This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCCN.2017.2758372, IEEE Transactions on Cognitive Communications and Networking

On Secrecy Outage of Relay Selection in Underlay Cognitive Radio Networks over Nakagami-m Fading Channels

Hongjiang Lei, *Member, IEEE,* Huan Zhang, Imran Shafique Ansari, *Member, IEEE,* Zhi Ren, Gaofeng Pan, *Member, IEEE,* Khalid A. Qaraqe, *Senior Member, IEEE,* and Mohamed-Slim Alouini, *Fellow, IEEE*

***Abstract*—In this paper, the secrecy outage performance of an underlay cognitive decode-and-forward relay network over independent but not necessarily identical distributed (i.n.i.d) Nakagami-m fading channels is investigated, in which the secondary user transmitter communicates with the secondary destination via relays, and an eavesdropper attempts to overhear the information. Based on whether the channel state information (CSI) of the wiretap links is available or not, we analyze the secrecy outage performance with optimal relay selection (ORS) and suboptimal relay selection (SRS) schemes, and multiple relays combining scheme (MRC) scheme is considered for comparison purpose. The exact and asymptotic closed-form expressions for the secrecy outage probability with three different relay selection schemes are derived and verified by Monte-Carlo simulations. The numerical results illustrate that ORS scheme always outperforms SRS and MRC schemes, and SRS scheme is better than MRC scheme in the lower fading parameters scenario. Furthermore, through asymptotic analysis, we find that these three different schemes achieve the same secrecy diversity order, which is determined by the number of the relays, and the fading parameters of the links among the relays and the destination.**

***Index Terms*—Underlay cognitive networks, decode-and-forward, relay selection, secrecy outage performance, Nakagami-m fading.**

Manuscript received.

This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant 61471076, Chinese Scholarship Council under Grant 201607845004, 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 and cstc2017jcyjAX0204, and the Scientific and Technological Research Program of Chongqing Municipal Education Commission under Grant KJ1600413 and KJ1704088. Parts of this publication were made possible by NPRP (National Priorities Research Program) grant # NPRP8-648-2-273. Part of this work has been presented at the IEEE International Conference on Communications, Paris, France, May 2017.

H. Lei, H. Zhang, and Z. Ren are with Chongqing Key Lab of Mobile Communications Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China. H. Lei is also with Computer, Electrical, and Mathematical Science and Engineering (CEMSE) Division, King Abdullah University of Science and Technology (KAUST), Thuwal 23955-6900, Kingdom of Saudi Arabia (e-mail: leihj@cqupt.edu.cn).

I. S. Ansari and K. A. Qaraqe are with the Department of Electrical and Computer Engineering (ECEN), Texas A&M University at Qatar (TAMUQ), Education City, Doha 23874, Qatar.

G. Pan is with the School of Computing and Communications, Lancaster University, LA1 4WA, UK.

M.-S. Alouini is with Computer, Electrical, and Mathematical Sciences and Engineering (CEMSE) Division, King Abdullah University of Science and Technology (KAUST), Thuwal 23955-6900, Kingdom of Saudi Arabia.

I. INTRODUCTION

A. Background

OVER the past few years, cognitive radio networks (CRNs) have rekindled enormous interest in the wireless community due to the fact that it can solve the spectrum scarcity problem by exploiting the existing wireless spectrum opportunistically. In CRNs, all the unlicensed secondary users (SUs) are permitted to transmit concurrently on the same frequency band with the licensed primary users (PUs) through underlay, overlay, and interweave paradigms [1]. Among these schemes, the underlay scheme is the most popular spectrum sharing technique due to its low implementation complexity, where the SUs are allowed to utilize the licensed spectrum if the interference caused to PUs is below a given interference threshold.

Security and privacy are of great importance in modern wireless communications. The physical layer security (PLS) has emerged as a key technique to provide trustworthiness and reliability for future wireless transmissions due to the broadcast nature of wireless transmission. Differing from the traditional cryptographic mechanisms that require private key exchange, the main idea of PLS is to exploit the wireless channels physical layer characteristics, such as fading, noise and/or interference, to realize secure communications [2]. More specifically, irrespective of the legitimate channel's propagating condition being better than the wiretap's channel, secret data transmission is theoretically possible without sharing any key, as shown by Wyner's wiretap model [3].

B. Related Works

Recently, the PLS of CRNs has attracted increasing research attention [4-13]. A comprehensive review of physical layer attacks in CRNs was presented [4] and [5]. The authors in refs. [6] and [7] analyzed the secrecy performance for a model comprising of multiple antennas SU transmitter in the presence of an eavesdropper. The secrecy performance of single-input multiple-output (SIMO) CRNs was investigated and the closed-form expression for the secrecy outage probability (SOP) was derived in [8]. Ref. [9] analyzed the secrecy performance of SIMO CRNs with generalized selection combining over Nakagami-m fading channels and the closed-form expression for the SOP was derived. The secrecy outage performance of optimal antenna selection and suboptimal antenna selection schemes for multiple-input and multiple-output (MIMO) underlay cognitive radio systems over Nakagami-m channels was investigated and the exact and asymptotic closed-form expressions for the SOP of various transmit antenna selection (TAS) schemes were derived in [10]. A secure switch-and-stay combining protocol was proposed for the secure cognitive relay networks with two DF relays and the analytical expressions of exact and asymptotic SOP were derived in [11]. The secrecy performance of full-duplex multi-antenna spectrum-sharing wiretap networks was investigated in [12] in which a jamming signal is simultaneously transmitted by the full-duplex cognitive receiver, and the two antenna reception schemes were designed to enhance the security. The secrecy performance of an underlay MIMO CRNs with energy harvesting was investigated in [13] and the closed-form expressions for the SOP of three different TAS schemes over Rayleigh channels were derived. Prior works on PLS mainly focus on the study of three-node wiretap channel model, and multiple antennas were utilized to improve secrecy performance. However, in some scenarios, such as hand-held terminals, sensor nodes, etc, it is difficult to implement MIMO technique due to the limitation in physical size and power consumption. In recent years, cooperative communications have emerged as a powerful spatial diversity technology that can effectively combat channel fading and increase system secrecy capacity [14].

The authors in [15] analyzed the secrecy capacity of the wireless transmissions in the presence of an eavesdropper with a relay node, where amplify-and-forward (AF), decode-and-forward (DF), and compress-and-forward (CF) relaying protocols were examined and compared with each other. Ref. [16] analyzed the design of the secrecy transmission in DF relay networks to maximize the secrecy throughput under a SOP constraint. The authors of [17] proposed several cooperation strategies in facilitating secure wireless communications and obtained the corresponding achievable performance bounds. In refs. [18] and [19], Zou *et al.* studied the cooperative relays to enhance PLS and showed the security can be improved by using relay selection over Rayleigh fading. Ref. [20] obtained the expressions for the intercept probability and the outage probability (OP) of the proposed relay selection schemes for a CRN with realistic spectrum sensing. In [21], the authors analyzed the outage performance of CRNs with the Nth best-relay selection scheme over independent and identically distributed (i.i.d.) fading channels. Three relay selection schemes were proposed in [22] for full-duplex heterogeneous networks in the presence of multiple cognitive eavesdroppers and the closed-form expressions for the exact and asymptotic SOP were derived under the attack of non-colluding/colluding eavesdroppers. While all of the aforementioned works substantially provide a good understanding of PLS for cooperative communication systems, all of them are limited to Rayleigh fading channels.

Comparing with Rayleigh fading, Nakagami-m model provides a good match to various empirically obtained measurement data [23] and is widely utilized for modeling wireless fading channels, including Rayleigh ($m = 1$) and one-sided Gaussian distribution ($m = 0.5$) as special cases. The OP of dual-hop CRNs with an AF relay over Nakagami-m fading channels was obtained in [24]. The performance of DF relay selection networks over Nakagami-m fading channels was analyzed in [25], and the closed-form expression for the OP was derived. In [26], the authors presented performance analysis for underlay cognitive DF relay networks with the Nth best relay selection scheme over Nakagami-m fading channels, and the exact and asymptotic closed-form expressions for the OP were derived. So far, to the best of the authors' knowledge, in the open literature, there is an absence in investigation of security performance for cognitive CRNs over independent but not necessarily identical distributed (i.n.i.d.) Nakagami-m fading channels with relay selection.

C. Motivation and Contributions

In this paper we investigate the PLS for the underlay cognitive network with multiple DF relays over i.n.i.d. Nakagami-m fading channels. Our main contributions are as follows[1]:

- The secrecy outage 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 ORS, SRS, and MRC schemes are derived, which build the relationship between the secrecy performance and the related systems parameters, and are verified via simulations.
- The asymptotic closed-form expressions for the SOP of three different selection schemes are derived, 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, which is closely related to the number of the relays and the fading parameters of the links among the relays and the destination.
- Compared to [32] or [33] wherein the secrecy performance for underlay CRNs with single or multiple relay nodes over Rayleigh fading channels was analyzed, we explore the secrecy performance for CRNs with multiple relay nodes over i.n.i.d Nakagami-m fading channels.
- Relative to [35]-[40] wherein the SOP for the cooperative systems with multiple relays over Rayleigh or Nakagami-m fading channels was derived, we analyze the secrecy outage performance with three different relay selection schemes in the underlay cognitive radio systems experiencing i.n.i.d. Nakagami-m fading.
- Relative to [41]-[43] wherein only the maximum interference power constraint is considered at the SU source node, we consider more general conditions that both the maximum interference power constraint and the maximum transmit power constraint must be met at the SU source node and all the relay nodes.

[1]The secrecy performance of AF/CF relays was investigated in the available literatures, such as [15], [24], [27]. Similar performance with AF relay selection was analyzed in [28], [29], [30], [31]. However, none of these works have considered CR scenarios. The secrecy performance of underlay CRNs with multiple AF or CF relays will be considered as part of our future works.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCCN.2017.2758372, IEEE Transactions on Cognitive Communications and Networking

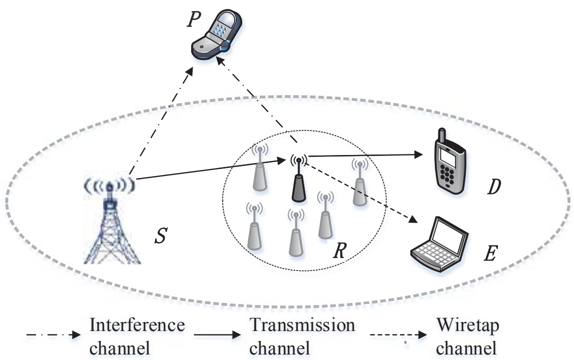

Fig. 1. System Model demonstrating a primary user (P), a secondary user/source transmitter (S), a collection of relays (R), a desired destination (D), and an undesired eavesdropper (E).

D. Structure

The rest of the paper is organized as follows. In Section II, the system model considered in our work is described and the ORS, SRS, and MRC schemes are presented. We derive the exact and asymptotic closed-form expressions for the SOP of the three different relay selection schemes in Section III and IV. In Section V, we present and discuss the numerical results and the Monte-Carlo simulations. Finally, Section VI concludes the paper.

II. System Model and Secrecy Capacity

A. System Model

In this paper, we consider an underlay cognitive relay wireless network model, as shown in Fig. 1. It consists of a primary user (P), a secondary transmitter (S), N secondary cooperative relays ($R_i, 1 \leq i \leq N$), one secondary destination (D), and an eavesdropper (E). Following [15]-[17], we consider that the directly links between S and D/E are unavailable due to severe shadowing and path-loss, and communication can be established only via relays. We assume that all nodes are equipped with a single antenna and the relays utilizing two adjacent time slots are employed. In the first time slot, S broadcasts its signal to the relays that attempt to decode their received signals. In the second time slot, only the optimal relay, which is selected from the successful decode relay set, forwards the decoded outcome to D, and E may overhear the confidential information, where a two slot protocol has been utilized, based on numerous works in the available literature [18]-[21]. All the channels are assumed to experience i.n.i.d. quasi-static Nakagami-m fading with fading parameters m_j and average channel power gains Ω_j, where $j \in (SP, SR_i, R_iP, R_iD, R_iE)$. 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 the channel gains can be expressed by

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

$$F_{Y_j}(y) = \frac{\Upsilon(m_j, \lambda_j y)}{\Gamma(m_j)}, \tag{2}$$

where $\lambda_j = m_j/\Omega_j$, $\Gamma(\cdot)$ is the gamma function, as defined by (8.310) of [44] and $\Upsilon(a, x) = \int_0^x \exp(-t) t^{a-1} dt$ is the lower incomplete gamma function, as defined by (8.350.1) of [44].

Using (8.352.1) of [44], the CDF of Y_j is rewritten as

$$F_{Y_j}(y) = 1 - \exp(-\lambda_j y) \sum_{n=0}^{m_j - 1} \frac{(\lambda_j y)^n}{n!}. \tag{3}$$

The channel capacity between S to the ith relay is given by

$$C_{SR_i} = \frac{1}{2} \log_2 \left(1 + \frac{P_S}{\sigma^2} Y_{SR_i}\right), \tag{4}$$

where the factor $\frac{1}{2}$ in front of $\log(\cdot)$ arises from the fact that relays operate in half-duplex mode and two time slots are required to complete the transmission of S to D via R_i [15], [37]. P_S is the transmit power at S, $Y_{SR_i} = |h_{SR_i}|^2$, and h_{SR_i} is the channel fading coefficients between S and R_i.

Similarly, the channel capacity from the ith relay to D/E can be given by

$$C_{R_iD} = \frac{1}{2} \log_2 \left(1 + \frac{P_i}{\sigma^2} Y_{R_iD}\right), \tag{5}$$

$$C_{R_iE} = \frac{1}{2} \log_2 \left(1 + \frac{P_i}{\sigma^2} Y_{R_iE}\right), \tag{6}$$

respectively, where P_i is the transmit power at the ith relay, $Y_{R_iD} = |h_{R_iD}|^2$, $Y_{R_iE} = |h_{R_iE}|^2$, h_{R_iD} and h_{R_iE} are the channel fading coefficients between R_i and D/E, respectively.

According to underlay cognitive radio transmission, the transmit power at S and relays must be limited at a given threshold to guarantee a reliable communication at P [10]. Due to the maximum interference power constraint and the maximum transmit power constraint, the transmit power at S and ith relay are strictly constrained by[2]

$$P_S = \min(P_{\max}, P_I/Y_{SP}), \tag{7}$$

$$P_i = \min(P_{\max}, P_I/Y_{R_iP}), \tag{8}$$

respectively, where $P_{\max}$ is the maximal transmit power at S and all the relays, and P_I is the maximum tolerated interference power at P.

Based on [26] and [37], the ith relay can successfully decode the received signal when C_{SR_i} is larger than the target data rate. Otherwise, the relays are unable to recover the signal from S. So the probability of the ith relay cannot successfully decode is

$$\begin{aligned} P_{fail}^i &= \Pr(C_{SR_i} \leq R_d) \\ &= \Pr\left(Y_{SR_i} \leq \frac{(\theta - 1)\sigma^2}{P_S}\right), \end{aligned} \tag{9}$$

[2]As similar to [32]-[43], it is assumed that source and relay nodes are with perfect CSI in our work. However, considering that the channel estimation is not perfect and always suffers from estimation errors, our derived results are optimistic compared to the practical ones. Analyzing the secrecy performance of CRN with outdated CSI is an interesting topic and will be part of our future work.

where R_d is the data rate threshold for successfully decode and $\theta = 2^{2R_d}$.

For notational convenience, let Φ denote the set of the relays that can successfully decode the received signal. There are 2^N possible subsets Φ and the sample space of Φ can be written as

$$\Phi = \{\emptyset, \Phi_1, \Phi_2, \cdots, \Phi_n, \cdots, \Phi_{2^N-1}\}, \tag{10}$$

where $\emptyset$ denotes an empty subset and Φ_n denotes the nth non-empty subset of Φ. we define $|\Phi|$ as the number of the relays in Φ, and $|\Phi_n| = L$.

Next, we will present the relay selection criterion of three different relay selection schemes when successful decode set is Φ_n.

B. The Optimal Relay Selection Scheme

When the channel state information (CSI) of all links is available at relays similar to [18] and [19], the relay that maximizes the secrecy capacity in successfully decode set is selected as the optimal relay. The relay selection criterion for ORS scheme in set Φ_n can be expressed as

$$b = \arg\max_{i\in\Phi_n} \left[C_{R_iD} - C_{R_iE}\right]^+, \tag{11}$$

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

Then the secrecy capacity with ORS scheme can be written as

$$\begin{aligned} C_S^{\mathrm{ORS}} &= \max_{i\in\Phi_n}\left[C_{R_iD} - C_{R_iE}\right]^+ \\ &= \max_{i\in\Phi_n}\left[\frac{1}{2}\log_2\left(1+\frac{P_i}{\sigma^2}Y_{R_iD}\right)\right. \\ &\qquad \left. - \frac{1}{2}\log_2\left(1+\frac{P_i}{\sigma^2}Y_{R_iE}\right)\right]^+. \end{aligned} \tag{12}$$

C. The Suboptimal Relay Selection Scheme

When only the CSI of R_i to D links are available, the relay that maximizes the power gains of R_i to D is selected as the best relay. The relay selection criterion for SRS scheme in set Φ_n can be expressed as

$$b = \arg\max_{i\in\Phi_n} Y_{R_iD}. \tag{13}$$

Then the secrecy capacity with SRS scheme can be written as

$$\begin{aligned} C_S^{\mathrm{SRS}} &= \left[C_{R_bD} - C_{R_bE}\right]^+ \\ &= \left[\frac{1}{2}\log_2\left(1+\frac{P_b}{\sigma^2}Y_{\mathrm{SRS}}\right) - \frac{1}{2}\log_2\left(1+\frac{P_b}{\sigma^2}Y_{R_bE}\right)\right]^+, \end{aligned} \tag{14}$$

where C_{R_bD} and C_{R_bE} is the channel capacity from the selected relay to D and E, respectively. P_b is the transmit power at the selected relay and $Y_{\mathrm{SRS}} = \max_{i\in\Phi_n} Y_{R_iD}$.

Lemma 1: The CDF of Y_{SRS} is

$$F_{Y_{SRS}}(y) = \sum_{SRS} (-1)^i A \exp(-By)\, y^M, \tag{15}$$

where $\sum\limits_{SRS} (-1)^i = \sum\limits_{i=0}^{|\Phi_n|}\sum\limits_{n_1=1}^{|\Phi_n|}\cdots\sum\limits_{n_i=1}^{|\Phi_n|}\sum\limits_{l_1=0}^{m_{R_{n_1}D}-1}\cdots \times \sum\limits_{l_i=0}^{m_{R_{n_i}D}-1}(-1)^i, (n_1 \neq \cdots \neq n_i)$, $A = \prod\limits_{t=1}^{i}\frac{{\lambda_{n_t}}^{l_t}}{l_t!}$, $B = \sum_{t=1}^{i}\lambda_{R_{n_t}D}$, and $M = \sum_{t=1}^{i} l_t$.

Proof: The proof is given in Appendix A. ■

The relay selected with SRS scheme is only optimum for D, which means E and P are not able to exploit any additional diversity from the multiple relays under this scheme.

D. The Multiple Relay Combining Scheme

In this subsection, the traditional DF multiple relay combing scheme is presented for comparison purposes, where all successful decode relays participate in forwarding the signal to D. D and E combine its received signals [18]. Without loss of generality, P also combines its received signals to judge whether the suffered interference is larger than the maximum tolerated interference power P_I or not. In order to make a fair comparison with other schemes, the total amount of transmit power at relays shall be limited to $P_{\max}$, with equal-power allocation, the transmit power of each successful relay is given by

$$P_i^* = \min\left(P_{\max}/L, P_I/Y_P\right), \tag{16}$$

where $Y_P = \sum\limits_{i\in\Phi_n} Y_{R_iP}$.

Hence, the secrecy capacity for this scheme is

$$\begin{aligned} C_S^{\mathrm{MRC}} &= \left[C_D^{\mathrm{MRC}} - C_E^{\mathrm{MRC}}\right]^+ \\ &= \left[\frac{1}{2}\log_2\left(1+\frac{P_i^*}{\sigma^2}Y_D\right) - \frac{1}{2}\log_2\left(1+\frac{P_i^*}{\sigma^2}Y_E\right)\right]^+, \end{aligned} \tag{17}$$

where $Y_g = \sum\limits_{i\in\Phi_n} Y_{R_ig}, g\in(P, D, E)$. Based on [45], the PDF and the CDF of Y_g is

$$f_{Y_g}(y) = \frac{{\lambda_{Rg}}^{m_{Rg}L}}{\Gamma(m_{Rg}L)} y^{m_{Rg}L-1}\exp(-\lambda_{Rg}y), \tag{18}$$

$$F_{Y_g}(y) = \frac{\Upsilon(m_{Rg}L, \lambda_{Rg}y)}{\Gamma(m_{Rg}L)}. \tag{19}$$

III. Exact Secrecy Outage Probability Analysis

SOP is defined as the probability that the instantaneous secrecy rate of the system is less than a predefined target rate R_s [2]. According to the law of total probability, the SOP can be written as

$$\begin{aligned} P_{out} &= \Pr(C_S \le R_s) \\ &= \Pr(\Phi=\emptyset) + \sum_{n=1}^{2^N-1}\Pr(C_S\le R_s, \Phi=\Phi_n) \\ &= \Pr(\Phi=\emptyset) \\ &\quad + \sum_{n=1}^{2^N-1}\Pr(\Phi=\Phi_n)\underbrace{\Pr(C_S\le R_s\,|\Phi=\Phi_n)}_{P_{\Phi_n}}. \end{aligned} \tag{20}$$

In the case of $\Phi=\emptyset$, no relay can forward signal to D, leading $C_S = 0$. In the case of $\Phi = \Phi_n$, the relays in set

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCCN.2017.2758372, IEEE Transactions on Cognitive Communications and Networking

Φ_n can forward signal to D and the relays in set $\bar{\Phi}_n$ cannot forward signal, where $\bar{\Phi}_n$ is the complementary set of Φ_n, so

$$\begin{aligned}\Pr\left(\Phi=\Phi_n\right)=&\prod_{i\in\Phi_n}\Pr\left(Y_{SR_i}\geq\frac{(\theta-1)\,\sigma^2}{P_S}\right)\\&\times\prod_{k\in\bar{\Phi}_n}\Pr\left(Y_{SR_k}\leq\frac{(\theta-1)\,\sigma^2}{P_S}\right)\\=&\Pr\left(\Phi=\Phi_n,P_S=P_{\max}\right)\\&+\Pr\left(\Phi=\Phi_n,P_S=P_I/Y_{SP}\right).\end{aligned}\tag{21}$$

Lemma 2: The expression of $\Pr\left(\Phi=\Phi_n\right)$ is given by (22), as shown at the top of the next page, where $\alpha=P_{\max}/\sigma^2$, $\beta=P_I/\sigma^2$, $\sum\limits_{SRS_1}A_1=\sum\limits_{l_1=0}^{m_{SR_1}-1}\cdots\sum\limits_{l_{|\Phi_n|}=0}^{m_{SR_{|\Phi_n|}}-1}\prod\limits_{t=1}^{|\Phi_n|}\frac{\left(\lambda_{SR_t}y\right)^{l_t}}{l_t!}$, $\sum\limits_{SRS_2}(-1)^i=\sum\limits_{i=0}^{|\bar{\Phi}_n|}\sum\limits_{n_1=1}^{|\bar{\Phi}_n|}\cdots\sum\limits_{n_i=1}^{|\bar{\Phi}_n|}\sum\limits_{l_1=0}^{m_{R_{n_1}D}-1}\cdots\sum\limits_{l_i=0}^{m_{R_{n_i}D}-1}(-1)^i\ (n_1\neq\cdots\neq n_i)$, $B_1=\sum\limits_{t=1}^{|\Phi_n|}\lambda_{SR_t}$, $M_1=\sum\limits_{t=1}^{|\Phi_n|}l_t$, $A_2=\prod\limits_{t=1}^{i}\frac{{\lambda_{n_t}}^{l_t}}{l_t!}$, $B_2=\sum_{t=1}^{i}\lambda_{R_{n_t}D}$, $M_2=\sum_{t=1}^{i}l_t$, and $\Gamma\left(a,x\right)=\int_x^{\infty}\exp\left(-t\right)t^{a-1}dt$ is the upper incomplete gamma function, as defined by (8.350.2) of [44].

Proof: The proof is given in Appendix B. ∎

Next, we will give the derivations of P_{Φ_n} for ORS, SRS, and MRC schemes, respectively.

A. The Optimal Relay Selection Scheme

Using (12) and (20), P_{Φ_n} with the ORS scheme can be expressed as

$$\begin{aligned}P_{\Phi_n}^{\rm ORS}&=\Pr\left(C_S^{\rm ORS}\leq R_s\left|\Phi=\Phi_n\right.\right)\\&=\Pr\left(\max_{i\in\Phi_n}\left[C_{R_iD}-C_{R_iE}\right]^+\leq R_s\right)\\&=\prod_{i\in\Phi_n}\underbrace{\Pr\left(C_{R_iD}-C_{R_iE}\leq R_s\right)}_{P_i^{\rm ORS}},\end{aligned}\tag{23}$$

where

$$\begin{aligned}P_i^{\rm ORS}=&\Pr\left(C_{R_iD}-C_{R_iE}\leq R_s,P_i=P_{\max}\right)\\&+\Pr\left(C_{R_iD}-C_{R_iE}\leq R_s,P_i=P_I/Y_{R_iP}\right)\\=&\underbrace{\Pr\left(Y_{R_iD}\leq\Theta Y_{R_iE}+\frac{(\Theta-1)}{\alpha},Y_{R_iP}\leq\frac{\beta}{\alpha}\right)}_{I_1}\\&+\underbrace{\Pr\left(Y_{R_iD}\leq\Theta Y_{R_iE}+\frac{(\Theta-1)\,Y_{R_iP}}{\beta},Y_{R_iP}>\frac{\beta}{\alpha}\right)}_{I_2},\end{aligned}\tag{24}$$

where $\Theta=2^{2R_s}$.

Substituting (1) and (3) into (24), and using (3.326.2) of [44], we achieve

$$\begin{aligned}I_1=&\Pr\left(Y_{R_iD}\leq\Theta Y_{R_iE}+\frac{(\Theta-1)}{\alpha},Y_{R_iP}\leq\frac{\beta}{\alpha}\right)\\=&F_{Y_{R_iP}}\left(\frac{\beta}{\alpha}\right)\int_0^{\infty}F_{Y_{R_iD}}\left(\Theta y+\frac{(\Theta-1)}{\alpha}\right)f_{Y_{R_iE}}\left(y\right)dy\\=&\frac{\Upsilon\left(m_{R_iP},\frac{\lambda_{R_iP}\beta}{\alpha}\right)}{\Gamma\left(m_{R_iP}\right)}\left(1-\sum_{n=0}^{m_{R_iD}-1}\sum_{l=0}^{n}\Xi_1\right.\\&\left.\times\left(\frac{(\Theta-1)}{\alpha}\right)^{n-l}\exp\left(-\frac{\lambda_{R_iD}\left(\Theta-1\right)}{\alpha}\right)\right),\end{aligned}\tag{25}$$

where $\Xi_1=\frac{C_n^l{\lambda_{R_iE}}^n\Theta^l{\lambda_{R_iE}}^{m_{R_iE}}\Gamma\left(m_{R_iE}+l\right)}{n!\Gamma\left(m_{R_iE}\right)\left(\lambda_{R_iE}+\lambda_{R_iE}\Theta\right)^{m_{R_iE}+l}}$ and $C_n^l=\frac{n!}{l!(n-l)!}$.

We rewrite I_2 as

$$\begin{aligned}I_2=&\Pr\left(Y_{R_iD}\leq\Theta Y_{R_iE}+\frac{(\Theta-1)\,Y_{R_iP}}{\beta},Y_{R_iP}>\frac{\beta}{\alpha}\right)\\=&\int_{\frac{\beta}{\alpha}}^{\infty}H_1\left(x\right)f_{Y_{R_iP}}\left(x\right)dx,\end{aligned}\tag{26}$$

where $H_1\left(x\right)=\int_0^{\infty}F_{Y_{R_iD}}\left(\Theta y+\frac{(\Theta-1)x}{\beta}\right)f_{Y_{R_iE}}\left(y\right)dy$.

Substituting eqs. (1) and (3) into H_1, and utilizing eq. (3.326.2) of [44], we obtain

$$\begin{aligned}H_1\left(x\right)=1-&\sum_{n=0}^{m_{R_iD}-1}\sum_{l=0}^{n}\Xi_1\left(\frac{(\Theta-1)\,x}{\beta}\right)^{n-l}\\&\times\exp\left(-\frac{\lambda_{R_iD}\left(\Theta-1\right)x}{\beta}\right).\end{aligned}\tag{27}$$

Substituting (27) into (26) and using eq. (3.351.2) and (8.356.3) of [44], we get

$$\begin{aligned}I_2=&\frac{\Gamma\left(m_{R_iP},\lambda_{R_iP}\frac{\beta}{\alpha}\right)}{\Gamma\left(m_{R_iP}\right)}-\frac{{\lambda_{R_iP}}^{m_{R_iP}}}{\Gamma\left(m_{R_iP}\right)}\sum_{n=0}^{m_{R_iD}-1}\sum_{l=0}^{n}\Xi_1\\&\times\left(\frac{(\Theta-1)}{\beta}\right)^{n-l}\left(\lambda_{R_iP}+\frac{\lambda_{R_iP}\left(\Theta-1\right)}{\beta}\right)^{-\left(m_{R_iP}+n-l\right)}\\&\times\Gamma\left(m_{R_iP}+n-l,\frac{\beta}{\alpha}\left(\lambda_{R_iP}+\frac{\lambda_{R_iP}\left(\Theta-1\right)}{\beta}\right)\right).\end{aligned}\tag{28}$$

Then, $P_i^{\rm ORS}$ can be obtained by substituting I_1 and I_2 into (24). Finally, the SOP with the ORS scheme is obtained by substituting (22) and (23) into (20).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCCN.2017.2758372, IEEE Transactions on Cognitive Communications and Networking

$$\Pr\left(\Phi = \Phi_n\right) = \frac{\Upsilon\left(m_{SP}, \lambda_{SP}\frac{\beta}{\alpha}\right)}{\Gamma\left(m_{SP}\right)} \prod_{i \in \Phi_n}\left(1 - \frac{\Upsilon\left(m_{SR_i}, \lambda_{SR_i}\left(\frac{\theta-1}{\alpha}\right)\right)}{\Gamma\left(m_{SR_i}\right)}\right) \prod_{j \in \bar{\Phi}_n}\left(1 - \frac{\Upsilon\left(m_{SR_j}, \lambda_{SR_j}\left(\frac{\theta-1}{\alpha}\right)\right)}{\Gamma\left(m_{SR_j}\right)}\right)$$
$$+ \frac{{\lambda_{SP}}^{m_{SP}}}{\Gamma\left(m_{SP}\right)} \sum_{SRS_1} \sum_{SRS_2} (-1)^i A_1 A_2 \left(\frac{(\theta-1)}{\beta}\right)^{M_1+M_2} \frac{\Gamma\left(M_1+M_2+m_{SP}, \frac{\beta}{\alpha}\left(\frac{(B_1+B_2)(\theta-1)}{\beta}+\lambda_{SP}\right)\right)}{\left(\frac{(B_1+B_2)(\theta-1)}{\beta}+\lambda_{SP}\right)^{M_1+M_2+m_{SP}}}. \quad (22)$$

B. The Suboptimal Relay Selection Scheme

Employing (14) and (20), and using the law of total probability, P_{Φ_n} with the SRS scheme can be written as

$$\begin{aligned} P_{\Phi_n}^{\rm SRS} &= \Pr\left(C_S^{\rm SRS} \le R_s \,|\Phi = \Phi_n\right) \\ &= \Pr\left(\frac{1}{2}\log_2\left(1+\frac{P_b}{\sigma^2}Y_{\rm SRS}\right) - \frac{1}{2}\log_2\left(1+\frac{P_b}{\sigma^2}Y_{R_b E}\right)\right) \\ &= \sum_{i\in\Phi_n} \Pr\left(Y_{\rm SRS} \le \Theta Y_{R_i E} + \frac{(\Theta-1)\,\sigma^2}{P_i}, b=i\right) \\ &= \sum_{i\in\Phi_n} \Pr\left(b=i\right) \underbrace{\Pr\left(Y_{\rm SRS} \le \Theta Y_{R_i E} + \frac{(\Theta-1)\,\sigma^2}{P_i}\right)}_{P_i^{\rm SRS}}, \end{aligned} \quad (29)$$

where $\Pr\left(b=i\right)$ means the probability that the ith relay in set Φ_n is selected to forward the decoded outcome to D.

Lemma 3: The expression of $\Pr\left(b=i\right)$ is

$$\Pr\left(b=i\right) = \sum_{SRS_3} \frac{(-1)^k A_3 {\lambda_{R_i D}}^{m_{R_i D}} \Gamma\left(M_3+m_{R_i D}\right)}{\Gamma\left(m_{R_i D}\right)\left(\lambda_{R_i D}+B_3\right)^{M_3+m_{R_i D}}}. \quad (30)$$

where $\sum\limits_{SRS_3} (-1)^k = \sum\limits_{k=0}^{|\Phi_n|-1} \sum\limits_{n_1=1}^{|\Phi_n|-1} \cdots \sum\limits_{n_k=1}^{|\Phi_n|-1} \sum\limits_{l_1=0}^{m_{R_{n_1}D}-1} \cdots \times \sum\limits_{l_k=0}^{m_{R_{n_k}D}-1} (-1)^k \left(n_1 \ne \cdots \ne n_k\right)$, $k \in \Phi_n - i$, $A_3 = \prod\limits_{t=1}^{k} \frac{{\lambda_{n_t}}^{l_t}}{l_t!}$, $B_3 = \sum_{t=1}^{k} \lambda_{R_{n_t}D}$, and $M_3 = \sum_{t=1}^{k} l_t$.

Proof: The proof is given in Appendix C. ■

Making use of (8), $P_i^{\rm SRS}$ can be rewritten as

$$P_i^{\rm SRS} = \underbrace{\left(Y_{\rm SRS} \le \Theta Y_{R_i E} + \frac{(\Theta-1)}{\alpha}, Y_{R_i P} \le \frac{\beta}{\alpha}\right)}_{I_3} + \underbrace{\left(Y_{\rm SRS} \le \Theta Y_{R_i E} + \frac{(\Theta-1)\,Y_{R_i P}}{\beta}, Y_{R_i P} > \frac{\beta}{\alpha}\right)}_{I_4}. \quad (31)$$

Substituting (1) and (15) into (31), and making use of eq. (3.326.2) of [44], we have

$$\begin{aligned} I_3 &= \Pr\left(Y_{\rm SRS} \le \Theta Y_{R_i E} + \frac{(\Theta-1)}{\alpha}, Y_{R_i P} \le \frac{\beta}{\alpha}\right) \\ &= \int_0^{\frac{\beta}{\alpha}} \Pr\left(Y_{\rm SRS} \le \Theta Y_{R_i E} + \frac{(\Theta-1)}{\alpha}\right) f_{Y_{R_i P}}\left(x\right) dx \\ &= F_{R_i P}\left(\frac{\beta}{\alpha}\right) \int_0^{\infty} F_{Y_{\rm SRS}}\left(\Theta y + \frac{(\Theta-1)}{\alpha}\right) f_{Y_{R_i E}}\left(y\right) dy \\ &= \frac{\Upsilon\left(m_{R_i P}, \lambda_{R_i P}\frac{\beta}{\alpha}\right)}{\Gamma\left(m_{R_i P}\right)} \\ &\quad \times \sum_{\rm SRS} \sum_{l=0}^{M} \Xi_2 \left(\frac{(\Theta-1)}{\alpha}\right)^{M-l} \exp\left(-\frac{B\left(\Theta-1\right)}{\alpha}\right), \end{aligned} \quad (32)$$

where $\Xi_2 = (-1)^i C_M^l \Theta^l \frac{A\Gamma\left(m_{R_i E}+l\right)}{\left(B\Theta+\lambda_{R_i E}\right)^{m_{R_i E}+l}}$.

Also, we can rewrite I_4 as

$$I_4 = \int_{\frac{\beta}{\alpha}}^{\infty} H_2\left(x\right) f_{Y_{R_i P}}\left(x\right) dx, \quad (33)$$

where $H_2\left(x\right) = \int_0^{\infty} F_{Y_{\rm SRS}}\left(\Theta y + \frac{(\Theta-1)x}{\beta}\right) f_{Y_{R_i E}}\left(y\right) dy$.

Substituting eqs. (1) and (15) into H_2, we can obtain

$$H_2\left(x\right) = \sum_{SRS} \sum_{l=0}^{M} \Xi_2 \left(\frac{(\Theta-1)}{\beta/x}\right)^{M-l} \exp\left(-\frac{B\left(\Theta-1\right)}{\beta/x}\right). \quad (34)$$

Substituting (1) and (34) into (33) and utilizing eq. (3.351.2) of [44], we obtain

$$\begin{aligned} I_4 &= \frac{{\lambda_{R_i P}}^{m_{R_i P}}}{\Gamma\left(m_{R_i P}\right)} \sum_{SRS} \sum_{l=0}^{M} \Xi_2 \left(\frac{(\Theta-1)}{\beta}\right)^{M-l} \\ &\quad \times \frac{\Gamma\left(m_{R_i P}+M-l, \frac{\beta}{\alpha}\left(\lambda_{R_i P}+\frac{B(\Theta-1)}{\beta}\right)\right)}{\left(\lambda_{R_i P}+\frac{B(\Theta-1)}{\beta}\right)^{m_{R_i P}+M-l}}. \end{aligned} \quad (35)$$

Then, $P_i^{\rm SRS}$ can be obtained by substituting I_3 and I_4 into (31). Finally, the SOP with SRS scheme is obtained by substituting (22) and (29) into (20).

C. The Multiple Relay Combining Scheme

It is noted that obtaining a closed-form expression for SOP of MRC scheme is challenging when all the channels are i.n.i.d. distributed. However numerical SOP results can be easily obtained through computer simulations. For simplicity, in this subsection the channels between relays and $P/D/E$ are assumed to experience i.i.d. quasi-static distributed as [18], [20], and [37]. Then the link between relays and $P/D/E$ can be

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCCN.2017.2758372, IEEE Transactions on Cognitive Communications and Networking

classified into three groups, $R_i \to P$, $R_i \to D$, and $R_i \to E$. The fading parameter and average channel fading gains of each groups is m_j and Ω_j, where $j \in (RP, RD, RE)$.

Based on (17) and (20), the P_{Φ_n} with the MRC scheme is written as

$$\begin{aligned} P_{\Phi_n}^{\mathrm{MRC}} &= \Pr\left(C_S^{\mathrm{MRC}} \le R_s \left|\Phi = \Phi_n\right.\right) \\ &= \Pr\left(Y_D \le \Theta Y_E + \frac{(\Theta-1)\,\sigma^2}{P_i^*}, P_i^*{=}P_{\max}/L\right) \\ &+ \Pr\left(Y_D \le \Theta Y_E + \frac{(\Theta-1)\,\sigma^2}{P_i^*}, P_i^*{=}P_I/Y_P\right) \\ &= \underbrace{\Pr\left(Y_D \le \Theta Y_E + \frac{(\Theta-1)\,L}{\alpha}, Y_P \le \frac{L\beta}{\alpha}\right)}_{I_5} \\ &+ \underbrace{\Pr\left(Y_D \le \Theta Y_E + \frac{(\Theta-1)\,Y_P}{\beta}, Y_P \ge \frac{L\beta}{\alpha}\right)}_{I_6}. \end{aligned} \tag{36}$$

Substituting eqs. (18) and (19) into (36), and making use of eqs. (3.326.2) and (8.352.1) of [44], we have

$$\begin{aligned} I_5 &= \Pr\left(Y_D \le \Theta Y_E + \frac{(\Theta-1)\,L}{\alpha}, Y_P \le \frac{L\beta}{\alpha}\right) \\ &= \int_0^{\frac{L\beta}{\alpha}} \Pr\left(Y_D \le \Theta Y_E + \frac{(\Theta-1)\,L}{\alpha}\right) f_{Y_P}(x)\,dx \\ &= F_{Y_P}\left(\frac{L\beta}{\alpha}\right) \int_0^\infty F_{Y_D}\left(\Theta y + \frac{(\Theta-1)\,L}{\alpha}\right) f_{Y_E}(y)\,dy \\ &= \frac{\Upsilon\left(m_{RP}L, \frac{\lambda_{RP}L\beta}{\alpha}\right)}{\Gamma(m_{RP})} \left(1 - \sum_{n=0}^{m_{RD}L-1} \sum_{l=0}^{n} \Xi_3 \right. \\ &\quad \left. \times \left(\frac{(\Theta-1)\,L}{\alpha}\right)^{n-l} \exp\left(-\frac{(\Theta-1)\,\lambda_{RD}L}{\alpha}\right)\right), \end{aligned} \tag{37}$$

where $\Xi_3 = \frac{C_n^l {\lambda_{RD}}^n \Theta^l (\lambda_{RE})^{m_{RE}L} \Gamma(m_{RE}L+l)}{n!\Gamma(m_{RE}L)(\lambda_{RE}+\lambda_{RD}\Theta)^{m_{RE}L+l}}$.

Also, we can rewrite I_6 as

$$I_6 = \int_{\frac{L\beta}{\alpha}}^\infty H_3(x)\, f_{Y_P}(x)\,dx, \tag{38}$$

where $H_3(x) = \int_0^\infty F_{Y_D}\left(\Theta y + \frac{(\Theta-1)x}{\beta}\right) f_{Y_E}(y)\,dy$.

Substituting eqs. (18) and (19) into H_3, we obtain

$$\begin{aligned} H_3(x) = 1 - &\sum_{n=0}^{m_{RD}L-1} \sum_{l=0}^{n} \Xi_3 \\ &\times \left(\frac{(\Theta-1)\,x}{\beta}\right)^{n-l} \exp\left(-\frac{(\Theta-1)\,\lambda_{RD}x}{\beta}\right). \end{aligned} \tag{39}$$

Substituting (18) and (39) into (38) and using (3.351.2) and (8.356.3) of [44], we have

$$\begin{aligned} I_6 = &\frac{\Gamma\left(m_{RP}L, \frac{\lambda_{RP}L\beta}{\alpha}\right)}{\Gamma(m_{RP}L)} - \sum_{n=0}^{m_{RD}L-1} \sum_{l=0}^{n} \left(\frac{\Xi_3 {\lambda_{RP}}^{m_{RP}L}}{\Gamma(m_{RP}L)}\right. \\ &\times \left(\frac{(\Theta-1)}{\beta}\right)^{n-l} \left(\lambda_{RP} + \frac{(\Theta-1)\,\lambda_{RD}}{\beta}\right)^{-(m_{RP}L+n-l)} \\ &\left.\times\Gamma\left(m_{RP}L+n-l, \frac{\beta}{\alpha}\left(\lambda_{RP} + \frac{(\Theta-1)\,\lambda_{RD}}{\beta}\right)\right)\right). \end{aligned} \tag{40}$$

Then, $P_{\Phi_n}^{\mathrm{MRC}}$ is obtained by substituting I_5 and I_6 into (36). Finally, the SOP with MRC scheme is obtained by substituting (22) and (36) into (20).

When $m_{SR} = m_{SP} = m_{RP} = m_{RD} = m_{RE} = 1$, our results are in compliance with the results of [34]. When $N = 1$ and $m_{SR} = m_{SP} = m_{RP} = m_{RD} = m_{RE} = 1$, our results match with the results of [32] and partly with the results of [35].

IV. Asymptotic Secrecy Outage Probability Analysis

In this section, we consider a special scenario that S and D locate quite closer to the relays with $\Omega_{SR_i} \to \infty$ and $\Omega_{R_iD} \to \infty$. So the links between relays and D can be assumed as i.i.d. Nakagami-m fading distributed with $m_{R_iD} = m_{RD}$ and $\Omega_{R_iD} = \Omega_{RD}$. These assumptions can help us to obtain the asymptotic SOP of three different relay selection schemes, and analyze the secrecy diversity order and the secrecy array gain.

As suggested by [10] and [46], in the high average channel fading gains regime with $\Omega_{RD} \to \infty$, the asymptotic SOP can be expressed as

$$P_{out}^\infty = (G_a \Omega_{RD})^{-G_d} + \mathcal{O}\left({\Omega_{RD}}^{-G_d}\right), \tag{41}$$

where G_a is the secrecy array gain, G_d is the secrecy diversity order that determines the slope of the asymptotic SOP curve, and $\mathcal{O}(\cdot)$ denotes higher order terms.

Observing (4), (9), and (20), when $\Omega_{SR_i} \to \infty$, all relays can decode received signal successfully ($\Pr(|\Phi| = N) = 1$). Then the asymptotic SOP can be rewritten as

$$P_{out}^\infty = \Pr\left(C_S^\infty \le R_s \left||\Phi| = N\right.\right), \tag{42}$$

where C_S^∞ is security capacity when $\Omega_{RD} \to \infty$.

Next we will give the derivations of asymptotic SOP and analyze G_a and G_d.

A. The Optimal Relay Selection Scheme

Based on (23), P_{out}^∞ of ORS scheme can be expressed as

$$P_{out}^{\infty,\mathrm{ORS}} {=} \prod_{1\le i\le N} (I_1^\infty {+} I_2^\infty). \tag{43}$$

Based on [10], when $\Omega_{RD} \to \infty$, the asymptotic CDF of Y_{RD} is given by

$$F_{Y_{RD}}^\infty(y) = \frac{(\lambda_{RD}y)^{m_{RD}}}{m_{RD}!} + \mathcal{O}\left(y^{m_{RD}}\right). \tag{44}$$

Substituting eqs. (1) and (44) into (24), and using eq. (3.326.2) of [44], we obtain

$$I_1^\infty = F_{Y_{R_iP}}\left(\frac{\beta}{\alpha}\right)\int_0^\infty F_{Y_{RD}}^\infty\left(\Theta x+\frac{(\Theta-1)}{\alpha}\right)f_{Y_{R_iE}}(x)\,dx = \frac{\Upsilon\left(m_{R_iP},\frac{\lambda_{R_iP}\beta}{\alpha}\right)}{\Gamma(m_{R_iP})}\sum_{l=0}^{m_{RD}}\Xi_4\alpha^{l-m_{RD}}, \tag{45}$$

where $\Xi_4=\frac{\lambda_{RD}{}^{m_{RD}}C_{m_{RD}}^l\Theta^l(\Theta-1)^{m_{RD}-l}\Gamma\left(m_{R_iE}+l\right)}{\lambda_{R_iE}{}^{-m_{R_iE}}\Gamma\left(m_{R_iE}\right)m_{RD}!\lambda_{R_iE}{}^{m_{R_iE}+l}}$.

Making use of eqs. (1) and (44), and utilizing eq. (3.326.2) of [44], we obtain

$$H_1^\infty(x) = \int_0^\infty F_{Y_{RD}}^\infty\left(\Theta y+\frac{(\Theta-1)x}{\beta}\right)f_{Y_{R_iE}}(y)\,dy = \sum_{l=0}^{m_{RD}}\Xi_4\beta^{l-m_{RD}}x^{m_{RD}-l}. \tag{46}$$

Substituting (46) into (26) and using eq. (3.351.2) of [44], we obtain

$$I_2^\infty = \int_{\frac{\beta}{\alpha}}^\infty H_1^\infty(x)f_{Y_{R_iP}}(x)\,dx = \frac{\beta^{l-m_{RD}}}{\Gamma(m_{R_iP})}\sum_{l=0}^{m_{RD}}\frac{\Gamma\left(m_{R_iP}+m_{RD}-l,\frac{\beta}{\alpha}\right)}{\Xi_4{}^{-1}\lambda_{R_iP}{}^{m_{RD}-l}}. \tag{47}$$

Finally, $P_{\Phi_n}^\infty$ with the ORS scheme is obtained by substituting I_1^∞ and I_2^∞ into (43).

Henceforth, utilizing (41), G_d and G_a for the ORS scheme are obtained as

$$G_d^{\rm ORS} = m_{RD}N, \tag{48}$$

$$G_a^{\rm ORS} = \left[\prod_{1\le i\le N}\sum_{l=0}^{m_{RD}}\frac{m_{RD}{}^{m_{RD}}\Theta^l(\Theta-1)^{m_{RD}-l}\Gamma(l)}{\Gamma(m_{R_iP})\,l!\,(m_{RD}-l)!\lambda_{R_iE}{}^l}\times\left(\frac{\Upsilon\left(m_{R_iP},\frac{\lambda_{R_iP}\beta}{\alpha}\right)}{\alpha^{m_{RD}-l}}+\frac{\Gamma\left(m_{R_iP}+m_{RD}-l,\frac{\beta}{\alpha}\right)}{(\lambda_{R_iP}\beta)^{m_{RD}-l}}\right)\right]^{-\frac{1}{m_{RD}N}}. \tag{49}$$

B. The Suboptimal Relay Selection Scheme

Because the links between relays to D are i.i.d. distributed, each relay have the same probability to be selected to forward signal. Based on (29), P_{out}^∞ of SRS scheme can be expressed as

$$P_{out}^{\infty,\rm SRS} = \frac{1}{N}\sum_{i=1}^N\left(I_3^\infty+I_4^\infty\right). \tag{50}$$

Using eq. (44), when $\Omega_{RD}\to\infty$, the asymptotic CDF of $Y_{\rm SRS}$ can be given by

$$F_{Y_{\rm SRS}}^\infty(y) = \prod_{i=1}^N F_{Y_{R_iD}}^\infty(y) = \left(F_{Y_{RD}}^\infty(y)\right)^N = \left(\frac{\lambda_{RD}{}^{m_{RD}}}{m_{RD}!}\right)^N y^{m_{RD}N}. \tag{51}$$

Substituting (1) and (51) into (50), and making use of eq. (3.326.2) of [44], we have

$$I_3^\infty = F_{Y_{R_iP}}\left(\frac{\beta}{\alpha}\right)\int_0^\infty F_{Y_{\rm SRS}}^\infty\left(\Theta y+\frac{(\Theta-1)}{\alpha}\right)f_{Y_{R_iE}}(y)\,dy = \frac{\Upsilon\left(m_{R_iP},\lambda_{R_iP}\frac{\beta}{\alpha}\right)}{\Gamma(m_{R_iP})}\sum_{l=0}^{m_{R_iD}N}\Xi_5\alpha^{l-m_{RD}N}, \tag{52}$$

where $\Xi_5=\frac{\lambda_{RD}{}^{m_{RD}N}C_{m_{RD}N}^l\Theta^l(\Theta-1)^{m_{RD}N-l}\Gamma\left(m_{R_iE}+l\right)}{\lambda_{R_iE}{}^{-m_{R_iE}}(m_{RD}!)^N\Gamma\left(m_{R_iE}\right)\lambda_{R_iE}{}^{m_{R_iE}+l}}$.

Making use of eqs. (1) and (51), and utilizing eq. (3.326.2) of [44], we obtain

$$H_2^\infty(x) = \int_0^\infty F_{Y_{SRS}}^\infty\left(\Theta y+\frac{(\Theta-1)x}{\beta}\right)f_{Y_{R_iE}}(y)\,dy = \sum_{l=0}^{m_{RD}N}\Xi_5\beta^{l-m_{RD}N}x^{m_{RD}N-l}. \tag{53}$$

Substituting (53) into (33) and using eq. (3.351.2) of [44], we get

$$I_4^\infty = \int_{\frac{\beta}{\alpha}}^\infty H_2^\infty(x)f_{Y_{R_iP}}(x)\,dx = \sum_{l=0}^{m_{RD}N}\frac{\Xi_5\Gamma\left(m_{R_iP}+m_{RD}N-l,\frac{\alpha}{\beta}\lambda_{R_iP}\right)}{\Gamma(m_{R_iP})\,\beta^{m_{RD}N-l}\lambda_{R_iP}{}^{m_{RD}N-l}}. \tag{54}$$

Finally, $P_{\Phi_n}^\infty$ with the SRS scheme is obtained by substituting (52) and (54) into (50).

Henceforth, based on (41) G_d and G_a for the SRS scheme are obtained as

$$G_d^{\rm SRS} = m_{RD}N, \tag{55}$$

$$G_a^{\rm SRS} = \left[\sum_{i=1}^N\sum_{l=0}^{m_{R_iD}N}\frac{m_{RD}{}^{m_{RD}N}C_{m_{RD}N}^l\Theta^l\Gamma(l)}{(m_{RD}!)^N(\Theta-1)^{l-m_{RD}N}\lambda_{R_iE}{}^l}\times\frac{1}{N\Gamma(m_{R_iP})}\left(\frac{\Upsilon\left(m_{R_iP},\lambda_{R_iP}\frac{\beta}{\alpha}\right)}{\alpha^{m_{RD}N-l}}+\frac{\Gamma\left(m_{R_iP}+m_{RD}N-l,\frac{\alpha}{\beta}\lambda_{R_iP}\right)}{(\lambda_{R_iP}\beta)^{m_{RD}N-l}}\right)\right]^{-\frac{1}{m_{RD}N}}. \tag{56}$$

C. The Multiple Relay Combining Scheme

Based on (36), $P_{\Phi_n}^\infty$ of MRC scheme can be expressed as

$$P_{out}^{\infty,\rm MRC} = I_5^\infty+I_6^\infty. \tag{57}$$

Based on [10], when $\Omega_{RD}\to\infty$, the CDF of Y_D can be written as (44)

$$F_{Y_D}^\infty(y) = \frac{1}{m_{RD}N!}(\lambda_{RD}y)^{m_{RD}N}+\mathcal{O}\left(y^{m_{RD}N}\right). \tag{58}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCCN.2017.2758372, IEEE Transactions on Cognitive Communications and Networking

Substituting eqs. (18) and (58) into (36), and making use of eqs. (3.326.2) of [44], we achieve

$$\begin{aligned} I_5^{\infty} &= F_{Y_P}\left(\frac{N\beta}{\alpha}\right)\int_0^{\infty} F_{Y_D}^{\infty}\left(\Theta y+\frac{(\Theta-1)}{\alpha}\right) f_{Y_E}(y)\,dy \\ &= \frac{\Upsilon\left(m_{RP}N, \frac{\lambda_{RP}N\beta}{\alpha}\right)}{\Gamma(m_{RP}N)}\sum_{l=0}^{m_{RD}N}\Xi_6\left(\frac{\alpha}{N}\right)^{l-m_{RD}N}, \end{aligned} \tag{59}$$

where $\Xi_6 = \frac{{\lambda_{RD}}^{m_{RD}N}{\lambda_{RE}}^{m_{RE}N}C^l_{m_{RD}N}\Theta^l\Gamma(m_{RE}N+l)}{(\Theta-1)^{l-m_{RD}N}(Nm_{RD})!\Gamma(m_{RE}N){\lambda_{RE}}^{m_{RE}N+l}}$.

Making use of eqs. (18) and (58), and utilizing eq. (3.326.2) of [44], we obtain

$$\begin{aligned} H_3^{\infty} &= \int_0^{\infty} F_{Y_D}^{\infty}\left(\Theta y+\frac{(\Theta-1)x}{\beta}\right) f_{Y_E}(y)\,dy \\ &= \sum_{l=0}^{m_{RD}N}\Xi_6\beta^{l-m_{RD}N}x^{m_{RD}N-l}. \end{aligned} \tag{60}$$

Substituting (18) and (60) into (38) and using (3.351.2) of [44], we have

$$\begin{aligned} I_6^{\infty} &= \int_{\frac{N\beta}{\alpha}}^{\infty} H_3^{\infty}(x)\, f_{Y_P}(x)\,dx \\ &= \sum_{l=0}^{m_{RD}N}\frac{\Xi_6\Gamma\left(m_{RP}N+m_{RD}N-l, \frac{N\beta}{\alpha}\lambda_{RP}\right)}{\beta^{m_{RD}N-l}\Gamma(m_{RP}N)\,{\lambda_{RP}}^{m_{RD}N-l}}. \end{aligned} \tag{61}$$

Finally, $P_{\Phi_n}^{\infty}$ with the MRC scheme is obtained by substituting (59) and (61) into (57).

Henceforth, based on (41), G_d and G_a for the MRC scheme are obtained as

$$G_d^{\mathrm{MRC}} = m_{RD}N, \tag{62}$$

$$\begin{aligned} G_a^{\mathrm{MRC}} = \Bigg[\sum_{l=0}^{m_{RD}N} &\frac{{m_{RD}}^{m_{RD}N}(\Theta-1)^{m_{RD}N-l}\Gamma(l)}{l!\,(m_{RD}N-l)!\,\Theta^{-l}{\lambda_{RE}}^{l}} \\ &\times\frac{1}{\Gamma(m_{RP}N)}\left(\frac{\Upsilon\left(m_{RP}N, \frac{\lambda_{RP}N\beta}{\alpha}\right)}{\alpha^{m_{RD}N-l}N^{l-m_{RD}N}}\right. \\ &\left.+\frac{\Gamma\left(m_{RP}N+m_{RD}N-l, \frac{N\beta}{\alpha}\lambda_{RP}\right)}{(\lambda_{RP}\beta)^{m_{RD}N-l}}\right)\Bigg]^{-\frac{1}{m_{RD}N}}. \end{aligned} \tag{63}$$

Observing the expression of each G_d, we find that the three different schemes achieve the same secrecy diversity order that is determined by the number of the relays and the fading parameters of the links among the relays and D. Furthermore, one can also observe that the impact of the interference and wiretap channels is only reflected in the secrecy array gain.

V. Numerical Results

In this section, numerical and Monte-Carlo simulation results are given to verify the proposed analytical models. The main parameters used in analysis and simulation are set as $R_d = R_s = 0.1\mathrm{bit/s/Hz}$, $\sigma^2 = 1$. For simplicity, we define $m_{SR_i} = m_{SR}$, $m_{R_iP} = m_{RP}$, $m_{R_iD} = m_{RD}$, $m_{R_iE} = m_{RE}$, $\Omega_{SP} = \Omega_{R_iP} = \Omega_P$, $\Omega_{SR_i} = \Omega_{SR}$, $\Omega_{R_iD} = \Omega_{RD}$, $\Omega_{R_iE} = \Omega_{RE}$ as [18]-[21], and $1 \le i \le N$. We plot the curves for various parameters for comparison purposes with N, P_I, $P_{\max}$, or Ω_{RD} varying. As shown in Figs. 2-8, analysis results match very well with Monte Carlo simulation curves.

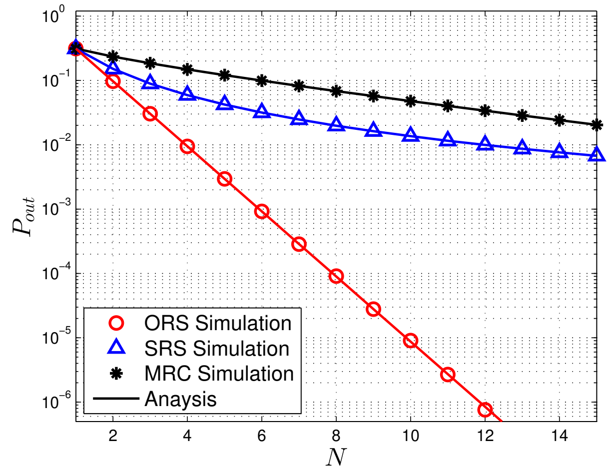

Fig. 2. SOP versus N with $m_{SP} = m_{RP} = m_{SR} = m_{RD} = m_{RE} = 2$, $\Omega_P = \Omega_{SR} = \Omega_{RD} = 2$, $\Omega_{RE} = 1$, and $P_I = P_{\max} = 10\,\mathrm{dBW}$.

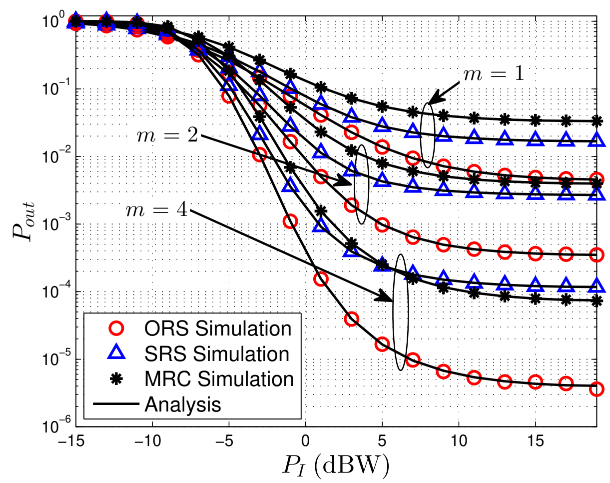

Fig. 3. SOP for ORS scheme versus P_I with $N = 3$, $m_{SP} = m_{SR} = m_{RP} = m_{RD} = m_{RE} = m$, $\Omega_P = \Omega_{SR} = \Omega_{RD} = 6$, $\Omega_{RE} = 1$, and $P_{\max} = 10\,\mathrm{dBW}$.

Fig. 2 shows the SOP with different schemes versus the number of relays. One can observe that the SOP decreases as the number of relays increases, which signifies that cooperative communications can improve the secrecy outage performance of the wireless transmissions in the presence of eavesdropping. Besides, the SOP of ORS decreases faster than the ones of SRS and MRC schemes, which means ORS is the most effective scheme with increasing N.

Figs. 3-6 plots the exact SOP with different schemes while interference power constraint P_I varies. With P_I increasing, the secrecy outage performance is enhanced, because a higher P_I implies a larger transmitting power at S and the relays. Furthermore, there exists a saturation for the SOP in the higher P_I region. It is because as $P_I \to \infty$, the transmitting power at S and the relays approach $P_{\max}$ leading the system to fall

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCCN.2017.2758372, IEEE Transactions on Cognitive Communications and Networking

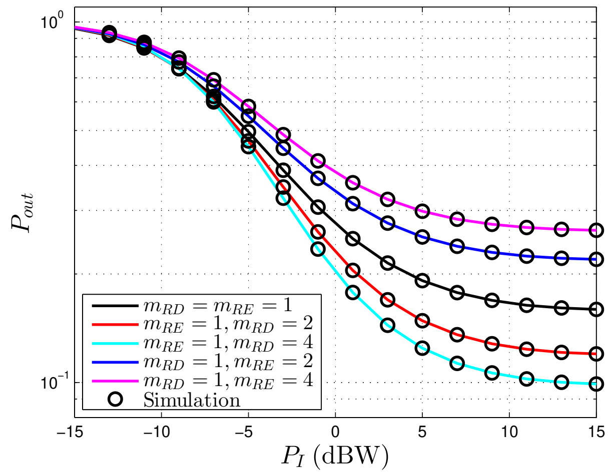

Fig. 4. SOP for ORS scheme versus P_I with $N = 3$, $m_{SP} = 1$, $\Omega_P = \Omega_{SR} = \Omega_{RD} = \Omega_{RE} = 2$, $m_{SP} = m_{SR} = m_{RP} = 1$, and $P_{\max} = 10\,\text{dBW}$.

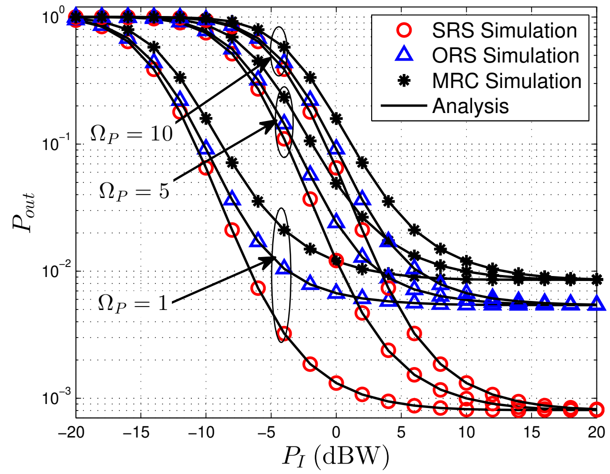

Fig. 6. SOP versus P_I with $N = 3$, $m_{SP} = m_{RP} = m_{SR} = m_{RD} = m_{RE} = 2$, $\Omega_{RE} = 1$, $\Omega_{SR} = \Omega_{RD} = 5$, and $P_{\max} = 10\,\text{dBW}$.

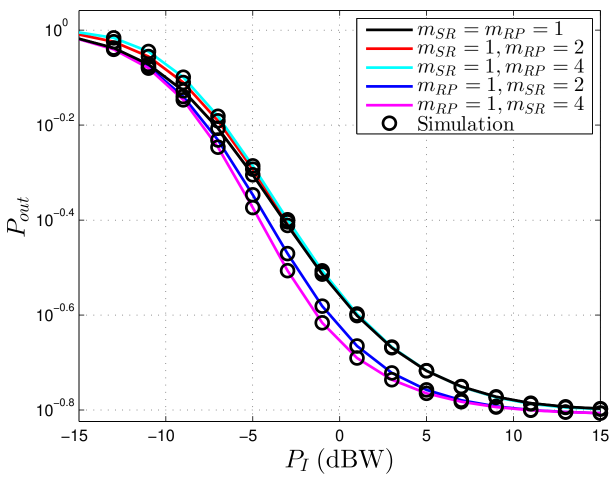

Fig. 5. SOP for ORS scheme versus P_I with $N = 3$, $m_{SP} = 1$, $\Omega_P = \Omega_{SR} = \Omega_{RD} = \Omega_{RE} = 2$, $m_{SP} = m_{RD} = m_{RE} = 1$, and $P_{\max} = 10\,\text{dBW}$.

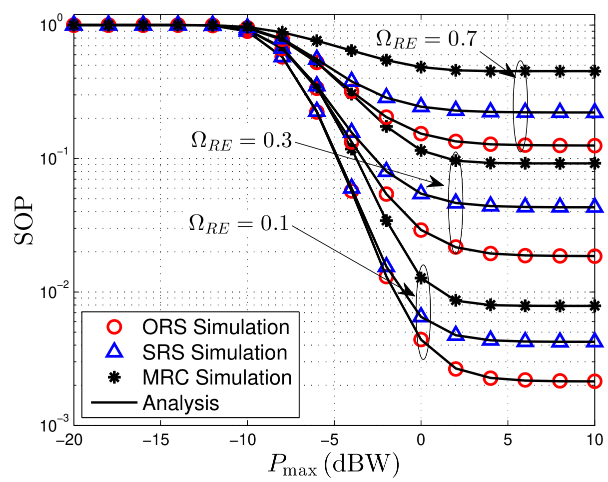

Fig. 7. SOP versus P_I with $N = 3$, $m_{SP} = m_{RP} = m_{SR} = m_{RD} = m_{RE} = 2$, $\Omega_P = \Omega_{SR} = \Omega_{RD} = 1$, and $P_I = 1\,\text{dBW}$

into a non-cognitive model wherein the interference power constraint from the PUs can be ignored. From the fig. 3, we can also observe that the ORS scheme always outperforms SRS and MRC schemes with different fading parameters. But SRS scheme performs better than MRC scheme only in the lower fading parameters scenario.

The impact of the fading parameters of the interference links, the transmission links, and the wiretap links on the secrecy outage performance is illustrated in figs. 4 and 5, respectively. For simplicity, we only consider ORS scheme as an example. It is observed that the fading parameters of the transmission links and wiretap links have great impact on the secrecy performance. The secrecy outage performance with a higher m_{RD} or lower m_{RE} outperforms the ones with a lower m_{RD} or higher m_{RE}. This is because a higher m_{RD} implies a stronger received SNR at D and a lower m_{RE} implies a weaker received SNR at E. Furthermore, higher m_{RD} means higher secrecy diversity order of the model, which can be proved by the conclusion of section IV. One can also observe from fig. 5 that the fading parameters of the interference links (m_{SP}) have little impact on the secrecy outage performance. This is in compliance with the results in [26]. Besides, secrecy outage performance for a higher m_{SR} outperforms the ones for a lower m_{SR} since the received SNR at the relays are enhanced and the number of successfully decoded relays increases.

Fig. 6 shows the SOP versus P_I with Ω_P varying. One can find that the SOP with a smaller Ω_P outperforms the one with a larger Ω_P scenario since transmit power at S and relays increase as Ω_P decreases. It is also observed that in the high P_I range ($P_I \to \infty$), different Ω_P of the same scheme achive the same secrecy outage performance, this is because the transmit power at S and relays is $P_{\max}$.

Fig. 7 illustrates the impact of the average channel power gains Ω_{RE} on the secrecy outage performance with $P_{\max}$ varying. We can see that with $P_{\max}$ increasing, the secrecy

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCCN.2017.2758372, IEEE Transactions on Cognitive Communications and Networking

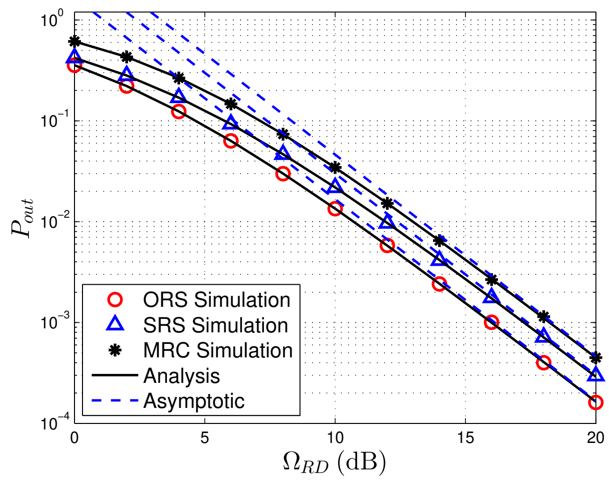

Fig. 8. The exact and asymptotic SOP versus Ω_{RD} with $N = 2$, $m_{SP} = m_{RP} = m_{SR} = m_{RD} = m_{RE} = 1$, $\Omega_{SR} = 10^5$, $\Omega_P = \Omega_{RE} = 1$, $P_{max} = 1\,\text{dBW}$, and $P_I = 2\,\text{dBW}$.

outage performance is enhanced, and there exists a floor in the higher $P_{\max}$ region. this is because there exists a ceiling for secrecy capacity in the high transmit power region, which is testified in [47]. Besides, the SOP for a lower Ω_{RE} is less than the one for a higher Ω_{RE}, since decreasing Ω_{RE} implies that the eavesdropper channel condition is getting weaker.

Fig. 8 presents the exact and asymptotic SOP versus Ω_{RD} for three different relay selection schemes according to Sections III and IV. One can observe that the asymptotic curves tightly approximate the exact curves with Ω_{RD} increasing and the slope of each asymptotic SOP curve is the same. It means that our asymptotic results accurately predict the secrecy diversity order and can be utilized to effectively evaluate the secrecy outage performance of this model in the high SNR regime. The secrecy diversity order of each scheme is $m_{RD}N$, which is consistent with the slope of the asymptotic curves in this figure.

VI. Conclusion

In this paper, we analyzed the security outage performance for an underlay cognitive DF relay network with three different relay selection schemes over i.n.i.d. Nakagami-m fading channels. The exact and asymptotic closed-form expressions for the SOP were derived and validated by simulations. Numerical results illustrated that with the number of relays increasing, the security outage performance of underlay CRNs transmissions can be improved. Besides, the ORS scheme is always the best scheme when the global CSI of all the links are available. According to the expressions for each G_d, we concluded that each scheme achieves the same secrecy diversity order of $m_{RD}N$, and the impact of the interference and wiretap channels is only reflected in the secrecy array gain. The model will be beneficial for designing practical cognitive relay systems, especially when the PLS issues and cooperative communications are considered.

Appendix A

Making use of (13), the CDF of Y_{SRS} is written as

$$\begin{aligned} F_{Y_{\text{SRS}}}(y) &= \Pr\left(\max_{i\in\Phi_n} Y_{R_iD} \le y\right) \\ &= \prod_{i\in\Phi_n} F_{Y_{R_iD}}(y) \\ &= \prod_{i=1}^{|\Phi_n|} (1 - x_i), \end{aligned} \tag{64}$$

where $x_i = \exp(-\lambda_{R_iD} y) \sum\limits_{l_i=0}^{m_{R_iD}-1} \frac{(\lambda_{R_iD} y)^{l_i}}{l_i!}$.

The product term in (64) can be described in a more tractable form with the help of the identity product [25] given by

$$\begin{aligned} &\prod_{i=1}^{|\Phi_n|} (1 - x_i) \\ &= \sum_{i=0}^{|\Phi_n|} (-1)^i \sum_{n_1=1}^{|\Phi_n|} \cdots \sum_{n_i=1}^{|\Phi_n|} \prod_{t=1}^{i} x_{n_t}, (n_1 \ne \cdots \ne n_i). \end{aligned} \tag{65}$$

The product of $x_{n_1} \cdots x_{n_i}$ can be described by

$$\prod_{t=1}^{i} x_{n_t} = \exp(-By) \sum_{l_1=0}^{m_{R_{n_1}D}-1} \cdots \sum_{l_i=0}^{m_{R_{n_i}D}-1} Ay^M, \tag{66}$$

where $A = \prod\limits_{t=1}^{i} \frac{\lambda_{n_t}{}^{l_t}}{l_t!}$, $B = \sum_{t=1}^{i} \lambda_{R_{n_t}D}$, and $M = \sum_{t=1}^{i} l_t$.

By substituting (65) and (66) into (64) the CDF of Y_{SRS} is obtained as

$$F_{Y_{\text{SRS}}}(y) = \sum_{\text{SRS}} (-1)^i A \exp(-By)\, y^M, \tag{67}$$

where $\sum\limits_{\text{SRS}} (-1)^i = \sum\limits_{i=0}^{|\Phi_n|} \sum\limits_{n_1=1}^{|\Phi_n|} \cdots \sum\limits_{n_i=1}^{|\Phi_n|} \sum\limits_{l_1=0}^{m_{R_{n_1}D}-1} \cdots \times \sum\limits_{l_i=0}^{m_{R_{n_i}D}-1} (-1)^i, (n_1 \ne \cdots \ne n_i)$.

Appendix B

Based on (7) and (9), the expression of $\Pr(\Phi = \Phi_n)$ can be written as

$$\begin{aligned} &\Pr(\Phi = \Phi_n) = \Pr(\Phi = \Phi_n, P_S = P_{\max}) \\ &+ \Pr(\Phi = \Phi_n, P_S = P_I / Y_{SP}) \\ &= \underbrace{F_{Y_{SP}}\left(\frac{\beta}{\alpha}\right) Z_1\left(\frac{\theta-1}{\alpha}\right) Z_2\left(\frac{\theta-1}{\alpha}\right)}_{J_1} \\ &+ \underbrace{\int_{\frac{\beta}{\alpha}}^{\infty} Z_1\left(\frac{(\theta-1)x}{\beta}\right) Z_2\left(\frac{(\theta-1)x}{\beta}\right) f_{Y_{SP}}(x)\, dx}_{J_2}, \end{aligned} \tag{68}$$

where $\alpha = P_{\max}/\sigma^2$, $\beta = P_I/\sigma^2$, $Z_1(y) = \prod\limits_{i\in\Phi_n} (1 - F_{Y_{SR_i}}(y))$, and $Z_2(y) = \prod\limits_{j\in\bar{\Phi}_n} \left(F_{Y_{SR_j}}(y)\right)$.

Substituting (3) into J_1, we have

$$J_1 = \frac{\Upsilon\left(m_{SP}, \lambda_{SP}\frac{\beta}{\alpha}\right)}{\Gamma(m_{SP})} \prod_{i\in\Phi_n}\left(1 - \frac{\Upsilon\left(m_{SR_i}, \lambda_{SR_i}\left(\frac{\theta-1}{\alpha}\right)\right)}{\Gamma(m_{SR_i})}\right) \times \prod_{j\in\bar{\Phi}_n}\left(1 - \frac{\Upsilon\left(m_{SR_j}, \lambda_{SR_j}\left(\frac{\theta-1}{\alpha}\right)\right)}{\Gamma(m_{SR_j})}\right). \quad (69)$$

Substituting (3) into $Z_1(y)$, $Z_1(y)$ can be written as

$$Z_1(y) = \prod_{i\in\Phi_n}\left(1 - F_{Y_{SR_i}}(y)\right) = \sum_{SRS_1} A_1 \exp(-B_1 y)\, y^{M_1}, \quad (70)$$

where $\sum\limits_{SRS_1} A_1 = \sum\limits_{l_1=0}^{m_{SR_1}-1}\cdots\sum\limits_{l_{|\Phi_n|}=0}^{m_{SR_{|\Phi_n|}}-1}\prod\limits_{t=1}^{|\Phi_n|}\frac{(\lambda_{SR_t}y)^{l_t}}{l_t!}$, $B_1 = \sum\limits_{t=1}^{|\Phi_n|}\lambda_{SR_t}$, and $M_1 = \sum\limits_{t=1}^{|\Phi_n|} l_t$.

Substituting (3) into $Z_2(y)$ and using the conclusion of appendix A, $Z_2(y)$ can be written as

$$Z_2(y) = \prod_{j\in\bar{\Phi}_n}\left(F_{Y_{SR_j}}(y)\right) = \sum_{SRS_2}(-1)^i A_2 \exp(-B_2 y)\, y^{M_2}, \quad (71)$$

where $\sum\limits_{SRS_2}(-1)^i = \sum\limits_{i=0}^{|\bar{\Phi}_n|}\sum\limits_{n_1=1}^{|\bar{\Phi}_n|}\cdots\sum\limits_{n_i=1}^{|\bar{\Phi}_n|}\sum\limits_{l_1=0}^{m_{R_{n_1}D}-1}\cdots \times \sum\limits_{l_i=0}^{m_{R_{n_i}D}-1}(-1)^i, (n_1 \neq \cdots \neq n_i)$, $A_2 = \prod\limits_{t=1}^{i}\frac{{\lambda_{n_t}}^{l_t}}{l_t!}$, $B_2 = \sum_{t=1}^{i}\lambda_{R_{n_t}D}$, and $M_2 = \sum_{t=1}^{i} l_t$.

Substituting (1), (70), and (71) into (68), and using (3.351.2) of [44], we obtain

$$J_2 = \frac{{\lambda_{SP}}^{m_{SP}}}{\Gamma(m_{SP})}\sum_{SRS_1}\sum_{SRS_2}(-1)^i A_1 A_2\left(\frac{(\theta-1)}{\beta}\right)^{M_1+M_2} \times \frac{\Gamma\left(M_1+M_2+m_{SP}, \frac{\beta}{\alpha}\left(\frac{(B_1+B_2)(\theta-1)}{\beta}+\lambda_{SP}\right)\right)}{\left(\frac{(B_1+B_2)(\theta-1)}{\beta}+\lambda_{SP}\right)^{M_1+M_2+m_{SP}}}, \quad (72)$$

where $\Gamma(a,x) = \int_x^\infty \exp(-t)\, t^{a-1}dt$ is the upper incomplete gamma function, as defined by (8.350.2) of [44]. Substituting (69) and (72) into (68) we obtain the expression of $\Pr(\Phi = \Phi_n)$ as shown in (22).

Appendix C

Utilizing [20], the probability of $b = i$ is written as

$$\Pr(b=i) = \Pr\left(\max_{k\in\Phi_n - i} Y_{R_kD} \leq Y_{R_iD}\right) = \int_0^\infty f_{Y_{R_iD}}(y)\prod_{k\in\Phi_n - i}F_{Y_{R_kD}}(y)dy. \quad (73)$$

Using the conclusion of appendix A, we have

$$\prod_{k\in\Phi_n - i}F_{Y_{R_kD}}(y) = \sum_{SRS_3}(-1)^k A_3 \exp(-B_3 y)\, y^{M_3}, \quad (74)$$

where $\sum\limits_{SRS_3}(-1)^k = \sum\limits_{k=0}^{|\Phi_n|-1}\sum\limits_{n_1=1}^{|\Phi_n|-1}\cdots\sum\limits_{n_k=1}^{|\Phi_n|-1}\sum\limits_{l_1=0}^{m_{R_{n_1}D}-1}\cdots \times \sum\limits_{l_k=0}^{m_{R_{n_k}D}-1}(-1)^k\ (n_1 \neq \cdots \neq n_k)$, $A_3 = \prod\limits_{t=1}^{k}\frac{{\lambda_{n_t}}^{l_t}}{l_t!}$, $B_3 = \sum_{t=1}^{k}\lambda_{R_{n_t}D}$, and $M_3 = \sum_{t=1}^{k} l_t$.

By substituting (1) and (74) into (73) the probability of $b = i$ can be determined as (30).

References

[1] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa,“Breaking spectrum gridlock with cognitive radios: an information theoretic perspective,” *Proc. IEEE*, vol. 97, no. 5, pp. 894-914, May 2009.

[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, Jun. 2008.

[3] A. D. Wyner, “The wire-tap channel,” *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[4] Z. Shu, Y. Qian, and S. Ci, “On physical layer security for cognitive radio networks,” *IEEE Netw.*, vol. 27, no. 3, pp. 28-33, Jun. 2013.

[5] Y. Zou, J. Zhu, L. Yang, Y.-C. Liang, and Y.-D. Yao, “Securing physical-layer communications for cognitive radio networks,” *IEEE. Commun. Mag.*, vol. 53, no. 9, pp. 48-54, Sept. 2015.

[6] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, “Secure communication over MISO cognitive radio channels,” *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494-1502, Apr. 2010.

[7] C. Wang and H.-M. Wang, “On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels,” *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1814-1827, Nov. 2014.

[8] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, “On the security of cognitive radio networks,” *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3790-3795, Aug. 2015.

[9] H. Lei, H. Zhang, I. S. Ansari, C. Gao, Y. Guo, G. Pan, and K. Qaraqe, “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, Dec. 2016.

[10] H. Lei, C. Gao, I. S. Ansari, Y. Guo, Y. Zou, G. Pan, and K. Qaraqe, “Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-m channels,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2237-2250, Mar. 2017.

[11] L. Fan, S. Zhang, T. Q. Duong, and G. K. Karagiannidis, “Secure switch-and-stay combining (SSSC) for cognitive relay networks,” *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 70-82, Jan. 2016.

[12] T. Zhang, Y. Cai, Y. Huang, T. Q. Duong, and W. Yang, “Secure full-duplex spectrum-sharing wiretap networks with different antenna reception schemes,” *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 335-346, Jan. 2017.

[13] H. Lei, M. Xu, I. S. Ansari, G. Pan, K. A. Qaraqe, and M.-S. Alouini, “On secrecy performance of underlay MIMO CRNS with energy harvesting and transmit antenna selection,” *IEEE Trans. Green Commun. Netw.*, vol. 1, no. 2, pp. 192-203, Jun. 2017.

[14] 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, Dec. 2015.

[15] M. Yuksel and E. Erkip, “Secure communication with a relay helping the wire-tapper,” in *Proc. IEEE ITW*, Tahoe City, Sep. 2007, pp. 595-600.

[16] T. X. Zheng, H. M. Wang, F. Liu, and M. H. Lee, “Outage constrained secrecy throughput maximization for DF relay networks,” *IEEE. Trans. Commun.,*, vol. 63, no. 5, pp. 1741-1755, May 2015.

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

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

[19] Y. Zou, X. Wang, and W. Shen, “Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack,” in *Proc. IEEE ICC2013*, Budapest, Jun. 2013, pp. 2183-2187.

[20] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE. Trans. Commun.*, vol. 63, no. 1, pp. 215-228, Jan. 2015.

[21] X. Zhang, Z. Yan, Y. Gao, and W. Wang, "On the study of outage performance for cognitive relay networks (CRN) with the Nth best-relay selection in Rayleigh-fading channels," *IEEE Wireless Commun. Lett.*, vol. 2, no. 1, pp. 110-113, Feb. 2013.

[22] N. P. Nguyen, C. Kundu, H. Q. Ngo, T. Q. Duong, and B. Canberk, "Secure full-duplex small-cell networks in a spectrum sharing environment," *IEEE Access*, vol. 4, pp. 3087-3099, Jun. 2016.

[23] Z. Kang, K. Yao, and F. Lorenzelli, "Nakagami-m fading modeling in the frequency domain for OFDM system analysis," *IEEE Commun. Lett.*, vol. 7, no. 10, pp. 484-486, Oct. 2003.

[24] T. Q. Duong, D. B. da Costa, M. Elkashlan, and B. Vo Nguyen Quoc, "Cognitive amplify-and-forward relay networks over Nakagami-m fading," *IEEE Trans. Veh. Technol.*, vol. 61, no. 5, pp. 2368-2374, Jun. 2012.

[25] T. Q. Duong, B. Vo Nguyen Quoc, and H. Zepernick, "On the performance of selection decode-and-forward relay networks over Nakagami-m fading channels," *IEEE Commun. Lett.*, vol. 13, no. 3, pp. 172-174, Mar. 2009.

[26] 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.

[27] B. Dai and Z. Ma, "Multiple-access relay wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1835-1849, Sept. 2015.

[28] L. Fan, X. Lei, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Secure multiuser communications in multiple amplify-and-forward relay networks," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3299-3310, Sept. 2014.

[29] B. V. Nguyen and K. Kim, "Secrecy outage probability of optimal relay selection for secure AnF cooperative networks," *IEEE Commun. Lett.*, vol. 19, no. 12, pp. 2086-2089, Dec. 2015.

[30] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with cochannel interference," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1494-1505, Dec. 2016.

[31] L. Fan, R. Zhao, F. Gong, N. Yang, and George K. Karagiannidis, "Secure multiple amplify-and-forward relaying over correlated fading channels," *IEEE Trans. Commun.*, vol. PP, no. 99, pp. 1-10, Arp. 2017.

[32] N. T. Do and B. An, "Secure transmission using decode-and-forward protocol for underlay cognitive radio networks," in *2015 Seventh International Conference on Ubiquitous and Future Networks (ICUFN)*, Sapporo, Jul. 2015, pp. 914-918.

[33] M. Al-jamali, A. Al-nahari, and M. AlKhawlani, "Relay selection schemes for secure transmission in cognitive radio networks," *Wireless Networks*, https: //doi.org/10.1007/s11276-016-1378-9.

[34] D.-B. Ha, T. T. Vu, T. T. Duy, and V. N. Q. Bao, "Secure cognitive reactive decode-and-dorward relay networks: with and without eavesdropper," *Wireless Pers. Commun.*, vol. 85, no. 4, pp. 2619-2641, Jul. 2015.

[35] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Commun.*, vol. 4, no. 15, pp. 1787-1791, Oct. 2010.

[36] H. Hui, G. Li, and J. Liang, "Secure relay and Jammer selection for physical layer security," *IEEE Signal Process. Lett.*, vol. 22, no. 8, pp. 1147-1151, Aug. 2015.

[37] 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, Jul. 2016.

[38] Y. Zhou, G. Pan, T. Li, H. Liu, C. Tang, and Y. Chen, "Secrecy outage performance for partial relay selection schemes in cooperative systems," *IET Commun.*, vol. 9, no. 16, pp. 1980-1987, Nov. 2015.

[39] Y. Yuan, R. Zhao, H. Lin, and A. Liu, "Secrecy outage probability of cognitive decode-and-forward relay networks," in *Proc. IEEE ICC2016*, May 2016, pp. 260-265.

[40] R. Zhao, Y. Yuan, L. Fan, and Y. C. He, "Secrecy performance analysis of cognitive decode-and-forward relay networks in Nakagami-m fading channels," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 549-563, Feb. 2017.

[41] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Commun.*, vol. 6, no. 16, pp. 2676-2687, Nov. 2012.

[42] 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, Feb. 2015.

[43] P. Chakraborty and S. Prakriya, "Secrecy outage performance of a cooperative cognitive relay network," *IEEE Commun. Lett.*, vol. 21, no. 2, pp. 326-329, Feb. 2017.

[44] I. S. Gradshteyn and I. M. Ryzik, *Table of Integrals, Series, and Products*, 7th. San Diego, USA: Academic Press, 2007.

[45] 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, Jan. 2009.

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

[47] H. Lei, I. S. Ansari, G. Pan, B. Alomair, and M.-S. Alouini, "Secrecy capacity analysis over $\alpha-\mu$ fading channels," *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1445-1448, Jun. 2017.

Hongjiang Lei (M'17) received the B.S. degree in Mechanical and Electrical Engineering from Shenyang Institute of Aeronautical Engineering, Shenyang, China, in 1998, the M.S. 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. In May 2004, he joined the School of Communication and Information Engineering of Chongqing University of Posts and Telecommunications (CQUPT), Chongqing, China, where he is currently an Associate Professor. Since Nov. 2016, he is also with Computer, Electrical, and Mathematical Science and Engineering (CEMSE) Division, King Abdullah University of Science and Technology (KAUST), Saudi Arabia, where he is a postdoc research fellow supported by Chinese Scholarship Council (CSC). His research interest spans special topics in communications theory and signal processing, including physical layer security, and cognitive radio networks. He is a TPC Member of IEEE Globecom'17. He has also served as a reviewer for major international journals, e.g., IEEE TVT, IEEE TCOM, IEEE TWC, IEEE TIFS, IEEE CL, etc.

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.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCCN.2017.2758372, IEEE Transactions on Cognitive Communications and Networking

Imran Shafique Ansari (S'07-M'15) received the B.Sc. degree in Computer Engineering from King Fahd University of Petroleum and Minerals (KFUPM) in 2009 (with First Honors) and M.Sc. and PhD degrees 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 with 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.

Dr. Ansari has authored/co-authored 60+ journal and conference publications. He has co-organized the GRASNET'2016, 2017 workshops in conjunction with IEEE WCNC'2016, 2017. 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.

Zhi Ren received the B.S. degree in applied electronics from the Southwest Jiaotong University, Chengdu, China in 1993, and the M.S. and Ph.D. degrees in measuring and testing technology and communication and information systems from the University of Electronic Science and Technology of China in 2002 and 2005, respectively. From 2006 to 2008, he was a postdoctoral research associate in the Department of Electrical and Computer Engineering, Stevens Institute of Technology, NJ, USA. He is now a professor in the School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications of China. His research interests include wireless networks and communication protocols.

Gaofeng Pan (M'12) received his B.S. 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 Sept. 2009 to Sept. 2011 as a joint-trained PhD student under the supervision of Prof. Eylem Ekici. In May 2012, he joined the School of Electronic and Information Engineering, Southwest University, Chongqing, China, where he is currently an Associate Professor. Since Jan. 2016, he is also with School of Computing and Communications, Lancaster University, Lancaster, U.K., where he is a postdoc under the supervision of Prof. Zhiguo Ding. His research interest spans special topics in communications theory, signal processing and protocol design, including secure communications, CR communications and MAC protocols. He is a TPC Member of Globecom'16 WEHCH, Globecom'17 MWN/WEHCH and VTC'17 Spring HMWC. He has also served as a reviewer for major international journals, e.g., IEEE JSAC, IEEE TCOM, IEEE TWC, IEEE TSP, IEEE TVT, etc.

Khalid A. Qaraqe (S'00) 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. Dr Qaraqe joined the department of Electrical and Computer Engineering of Texas A&M University at Qatar, in July 2004, where he is now a professor.

Dr Qaraqe's research interests include communication theory and its application to design and performance, analysis of cellular systems and indoor communication systems. Particular interests are in mobile networks, broadband wireless access, cooperative networks, cognitive radio, diversity techniques and beyond 4G systems.

Mohamed-Slim Alouini was born in Tunis, Tunisia. He received the Ph.D. degree in Electrical Engineering from the California Institute of Technology (Caltech), Pasadena, CA, USA, in 1998. He served as a faculty member in the University of Minnesota, Minneapolis, MN, USA, then in the Texas A&M University at Qatar, Education City, Doha, Qatar before joining King Abdullah University of Science and Technology (KAUST), Thuwal, Makkah Province, Saudi Arabia as a Professor of Electrical Engineering in 2009. His current research interests include the modeling, design, and performance analysis of wireless communication systems.