}+n)}{\Theta^{-n}m_{RE}{}^{n}} \end{aligned}. \tag{31}$$

Henceforth, using eqs. (23) and (31), the secrecy diversity order and the secrecy array gain for the SRS scheme are obtained as

$$G_d^{\mathrm{SRS}}=Nm_{RD}, \tag{32}$$

$$G_a^{\mathrm{SRS}} = \left[\frac{m_{RD}{}^{Nm_{RD}}}{\Gamma\left(m_{RE}\right)\left(m_{RD}!\right)^N} \sum_{n=0}^{Nm_{RD}} \binom{Nm_{RD}}{n} \left(\frac{\Theta-1}{\beta}\right)^{Nm_{RD}-n} \frac{\Theta^n \Gamma\left(m_{RE}+n\right)}{\lambda_{RE}{}^n} \right]^{-\frac{1}{Nm_{RD}}}. \quad (33)$$

4.3 The Multiple Relays Combining Scheme

Utilizing the same method as ORS, we obtain the asymptotic CDF of Y_D as

$$F_{Y_D}^{\infty}\left(y\right) = \frac{1}{\left(Nm_{RD}\right)!}\left(\lambda_{RD} y\right)^{Nm_{RD}} + \mathcal{O}\left(y^{Nm_{RD}}\right). \quad (34)$$

Substituting eqs. (14) and (34) into (21), and using eq. (3.326.2) of [36], we obtain

$$\begin{aligned} P_{out}^{\infty,\mathrm{MRC}} &= \int_0^{\infty} F_{Y_D}^{\infty}\left(\Theta y + \frac{\Theta-1}{\beta}\right) f_{Y_E}\left(y\right) dy \\ &= \frac{\left(\Omega_{RD}\right)^{-Nm_{RD}} m_{RD}{}^{Nm_{RD}}}{\Gamma\left(Nm_{RE}\right)\left(Nm_{RD}\right)!} \sum_{n=0}^{Nm_{RD}} \Omega_{RE}{}^n \binom{Nm_{RD}}{n} \left(\frac{\Theta-1}{\beta}\right)^{Nm_{RD}-n} \frac{\Theta^n \Gamma\left(Nm_{RE}+n\right)}{\Theta^{-n} m_{RE}{}^n} \end{aligned}. \quad (35)$$

Henceforth, using eqs. (23) and (35), the secrecy diversity order and the secrecy array gain for the MRC scheme are obtained as

$$G_d^{\mathrm{MRC}} = Nm_{RD}, \quad (36)$$

$$G_a^{\mathrm{MRC}} = \left[\frac{m_{RD}{}^{Nm_{RD}}}{\Gamma\left(Nm_{RE}\right)\left(Nm_{RD}\right)!} \sum_{n=0}^{Nm_{RD}} \binom{Nm_{RD}}{n} \left(\frac{\Theta-1}{\beta}\right)^{Nm_{RD}-n} \frac{\Gamma\left(Nm_{RE}+n\right)}{\Theta^{-n} \lambda_{RE}{}^n} \right]^{-\frac{1}{Nm_{RD}}}. \quad (37)$$

Remark 1: Obviously, one can find that the exact or asymptotic closed-form expressions for SOP of each scheme are consistent when only one relay ($N=1$) is utilized. Besides, the secrecy performance of each scheme will be improved as Ω_D increases or Ω_E decreases as can be seen from eqs. (27), (31), and (35).

Remark 2: It can be observed that the expression of secrecy diversity order with three different selection schemes are same and only relate to the number of relays and the fading parameters between the selected relay and D as can be seen from eqs. (28), (32), and (36). From eqs. (29), (33), and (37) we find that the impact of the wiretap channels (m_{RE} and Ω_{RE}) is only reflected in the secrecy array gain.

5. Numerical and Simulation Results

In this section, we present the exact and asymptotic numerical results by using the derived expressions of the three different selection schemes and investigate the impact of various key system parameters on the system secrecy performance. Monte Carlo simulations are also presented to validate our analysis. The main parameters utilized in analysis and simulation are set as, $m_{SR} = m_{RD} = m_{RE} = m$, $\sigma^2 = 1$, and the unit of R_d / R_S is bit/s/Hz. As shown in **Fig. 2** to **Fig. 5**, it is clear that the results of exact analysis match very well with the simulation, and ORS scheme always outperforms other schemes when the global CSI of all links are available.

One can observe in **Fig. 2**, when $N=1$, the three different selection schemes have same security performance. This is because only one relay can be used to transmit signal and instantaneous secrecy capacity of each scheme are same as can be seen from in eqs. (8), (10), and (12). With the number of relays increasing, the security performance of all schemes can be enhanced. It indicates that cooperative technology can enhance the wireless security against eavesdropping attack as MIMO. Besides, with the number of relays increasing, secrecy performance of MRC scheme performs better than SRS scheme in the high Ω_{RD} region.

Fig. 3 plots the SOP of the three different selection schemes versus P_R while m varying. From this figure, we can observe that SOP decreases with the transmitting power increasing, while there exists a floor for the SOP in the high P_R region, which is testified in [37]. The security performance with lower m worse than the one with higher m, since a higher m typically refers to a stronger received SNR and the number of successfully decoded relays increasing. Besides, higher m means a higher secrecy diversity order of the model as the conclusion of section 3. One can also observe that SRS scheme may perform better than MRC in the high m region.

Fig. 4 demonstrates the SOP versus Ω_{SR} with varying R_S. One can find that with Ω_{SR} increasing, the secrecy performance is enhanced because a higher Ω_{SR} signifies that the received SNR at the relays is improving and more relays can decode signal successfully. Besides, the SOP decreases as the desired secrecy rate decreases.

Fig. 5 plots the exact and asymptotic numerical results for the three different selection schemes while Ω_{RD} varying. It is shown in **Fig. 5** that the asymptotic curves tightly approximate the exact curves with Ω_{RD} increasing and very close to the exact curves in the high SNR regime, which corroborates the accuracy of our derivation and can be utilized to effectively evaluate the secrecy outage performance of this model in the high SNR regime.

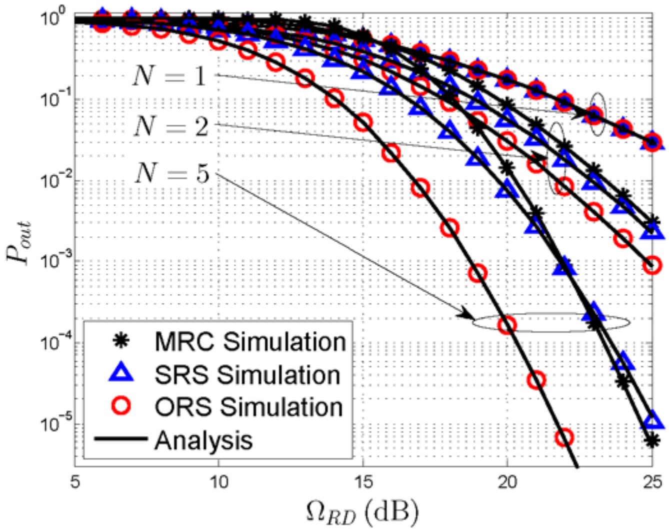

Fig. 2. SOP versus Ω_{RD} with $\Omega_{SR} = \Omega_{RD}$, $m = 2$, $P_S = P_R = 1\text{dBW}$, $R_d = R_S = 0.1$, and $\Omega_{RE} = 15\text{ dB}$.

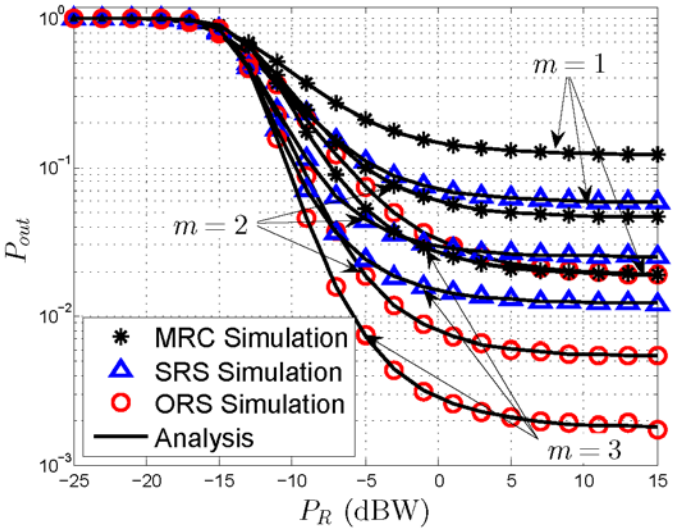

Fig. 3. SOP versus P_R with $P_S = P_R$, $N = 3$, $\Omega_{SR} = \Omega_{RD} = 6\,\text{dB}$, $R_d = R_S = 0.1$, and $\Omega_{RE} = 1\,\text{dB}$.

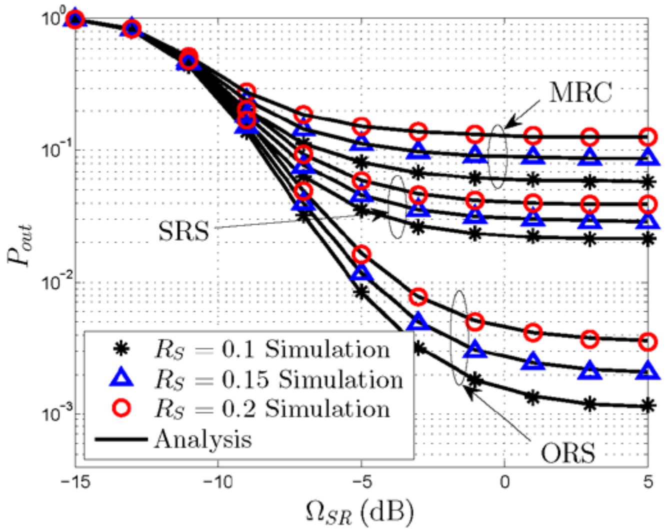

Fig. 4. SOP versus Ω_{SR} with $P_S = P_R = 1\,\text{dBW}$, $N = 5$, $R_d = 0.1$, $\Omega_{RD} = 5\,\text{dB}$, and $\Omega_{RE} = 1\,\text{dB}$.

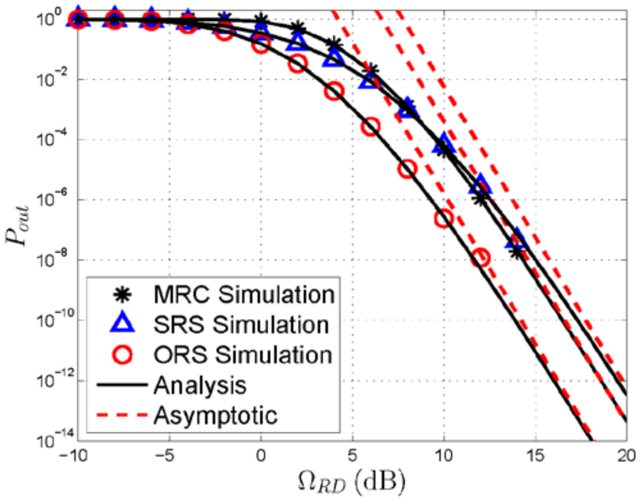

Fig. 5. SOP versus Ω_{RD} with $\Omega_{SR} = \Omega_{RD}$, $m = 2$, $P_S = P_R = 1\text{dBW}$, $R_d = R_S = 0.1$, and $\Omega_{RE} = 1\text{dB}$.

6. Conclusion

In this paper, we studied the security performance of cooperative wireless networks with ORS, SRS, and MRC schemes over Nakagami-m fading channels. The exact and asymptotic closed-form expressions for SOP of the three different selection schemes were derived and validated by simulations. Numerical results illustrated that ORS scheme always performs better than SRS and MRC schemes and the secrecy performance of SRS scheme is better than MRC scheme in some special scenario such as when the destination is far away from the relays (i.e. then the average main channel fading gain falls in the low region). Also, we obtained the secrecy diversity order which is Nm_{RD} and the secrecy array gain. It is indicated that the number of relays and parameters between the relay and D have a great impact on the secrecy diversity order, and the impact of the wiretap channels is only reflected in the secrecy array gain. The model will be beneficial for designing practical cooperative communication system, especially where the PLS issues is considered. However, comparing with DF, AF protocol is easier to implement in practice, which can be an interesting topic of our future works.

References

[1] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, October 1975. Article (CrossRef Link)

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

[3] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088-3104, July 2010. Article (CrossRef Link)

[4] A. Khisti and G. W. Wornell, A. Khisti and G. W. Wornell, "Secure transmission with multiple antenna-part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515-5532, November 2010. Article (CrossRef Link)

[5] H. Alves, R. D. Souza, M. R. Debbah, and M. Bennis, “Performance of transmit antenna selection physical layer security schemes,” *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372-375, June 2012. Article (CrossRef Link)

[6] 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, January 2013. Article (CrossRef Link)

[7] H. Lei, C. Gao, I. Ansari, Y. Guo, Y. Zou, G. Pan, K. A. Qaraqe, “Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-*m* channels,” *IEEE Trans. Veh. Technol.* Article (CrossRef Link)

[8] H. M. Wang and X. G. Xia, “Enhancing wireless secrecy via cooperation: signal design and optimization,” *IEEE Commun,. Mag.*, vol.53, no. 12, pp. 47-53, December 2015. Article (CrossRef Link)

[9] S. Zhang and S. C. Liew, “Channel coding and decoding in a relay system operated with physical-layer network coding,” *IEEE J. Sel. Areas Commun.*, vol. 27, no. 5, pp. 788-796, June 2009. Article (CrossRef Link)

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

[11] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus, and A. Yener, “Cooperative security at the physical layer: a summary of recent advances,” *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16-28, September 2013. Article (CrossRef Link)

[12] J. H. Fan and C. W. Yuan, “Outage performance for DF two-way relaying with co-channel interference over Nakagami-*m* fading,” *KSII Trans. Internet Inf. Syst.*, vol. 9, no. 11, pp. 4469-4482, November 2015. Article (CrossRef Link)

[13] P. Chen, O. Jian, and W. P. Zhu, “Secrecy analysis of amplify-and-forward relay networks with beamforming,” *KSII Trans. Internet Inf. Syst.*, vol. 10, no. 10, pp. 5049 - 5062, October 2016. Article (CrossRef Link)

[14] M. Yuksel and E. Erkip, “Secure communication with a relay helping the wire-tapper,” in *Proc. of IEEE Information Theory Workshop (ITW)*, Tahoe City, September, pp. 595-600, 2007. Article (CrossRef Link)

[15] 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, no. 12, pp. 3062-3080, December 2004. Article (CrossRef Link)

[16] I. Krikidis, “Opportunistic relay selection for cooperative networks with secrecy constraints,” *IET Commun.*, vol. 4, no.15, pp. 1787-1791, October 2010. Article (CrossRef Link)

[17] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, “Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers,” *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6076-6085, December 2013. Article (CrossRef Link)

[18] J. Mo, M. Tao, and Y. Liu, “Relay placement for physical layer security: a secure connection perspective,” *IEEE Commun.Lett.*, vol. 16, no. 6, pp. 878-881, June 2012. Article (CrossRef Link)

[19] 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, October 2013. Article (CrossRef Link)

[20] W. Wang, K. C. Teh, and K. H. Li, “Generalized relay selection for improved security in cooperative DF relay networks,” *IEEE Wireless Communications Letters*, vol. 5, no. 1, pp. 28-31, February 2016. Article (CrossRef Link)

[21] L. Fan, N. Yang, T. Duong, M. Elkashlan, and G. Karagiannidis, “Exploiting direct links for physical layer security in multi-user multi-relay networks,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 3856 - 3867, June 2016. Article (CrossRef Link)

[22] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan and T. Q. Duong, “Relay selection for security enhancement in cognitive relay networks,” *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 46-49, February 2015. Article (CrossRef Link)

[23] Y. Huang, J. Wang, C. Zhong, T. Q. Duong and G. K. Karagiannidis, "Secure transmission in cooperative relaying networks with multiple antennas," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6843-6856, October 2016. Article (CrossRef Link)

[24] H. Zhang, H. Xing, J. Cheng, A. Nallanathan and V. C. M. Leung, "Secure resource allocation for OFDMA two-way relay wireless sensor networks without and with cooperative jamming," *IEEE Trans. Ind. Inf.*, vol. 12, no. 5, pp. 1714-1725, October 2016. Article (CrossRef Link)

[25] N. Zhao, F. R. Yu, M. Li, Q. Yan and V. C. M. Leung, "Physical layer security issues in interference- alignment-based wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 162-168, August 2016. Article (CrossRef Link)

[26] H. Lei, H. Zhang, I. S. Ansari, C. Gao, Y. Guo, G. Pan, et al., "Secrecy outage performance for SIMO underlay cognitive radio systems with generalized selection combining over Nakagami-m channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10126 - 10132, December 2016. Article (CrossRef Link)

[27] Y. Lee, M. H. Tsai, and S. I. Sou, "Performance of decode-and-forward cooperative communications with multiple dual-hop relays over Nakagami-*m* fading channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 6, pp. 2853-2859, June 2009. Article (CrossRef Link)

[28] C. Zhong, S. Jin, and K. K. Wong, "Dual-hop systems with noisy relay and interference-limited destination," *IEEE Trans. Commun.*, vol. 58, no. 3, pp. 764-768, March 2010. Article (CrossRef Link)

[29] T. Q. Duong, D. Benevides da Costa, T. A. Tsiftsis, C. Zhong, and A. Nallanathan, "Outage and diversity of cognitive relaying systems under spectrum sharing environments in Nakagami-*m* fading," *IEEE Commun. Lett.*, vol. 16, no. 12, pp. 2075-2078, December 2012. Article (CrossRef Link)

[30] X. Zhang, Y. Zhang, Z. Yan, J. Xing, and W. Wang, "Performance analysis of cognitive relay networks over Nakagami-*m* fading channels," IEEE *J. Sel. Areas Commun.*, vol. 33, no. 5, pp. 865-877, May 2015. Article (CrossRef Link)

[31] Y. Wang, Y. Xu, N. Li, W. Xie, K. Xu, and X. Xia, "Relay selection of full-duplex decode-and-forward relaying over Nakagami-*m* fading channels," *IET Commun.*, vol. 10, no. 2, pp. 170-179, February 2016. Article (CrossRef Link)

[32] J. Zhu, Y. Zou, B. Champagne, W. P. Zhu, and L. Hanzo, "Security-reliability trade-off analysis of multi-relay aided decode-and-forward cooperation systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5825 - 5831, July 2016. Article (CrossRef Link)

[33] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-*m* fading channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054-6067, November 2014. Article (CrossRef Link)

[34] W. Feller, *An Introduction to Probability Theory and Its Applications*, 3rd ed. Hoboken, NJ, USA: Wiley, 1968.

[35] Z. Chen, Z. Chi, Y. Li, and B. Vucetic, "Error performance of maximal-ratio combining with transmit antenna selection in flat Nakagami-*m* fading channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 1, pp. 424-431, January 2009. Article (CrossRef Link)

[36] I. S. Gradshteyn and I. M. Ryzik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, USA: Academic Press, 2007. Article (CrossRef Link)

[37] H. Lei, I. S. Ansari, G. Pan, B. Alomair, and M.-S. Alouini, "Secrecy capacity analysis over α-μ fading channels," *IEEE Commun. Lett.*, doi: 10.1109/LCOMM.2017.2669976, 2017. Article (CrossRef Link)

Huan Zhang received the B.S. degree from the Chongqing University of Posts and Telecommunications (CQUPT), Chongqing, China, in 2014. He is currently pursuing the M.S. degree in information and communication engineering at CQUPT. His research interests include cognitive radio networks, physical layer security, and cooperative communications.

Hongjiang Lei received the B.Eng degree in Mechanical and Electrical Engineering from Shenyang Institute of Aeronautical Engineering, Shenyang, China, in 1998, the M.Sc. degree in Computer Application Technology from Southwest Jiaotong University, Chengdu, China, in 2004, and the Ph.D. degree in Instrument Science and Technology from Chongqing University, Chongqing, China, in 2015, respectively. Since 2004, he has been with School of Communication and Information Engineering of Chongqing University of Posts and Telecommunications, Chongqing, China, where he is currently an Associate Professor. His research interest spans special topics in communications theory and signal processing, including secure communications, and CR communications.

Imran Shafique Ansari received the B.S. degree in Computer Engineering from King Fahd University of Petroleum and Minerals (KFUPM) in 2009 (with First Honors) and M.Sc. and Ph. D. degree from King Abdullah University of Science and Technology (KAUST) in 2010 and 2015, respectively. Currently, he is a Postdoctoral Research Associate (PRA) with Texas A&M University at Qatar (TAMUQ). From May 2009 through Aug. 2009, he was a visiting scholar at Michigan State University (MSU), East Lansing, MI, USA, and from Jun. 2010 through Aug. 2010, he was a research intern with. Carleton University, Ottawa, ON, Canada. His current research interests include free-space optics (FSO), channel modeling/signal propagation issues, relay/multihop communications, physical layer secrecy issues, full duplex systems, and diversity reception techniques among others

Gaofeng Pan received the B.S. degree in communication engineering from Zhengzhou University, Zhengzhou, China, in 2005, and the Ph.D. degree in communication and information systems from Southwest Jiaotong University, Chengdu, China, in 2011. He was with The Ohio State University, Columbus, OH USA, from 2009 to 2011, as a Joint-Trained Ph.D. Student under the supervision of Prof. E. Ekici. In 2012, he joined the School of Electronic and Information Engineering, Southwest University, Chongqing, China, where he is currently an Associate Professor. Since 2016, he has been with the School of Computing and Communications, Lancaster University, Lancaster, U.K., where he holds a post-doctoral position under the supervision of Prof. Z. Ding. His research interest spans special topics in communications theory, signal processing, and protocol design, including secure communications, CR/cooperative communications, and MAC protocols.

Khalid A. Qaraqe received the B.S. degree in EE from the University of Technology, Bagdad, Iraq in 1986, with honors. He received the M.S. degree in EE from the University of Jordan, Jordan, Amman, Jordan, in 1989, and he earned his Ph.D. degree in EE from Texas A&M University, College Station, TX, in 1997. From 1989 to 2004, Dr. Qaraqe has held a variety positions in many companies and he has over 12 years of experience in the telecommunication industry. Dr. Qaraqe has worked on numerous GSM, CDMA, and WCDMA projects and has experience in product development, design, deployments, testing, and integration.