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/TGCN.2017.2684827, IEEE Transactions on Green Communications and Networking

On Secure Underlay MIMO Cognitive Radio Networks with Energy Harvesting and Transmit Antenna Selection

Hongjiang Lei, *Member, IEEE,* Ming Xu, Imran Shafique Ansari, *Member, IEEE,* Gaofeng Pan, *Member, IEEE,* Khalid A. Qaraqe, *Senior Member, IEEE,* and Mohamed-Slim Alouini, *Fellow, IEEE*

***Abstract*—In this paper, we consider an underlay multiple-input-multiple-output (MIMO) cognitive radio network (CRN) including a pair of primary nodes, a couple of secondary nodes, and an eavesdropper, where the secondary transmitter is powered by the renewable energy harvested from the primary transmitter in order to improve both energy efficiency and spectral efficiency. Based on whether the channel state information (CSI) of wiretap links are available or not, the secrecy outage performance of the optimal antenna selection (OAS) scheme and suboptimal antenna selection (SAS) scheme for underlay MIMO CRN with energy harvesting are investigated and compared with traditional space-time transmission scheme. The closed-form expressions for exact and asymptotic secrecy outage probability are derived. Monte-Carlo simulations are conducted to testify the accuracy of the analytical results. The analysis illustrates that OAS scheme outperforms SAS scheme. Furthermore, the asymptotic result shows that no matter which scheme is considered, the OAS and SAS schemes can achieve the same secrecy diversity order.**

***Index Terms*—Multiple-input-multiple-output, cognitive radio networks, energy harvesting, secrecy outage performance, transmit antenna selection.**

I. Introduction

A. Background

Manuscript received.

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, and the Scientific and Technological Research Program of Chongqing Municipal Education Commission under Grant KJ1600413. 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)).

H. Lei and M. Xu are with Chongqing Key Lab of Mobile Communications Technology, Chongqing University of Posts and Communications, 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, Saudi Arabia (e-mail: leihj@cqupt.edu.cn; cquptxm@gmail.com).

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, Qatar (e-mail: {imran.ansari, khalid.qaraqe}@qatar.tamu.edu).

G. Pan is with Chongqing Key Laboratory of Nonlinear Circuits and Intelligent Information Processing, Southwest University, Chongqing, 400715, China (e-mail: gfpan@swu.edu.cn).

M.-S. Alouini is with the Computer, Electrical, and Mathematical Sciences and Engineering (CEMSE) Division, King Abdullah University of Science and Technology (KAUST), Thuwal 23955-6900, Saudi Arabia (e-mail: slim.alouini@kaust.edu.sa).

Energy harvesting (EH) technology is integrated into wireless communication as a powerful solution to the problem of limited network lifetime, which collects energy from natural resources (solar, wind, vibration, etc.) and synthesized resources (microwave power transfer) and transforms into electricity to power wireless equipments [1], [2]. In recent years, simultaneous wireless information and power transfer (SWIPT) has gained a great deal of attention from researchers, which transport both energy and information to destinations by utilizing the same emitted electromagnetic wave [3], [4]. Two practical receiver designs for SWIPT, time splitting (TS) and power splitting (PS) schemes, were proposed for practical SWIPT receiver designs to realize receiving the information and energy simultaneously in [5] and [6]. A dynamic gradient-aware hierarchical packet forwarding mechanism is designed in [7] to extend the SWIPT networks life. The outage and capacity performance of a wireless sensor networks with TS/PS schemes over Nakagami-m fading channels was investigated in [8].

Cognitive radio networks (CRNs) have been a research focus since they can effectively resolve the spectrum scarcity issue [9]. In CRNs, secondary users (SU) can make use of the wireless spectrum with primary users (PU) in underlay, overlay, and interweave modes [10]. The underlay mode is the most simple mode wherein PUs allow SUs to utilize the same wireless spectrum concurrently when the interference caused by SU is below a given threshold. Since SU is allowed to share the spectrum with PU, security issue in such networks becomes more complex [11], [12], [13]. The physical layer security technique can provide secure communication through time-variability of wireless channel without secret key [14]. It can greatly improve the security of wireless communication system both in theory and in practical engineering applications [15]. If the physical layer security technique is utilized in underlay cognitive systems with EH technique, it will ensure secure communications under the premise of saving energy and spectrum.

B. Related Works

Recently, many works have studied the performance for SWIPT. The outage probability for a cooperative system with an EH relay in [16]. The secrecy performance for a single-input multiple-output (SIMO) with an information receivers and multiple EH eavesdroppers was studied and 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/TGCN.2017.2684827, IEEE Transactions on Green Communications and Networking

outage probability (SOP) and average secrecy capacity (ASC) were derived in [17]. The SOP and ASC for a multiple-input single-output (MISO) system were derived when transmit antenna selection (TAS) scheme was utilized at base station and imperfect channel state information (CSI) is available in [18]. The authors of [19] studied the secrecy rate of a multiple-input multiple-output (MIMO) wiretap channel for SWIPT, in which the eavesdropper pretended to be an EH receiver, and designed the optimal transmit covariance matrix at the source node. The joint information and energy beamforming design to maximize the secret capacity to the information receivers is investigated and effeicient algorithms are proposed in [20]. The authors designed a resource allocation algorithm minimizing the total transmit power for secure MISO systems with EH receivers as a non-convex optimization problem in [21]. The robust transceiver design problem in underlay MIMO SWIPT CRNs was investigated and the alternative optimization scheme was utilized to optimize the transmit covariance matrix at the SU transmitter and the preprocessing matrix at the SU receiver in [22].

In CRNs, the secondary transmitter powered by the EH technology can improve both energy efficiency and spectral efficiency [23]. Thus the CRNs with EH technology has become a focus in recent years [24]-[30]. The idea of utilizing radio frequency (RF) signals from the primary transmitter to power the secondary devices was proposed firstly in [24]. Cognitive SWIPT relay system was investigated and a near optimal joint relay selection and a power allocation scheme was proposed in [25]. In order to maximize the secrecy performance and minimize the energy consumption, a relay selection scheme was proposed that considered both the best relay selection and dynamic power allocation in [26]. The secrecy performance of the primary system where the SUs are potential eavesdroppers was analyzed in [27]. The authors investigated the secrecy performance of the device-to-device transmission in cognitive cellular networks with an energy constrained transmitter and proposed three different wireless power transfer schemes in [28]. The secrecy outage performance of cognitive SWIPT was investigated where the EH receivers act as eavesdroppers in [29]. The secrecy performance of an underlay CRN is investigated in [30] when the interference level of the primary users is not available at SU.

TAS is a very flexible approach method to make full use of the advantages of MIMO system [31], [32], [33], [34]. Zhu J. *et al.* proposed optimal antenna selection (OAS) and suboptimal antenna selection (SAS) schemes depending on whether the channel state information (CSI) of the wiretap channels is available at the source or not in [35]. The secrecy performance of the OAS and SAS schemes in underlay CRNs MIMO system over Nakagami-m channels were investigated and compared with the space-time transmission (STT) scheme in [36]. A simple protocol was proposed to enhance security via TAS and the closed-form expression for SOP and successful transmission probability were derived in [37]. But the EH technology was not considered in these works.

C. Motivation and Contributions

To the best of the author's knowledge, no open literature addresses the secrecy performance for underlay cognitive MIMO systems with EH and TAS schemes. In this work, we consider that the cognitive transmitter is powered by the renewable energy harvested from the primary transmitter in order to improve both energy and spectral efficiencies. Compared with existing works, the main difficulties in our works are: 1) Both the proportional interference power constraint and the fixed interference power constraint must meet at the cognitive transmitter; 2) Furthermore, when the EH technology is utilized at transmitter, the maximal transmit power is not a constant any longer since the harvested energy is a function of EH efficiency, channel power gains between the primary user, and the cognitive transmitter. We analyzed the secrecy outage performance in such scenario and investigated the relationship between secrecy performance and all the systems parameters. The main contributions of our work are listed as follows:

- We study the secrecy outage performance of a MIMO underlay CRN consisting of a primary system and a cognitive system, and each network includes one source and one destination. There is an eavesdropper that attempts to decode the signal received from the secondary transmitter that has no power supply due to unfortunate reasons (for instance: exhausted battery) and relies on the energy harvests via RF signals received from the primary source to communicate with the primary destination.
- The exact and asymptotic closed-form expressions for the SOP with the OAS and SAS schemes are derived, and the accuracy of the analytical results is validated by Monte-Carlo simulations. Furthermore, the secrecy array gain and the secrecy diversity order of different schemes are obtained.
- Although the security performance of EH systems was analyzed in some references, such as [17], [19], and [29], the EH technology was utilized at receivers. Relative to these works, a more complex and practical CR scenario is considered in our work, wherein the transmitter of the secondary system is powered by the renewable energy harvested from the primary transmitter in order to improve both energy and spectral efficiencies, and multiple antennas are equipped with all the CR systems.

D. Structure

The rest of this paper is organized as follows. In Section II, the system model considered in our work is described. The exact and asymptotic secrecy performance are analyzed in Sections III and IV. Section V presents and discusses the numerical and Monte-Carlo simulation results. Finally, we conclude the paper in Section VI.

II. System Model

As shown in fig. 1, we consider an underlay cognitive network where an energy constrained secondary source (S) communicates with an energy sufficient secondary destination (D) utilizing the same spectrum licensed to the primary network, and there is an eavesdropper (E) near D. The primary

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/TGCN.2017.2684827, IEEE Transactions on Green Communications and Networking

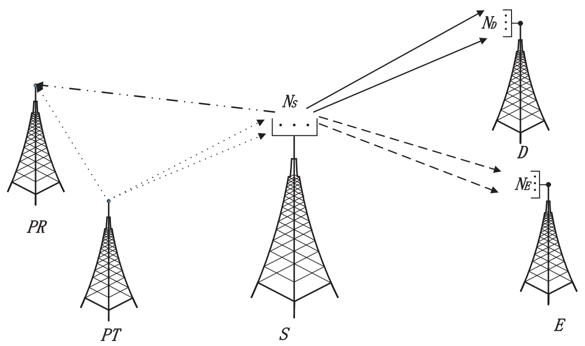

Fig. 1. System model demonstrating a primary transmitter (PT), a primary receiver (PR), a secondary transmitter (S), a secondary receiver (D), and an undesired eavesdropper (E).

network consists of a primary transmitter (PT) and a primary receiver (PR). All primary nodes are equipped with a single antenna and S, D, and E are equipped with $N_S \geq 1$, $N_D \geq 1$, and $N_E \geq 1$ antennas, respectively. S is equipped with a rechargeable EH battery that harvests the RF energy broadcasted from PT, and E can overhear the transmitting signal via wiretap channels when S communicates with D. The thermal noise at each receiver is modeled as additive white Gaussian noise (AWGN) with variance σ^2. It is assumed that all the channels experience independent and identically distributed (i.i.d.) Rayleigh fading with average channel power gains Ω_S, Ω_R, Ω_D, and Ω_E, respectively. Further, we assumed that maximal ratio combining (MRC) scheme is adopted at D and E

Two time phases are required to complete the transmission from S to D that include $\alpha\,(0 \leq \alpha \leq 1)$ portion for EH and $1-\alpha$ portion for information transmissions (IT) [38]. In EH phases, S harvests the energy from the RF signal received from PT by utilizing all antennas, and stores the harvested energy in an infinite capacity buffer[1]. The harvested energy at S can be written as

$$E_S = \eta \alpha P_t Y_S, \tag{1}$$

where $0 \leq \eta \leq 1$ denotes the EH efficiency [42], P_t denotes transmit power at PT, $Y_S = \sum_{i=1}^{N_S} |h_{PS_i}|^2$, and h_{PS_i} is the channel fading coefficients between PT and the ith antenna at S.

The probability density function (PDF) and cumulative distribution function (CDF) of Y_S is given as [43]

$$f_{Y_S}(y) = \frac{{\lambda_S}^{N_S}}{(N_S-1)!} y^{N_S-1} e^{-\lambda_S y}, \tag{2}$$

$$F_{Y_S}(y) = 1 - e^{-\lambda_S y} \sum_{k=0}^{N_S-1} \frac{1}{k!} (\lambda_S y)^k, \tag{3}$$

respectively, where $\lambda_S = \frac{1}{\Omega_S}$.

Based on eq. (1), the maximal transmit power at S can be written as

$$P_{\max} = \frac{E_S}{1-\alpha} = \frac{\eta \alpha P_t Y_S}{1-\alpha}. \tag{4}$$

In IT phases, only the optimal antenna at S is selected to send messages to D. According to the underlay spectrum sharing technique, the transmit power at S is strictly constrained by [36], [44]

$$P_S = \min\left(P_{\max}, \frac{P_I}{Y_R}\right), \tag{5}$$

where P_I is the maximum tolerated interference power at PR, $Y_R = |h_{S_b R}|^2$, $h_{S_b R}$ is the channel fading coefficient from the bth antenna at S to PR, and b denotes the selected antenna.

The PDF and CDF of Y_R can be presented as

$$f_{Y_R}(y) = \lambda_R e^{-\lambda_R y}, \tag{6}$$

$$F_{Y_R}(y) = 1 - e^{-\lambda_R y}, \tag{7}$$

respectively, where $\lambda_R = \frac{1}{\Omega_R}$.

The channel capacity between the ith antenna at S and the destination or the eavesdropper is

$$C_{S_i v} = \ln\left(1 + \frac{P_S}{\sigma^2} Y_{S_i v}\right), \tag{8}$$

respectively, where $v \in \{D, E\}$, $Y_{S_i v} = \sum_{j=1}^{N_v} \left|h_{S_i v_j}\right|^2$, $h_{S_i v_j}$ is the fading coefficients between the ith antenna at S and the jth antenna at v.

The PDF and CDF of $Y_{S_i v}$ can be expressed as [43]

$$f_{Y_{S_i v}}(y) = \frac{{\lambda_v}^{N_v}}{(N_v-1)!} y^{N_v-1} e^{-\lambda_v y}, \tag{9}$$

$$F_{Y_{S_i v}}(y) = 1 - e^{-\lambda_v y} \sum_{k=0}^{N_v-1} \frac{1}{k!} (\lambda_v y)^k, \tag{10}$$

respectively, where $\lambda_v = \frac{1}{\Omega_v}$.

A. The Optimal Antenna Selection Scheme

In the OAS scheme, in which the global CSI knowledge remains known[2], the antenna at S that maximizes the achievable secrecy rate of the secondary system is selected and used to transmit signals to D [35], [36]. Mathematically, the indices of the selected antenna with the OAS scheme is expressed as

$$b^{\text{OAS}} = \arg \max_{1 \leq i \leq N_S} C_i, \tag{11}$$

where C_i is the achievable secrecy rate via the ith antenna at S. Thus the instantaneous secrecy capacity of OAS scheme can be written as [36], [45]

$$\begin{aligned} C_S &= \max_{1 \leq i \leq N_S} C_i \\ &= \max_{1 \leq i \leq N_S} \left[C_{S_i D} - C_{S_i E}\right]^+, \end{aligned} \tag{12}$$

where $[x]^+ = \max(x, 0)$.

[1]To simplify the analysis, the infinity capacity EH buffer and the linear EH model are assumed at the CR transmitter. The non-linear EH model [39], [40], [41] and finite capacity EH buffer will be considered in our future works.

[2]In active eavesdropping scenarios, all the CSI are perfect and available at the transmitter; in passive eavesdropping scenarios, the source node has perfect CSI of the main channel and the distribution information of eavesdropping channel fading. These fundamental assumptions have well been adopted to study the physical layer security in various systems [45], [46], [47], [48].

B. The Suboptimal Antenna Selection Scheme

In the SAS scheme, in which the eavesdropper's CSI is unavailable (called passive eavesdropping scenario), the antenna at S that maximizes the achievable rate of S-D is selected as the best antenna [35], [36]. Mathematically, the indices of the selected antenna with the SAS scheme is expressed as

$$b^{\text{SAS}} = \arg\max_{1\le i\le N_S} C_{S_iD}. \tag{13}$$

The CDF of Y_{S_bD} is expressed as

$$\begin{aligned} F_{Y_{S_bD}}(x) &= \left[F_{Y_{S_iD}}(x)\right]^{N_S} \\ &= \sum_{SS} Ax^C e^{-Bx}, \end{aligned} \tag{14}$$

where $A = \frac{N_S!}{\prod_{i=1}^{N_D+1} n_i!}\prod_{p=1}^{N_D}\left(-\frac{\lambda_D{}^{p-1}}{(p-1)!}\right)^{n_p}$, $B = \lambda_D(N_S - n_{N_D+1})$, and $C = \sum_{p=1}^{N_D} n_p(p-1)$. SS denotes a set of N_D+1 tuples satisfying the condition: $SS = \left\{(n_1, n_2, \cdots, n_{N_D+1}) \middle| \sum_{i=1}^{N_D+1} n_i = N_S\right\}$, $n_i \in N$, where N refers to the set of natural numbers.

The instantaneous secrecy capacity of the SAS scheme can be written as [36]

$$C_S = \left[C_{S_bD} - C_{S_bE}\right]^+, \tag{15}$$

where $C_{S_bD} = \max_{1\le i\le N_S} C_{S_iD}$ and $C_{S_bE} = \ln\left(1 + \frac{P_S}{\sigma^2}Y_{S_bE}\right)$. It should be noted that selecting the best transmit antenna for D means selecting a random transmit antenna for E, and the PDF of Y_{S_bE} is the same as Y_{S_iE} [36], [49].

C. The Space-Time Transmission Scheme

To evaluate secrecy performance with TAS scheme, the traditional space-time transmission (STT) is considered in this subsection as a benchmark. In the STT scheme, all the antennas are utilized to transmit the signal encoded by space-time coding with power $\left(\frac{P_S}{N_S}\right)$ since the perfect CSI of the channels are known. Thus the channel capacity between S and the the destination or the eavesdropper is

$$C_{Sv}^{\text{STT}} = \ln\left(1 + \frac{P_S}{N_S\sigma^2}Y_{Sv}^{\text{STT}}\right), \tag{16}$$

respectively, where $Y_{Sv}^{\text{STT}} = \sum_{i=1}^{N_S}\sum_{j=1}^{N_k}\left|h_{S_iv_j}\right|^2$. Similar to (9) and (10), the PDF and CDF of Y_{Sv}^{STT} can be expressed as

$$f_{Y_{Sv}^{\text{STT}}}(y) = \frac{\lambda_v^{N_SN_v}}{(N_SN_v-1)!}y^{N_SN_v-1}e^{-\lambda_v y}, \tag{17}$$

$$F_{Y_{Sv}^{\text{STT}}}(y) = 1 - e^{-\lambda_v y}\sum_{k=0}^{N_SN_v-1}\frac{1}{k!}(\lambda_v y)^k. \tag{18}$$

The PDF and CDF of $Y_R^{\text{STT}} = \sum_{i=1}^{N_S}|h_{S_iR}|^2$ can be expressed as

$$f_{Y_R^{\text{STT}}}(y) = \frac{\lambda_R^{N_S}}{(N_S-1)!}y^{N_S-1}e^{-\lambda_R y}, \tag{19}$$

$$F_{Y_R^{\text{STT}}}(y) = 1 - e^{-\lambda_R y}\sum_{k=0}^{N_S-1}\frac{1}{k!}(\lambda_R y)^k. \tag{20}$$

The PDF and CDF of $Y_S^{\text{STT}} = \sum_{i=1}^{N_S}|h_{PS_i}|^2$ can be expressed as

$$f_{Y_S^{\text{STT}}}(y) = \frac{\lambda_S^{N_S}}{(N_S-1)!}y^{N_S-1}e^{-\lambda_S y}, \tag{21}$$

$$F_{Y_S^{\text{STT}}}(y) = 1 - e^{-\lambda_S y}\sum_{k=0}^{N_S-1}\frac{1}{k!}(\lambda_S y)^k. \tag{22}$$

III. Exact Secrecy Outage Probability Analysis

The SOP is defined the probability that the instantaneous secrecy capacity is less than a target secrecy rate and expressed as [36], [44], [45]

$$P_{out}(R_s) = \Pr\{C_s \le R_s\}, \tag{23}$$

where $R_s \ge 0$ is the target secrecy rate[3] and $C_s = C_D - C_E$, where C_D and C_E signify the capacity of the main and eavesdropper's channels, respectively. The operational significance of this definition of SOP can be explained as follow i.e. for a given constant R_s, the source node is assuming that the maximum rate of the eavesdropper's channel is given by $C_E^{'} = C_D - R_s$. If $C_E^{'} > C_E$, perfect secrecy can be achieved. In other words, perfect secrecy cannot be guaranteed by the wiretap codes utilized by the source node if $C_E^{'} < C_E$. In this following, the closed-form expression for the SOP with two different TAS schemes are derived and compared with the tradition STT scheme.

A. The Optimal Antenna Selection Scheme

The SOP of the OAS scheme can be expressed as

$$\begin{aligned} P_{out}^{\text{OAS}}(R_s) &= \Pr(C_S \le R_S) \\ &= \Pr\left(\max_{1\le i\le N_S}\left[C_{S_iD} - C_{S_iE}\right]^+ \le R_S\right) \\ &= \prod_{i=1}^{N_S}\Pr\left(C_{S_iD} - C_{S_iE} \le R_S\right) \\ &= \left(P_{out}(R_s)\right)^{N_S}, \end{aligned} \tag{24}$$

where $P_{out}(R_s) = \Pr\left(C_{S_iD} - C_{S_iE} \le R_S\right)$ signifies the SOP when S is equipped with a single antenna while D and E are equipped with $N_D \ge 1$ and $N_E \ge 1$ antennas, respectively [36]. Making use of eqs. (5) and (16), we obtain $P_{out}(R_s)$ by Eq. (25), as shown on the top of next page, where $\Theta = e^{R_S}$, $\varsigma = \frac{(\Theta-1)(1-\alpha)\sigma^2}{\eta\alpha P_t}$, $\xi = \frac{P_I(1-\alpha)}{\eta\alpha P_t}$, and $\omega = \frac{(\Theta-1)\sigma^2}{P_I}$.

Substituting eq. (4) into eq. (25), I_1 can be written as

$$I_1 = \int_0^\infty f_{Y_S}(x)F_{Y_R}\left(\frac{\xi}{x}\right)H_1(x)\,dx, \tag{26}$$

[3]Generally, the target secrecy rate R_s is chosen based on the specific application scenarios. A common method in choosing a suitable R_s is to maximize the secrecy throughput, which is expressed as $\eta(R_s) = (1 - P_{out}(R_s))R_s$. It should be noted that $P_{out}(R_s)$ will increase with increasing R_s. So there must be a R_s to maximize the secrecy throughput. Based on the results in this work, one can easily obtain the optimal R_s by solving a simple convex problem.

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/TGCN.2017.2684827, IEEE Transactions on Green Communications and Networking

$$\begin{aligned} P_{out}(R_s) &= \Pr\left(Y_{S_iD} \le \Theta Y_{S_iE} + \frac{(\Theta-1)\sigma^2}{P_S}, P_S = P_{\max}\right) + \Pr\left(Y_{S_iD} \le \Theta Y_{S_iE} + \frac{(\Theta-1)\sigma^2}{P_S}, P_S = \frac{P_I}{Y_R}\right) \\ &= \Pr\left(Y_{S_iD} \le \Theta Y_{S_iE} + \frac{(\Theta-1)\sigma^2}{P_{\max}}, Y_R \le \frac{P_I}{P_{\max}}\right) + \Pr\left(Y_{S_iD} \le \Theta Y_{S_iE} + \frac{(\Theta-1)Y_R\sigma^2}{P_I}, Y_R > \frac{P_I}{P_{\max}}\right) \\ &= \underbrace{\Pr\left(Y_{S_iD} \le \Theta Y_{S_iE} + \frac{\varsigma}{Y_S}, Y_R \le \frac{\xi}{Y_S}\right)}_{I_1} + \underbrace{\Pr\left(Y_{S_iD} \le \Theta Y_{S_iE} + \omega Y_R, Y_S > \frac{\xi}{Y_R}\right)}_{I_2}, \end{aligned} \tag{25}$$

where $H_1(x) = \int_0^\infty F_{Y_{S_iD}}\left(\Theta y + \frac{\varsigma}{x}\right) f_{Y_{S_iE}}(y)\,dy$.

Substituting eqs. (9) and (10) into $H_1(x)$, and using eq. (3.326.2) of [50], we obtain

$$\begin{aligned} H_1(x) &= 1 - \frac{{\lambda_E}^{N_E}}{(N_E-1)!} e^{-\frac{\lambda_D\varsigma}{x}} \sum_{k=0}^{N_D-1}\sum_{l=0}^{k}\left(\frac{\varsigma}{x}\right)^{k-l} \\ &\quad \times \frac{{\lambda_D}^k\Theta^l}{l!(k-l)} \int_0^\infty y^{N_E+l-1} e^{-(\lambda_E+\lambda_D\Theta)y}\,dy \\ &= 1 - e^{-\frac{\lambda_D\varsigma}{x}} \sum_{k=0}^{N_D-1}\sum_{l=0}^{k} \Xi_1 \left(\frac{\varsigma}{x}\right)^{k-l}, \end{aligned} \tag{27}$$

where $\Xi_1 = \frac{\Theta^l {\lambda_E}^{N_E} {\lambda_D}^k \Gamma(N_E+l)}{(N_E-1)! l! (k-l)! (\lambda_E+\lambda_D\Theta)^{N_E+l}}$ and $\Gamma(\cdot)$ is the Gamma function as defined by eq. (8.310.1) of [50].

Substituting eqs. (2), (7), and (27) into (26), and using eq. (3.471.9) of [50], we obtain

$$\begin{aligned} I_1 &= 1 - \frac{2{\lambda_S}^{N_S}}{(N_S-1)!}\left(\frac{\lambda_R\xi}{\lambda_S}\right)^{\frac{N_S}{2}} K_{N_S}\left(2\sqrt{\lambda_S\lambda_R\xi}\right) \\ &- \sum_{k=0}^{N_D-1}\sum_{l=0}^{k} \frac{2{\lambda_S}^{N_S}\varsigma^{k-l}\Xi_1}{(N_S-1)!}\left(\frac{\lambda_D\varsigma}{\lambda_S}\right)^{\frac{\upsilon_1}{2}} K_{\upsilon_1}\left(2\sqrt{\lambda_S\lambda_D\varsigma}\right) \\ &+ \sum_{k=0}^{N_D-1}\sum_{l=0}^{k} \frac{2{\lambda_S}^{N_S}\varsigma^{k-l}\Xi_1}{(N_S-1)!}\left(\frac{\lambda_D\varsigma+\lambda_R\xi}{\lambda_S}\right)^{\frac{\upsilon_1}{2}} \\ &\times K_{\upsilon_1}\left(2\sqrt{\lambda_S(\lambda_D\varsigma+\lambda_R\xi)}\right), \end{aligned} \tag{28}$$

where $\upsilon_1 = N_S + l - k$ and $K_{\upsilon_1}(x)$ is the modified Bessel function of order υ_1, as defined by eq. (8.407.1) of [50].

By substituting eq. (4) into eq. (25), I_2 is expressed as

$$I_2 = \int_0^\infty f_{Y_R}(x)\left(1 - F_{Y_S}\left(\frac{\xi}{x}\right)\right) H_2(x)\,dx, \tag{29}$$

where $H_2(x) = \int_0^\infty F_{Y_{S_iD}}(\Theta y + \omega x) f_{Y_{S_iE}}(y)\,dy$.

Substituting (9) and (10) into $H_2(x)$, and utilizing (3.326.2) of [50], we obtain

$$H_2(x) = 1 - \sum_{k=0}^{N_D-1}\sum_{l=0}^{k} \Xi_1 e^{-\lambda_D\omega x}(\omega x)^{k-l}. \tag{30}$$

By substituting eqs. (3), (6), and (30) into eq. (29), and utilizing eq. (3.471.9) of [50], we obtain

$$\begin{aligned} I_2 &= \sum_{t=0}^{N_S-1} \frac{2\lambda_R(\lambda_S\xi)^t}{t!}\left(\frac{\lambda_R}{\lambda_S\xi}\right)^{\frac{1-t}{2}} K_{1-t}\left(2\sqrt{\lambda_R\lambda_S\xi}\right) \\ &- \sum_{t=0}^{N_S-1}\sum_{k=0}^{N_D-1}\sum_{l=0}^{k} \frac{2\lambda_R\Xi_1(\lambda_S\xi)^t\omega^{k-l}}{t!}\left(\frac{\lambda_R+\lambda_D\omega}{\lambda_S\xi}\right)^{\frac{\upsilon_2}{2}} \\ &\times K_{\upsilon_2}\left(2\sqrt{(\lambda_R+\lambda_D\omega)\lambda_S\xi}\right), \end{aligned} \tag{31}$$

where $\upsilon_2 = k+t-l+1$. Then, P_{out} is obtained by substituting eqs. (28) and (31) into eq. (25). Finally, we obtain the SOP of the OAS scheme by substituting eq. (25) into eq. (24).

B. The Suboptimal Antenna Selection Scheme

Similar to (25), we can express the SOP of the SAS scheme by (32), as shown on the top of next page.

Substituting eq. (4) into eq. (32), we obtain J_1 as

$$J_1 = \int_0^\infty f_{Y_S}(x) F_{Y_R}\left(\frac{\xi}{x}\right) G_1(x)\,dx, \tag{33}$$

where $G_1(x) = \int_0^\infty F_{Y_{S_bD}}\left(\Theta y + \frac{\varsigma}{x}\right) f_{Y_{S_iE}}(y)\,dy$.

By substituting (9) and (14) into $G_1(x)$, we obtain

$$G_1(x) = \sum_{SS}\sum_{j=0}^{C} \Xi_2 e^{-\frac{B\varsigma}{x}}\left(\frac{\varsigma}{x}\right)^{C-j}, \tag{34}$$

where $\Xi_2 = \frac{C! A \Theta^j \lambda_E^{N_E}\Gamma(N_E+j)}{j!(C-j)!(N_E-1)!(B\Theta+\lambda_E)^{N_E+j}}$.

Substituting eqs. (2), (7), and (34) into eq. (33), and using eq. (3.471.9) of [50], we obtain

$$\begin{aligned} J_1 &= \sum_{SS}\sum_{j=0}^{C} \frac{\varsigma^{C-j}\Xi_2\lambda_S^{N_S}}{(N_S-1)!} \\ &\times \left(\Psi - 2\left(\frac{B\varsigma+\lambda_R\xi}{\lambda_S}\right)^{\frac{\upsilon_3}{2}} K_{\upsilon_3}\left(2\sqrt{\lambda_S(B\varsigma+\lambda_R\xi)}\right)\right), \end{aligned} \tag{35}$$

where $\upsilon_3 = N_S + j - C$ and $\Psi = \begin{cases} \frac{\Gamma(\upsilon_3)}{{\lambda_S}^{\upsilon_3}}, N_S = n_{N_D+1} \\ 2\left(\frac{B\varsigma}{\lambda_S}\right)^{\frac{\upsilon_3}{2}} K_{\upsilon_3}\left(2\sqrt{\lambda_S B\varsigma}\right), N_S \ne n_{N_D+1} \end{cases}$.

By substituting eq. (4) into eq. (32), we obtain J_2 as

$$J_2 = \int_0^\infty f_{Y_R}(x)\left(1 - F_{Y_S}\left(\frac{\xi}{x}\right)\right) G_2(x)\,dx, \tag{36}$$

where $G_2(x) = \int_0^\infty F_{Y_{S_bD}}(\Theta y + \omega x) f_{Y_{S_iE}}(y)\,dy$.

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/TGCN.2017.2684827, IEEE Transactions on Green Communications and Networking

$$\begin{aligned}P_{out}^{\mathrm{SAS}}(R_s) &= \Pr\left(Y_{S_bD} \le \Theta Y_{S_iE} + \frac{(\Theta-1)\sigma^2}{P_S}, P_S = P_{\max}\right) + \Pr\left(Y_{S_bD} \le \Theta Y_{S_iE} + \frac{(\Theta-1)\sigma^2}{P_S}, P_S = \frac{P_I}{Y_R}\right)\\ &= \underbrace{\Pr\left(Y_{S_bD} \le \Theta Y_{S_iE} + \frac{\varsigma}{Y_S}, Y_R \le \frac{\xi}{Y_S}\right)}_{J_1} + \underbrace{\Pr\left(Y_{S_bD} \le \Theta Y_{S_iE} + \omega Y_R, Y_S > \frac{\xi}{Y_R}\right)}_{J_2}\end{aligned} \tag{32}$$

Substituting eqs. (14) and (9) into $G_2(x)$, we obtain

$$G_2(x) = \sum_{SS}\sum_{j=0}^{C} \Xi_2 e^{-B\omega x}(\omega x)^{C-j}. \tag{37}$$

Substituting eqs. (2), (7), and (37) into eq. (36), we obtain

$$\begin{aligned}J_2 = &\sum_{SS}\sum_{j=0}^{C}\sum_{k=0}^{N_S-1}\frac{2\Xi_2\lambda_R\omega^{C-j}(\lambda_S\xi)^k}{k!}\\ &\times\left(\frac{\lambda_S\xi}{B\omega+\lambda_R}\right)^{\frac{\upsilon_4}{2}}K_{\upsilon_4}\left(2\sqrt{\lambda_S\xi(B\omega+\lambda_R)}\right),\end{aligned} \tag{38}$$

where $\upsilon_4 = C-k-j+1$.

Then, the SOP of SAS scheme is obtained by substituting (35) and (38) into eq. (32).

C. The Space-Time Transmission Scheme

Similar to (25) and (32), we express the SOP of the STT scheme by (39), as shown on the top of next page, where $\varsigma_0 = N_S\varsigma$ and $\omega_0 = N_S\omega$.

Substituting (4) into (39), we obtain the K_1 as

$$K_1 = \int_0^\infty f_{Y_S^{\mathrm{STT}}}(x)\, F_{Y_R^{\mathrm{STT}}}\left(\frac{\xi}{x}\right) T_1(x)\,dx, \tag{40}$$

where $\varsigma_0 = \frac{(\Theta-1)(1-\alpha)N_S\sigma^2}{\eta\alpha P_t}$, $\xi = \frac{P_I(1-\alpha)}{\eta\alpha P_t}$, and $T_1(x) = \int_0^\infty F_{Y_{SD}^{\mathrm{STT}}}\left(\Theta y + \frac{\varsigma_0}{x}\right) f_{Y_{SD}^{\mathrm{STT}}}(y)\,dy$. By substituting (16) and (17) into $T_1(x)$ and making use of (3.326.2) of [50], we obtain

$$\begin{aligned}T_1(x) &= 1 - \sum_{k=0}^{N_SN_D-1}\sum_{l=0}^{k}\frac{\Theta^l\lambda_E^{N_SN_E}\lambda_D{}^k}{(N_SN_E-1)!l!(k-l)!}\left(\frac{\varsigma_0}{x}\right)^{k-l}\\ &\quad\times e^{-\frac{\lambda_D\varsigma_0}{x}}\int_0^\infty e^{-\lambda_D\Theta y-\lambda_E y}y^{N_SN_E+l-1}dy\\ &= 1 - \sum_{k=0}^{N_SN_D-1}\sum_{l=0}^{k}\Xi_3 e^{-\frac{\lambda_D\varsigma_0}{x}}\left(\frac{\varsigma_0}{x}\right)^{k-l},\end{aligned} \tag{41}$$

where $\Xi_3 = \frac{\Theta^l\lambda_E^{N_SN_E}\lambda_D^k\Gamma(N_SN_E+l)}{(N_SN_E-1)!l!(k-l)!(\lambda_E+\lambda_D\Theta)^{N_SN_E+l}}$.

Substituting (19), (20), and (40) into (40), we obtain

$$\begin{aligned}K_1 = 1 &- \sum_{t=0}^{N_S-1}\frac{2\lambda_S^{N_S}(\lambda_R\xi)^t}{t!(N_S-1)!}\left(\frac{\lambda_R\xi}{\lambda_S}\right)^{\frac{N_S-t}{2}}K_{N_S-t}\left(2\sqrt{\lambda_S\lambda_R\xi}\right)\\ &- \sum_{k=0}^{N_SN_D-1}\sum_{l=0}^{k}\Xi_4\left(\frac{\lambda_D\varsigma_0}{\lambda_S}\right)^{\frac{N_S+l-k}{2}}K_{N_S+l-k}\left(2\sqrt{\lambda_S\lambda_D\varsigma_0}\right)\\ &+ \sum_{t=0}^{N_S-1}\sum_{k=0}^{N_SN_D-1}\sum_{l=0}^{k}\Xi_4\frac{(\lambda_R\xi)^t}{t!}\left(\frac{\lambda_R\xi+\lambda_D\varsigma_0}{\lambda_S}\right)^{\frac{N_S+l-k-t}{2}}\\ &\times K_{N_S+l-k-t}\left(2\sqrt{\lambda_S(\lambda_R\xi+\lambda_D\varsigma_0)}\right)\end{aligned} \tag{42}$$

where $\Xi_4 = \frac{2\Xi_3\lambda_S^{N_S}\varsigma_0{}^{k-l}}{(N_S-1)!}$.

Substituting (4) into (39), we obtain

$$K_2 = \int_0^\infty f_{Y_R^{\mathrm{STT}}}(x)\left(1 - F_{Y_S^{\mathrm{STT}}}\left(\frac{\xi}{x}\right)\right)T_2(x)\,dx, \tag{43}$$

where $T_2(x) = \int_0^\infty F_{Y_{SD}^{\mathrm{STT}}}(\Theta y + \omega_0 x)\, f_{Y_{SE}^{\mathrm{STT}}}(y)\,dy$.

Substituting eqs. (16) and (17) into $T_2(x)$, we obtain

$$T_2(x) = 1 - \sum_{k=0}^{N_SN_D-1}\sum_{l=0}^{k}\Xi_3 e^{-\lambda_D\omega_0 x}(\omega_0 x)^{k-l}. \tag{44}$$

Substituting eqs. (18), (21), and (44) into eq. (43), we obtain

$$\begin{aligned}K_2 = &\sum_{t=0}^{N_S-1}\frac{2\lambda_R^{N_S}(\lambda_S\xi)^t}{t!(N_S-1)!}\left(\frac{\lambda_S\xi}{\lambda_R}\right)^{\frac{N_S-t}{2}}K_{N_S-t}\left(2\sqrt{\lambda_S\lambda_R\xi}\right)\\ &- \sum_{t=0}^{N_S-1}\sum_{l=0}^{k}\sum_{k=0}^{N_SN_D-1}K_{N_S+k-l-t}\left(2\sqrt{\lambda_S\xi(\lambda_R+\lambda_D\omega_0)}\right)\\ &\times\frac{2\Xi_3\lambda_R^{N_S}\omega_0{}^{k-l}(\lambda_S\xi)^t}{t!(N_S-1)!}\left(\frac{\lambda_S\xi}{\lambda_R+\lambda_D\omega_0}\right)^{\frac{N_S+k-l-t}{2}}.\end{aligned} \tag{45}$$

Then, the SOP of STT scheme is obtained by substituting eqs. (42) and (45) into eq. (39).

IV. Asymptotic Secrecy Outage Probability Analysis

In this section, we investigate the system behavior in a special case that D is located quite closer to S with $\Omega_D \to \infty$. This assumption can help us obtain the closed-form expressions for asymptotic SOP, and analyze the secrecy diversity order and the secrecy array gain with different antenna selection schemes.

As defined in [49], the asymptotic SOP in the high SNR regime with $\Omega_D \to \infty$ is given as

$$P_{out}^{\infty} = (G_a\Omega_D)^{-G_d} + \mathcal{O}\left(\Omega_D{}^{-G_d}\right), \tag{46}$$

$$\begin{aligned} P_{out}^{\mathrm{STT}}(R_s) &= \Pr\left(Y_{SD}^{\mathrm{STT}} \le \Theta Y_{SE}^{\mathrm{STT}} + \frac{(\Theta-1)N_S\sigma^2}{P_S}, P_S = P_{\max}\right) + \Pr\left(Y_{SD}^{\mathrm{STT}} \le \Theta Y_{SE}^{\mathrm{STT}} + \frac{(\Theta-1)N_S\sigma^2}{P_S}, P_S = \frac{P_I}{Y_R^{\mathrm{STT}}}\right) \\ &= \underbrace{\Pr\left(Y_{SD}^{\mathrm{STT}} \le \Theta Y_{SE}^{\mathrm{STT}} + \frac{\varsigma_0}{Y_S}, Y_R^{\mathrm{STT}} \le \frac{\xi}{Y_S}\right)}_{K_1} + \underbrace{\Pr\left(Y_{SD}^{\mathrm{STT}} \le \Theta Y_{SE}^{\mathrm{STT}} + \omega_0 Y_R, Y_R^{\mathrm{STT}} > \frac{\xi}{Y_S}\right)}_{K_2} \end{aligned} \tag{39}$$

where G_a is the secrecy array gain, G_d is the secrecy diversity order, and $\mathcal{O}(\cdot)$ denotes higher order terms.

A. The Optimal Antenna Selection Scheme

Utilizing (24) and (25), P_{out}^{∞} of OAS scheme can be written as

$$P_{out}^{\mathrm{OAS},\infty} = \left(I_1^{\infty} + I_2^{\infty}\right)^{N_S}, \tag{47}$$

where I_1^{∞} and I_2^{∞} is the asymptotic expression of I_1 and I_2 with $\Omega_D \to \infty$, respectively.

According to lemma 2 of [36], the asymptotic CDF of Y_{S_iD} can be expressed as

$$\begin{aligned} F_{Y_{S_iD}}^{\infty}(y) &= 1 - e^{-\lambda_D y} \\ &\quad \times \left(e^{\lambda_D y} - \frac{(\lambda_D y)^{N_D}}{N_D!} + \mathcal{O}\left(y^{N_D}\right)\right) \\ &= \frac{(\lambda_D y)^{N_D}}{N_D!} + \mathcal{O}\left(y^{N_D}\right). \end{aligned} \tag{48}$$

Substituting (9) and (48) into (27) and utilizing (3.326.2) of [50], we obtain

$$\begin{aligned} H_1^{\infty}(x) &= \int_0^{\infty} F_{Y_{S_iD}}^{\infty}\left(\Theta y + \frac{\varsigma}{x}\right) f_{Y_{S_iE}}(y)\, dy \\ &= \sum_{k=0}^{N_D} \Xi_5 \lambda_D^{N_D} \left(\frac{\varsigma}{x}\right)^{N_D-k}, \end{aligned} \tag{49}$$

where $\Xi_5 = \frac{\Gamma(N_E+k)\Theta^k}{{\lambda_E}^k k!(N_D-k)!(N_E-1)!}$.

Substituting (2), (7), and (49) into (26), and utilizing (3.326.2) and (3.471.9) of [50], we have

$$\begin{aligned} I_1^{\infty} &= \int_0^{\infty} f_{Y_S}(x) F_{Y_R}\left(\frac{\xi}{x}\right) H_1^{\infty}(x)\, dx \\ &= \sum_{k=0}^{N_D} \Xi_6 \left(\Delta - 2\left(\frac{\lambda_R \xi}{\lambda_S}\right)^{\frac{\upsilon_5}{2}} K_{\upsilon_5}\left(2\sqrt{\lambda_S \lambda_R \xi}\right)\right), \end{aligned} \tag{50}$$

where $\Xi_6 = \frac{\Xi_5 \lambda_D^{N_D} {\lambda_S}^{N_S} \varsigma^{N_D-k}}{(N_S-1)!}$, $\upsilon_5 = N_S - N_D + k$, $\Delta = \begin{cases} \frac{\Gamma(\upsilon_5)}{{\lambda_S}^{\upsilon_5}}, \upsilon_5 > 0 \\ 1, \upsilon_5 = 0 \\ \frac{\Gamma(\upsilon_5, 0)}{{\lambda_S}^{\upsilon_5}}, \upsilon_5 < 0 \end{cases}$, and $\Gamma(\alpha, x) = \int_x^{\infty} e^{-t} t^{\alpha-1} dt$ is the upper incompletely Gamma function as defined by eq. (8.350.2) of [50].

Substituting (9) and (48) into (30) and utilizing (3.326.2) of [50], it deduces

$$\begin{aligned} H_2^{\infty}(x) &= \int_0^{\infty} F_{Y_{S_iD}}(\Theta y + \omega x) f_{Y_{S_iE}}(y)\, dy \\ &= \sum_{k=0}^{N_D} \Xi_5 \lambda_D^{N_D} (\omega x)^{N_D-k}. \end{aligned} \tag{51}$$

Substituting (2), (7), and (51) into (29), and utilizing (3.471.9) of [50], one can achieve

$$\begin{aligned} I_2^{\infty} &= \int_0^{\infty} f_{Y_S}(x) \left(1 - F_{Y_R}\left(\frac{\xi}{x}\right)\right) H_2^{\infty}(x)\, dx \\ &= \sum_{t=0}^{N_S-1} \sum_{k=0}^{N_D} \Xi_7 K_{\upsilon_6}\left(2\sqrt{\lambda_S \lambda_R \xi}\right). \end{aligned} \tag{52}$$

where $\Xi_7 = \frac{2\Xi_5 \lambda_D^{N_D} \omega^{N_D-k} {\lambda_R}^{1-\frac{\upsilon_6}{2}} (\lambda_S \xi)^{t+\frac{\upsilon_6}{2}}}{t!}$ and $\upsilon_6 = N_D + t - k + 1$. Then, P_{out}^{∞} of OAS scheme is obtained by substituting I_1^{∞} and I_2^{∞} into (47).

Making use of (46), we obtain $G_d^{\mathrm{OAS}} = N_D N_S$ and G_a by (53), as shown on the top of next page.

B. The Suboptimal Antenna Selection Scheme

Based on (32), the asymptotic SOP of SRS scheme can be written as

$$P_{out}^{\mathrm{SAS},\infty} = J_1^{\infty} + J_2^{\infty}, \tag{54}$$

where J_1^{∞} and J_2^{∞} is the asymptotic expression of J_1 and J_2 with $\Omega_D \to \infty$, respectively.

Based on (14), the asymptotic CDF of Y_{S_bD} can be written as

$$\begin{aligned} F_{Y_{S_bD}}^{\infty}(x) &= \left[F_{Y_{S_iD}}^{\infty}(x)\right]^{N_S} \\ &\approx \frac{(\lambda_D y)^{N_D N_S}}{(N_D!)^{N_S}}. \end{aligned} \tag{55}$$

Substituting (9) and (55) into $G_1(x)$, and utilizing (3.326.2) of [50], one can have

$$\begin{aligned} G_1^{\infty}(x) &= \int_0^{\infty} F_{Y_{S_bD}}^{\infty}\left(\Theta y + \frac{\varsigma}{x}\right) f_{Y_{S_iE}}(y)\, dy \\ &= \sum_{j=0}^{N_D N_S} \Xi_8 {\lambda_D}^{N_D N_S} \left(\frac{\varsigma}{x}\right)^{N_D N_S - r}, \end{aligned} \tag{56}$$

where $\Xi_8 = \frac{(N_D N_S)!\Gamma(N_E+j)\Theta^j}{j!(N_D N_S - j)!(N_D!)^{N_S} {\lambda_E}^r (N_E-1)!}$.

Substituting (2), (7), and (56) into eq. (33), and using eq.

$$G_a^{\mathrm{OAS}} = \left(\sum_{k=0}^{N_D}\left(\Xi_6\left(\Delta - 2\left(\frac{\lambda_R\xi}{\lambda_S}\right)^{\frac{\upsilon_5}{2}} K_{\upsilon_5}\left(2\sqrt{\lambda_S\lambda_R\xi}\right)\right) + \sum_{t=0}^{N_S-1}\Xi_7 K_{\upsilon_6}\left(2\sqrt{\lambda_S\lambda_R\xi}\right)\right)\right)^{-\frac{1}{N_D}} \quad (53)$$

(3.471.9) of [50], we obtain

$$\begin{aligned} J_1^\infty &= \int_0^\infty f_{Y_S}(x) F_{Y_R}\left(\frac{\xi}{x}\right) G_1^\infty(x)\,dx \\ &= \sum_{j=0}^{N_D N_S} \frac{\Xi_8 {\lambda_D}^{N_D N_S} {\lambda_S}^{N_S} \varsigma^{N_D N_S - j}}{(N_S-1)!} \\ &\times \left(\Lambda - 2\left(\frac{\lambda_R\xi}{\lambda_S}\right)^{\frac{\upsilon_7}{2}} K_{\upsilon_7}\left(2\sqrt{\lambda_R\lambda_S\xi}\right)\right), \end{aligned} \quad (57)$$

where $\upsilon_7 = N_S - N_S N_D + j$ and $\Lambda = \begin{cases} \frac{\Gamma(\upsilon_7)}{{\lambda_S}^{\upsilon_7}}, \upsilon_7 > 0 \\ 1, \upsilon_7 = 0 \\ \frac{\Gamma(\upsilon_7, 0)}{{\lambda_S}^{\upsilon_7}}, \upsilon_7 < 0 \end{cases}$.

Substituting (9) and (55) into $G_2(x)$, and utilizing (3.326.2) of [50], we can achieve

$$\begin{aligned} G_2^\infty(x) &= \int_0^\infty F_{Y_{S_bD}}^\infty(\Theta y + \omega x) f_{Y_{S_iE}}(y)\,dy \\ &= \sum_{j=0}^{N_D N_S} \Xi_8 {\lambda_D}^{N_D N_S} (\omega x)^{N_D N_S - j}. \end{aligned} \quad (58)$$

Substituting (2), (7), and (58) into eq. (36), and using eq. (3.471.9) of [50], it deduces

$$\begin{aligned} J_2^\infty &= \int_0^\infty f_{Y_R}(x)\left(1 - F_{Y_S}\left(\frac{\xi}{x}\right)\right) G_2^\infty(x)\,dx \\ &= \sum_{j=0}^{N_D N_S}\sum_{k=0}^{N_S-1} \frac{2\Xi_8 {\lambda_D}^{N_D N_S} \omega^{N_D N_S - j} (\lambda_S\xi)^{\frac{\upsilon_8}{2}}}{{\lambda_R}^{\frac{\upsilon_8}{2}} k!} \\ &\times K_{\upsilon_8}\left(2\sqrt{\lambda_R\lambda_S\xi}\right), \end{aligned} \quad (59)$$

where $\upsilon_8 = N_D N_S - j - k - 1$. Then, P_{out}^∞ of SAS scheme is obtained by substituting J_1^∞ and J_2^∞ into (54).

Based on (46), the expression for G_d and G_a of SAS scheme are obtained as

$$G_d^{\mathrm{SAS}} = N_D N_S, \quad (60)$$

$$\begin{aligned} G_a^{\mathrm{SAS}} = &\left(\sum_{j=0}^{N_D N_S} \frac{\Xi_8 {\lambda_S}^{N_S} \varsigma^{N_D N_S - j}}{(N_S-1)!}\right. \\ &\times \left(\Lambda - 2\left(\frac{\lambda_R\xi}{\lambda_S}\right)^{\frac{\upsilon_7}{2}} K_{\upsilon_7}\left(2\sqrt{\lambda_R\lambda_S\xi}\right)\right) \\ &+ \sum_{j=0}^{N_D N_S}\sum_{k=0}^{N_S-1} \frac{2\Xi_8 \omega^{N_D N_S - j} (\lambda_S\xi)^{\frac{\upsilon_8}{2}}}{{\lambda_R}^{\frac{\upsilon_8}{2}} k!} \\ &\left.\times K_{\upsilon_8}\left(2\sqrt{\lambda_R\lambda_S\xi}\right)\right)^{-\frac{1}{N_D N_S}}, \end{aligned} \quad (61)$$

respectively.

One can easily observe that the ORS and SRS schemes achieve the same secrecy diversity order which is determined by the number of antenna on S and D. Furthermore, one can observe that the impact of PT, PR, and E is only reflected in the secrecy array gain.

C. The Space-Time Transmission Scheme

Similarly, the asymptotic SOP of STT scheme can be written as

$$P_{out}^{\mathrm{STT},\infty} = K_1^\infty + K_2^\infty, \quad (62)$$

where K_1^∞ and K_2^∞ is the asymptotic expression of K_1 and K_2 with $\Omega_D \to \infty$, respectively.

The asymptotic CDF of Y_{SD}^{STT} can be expressed as

$$F_{Y_{SD}^{\mathrm{STT},\infty}}(y) = \frac{(\lambda_D y)^{N_S N_D}}{(N_S N_D)!} + \mathcal{O}\left(y^{N_S N_D}\right). \quad (63)$$

Substituting (16) and (63) into (41) and utilizing (3.326.2) of [50], we obtain

$$\begin{aligned} T_1^\infty(x) &= \int_0^\infty F_{Y_{SD}^{\mathrm{STT},\infty}}\left(\Theta y + \frac{\varsigma_0}{x}\right) f_{Y_{SE}^{\mathrm{STT}}}(y)\,dy \\ &= \sum_{k=0}^{N_S N_D} \Xi_9 \lambda_D^{N_S N_D}\left(\frac{\varsigma_0}{x}\right)^{N_S N_D - k}, \end{aligned} \quad (64)$$

where $\Xi_9 = \frac{\Theta^k \Gamma(N_S N_E + k)}{(N_S N_D - k)!(N_S N_E - 1)! k! \lambda_E^k}$.

Substituting (19), (20), and (64) into (40), and utilizing (3.326.2) and (3.471.9) of [50], we have

$$\begin{aligned} K_1^\infty &= \int_0^\infty f_{Y_S^{\mathrm{STT}}}(x) F_{Y_R^{\mathrm{STT}}}\left(\frac{\xi}{x}\right) T_1^\infty(x)\,dx \\ &= \sum_{k=0}^{N_S N_D} \frac{\Xi_9 \lambda_D^{N_S N_D} \lambda_S^{N_S} {\varsigma_0}^{N_S N_D - k}}{(N_S-1)!} \\ &\times \left(\Phi - \sum_{t=0}^{N_S-1} \frac{2(\lambda_R\xi)^t}{t!}\left(\frac{\lambda_R\xi}{\lambda_S}\right)^{\frac{\upsilon_9 - t}{2}} K_{\upsilon_9 - t}\left(2\sqrt{\lambda_S\lambda_R\xi}\right)\right), \end{aligned} \quad (65)$$

where $\upsilon_9 = N_S - N_S N_D + k$ and $\Phi = \begin{cases} \frac{\Gamma(\upsilon_9)}{\lambda_S^{N_S - N_S N_D + k}}, \upsilon_9 > 0 \\ 1, \quad \upsilon_9 = 0 \\ \frac{\Gamma(\upsilon_9, 0)}{\lambda_S^{N_S - N_S N_D + k}}, \upsilon_9 < 0 \end{cases}$.

Substituting (16) and (63) into (44), it deduces

$$\begin{aligned} T_2^\infty(x) &= \int_0^\infty F_{Y_{SD}^{\mathrm{STT},\infty}}(\Theta y + \omega_0 x) f_{Y_{SE}^{\mathrm{STT}}}(y)\,dy \\ &= \sum_{k=0}^{N_S N_D} \Xi_9 \lambda_D^{N_S N_D} (\omega_0 x)^{N_S N_D - k}. \end{aligned} \quad (66)$$

Substituting (18), (21), and (66) into (43), and utilizing

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/TGCN.2017.2684827, IEEE Transactions on Green Communications and Networking

(3.471.9) of [50], one can achieve

$$K_2^\infty = \int_0^\infty f_{Y_R^{\rm STT}}(x)\left(1 - F_{Y_S^{\rm STT}}\left(\frac{\xi}{x}\right)\right) T_2^\infty(x)\,dx$$
$$= \sum_{k=0}^{N_S N_D} \sum_{t=0}^{N_S-1} \frac{2\Xi_9 \lambda_D^{N_S N_D} \lambda_R^{N_S - \frac{v_{10}}{2}} {\omega_0}^{N_S N_D - k} (\lambda_S \xi)^{t+\frac{v_{10}}{2}}}{t!\,(N_S-1)!}$$
$$\times K_{v_{10}}\left(2\sqrt{\lambda_S \lambda_R \xi}\right), \tag{67}$$

where $v_{10} = N_S + N_S N_D - k - t$. Then, P_{out}^∞ of STT scheme is obtained by substituting K_1^∞ and K_2^∞ into (62).

Finally, we obtain the G_d and G_a of STT scheme as

$$G_d^{\rm STT} = N_D N_S, \tag{68}$$

$$G_a^{\rm STT} = \Bigg(\sum_{k=0}^{N_S N_D}\Bigg(\sum_{t=0}^{N_S-1} \frac{2\Xi_9 \lambda_R^{N_S-\frac{v_{10}}{2}} {\omega_0}^{N_S N_D - k} (\lambda_S \xi)^{t+\frac{v_{10}}{2}}}{t!\,(N_S-1)!}$$
$$\times K_{v_{10}}\left(2\sqrt{\lambda_S\lambda_R\xi}\right) + \frac{\Xi_9 \lambda_S^{N_S} {\varsigma_0}^{N_S N_D - k}}{(N_S-1)!}$$
$$\times \left(\Phi - \sum_{t=0}^{N_S-1} \frac{2(\lambda_R\xi)^t}{t!}\left(\frac{\lambda_R \xi}{\lambda_S}\right)^{\frac{v_9 - t}{2}}\right.$$
$$\times \left(K_{v_9-t}\left(2\sqrt{\lambda_S\lambda_R\xi}\right)\right)\Bigg)\Bigg)^{-\frac{1}{N_D N_S}}, \tag{69}$$

respectively.

Obviously, the three different TAS schemes achieve the same secrecy diversity order, which is equal to the product of the number of antennas at S and the number of antennas at D. Furthermore, we can find that the secrecy diversity order is independent of the number of antennas at E and α.

V. Numerical results

In this section, numerical and Monte-Carlo simulation results are presented to highlight the impact of different related parameters on the SOP of the considered cognitive MIMO system. The main parameters used in analysis and simulation are set as $\eta = 0.8$, $\sigma^2 = 1$, and $R_S = 1$ nat/s/Hz. As shown in Figs. 2-5, analysis results match very well with simulation curves that verify the proposed analytical results. Further, one can find that the OAS scheme strictly achieves the best SOP than the SAS and STT schemes.

As shown in Fig. 2, one can find that SOP is enhanced while P_I increasing since a higher P_I implies a larger transmitting power at S. Meanwhile, we can also observe that there exists a floor in the higher P_I region. It is because as $P_I \to \infty$, the transmit power at S approaches P_{max} and the system falls into a non-cognitive model wherein the interference to the primary users is ignored. Furthermore, we can see that SOP is improved while increasing N_S because increasing N_S signifies more diversity gain at S, and the EH ability of S is improved and more antennas can be selected for transmitting information.

Figs. 3 and 4 demonstrate SOP versus P_t with N_S and Ω_S varying, respectively. It can be observed that the secrecy outage performance can be improved while increasing P_t or Ω_S. This is because a higher Ω_S signifies a better primary channel quality and a higher P_t signifies a higher transmit power at S. One can also observe that there exists a floor in the higher P_t region, which means increasing power at S cannot improve the secrecy performance unlimitedly, as testified in [51]. Furthermore, one can find that the OAS scheme strictly achieves the best SOP than the SAS and STT schemes with N_S or Ω_S increasing, also noting that the OAS scheme must pay more to obtain the CSI of the eavesdropping node.

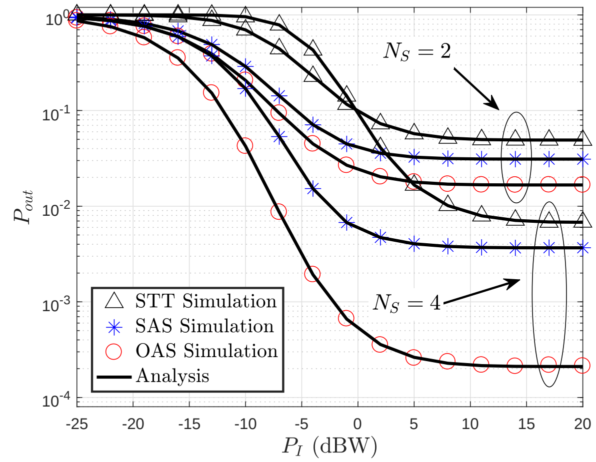

Fig. 2. SOP versus P_I with $\alpha = 0.5$, $\Omega_D = 10$ dB, $\Omega_S = \Omega_E = \Omega_R = 0$ dB, $N_D = 3$, $N_E = 4$, and $P_t = 5$ dBW.

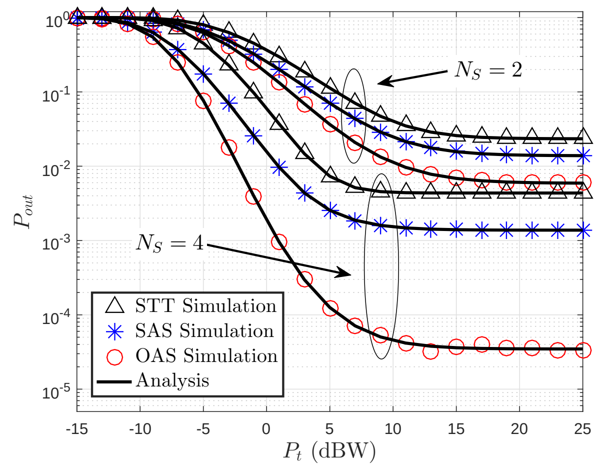

Fig. 3. SOP versus P_t with $\alpha = 0.5$, $\Omega_D = 5$ dB, $\Omega_S = \Omega_E = \Omega_R = -5$ dB, $N_D = N_E = 3$, and $P_I = 5$ dBW.

Fig. 5 plots the SOP versus with α and N_D varying. It can be observed that the security outage performance of OAS and SAS schemes can be improved while increasing α or N_D. This is because higher α means more energy at S is harvested and less time will be allocated for IT phase. Based on (4), the P_{max} would become more large as improving α. However, higher α will cut down the reliability of the cognitive systems since most of time is in harvesting energy. We observe that there is a floor in the higher α region, which is similar to Figs. 3 and 4. Therefore, we can find out a superior α to achieve the tradeoff between the EH and the information transmission at S. Therefore the best α will be an interesting topic in our

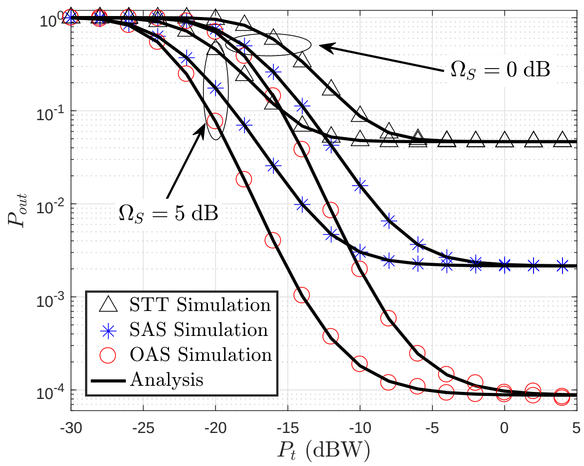

Fig. 4. SOP versus P_t with $\Omega_D = 10\,\text{dB}$, $\Omega_R = \Omega_E = 0\,\text{dB}$, $N_D = N_E = 3$, $N_S = 4$, and $P_I = 0\,\text{dBW}$.

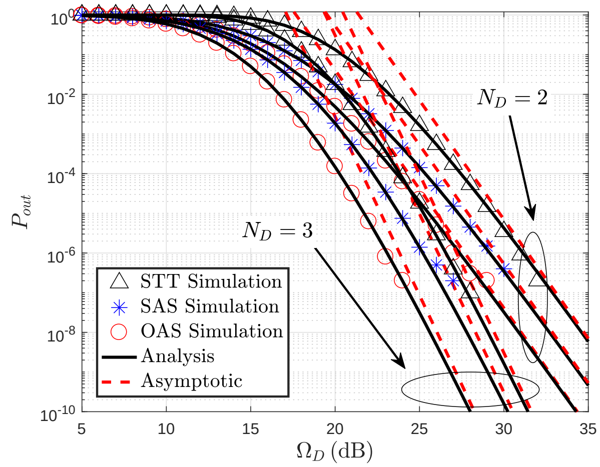

Fig. 6. Asymptotic SOP versus Ω_D with $\alpha = 0.5$, $\Omega_S = \Omega_E = \Omega_R = 10\,\text{dB}$, $N_S = 3$, $N_E = 2$, $P_t = 0\,\text{dBW}$, and $P_I = 0\,\text{dBW}$.

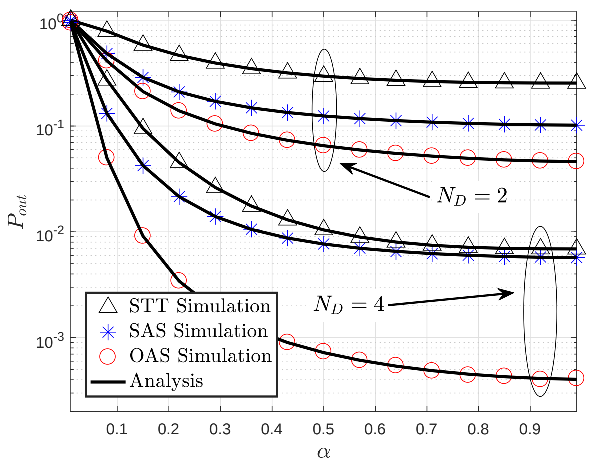

Fig. 5. SOP versus α with $\Omega_D = 8\,\text{dB}$, $\Omega_S = \Omega_R = \Omega_E = 0\,\text{dB}$, $N_S = N_E = 3$, $P_t = 0\,\text{dBW}$, and $P_I = 10\,\text{dBW}$.

future works.

Fig. 6 plots SOP versus Ω_D with N_D varying. It can be observed that a higher N_D outperforms the ones with a lower N_D as the MRC diversity gain increases at D. Furthermore, one also can observe that all the asymptotic curves tightly approximate the exact curves in high Ω_D regime.

VI. Conclusion

In this paper, we investigated the secrecy outage performance of an underlay MIMO CRN with EH and TAS. The closed-form expressions for the SOP of OAS and SAS schemes over Rayleigh channels were derived and validated by simulations. Numerical results illustrated that when the number of antennas at S and/or D increases, the secrecy outage performance of the system can be improved. The results in our work will be beneficial for designing practical cognitive systems with EH and TAS, where security issue is considered. The outdated CSI and channel estimation errors will be considered in our future works.

References

[1] R. Amirtharajah and A. P. Chandrakasan, "Self-powered signal processing using vibration-based power generation," *IEEE. J. Solid-st. Circ*, vol. 33, no. 5, pp. 687-695, May 1998.

[2] T. Soyata, L. Copeland, and W. Heinzelman, "RF energy harvesting for embedded systems: A survey of tradeoffs and methodology," *IEEE Circuits Syst. Mag.*, vol. 16, no. 1, pp. 22-57, Feb. 2016.

[3] L. R. Varshney, "Transporting information and energy simultaneously," in *IEEE International Symposium on Information Theory (ISIT 2008)*, Toronto, ON, Canada, Jul. 2008, pp. 1612-1616.

[4] P. Grover and A. Sahai, "Shannon meets Tesla: Wireless information and power transfer," in *2010 IEEE International Symposium on Information Theory Proceedings (ISIT 2010)*, Austin, TX, Jun. 2010, pp. 2363-2367.

[5] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989-2001, May 2013.

[6] A. A. Nasir, X. Zhou, S. Durrani, and R. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622-3636, Jul. 2013.

[7] D. Wu, J. He, H. Wang, C. Wang, and R. Wang, "A hierarchical packet forwarding mechanism for energy harvesting wireless sensor networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 92-98, Aug. 2015.

[8] G. Pan, H. Lei, Y. Yuan, Z. Ding, "Performance analysis and optimization for SWIPT wireless sensor networks," to appear in *IEEE Trans. Wireless Commun.*, doi: 10.1109/TCOMM.2017.2676815

[9] J. Zhang, C. K. Wen, C. Yuen, S. Jin, and X. Gao, "Large system analysis of cognitive radio network via partially-projected regularized zero-forcing precoding," *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 4934-4947, Sept. 2015.

[10] 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.

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

[12] J. Zhang, G. Pan, and H. M. Wang, "On physical-layer security in underlay cognitive radio networks with full-duplex wireless-powered secondary system," *IEEE Access*, vol. 4, pp. 3887-3893, Aug. 2016.

[13] H. Lei, H. Zhang, I. S. Ansari, G. Pan, and K. A. Qaraqe, "Secrecy outage analysis for SIMO underlay cognitive radio networks over generalized-K fading channels," *IEEE Signal Process. Lett.*, vol. 23, no. 8, pp. 1106-1110, Aug. 2016.

[14] A. Hyadi, Z. Rezki, and M.-S. Alouini, "An overview of physical layer security in wireless communication systems with CSIT uncertainty," *IEEE Access*, vol. PP, pp. 1-12, Sept. 2016.

[15] Y. Jiang, J. Zhu, and Y. Zou, "Secrecy outage analysis of multi-user multi-eavesdropper cellular networks in the face of cochannel interference," *Digital Communications and Networks*, vol. 1, no. 1, pp. 68-74, Mar. 2015.

[16] Z. Ding and H. V. Poor, "Cooperative energy harvesting networks with spatially random users," *IEEE Signal Process. Lett.*, vol. 20, no. 12, pp. 1211-1214, Dec. 2013.

[17] G. Pan, C. Tang, T. Li, and Y. Chen, "Secrecy performance analysis for SIMO simultaneous wireless information and power transfer systems," *IEEE Trans. Commun.*, vol. 63, no. 9, pp. 3423-3433, Sept. 2015.

[18] G. Pan, H. Lei, Y. Deng, L. Fan, J. Yang, Y. Chen, and Z. Ding, "On secrecy performance of MISO SWIPT systems with TAS and imperfect CSI," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3831 - 3843, Sept. 2016.

[19] J. Zhang, C. Yuen, C.-K. Wen, S. Jin, K.-K. Wong, and H. Zhu, "Large system secrecy rate analysis for SWIPT MIMO wiretap channels," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 74-85, Jan. 2016.

[20] L. Liu, R. Zhang, and K. C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Trans. Signal Proces.*, vol. 62, no. 7, pp. 1850-1863, Apr. 2014.

[21] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599-4615, Aug. 2014.

[22] C. Xu, Q. Zhang, Q. Li, Y. Tan, and J. Qin, "Robust transceiver design for wireless information and power transmission in underlay MIMO cognitive radio networks," *IEEE Commun. Lett.*, vol. 18, no. 9, pp. 1665-1668, Sept. 2014.

[23] S. Park, H. Kim, and D. Hong, "Cognitive radio networks with energy harvesting," *IEEE Trans. Wireless Commun.*, vol. 12, no. 3, pp. 1386-1397, Mar. 2013.

[24] S. Lee, R. Zhang, and K. Huang, "Opportunistic wireless energy harvesting in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 9, pp. 4788-4799, Sept. 2013.

[25] X. Lu, W. Xu, S. Li, Z. Liu, and J. Lin, "Simultaneous wireless information and power transfer for cognitive two-way relaying networks," in *2014 IEEE 25th Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC)*, Washington, DC, Sept. 2014, pp. 748-752.

[26] L. Jiang and H. Tian, "Energy-efficient relay selection scheme for physical layer security in cognitive radio networks," *Math. Probl. Eng.*, vol. 2015, Jan. 2015.

[27] L. Jiang, H. Tian, C. Qin, S. Gjessing, and Y. Zhang, "Secure beamforming in wireless-powered cooperative cognitive radio networks," *IEEE Commun. Lett.*, vol. 20, no. 3, pp. 522-525, Mar. 2016.

[28] Y. Liu, L. Wang, S. A. Raza Zaidi, M. Elkashlan, and T. Q. Duong, "Secure D2D communication in large-scale cognitive cellular networks: A wireless power transfer model," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 329-342, Jan. 2016.

[29] A. Singh, M. R. Bhatnagar, and R. K. Mallik, "Secrecy outage of a simultaneous wireless information and power transfer cognitive radio system," *IEEE Wireless Commun. Lett.*, vol. 5, no. 3, pp. 288-291, Jun. 2016.

[30] L. Yang, H. Jiang, S. A. Vorobyov, J. Chen, and H. Zhang, "Secure communications in underlay cognitive radio networks: User scheduling and performance analysis," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1191-1194, Jun. 2016.

[31] S. Sanayei and A. Nosratinia, "Antenna selection in MIMO systems," *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 68-73, Oct. 2004.

[32] S. Prakash and I. McLoughlin, "Effects of channel prediction for transmit antenna selection with maximal-ratio combining in rayleigh fading," *IEEE Trans. Veh. Technol.*, vol. 60, no. 6, pp. 2555-2568, Jul. 2011.

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

[34] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, J. Wang, and C. Cai, "Secure transmission in spectrum sharing MIMO channels with generalized antenna selection over Nakagami-m channels," *IEEE Access*, vol. 4, pp. 4058-4065, Aug. 2016.

[35] J. Zhu, Y. Zou, G. Wang, Y.-D. Yao, and G. K. Karagiannidis, "On secrecy performance of antenna-selection-aided MIMO systems against eavesdropping," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 214-225, Jan. 2016.

[36] 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.

[37] H. Alves, M. De Castro Tome, P. H. J. Nardelli, C. H. M. De Lima, and M. Latva-Aho, "Enhanced transmit antenna selection scheme for secure throughput maximization without CSI at the transmitter," *IEEE Access*, vol. 4, pp. 4861-4873, Sept. 2016.

[38] Z. Hadzi-Velkov, I. Nikoloska, G. K. Karagiannidis, and T. Q. Duong, "Wireless networks with energy harvesting and power transfer: Joint power and time allocation," *IEEE Signal Process. Lett.*, vol. 23, no. 1, pp. 50-54, Jan. 2016.

[39] E. Boshkovska, D. W. K. Ng, N. Zlatanov, and R. Schober, "Practical non-linear energy harvesting model and resource allocation for SWIPT systems," *IEEE Commun. Lett.*, vol. 19, no. 12, pp. 2082-2085, Dec. 2015.

[40] J. Zhang and G. Pan, "Outage analysis of wireless-powered relaying MIMO systems with non-linear energy harvesters and imperfect CSI," *IEEE Access*, vol. 4, pp. 7046-7053, Oct. 2016.

[41] J. Zhang, G. Pan, and Y. Xie, "Secrecy outage performance for wireless-powered relaying systems with non-linear energy harvesters," *Frontiers of Information Technology & Electronic Engineering*, vol. 18, no. 2, pp. 246-252, Feb. 2017.

[42] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4754-4767, Nov. 2013.

[43] H. Zhao, Y. Tan, G. Pan, Y. Chen, and N. Yang, "Secrecy outage on transmit antenna selection/maximal ratio combining in MIMO cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp.10236-10242, Dec. 2016.

[44] 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.

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

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

[47] 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.

[48] H. Lei, H. Zhang, I. S. Ansari, C. Gao, Y. Guo, G. Pan, and K. Qaraqe, "Performance analysis of physical layer security over generalized-K fading channels using a mixture Gamma distribution," *IEEE. Commun. Lett.*, vol. 20, no. 2, pp. 408-411, Feb. 2016.

[49] 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.

[50] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series and products, 7th*. San Diego, CA: Academic Press, 2007.

[51] H. Lei, I. S. Ansari, G. Pan, B. Alomair, and M.-S. Alouini, "Secrecy capacity analysis over $\alpha-\mu$ fading channels," *IEEE Commun. Lett.*, doi: 10.1109/LCOMM.2017.2669976, Feb. 2017.

Hongjiang Lei (M'17) received the B.Sc. 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 physical layer security, and cognitive radio networks. He has served as the reviewer for IEEE TVT, IEEE TCOM, IEEE CL, Transactions on Emerging Telecommunications Technologies (Wiley), and Computer Standards & Interfaces (Elsevier), etc.

Ming Xu received the B.Sc. degree in Communication Engineering from the Taiyuan University of Science and Technology, Taiyuan, China, in 2013. He is currently pursuing the M.Sc. degree in Information and Communication Engineering at Chongqing University of Posts and Telecommunications, Chongqing, China. His research interests include cognitive radio networks, physical layer security, and cooperative communications.

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.

He has been affiliated with IEEE and IET since 2007 and has served in various capacities. He is serving on the IEEE ComSoc Young Professionals (YP) Board since April 2016. He has served on IET CC-EMEA (Communities Committee-Europe, Middle-East and Africa) for a complete term from Oct. 2010-Sep. 2013 and has been re-elected to serve for another term from Oct. 2015-Sep. 2018. He is an active reviewer for various IEEE Transactions and various other journals. He has served as a TPC for various IEEE conferences. He is a recipient of appreciation for an exemplary reviewer for IEEE Transaction on Communications (TCOM) in 2016, a recipient of TAMUQ Research Excellence Award 2016, a recipient of recognized reviewer certificate by Elsevier Optics Communications in 2015, a recipient of recognized reviewer certificate by OSA Publishing in 2014, a recipient of appreciation for an exemplary reviewer for IEEE Wireless Communications Letters (WCL) in 2014, a recipient of post-doctoral research award (PDRA) (first cycle) with Qatar national research foundation (QNRF) in 2014, a recipient of KAUST academic excellence award (AEA) in 2014, and a recipient of IEEE Richard E. Merwin student scholarship award in Jul. 2013.

Imran has authored/co-authored 50+ journal and conference publications. He has co-organized the GRASNET'2016 workshop in conjunction with IEEE WCNC'2016 and co-organizing the second edition GRASNET'2017 workshop in conjunction with IEEE WCNC'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.

Gaofeng Pan (M'12) received his B.Sc 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 IEEE Globecom16 Workshop on Wireless Energy Harvesting Communication Networks. He has also served as a reviewer for major international journals, e.g., IEEE TCOM, IEEE TWC, IEEE TSP, IEEE TVT, IEEE CL, IEEE WCL, 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.