IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 6, 2019, accepted December 18, 2019, date of publication December 26, 2019, date of current version January 7, 2020.

Digital Object Identifier 10.1109/ACCESS.2019.2962382

Secrecy Outage Performance of SWIPT Cognitive Radio Network With Imperfect CSI

AJAY SINGH[1], (Member, IEEE), MANAV R. BHATNAGAR[2], (Senior Member, IEEE), AND RANJAN K. MALLIK[2], (Fellow, IEEE)

[1]Department of Electrical Engineering, Indian Institute of Technology Jammu, Jammu 181221, India
[2]Department of Electrical Engineering, India Institute of Technology Delhi, New Delhi 110016, India

Corresponding author: Ajay Singh (ajay.singh@iitjammu.ac.in)

This work was supported in part by the Science and Engineering Research Board (SERB), Department of Science and Technology (DST), Government of India, for the Project ''Physical Layer Security of Cognitive Radio Networks'' under Project YSS/2015/001738, in part by the Media Lab Asia (Sir Visvesvaraya Young Faculty Research Fellowship) under the Ministry of Electronics and Information Technology (MeiTY), Government of India, and in part by the Brigadier Bhopinder Singh Chair, Indian Institute of Technology-Delhi, New Delhi, India.

ABSTRACT We consider a cognitive radio (CR) network with simultaneous wireless information and power transfer (SWIPT) system having one base station (BS) with multiple antennas that acts as a secondary transmitter, one desired information receiver (IR) acting as secondary receiver, multiple primary users (PUs) having licenses band of spectrum, and multiple energy harvesting receivers (EHRs). The EHRs harvests energy from the BS and eavesdrop the information from signal. In order to extract the information and then harvest energy from that signal, power splitting is considered in each EHR. On the basis of an imperfect channel state information (CSI) in IR, selection of the best transmit antenna at the BS is made. The effect of path loss on the system is also considered. The derivation of analytical expression in closed-form is provided for the exact secrecy outage probability (SOP) of the network. The derived expression highlights the variation in the secrecy outage of the considered CR SWIPT system relying on imperfect CSI with respect to the system parameters, which is depicted through numerical analysis. Furthermore, we derive the asymptotic SOP and study the effects of different system parameters on the secrecy diversity order and secrecy array gain.

INDEX TERMS Cognitive radio (CR), energy harvesting, physical layer security, secrecy outage probability.

I. INTRODUCTION

In these days, simultaneous wireless information and power transfer (SWIPT) system is emerging as an important research area [1], [2], where a basic compromise between energy harvesting and the rate of information transmission over noisy channels has gained a significant attention of the research community. It is to be noted that a sophisticated hardware is needed to satisfactorily extract the information along with power, through the exactly same received signal. However, power splitting hybrid receivers [3] as-well-as separated receivers [4] have emerged in simple and effective solutions for this purpose. Furthermore, the authors in [5] focused on a SWIPT system using dynamic power splitting.

Recently, cognitive radio (CR) has come up as a useful technology for improving spectrum utilization efficiency. Energy harvesting in CR networks is an important issue and is addressed in [6]. Authors of [7] discussed the output of a CR system employing energy harvesting through a slotted mode; in this mode, the user at the secondary end is assumed to be strengthened by the energy harvested through natural sources of energy. In [8], authors provided an analysis of throughput maximization for the CR system based on energy harvesting, where the user at secondary end has a finite capacity of battery. However, there is a possibility that energy harvesting based receivers may try to behave as eavesdroppers. The authors in [9] highlighted a spectrum sensing policy which is optimal for a CR based on energy harvesting, and increases the expected throughput with energy causality constraints and collision constraints. It is well known that for a better energy harvesting, a transmitter has to transmit energy. Due to increase of transmit energy, information can be leaked with more ease. Therefore, a higher information energy will result in more susceptibility for eavesdropping.

The associate editor coordinating the review of this manuscript and approving it for publication was Francesco Benedetto.

It is difficult to prevent an eavesdropper who tries to intercept the information due to a high energy of the received signal. For a CR network, the capacity of sensing and learning of the existing radio frequency (RF) environment can create problems for security at the physical layer. Therefore, it is easy to launch an adversary for malicious activities. Hence, CR networks' physical layer security has emerged as an important topic of research in recent times [10], [11]. In [12], the physical layer security of a multiuser multiple-input single-output (MISO) based SWIPT system is discussed. It is assumed in [12] that a multi-antenna based transmitter conveys the information simultaneously with the energy to an intended information receiver (IR) and multiple energy harvesting receivers (EHRs).

Secrecy outage performance of an underlay multiple-input multiple-output (MIMO) system with energy harvesting and transmit antenna selection scheme is investigated in [13]. A closed-form expressions for the secrecy outage probability of optimal antenna selection and sub optimal antenna selection schemes over Rayleigh channels were derived in [13]. In [14], the secrecy outage performance of an underlay cognitive decode-and-forward relay network over independent but not necessarily identical distributed Nakagami-m fading channels is investigated, where the secondary user communicates with the secondary destination via relays and an eavesdropper attempts to overhear the information. In [15], MIMO cognitive wiretap system over Nakagami-m channels is considered with generalized selection combining, where confidential messages, transmitted from a multiple-antenna based transmitter to a multiple-antenna based legitimate receiver, are overheard by a multiple-antenna based eavesdropper. A closed-form expressions for exact and asymptotic secrecy outage probabilities (SOPs) are derived in [15]. In [16], an analytical model for the secrecy performance for single-input multiple-output (SIMO) underlay CR systems over Nakagami-m channels has been discussed. The results obtained in [16] provide a unified model to analyze the secrecy performance over SIMO Nakagami-m fading channels in CR network and can be readily applied to a practical CR design. Authors in [26] derive an exact closed-form expression for the SOP and the intercept probability of the secondary network in Rayleigh fading. In [27], a CR-based SWIPT system consisting of a base station (BS), a desired information receiver, multiple primary users, and multiple energy harvesting receivers is considered. Each link in the system suffers from small scale fading and path loss. The main drawback of the majority of existing research studies is that the global channel state information (CSI) is considered to be perfectly known at the transmitter for analysis. When the CSI of eavesdroppers is known in the transmitter, best transmit antenna is selected to maximize the secrecy capacity [28], [29]. However, practically, it is difficult for the transmitter to obtain perfect CSI because of channel estimation errors as-well-as quantization [17], [18]. For instance, in a scenario where all the EHRs are not able to continuously interact with the corresponding transmitter, the CSI available in transmitter will become outdated [19]. In the presence of imperfect CSI, the secrecy performance of a simple MISO SWIPT system is investigated in [20]; this investigation is however limited to a simple wireless communication model having a single transmitter, an intended receiver, and multiple EHRs (acting as eavesdroppers). All the aforementioned works on the physical layer security of SWIPT systems have not considered CR set-up even under perfect CSI. This motivates the study of CR based SWIPT systems from a physical layer security point-of-view. This paper analyzes the secrecy performance of a CR SWIPT system having multiple primary users (PUs) and imperfect CSI. Analytical expressions of an exact and asymptotic SOPs of this system are derived in closed-form. Some important insights are further presented.

Contributions of this paper are:

- We derive new closed-form expression for cumulative distribution function (CDF) of the instantaneous received signal-to-noise ratio (SNR) in IR (with imperfect CSI).
- We derive closed-form analytical expressions for exact and the asymptotic SOPs while assuming imperfect CSI between transmitter and receiver.
- Compared to [13]–[16], wherein the SOP of underlay cognitive radio network is derived with perfect CSI assumption, we explore the secrecy performance under imperfect CSI conditions. Note that, impact of imperfect CSI on the secrecy performance of underlay CR with considered parameters (such as path loss, power spiting factor etc) in the presence of multiple PUs and multiple EHRs has not been examined in the literature.

It can be noticed that:

- The considered model in this manuscript can be compared to the model given in [20] without interference power constraint.
- The given model in this manuscript can be compared to the model assumed in [21] without interference power constraint and perfect CSI condition.
- The system model in this manuscript is similar to the model considered in [22] for $\eta = 1$, $\rho = 1$, $K = 1$, $N = 1$, and $\gamma_p \to \infty$.
- The model considered in this manuscript leads to the model refereed in [11] when $\eta = 1$, $\rho = 1$, $K = 1$, and $N = 1$.

The rest of this paper is organized as follows. In Section II, the system model considered in our work is described. The secrecy outage performance analysis is proposed in Section III. Section IV contains the asymptotic secrecy outage probability analysis. In Section V, we present and discuss the numerical results. Finally, Section VI concludes this paper.

II. SYSTEM MODEL

The system under study contains a BS that works as a secondary transmitter, an intended IR that works as secondary receiver, K PUs along with N EHRs. The BS has N_T transmit antennas while each of the IR, the EHRs, and the PUs have a single antenna. We assume that independent Rayleigh fading exists over each communication link. The EHRs are legitimate users in the system and act as eavesdroppers [21]. For a given transmission time, the BS transmits the information to IR. It also supplies energy to each of the EHRs. It is also assumed that each of the EHRs harvest energy using radio frequency signals. The underlay CR network is considered, where the BS uses the licensed spectrum of PU, to transmit signals to the IR. Perhaps, a bottleneck exists for CR networks for providing high date rate because of the devices that are energy-constrained. To increase the life-time of such energy-constrained devices, SWIPT is considered as a reliable technique in CR networks. The BS is interested in sending the confidential information over that spectrum band which is used by a PU in a manner that the power of interference at PU from the BS does not surpass a given threshold. Thus we have a CR network in which the BS transmits in the presence K PUs and N EHRs behaving as eavesdroppers. We focus on the enhancement of secure communication from the BS to the IR, keeping in view the peak constraint of interference of primary network. This is possible by using the maximum power of transmission at the BS. The BS locations, the IR, and all the EHRs are considered to be very far from the PUs such that effect of the signals from all of the transmitters of PUs could be neglected on the secondary network. However, the interference to the PUs from the BS cannot be neglected, as the BS transmits at a high transmit power in order to provide sufficient energy for energy harvesting. Each EHR uses power splitting in order to extract, from the same received signal, the information and energy. In all EHRs, the received signal is split through a power splitter into information decoder and energy harvester. The power splitter uses a fraction ρ of the received signal to information decoder, such that $0 \leq \rho \leq 1$, and the balance part of the signal is sent for harvesting of energy. To guarantee reliable communication in the PUs in this underlay CR system, the power of the transmitted signal of the BS is restricted by a peak threshold. Hence, the transmit power of the BS is given by

$$P_{\mathrm{BS}} = \min\left(\frac{I_p}{\max_{k=1,\ldots,K} |h_{0_k}|^2},\ P_t\right), \tag{1}$$

where P_t is the transmitted power at the BS, I_p is the maximum power of interference in PUs, and h_{0_k} represents complex Gaussian channel gain of primary channel from BS to k^{th} PU having zero mean and Ω_0 variance. Therefore, signal received in IR is expressed as [21]

$$y_{\mathrm{IR}} = \sqrt{\frac{P_{\mathrm{BS}} L_c}{r_1^{\kappa}}} h_{\mathrm{IR}} s + n_{\mathrm{IR}}, \tag{2}$$

where h_{IR} represents complex Gaussian channel gain from BS to IR with zero mean and Ω_1 variance, L_c is the constant for propagation loss, r_1 represents the distance between the BS and the IR, κ represents the exponent of path loss, s is the transmitted signal from the BS, and n_{IR} represents the complex additive white Gaussian noise (AWGN) having zero mean and N_0 variance. Furthermore, n_{IR} is assumed to be independent of h_{IR}. Typical values of κ lie between 2.7 and 3.5. The signal received in the n^{th} EHR is given by [21]

$$y_{\mathrm{EHR}_n} = \sqrt{\rho}\left(\sqrt{\frac{P_{\mathrm{BS}} L_c}{r_2^{\kappa}}} h_{\mathrm{EHR}_n} s + z_n\right) + v_n, \quad , \tag{3}$$

where $n = 1, \ldots, N$, h_{EHR_n} represents the complex Gaussian channel gain from each antenna of BS to n^{th} EHR, having zero mean and Ω_2 variance, z_n represents complex AWGN with zero mean and N_0 variance, v_n represents the noise of signal processing introduced by information decoder at n^{th} EHR that is considered to be complex Gaussian with zero mean and μ^2 variance, and r_2 is the distance of EHRs from BS. From (2), the instantaneous SNR in the IR channel is expressed as

$$\gamma_{\mathrm{IR}} = \frac{P_{\mathrm{BS}} L_c}{N_0 r_1^{\kappa}} |h_{\mathrm{IR}}|^2. \tag{4}$$

From (3), the instantaneous SNR of EHR's channel is

$$\gamma_{\mathrm{EHR}} = \frac{\rho P_{\mathrm{BS}} L_c}{r_2^{\kappa}\left(\rho + \frac{\mu^2}{N_0}\right)} \max_{n=1,\ldots,N} |h_{\mathrm{EHR}_n}|^2. \tag{5}$$

Using (1) and (4), the instantaneous SNR in the IR channel can be written as

$$\gamma_{\mathrm{IR}} = \min\left(\frac{\gamma_p}{X}, \gamma_0\right) \frac{L_c |h_{\mathrm{IR}}|^2}{r_1^{\kappa}}, \tag{6}$$

where $\gamma_p = I_p/N_0$, $\gamma_0 = P_t/N_0$, $X = \max_{k=1,\ldots,K} |h_{0_k}|^2$, and h_{0_k} represents complex channel gain from the BS to k^{th} PU having zero mean and Ω_0 variance. X's probability density function (PDF) of is expressed as [11]

$$f_X(x) = \sum_{k=0}^{K-1} \binom{K-1}{k} \frac{(-1)^k K}{\Omega_0} \exp\left\{-\frac{(k+1)x}{\Omega_0}\right\}, \quad x \geq 0. \tag{7}$$

Using (1) and (5), the instantaneous SNR at EHRs is given by

$$\gamma_{\mathrm{EHR}} = \min\left(\frac{\gamma_p}{X}, \gamma_0\right) \frac{\rho L_c}{r_2^{\kappa}\left(\rho + \frac{\mu^2}{N_0}\right)} \max_{n=1,\ldots,N} |h_{\mathrm{EHR}_n}|^2. \tag{8}$$

III. SECRECY OUTAGE PERFORMANCE

For a transmitter with multiple antennas, it is practically hard to get the correct information about the phase of the channel in the receiver. Due to this, the received signals are not properly combined. However, estimation of channel magnitude is relatively easier than estimation of phase. For a BS with multiple antennas, it is better to transmit the signal on that antenna only which is associated with the best channel gain magnitude such that destructive interference can be minimized. This phenomenon of selection of the best antenna is generally called as antenna selection scheme [23]–[25]. We consider here a situation that the best transmit antenna in IR is selected through forward training; then the index of antenna having best channel is sent back to BS. We consider the case when the IR feeds back BS-IR channel's CSI to BS and also the CSI of links between BS and EHRs is available at the BS. While the EHRs are trying to behave as eavesdroppers, the BS, for secure communication, conveys the information at a transmission rate in accordance with the the BS-IR channel's CSI and the BS-EHR channels. The IR has to only compare the received signals on the links between itself and all transmitting antennas, and it then feeds the relating antenna index back to the BS. The best antenna selection scheme results into the low cost of implementation. The feedback of CSI from the IR gets delayed and the BS then encodes the information to the IR by using the outdated CSI of IR. The best transmit antenna is selected which the maximizes the instantaneous SNR in the IR. The expression for the magnitude of largest channel gain from the links between the IR and the selected antenna at BS, at the time of selection, is

$$|\tilde{h}| = \max_{t=1,\ldots,N_T} |\tilde{h}_{\mathrm{IR}_t}|, \tag{9}$$

where $\tilde{h}_{\mathrm{IR}}$ represents the coefficient of delayed channel between the IR and the t^{th} antenna of BS. It can be shown after some algebra that the relationship between $\tilde{h}_{\mathrm{IR}_t}$ and h_{IR_t} is

$$\tilde{h}_{\mathrm{IR}_t} = \sqrt{\eta}\, h_{\mathrm{IR}_t} + \sqrt{1-\eta}\, w_t, \tag{10}$$

where w_t is a complex Gaussian variable having zero mean and Ω_w variance, and η is given by [17], [18]

$$\eta = [J_0(2\pi f_d \tau_d)]^2, \tag{11}$$

where $J_0(\cdot)$ represents the Bessel function in zeroth order of the first kind, f_d represents the maximum frequency of Doppler, and τ_d represents the time delay. After the selection of antenna, the BS sends the message to the IR and the energy is transferred to each EHR at the same time in presence of multiple PUs. From the radio frequency, all the EHRs harvest energy. Each EHR may overhear the signals meant for the target IR because of them being in the coverage range. EHRs will try to eavesdrop the message of the target IR if they are malicious. Therefore, each EHR is a potential eavesdroppers and try to degrade the performance of this CR network. Furthermore, we consider that all the EHRs perform independently and there is no exchange of information between all the EHRs. The secrecy rate is given by [10]

$$C_S \triangleq \begin{cases} C_{\mathrm{IR}} - C_{\mathrm{EHR}} = \log_2\left(\dfrac{1+\gamma_{\mathrm{IR}}}{1+\gamma_{\mathrm{EHR}}}\right) & \text{if } \gamma_{\mathrm{IR}} > \gamma_{\mathrm{EHR}}, \\ 0 & \text{if } \gamma_{\mathrm{IR}} \le \gamma_{\mathrm{EHR}}, \end{cases}$$

where $C_{\mathrm{IR}} = \log_2(1+\gamma_{\mathrm{IR}})$ represents IR channel's capacity and $C_{\mathrm{EHR}} = \log_2(1+\gamma_{\mathrm{EHR}})$ represents EHR's channel's capacity. In passive eavesdropping, if $R_S \le C_S$, then perfect secrecy is guaranteed. Otherwise, if $R_S > C_S$, then the information-theoretic security will be compromised. The SOP is the probability that C_S falls below R_S, and is given by

$$P_{\mathrm{out}} = \Pr(C_S < R_S) = \Pr(\gamma_{\mathrm{IR}} \le \gamma_{\mathrm{EHR}}) + \Pr(\gamma_{\mathrm{IR}} > \gamma_{\mathrm{EHR}}) \times \Pr(C_S < R_S \mid \gamma_{\mathrm{IR}} > \gamma_{\mathrm{EHR}}), \tag{12}$$

which can be simplified to [11]

$$P_{\mathrm{out}} = \int_0^\infty \int_0^\infty F_{\gamma_{\mathrm{IR}}|X=x}(\epsilon(\gamma_{\mathrm{ehr}})) f_{\gamma_{\mathrm{EHR}}|X=x}(\gamma_{\mathrm{ehr}}) \times f_X(x)\, d\gamma_{\mathrm{ehr}}\, dx, \tag{13}$$

where $\epsilon(\gamma_{\mathrm{ehr}}) = 2^{R_S}(1+\gamma_{\mathrm{ehr}})-1$, $f_{\gamma_{\mathrm{EHR}}|X=x}(\cdot)$ represents PDF of γ_{EHR} conditioned on X, and $F_{\gamma_{\mathrm{IR}}|X=x}(\cdot)$ represents CDF of γ_{IR} conditioned on X. Let $\gamma_1 = \Omega_1\gamma_0 = \frac{\gamma_p\Omega_1}{\sigma}$ be the average SNR, which is maximum possible, of the channel between BS and IR, and $\gamma_2 = \Omega_2\gamma_0 = \frac{\gamma_p\Omega_2}{\sigma}$ is the maximum possible average SNR of channel between BS and EHRs.

Furthermore, since

$$\min\left(\frac{\gamma_p}{X}, \gamma_0\right) = \begin{cases} \gamma_0, & X \le \dfrac{\gamma_p}{\gamma_0}, \\ \dfrac{\gamma_p}{X}, & X > \dfrac{\gamma_p}{\gamma_0}, \end{cases} \tag{14}$$

the CDF of γ_{IR} conditioned on X may be expressed as

$$F_{\gamma_{\mathrm{IR}}|X=x}(\epsilon(\gamma_{\mathrm{ehr}})) = N_T \sum_{t=0}^{N_T-1} \binom{N_T-1}{t} \frac{(-1)^t}{(t+1)} \times \left\{1 - \exp\left(-\frac{\lambda(t+1)\left(2^{R_S}(1+\gamma_{\mathrm{ehr}})-1\right)}{1+(1-\eta)t}\right)\right\}, \tag{15}$$

where

$$\lambda = \begin{cases} \dfrac{r_1^\kappa}{L_c\gamma_0(\eta\Omega_1 + (1-\eta)\Omega_w)}, & x \le \dfrac{\gamma_p}{\gamma_0}, \\ \dfrac{r_1^\kappa x}{L_c\gamma_p(\eta\Omega_1 + (1-\eta)\Omega_w)}, & x > \dfrac{\gamma_p}{\gamma_0}. \end{cases} \tag{16}$$

From [30], [31], the PDF of γ_{EHR} conditioned on X may be written as

$$f_{\gamma_{\mathrm{EHR}}|X=x}(\gamma_{\mathrm{ehr}}) = \sum_{n=0}^{N-1} \binom{N-1}{n} \frac{(-1)^n N}{v\Omega_2} \times \exp\left\{-\frac{(n+1)\gamma_{\mathrm{ehr}}}{\Omega_2}\right\}, \quad \gamma_{\mathrm{ehr}} \ge 0, \tag{17}$$

where

$$v = \begin{cases} \dfrac{\rho\gamma_0 L_c}{r_2^\kappa(\rho N_0 + \mu^2)}, & x \le \dfrac{\gamma_p}{\gamma_0}, \\ \dfrac{\rho\gamma_p L_c}{x r_2^\kappa(\rho N_0 + \mu^2)}, & x > \dfrac{\gamma_p}{\gamma_0}. \end{cases} \tag{18}$$

Substitution of (7), (15), and (17) into (13) results in the closed-form expression (19) for P_{out}. The exact SOP in closed-form is

$$P_{\mathrm{out}} = NKN_T \sum_{t=0}^{N_T-1} \sum_{n=0}^{N-1} \sum_{k=0}^{K-1} \binom{N_T-1}{t} \binom{N-1}{n} \times \binom{K-1}{k} \frac{(-1)^{t+n+k} r_2^\kappa(\rho N_0 + \mu^2)}{\gamma_2(t+1)\rho L_c} \Bigg\{ \frac{L_c}{r_1^\kappa + L_c}$$

$$
\begin{aligned}
&\times \left(1-\exp\left(-\frac{(k+1)\sigma}{\Omega_0}\right)\right)\Bigg[\frac{\rho L_c\gamma_2}{r_2^{\kappa}(\rho N_0+\mu^2)(n+1)} \\
&\quad + \exp\left(-L_c\left(2^{R_S}-1\right)\right)\left(\frac{(n+1)L_c}{r_1^{\kappa}\gamma_2}+L_c 2^{R_S}\right)^{-1}\Bigg] \\
&\quad + \frac{1}{\sigma\Omega_0}\exp\left(-\frac{(k+1)\sigma}{\Omega_0}\right)\Bigg[\frac{\rho\sigma L_c\gamma_2\Omega_0 r_2^{-\kappa}}{(n+1)(k+1)(\rho N_0+\mu^2)} \\
&\quad - \left(\frac{(n+1)r_2^{\kappa}(\rho N_0+\mu^2)}{\rho\sigma L_c\gamma_2}+\beta(t)2^{R_S}\right)^{-1} \\
&\quad \times \left(\frac{r_1^{\kappa}+L_c}{\Omega_0 L_c}+\beta(t)\left(2^{R_S}-1\right)\right)^{-1} \\
&\quad \times \exp\left(-\sigma\beta(t)\left(2^{R_S}-1\right)\right)\Bigg]\Bigg\},
\end{aligned} \tag{19}
$$

where $\sigma = I_p/P_t$ and

$$
\beta(t) = \frac{r_1^{\kappa}(t+1)}{L_c\left[\frac{\rho\sigma\eta L_c\gamma_1}{r_2^{\kappa}(\rho N_0+\mu^2)}+\gamma_p\Omega_w(1-\eta)\right]\left[1+(1-\eta)t\right]}.
$$

IV. ASYMPTOTIC SECRECY OUTAGE PROBABILITY ANALYSIS

In this section, we consider a special scenario that BS and IR located quite closer to each other so that $\gamma_1 \to \infty$. This assumption will lead to obtain the asymptotic secrecy outage probability and analyse the secrecy diversity order and the secrecy array gain. Asymptotic SOP (P_{out}^{∞}) is obtained by setting $\Omega_1 \to \infty$ in (15) and neglecting the higher order terms. Further, using the Taylor series expansion of the exponential function in (15) yields

$$
\begin{aligned}
F_{\gamma_{\text{IR}}|X=x}(\epsilon(\gamma_{\text{ehr}})) \approx N_T \sum_{t=0}^{N_T-1}\binom{N_T-1}{n}\frac{(-1)^t}{(t+1)} \\
\times \frac{\lambda(t+1)\left(2^{R_S}(1+\gamma_{\text{ehr}})-1\right)}{1+(1-\eta)t}.
\end{aligned} \tag{20}
$$

Upon substituting (20), (7), and (17) into (13), we obtain

$$
P_{\text{out}}^{\infty} = \frac{B}{\eta}\left(\frac{1}{\gamma_1}\right)+o\left(\frac{1}{\gamma_1}\right), \tag{21}
$$

where

$$
\begin{aligned}
B = A^2 N N_T L_c r_1^{\kappa}\left(S_5+S_6\right)\Bigg\{S_1\left(2^{R_S}-1\right)+S_2\frac{2^{R_S}\sigma\gamma_2}{\gamma_p} \\
+S_3\left(2^{R_S}-1\right)\frac{\sigma\gamma_2}{\gamma_p}+S_4 2^{R_S}\frac{\sigma^2\gamma_2^2}{\gamma_p^2}\Bigg\},
\end{aligned} \tag{22a}
$$

and

$$
A = \begin{cases} \dfrac{\gamma_0\rho}{r_2^{\kappa}\left(\rho N_0+\mu\right)}, & x \le \frac{\gamma_p}{\gamma_0} \\ \dfrac{\gamma_p\rho}{x r_2^{\kappa}\left(\rho N_0+\mu\right)}, & x > \frac{\gamma_p}{\gamma_0} \end{cases} \tag{22b}
$$

$$
\begin{aligned}
S_1 = \sum_{t=0}^{N_T-1}\sum_{n=0}^{N-1}\binom{N_T-1}{t}\binom{N-1}{n}\frac{(-1)^{n+t}}{(n+1)} \\
\times\left(1-\mathrm{e}^{-\frac{\gamma_p(\eta+1)}{\gamma_2}}\right),
\end{aligned} \tag{22c}
$$

$$
\begin{aligned}
S_2 = \sum_{t=0}^{N_T-1}\sum_{n=0}^{N-1}\binom{N_T-1}{t}\binom{N-1}{n}\frac{(-1)^{n+t}}{(n+1)^2} \\
\times\left\{1-\left(1+\frac{\gamma_p\left(\eta+1\right)}{\gamma_2}\right)\mathrm{e}^{-}\frac{\gamma_p\left(\eta+1\right)}{\gamma_2}\right\},
\end{aligned} \tag{22d}
$$

$$
\begin{aligned}
S_3 = \sum_{t=0}^{N_T-1}\sum_{n=0}^{N-1}\binom{N_T-1}{t}\binom{N-1}{n}\frac{(-1)^{n+t}}{(n+1)^2} \\
\times\left\{\left(1+\frac{\gamma_p\left(n+1\right)}{\gamma_2}\right)\mathrm{e}^{-\frac{\gamma_p(n+1)}{\gamma_2}}\right\},
\end{aligned} \tag{22e}
$$

$$
S_4 = \sum_{t=0}^{N_T-1}\sum_{n=0}^{N-1}\binom{N_T-1}{t}\binom{N-1}{n}\frac{(-1)^{n+t}}{(n+1)^3} \tag{22f}
$$

$$
\times\left\{2-\left(1+\frac{\gamma_p\left(n+1\right)}{\gamma_2}+\frac{1}{2}\frac{\gamma_p^2\left(n+1\right)^2}{\gamma_2^2}\right)\mathrm{e}^{-\frac{\gamma_p(n+1)}{\gamma_2}}\right\}, \tag{22g}
$$

$$
S_5 = K\sum_{k=0}^{K-1}\binom{K-1}{k}\frac{(-1)^k}{(k+1)}\left(1-\mathrm{e}^{-\frac{\gamma_p(k+1)}{\gamma_0\Omega_0}}\right), \tag{22h}
$$

$$
S_6 = \frac{K}{\Omega_0^2}\sum_{k=0}^{K-1}\binom{K-1}{k}(-1)^k\,(k+1)\,\frac{\Omega_0\gamma_0}{(k+1)\gamma_p}. \tag{22i}
$$

As suggested by [25] and [15], in the high average channel fading gains regime the asymptotic SOP can be expressed as

$$
P_{\text{out}}^{\infty} = (G_A\gamma_1)^{-G_d}+o(\gamma_1^{-G_d}), \tag{23}
$$

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 $o(\cdot)$ denotes higher order terms. The asymptotic outage probability facilitates valuable insights via the secrecy diversity order G_d, which determines the slope of the asymptotic outage probability curve, and the secrecy array gain G_a, which shows the SNR advantage of the asymptotic outage relative to the reference curve γ^{-G_d}. Using (21) and (23), we obtain

$$
G_d = 1, \tag{24}
$$

and

$$
G_a = \frac{\eta}{B}. \tag{25}
$$

Following observations can be made from (24) and (25)

- Secrecy diversity order G_a is independent of the parameters like γ_2, η, ρ etc. The parallel slopes of the asymptotes in Figs. 6 and 7 will confirm this. It means that secrecy diversity gain is independent on the primary network.
- G_a decreases as the number of PUs increases. The asymptotic SOP degrades by increasing the number of PUs.
- Secrecy array gain G_a increases with η which indicates an improvement in SOP with the perfect CSI estimation.
- G_a is inversely proportional to B. As observed from (22a), B is an increasing function of ρ. Therefore, it can

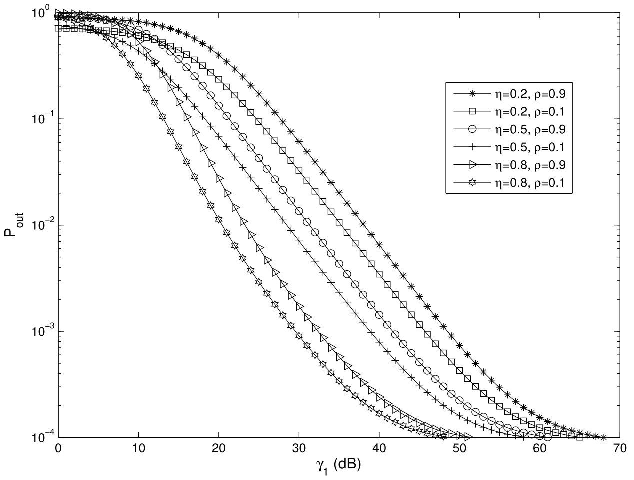

FIGURE 1. SOP versus γ_1 for varying ρ and η with $\gamma_2 = 10$ dB, $\gamma_p = 5$ dB, $N_T = 4$, $N = 4$, $K = 10$, $R_S = 0.0001$, $r_1 = r_2 = 4$ m, $\Omega_0 = \Omega_1 = \Omega_2 = \Omega_W = 1$, $\sigma = 0.5$, $\kappa = 3.2$, and $L_c = 0.005$.

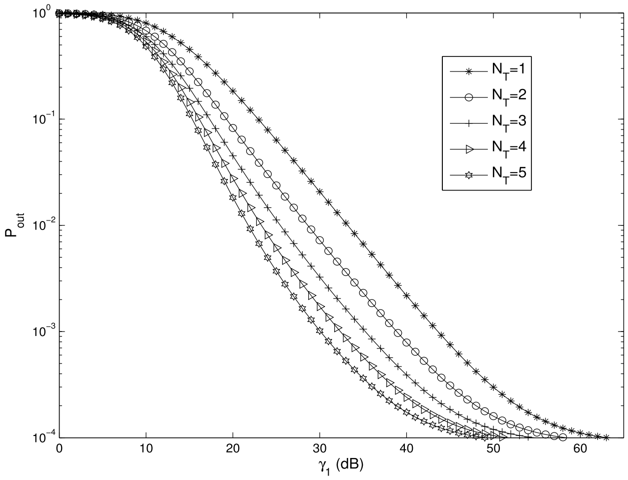

FIGURE 2. SOP versus γ_1 for varying N_T with $\rho = 0.9$, $\eta = 0.8$, $\gamma_2 = 10$ dB, $\gamma_p = 5$ dB, $N = 4$, $K = 10$, $R_S = 0.0001$, $r_1 = r_2 = 4$ m, $\Omega_0 = \Omega_1 = \Omega_2 = \Omega_W = 1$, $\sigma = 0.5$, $\kappa = 3.2$, and $L_c = 0.005$.

be concluded that lower value ρ outperforms the higher value of ρ due to higher secrecy array gain.

- Secrecy array gain in (25) is a decreasing function of γ_2. It indicates that the asymptotic SOP increases with increasing γ_2.
- B is directly proportional to $\left(\frac{r_1}{r_2^2}\right)^{\kappa}$, as indicated (22a). It can be observed that $\left(\frac{r_1}{r_2^2}\right) < 1$ if $r_1 > 1$ and $r_2 > 1$. Therefore, we can say that that G_A decreases with an increasing value of κ because low secrecy array gain leads to the higher SOP.
- It can be seen from (22a) and (25) that secrecy array gain increases with increasing σ. It can be concluded that SOP of the system improves with higher σ. This is due to relaxing the peak interference power constraint, which in turn increases transmit power.
- The secrecy diversity gain improves with increasing the number of transmit antennas N_T.

V. NUMERICAL RESULTS

This section deals in providing the numerical results to examine the secrecy performance of SWIPT CR system. Our interest is in examining the effects of power splitting fraction ρ, quantity η (related to channel estimation), number of antennas for transmission N_T, number of EHRs N, path loss exponent κ along with number of PUs K on secrecy performance which is quantified by the secrecy outage probability P_{out}. The constant for propagation loss L_c may be arrived at as $L_c = G_T G_R \left(c/[4\pi f]\right)^2$, where G_T and G_R are transmitter and receiver antenna gains, respectively, c denotes speed of light, whereas, f is the frequency of carrier.

The parameters have been set as: $\gamma_2 = 5, 8, 10, 12, 15$ dB, $K = 1, 4, 7, 10, 13, 17$, $N = 1, 4, 7, 9, 13, 17$, $\kappa = 2.7, 2.9, 3.1, 3.3, 3.5$, $\Omega_0 = 1$, $\Omega_1 = 1$, $\Omega_w = 1$, $\gamma_p = 5$ dB, $R_S = 0.0001, 1$, $N_T = 1, 2, 3, 4, 5$, $r_1 = r_2 = 4$m, $L_c = 0.005$, $\gamma_0 = 10000$, $\gamma_p = 5$ dB, $\rho = 0.1, 0.8, 0.9$, $N_0 = 1$, $\mu^2 = 1$, and $\sigma = 0.5$ unless explicitly specified otherwise.

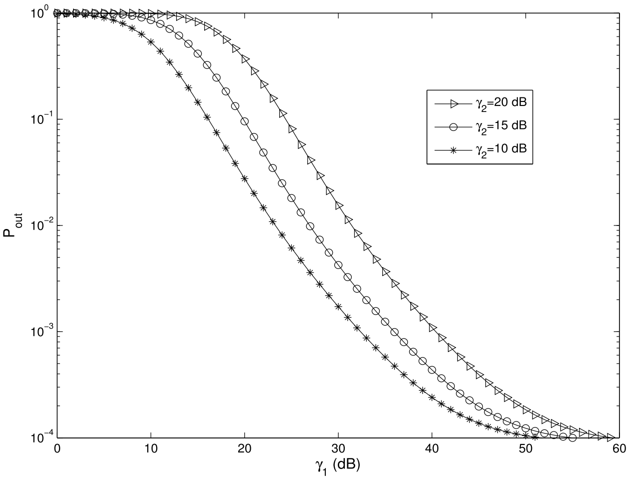

FIGURE 3. SOP versus γ_1 for varying γ_2 with $\rho = 0.9$, $\eta = 0.8$, $\gamma_2 = 10$ dB, $\gamma_p = 5$ dB, $N = 4$, $N_T = 4$, $K = 10$, $R_S = 0.0001$, $r_1 = r_2 = 4$ m, $\Omega_0 = \Omega_1 = \Omega_2 = \Omega_W = 1$, $\sigma = 0.5$, $\kappa = 3.2$, and $L_c = 0.005$.

We can see from Figure 1 that the SOP increases (P_{out} decreases) with an increase in γ_1, as an improved γ_1 means a more secure condition of channel for the link of BS-IR in comparison to the links of BS-EHR eavesdropping. It is also seen from Figure 1 that P_{out} increases with increase in ρ. This is due to the fact that a low value of ρ results in a very small amount of the signal power received that is used by message decoder and the energy harvester uses a high value of power in all EHRs; this results in a decreased value of SNR received in all of the EHRs leading to a poor capacity of eavesdropping. Figure 1 also shows that the secrecy performance improves with increase in η. The reason behind this is that an increased value of η denotes a high correlation among channel gains of links between the IR and the selected antenna for transmission at the BS. Figure 2 depicts that the secrecy performance improves with an increase in N_T because of the higher

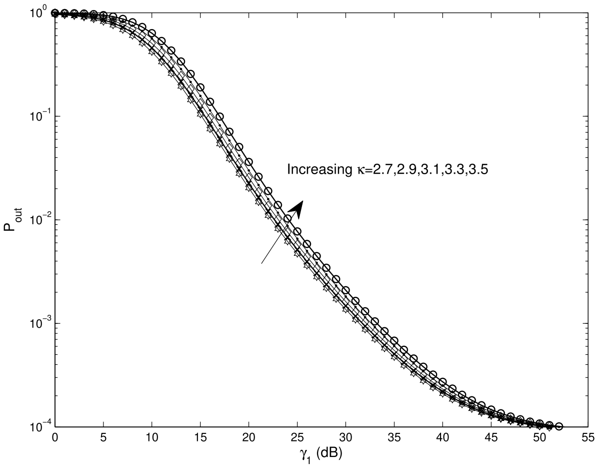

FIGURE 4. SOP versus γ_1 for varying κ with $\rho = 0.9$, $\eta = 0.8$, $\gamma_2 = 10$ dB, $\gamma_P = 5$ dB, $N = 4$, $K = 10$, $R_S = 0.0001$, $r_1 = r_2 = 4$ m, $\Omega_0 = \Omega_1 = \Omega_2 = \Omega_W = 1$, $\sigma = 0.5$, and $L_c = 0.005$.

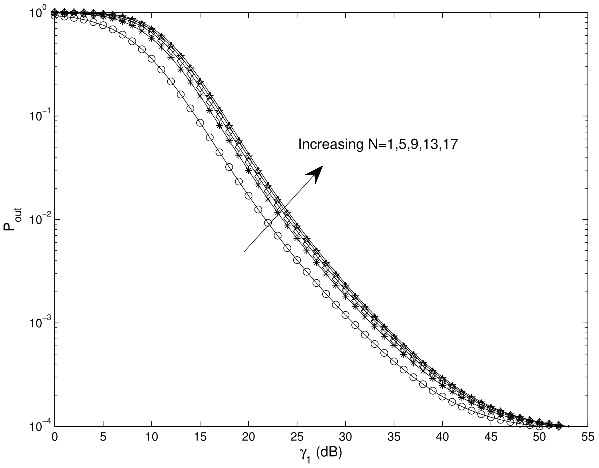

FIGURE 5. SOP versus γ_1 for varying N with $\rho = 0.9$, $\eta = 0.8$, $\gamma_2 = 10$ dB, $\gamma_P = 5$ dB, $N_T = 4$, $\kappa = 3.2$, $K = 10$, $R_S = 0.0001$, $r_1 = r_2 = 4$ m, $\Omega_0 = \Omega_1 = \Omega_2 = \Omega_W = 1$, $\sigma = 0.5$, and $L_c = 0.005$.

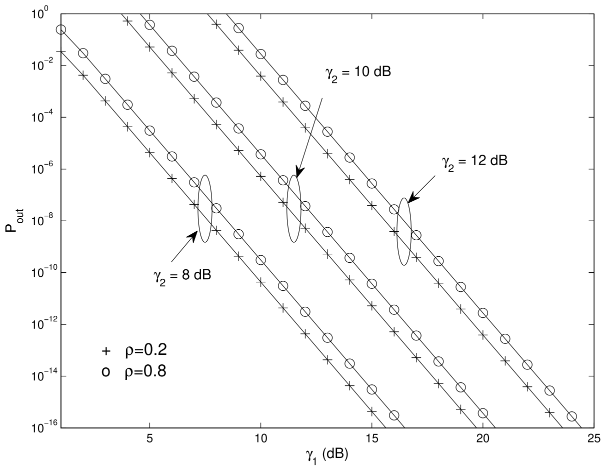

FIGURE 6. Asymptotic SOP versus γ_1 for $\gamma_P = 5$ dB, $N_T = 4$, $\kappa = 3.2$, $K = 10$, $R_S = 1$, $r_1 = r_2 = 4$ m, $\Omega_0 = \Omega_1 = \Omega_2 = \Omega_W = 1$, $\sigma = 0.5$, and $L_c = 0.005$.

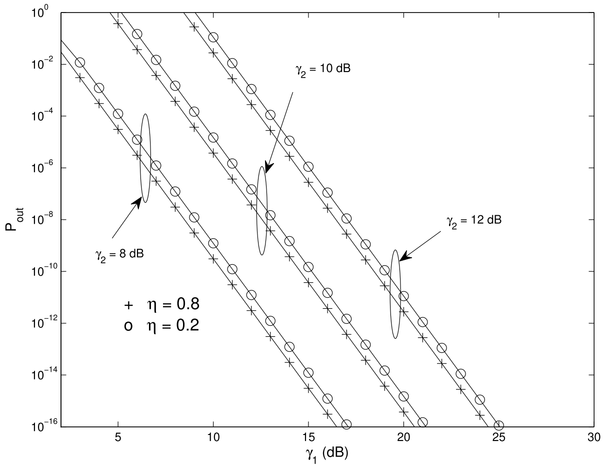

FIGURE 7. Asymptotic SOP versus γ_1 for $\gamma_P = 5$ dB, $N_T = 4$, $\kappa = 3.2$, $K = 10$, $R_S = 1$, $r_1 = r_2 = 4$ m, $\Omega_0 = \Omega_1 = \Omega_2 = \Omega_W = 1$, $\sigma = 0.5$, and $L_c = 0.005$.

diversity gain from the scheme of best antenna selection adopted at BS as N_T varies from 1 to 5. On the other hand, the P_{out} increases with increasing eavesdropper channel's SNR (i.e., γ_2) which is depicted in Figure 3. Moreover, the secrecy performance improves with decrease of κ, as shown in Figure 4. This is due to the fact that a high rate of κ shows a great loss of path suffered by the signals transmitted, that results in a lower power of received signal. The multiple EHRs have a poor secrecy performance as compared to the single-EHR, as shown in Figure 5. The reason behind this is that, at one end, the capability of eavesdropping is increased, whereas at the other end, more degrees of spatial freedom must be utilized for eavesdropper combating; so, the legitimate signal quality is accordingly decreased. It can be further proved that when eavesdroppers are in large number, the SOP reaches one.

It can be observed from Figure 6 that the considered system with a lower value of ρ outperforms that with the higher value of ρ. Further, asymptotic SOP increases with the SNR of eavesdropper channel. In Figure 7, the asymptotic SOP improves with increasing the value of η from 0.2 to 0.8. As expected, the system goes to the secrecy outage with improvement in SNR of eavesdropper.

VI. CONCLUSION

In this paper, SWIPT CR system's secrecy performance has been discussed when the CSI is imperfect. The SOP has been derived in the presence of multiple PUs for a scenario in which the confidential information from the BS to the IR can be overheard by malicious EHRs. Our results have shown that imperfect CSI a has negative impact on secrecy performance. Analysis performed in this paper will be of great use in designing the practical SWIPT CR systems that are subject to channel estimation errors.

REFERENCES

[1] L. R. Varshney, "Transporting information and energy simultaneously," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, Jul. 2008, pp. 1612–1616.

[2] P. Grover and A. Sahai, "Shannon meets Tesla: Wireless information and power transfer," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, USA, Jun. 2010, pp. 2363–2367.

[3] 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.

[4] 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.

[5] L. Liu, R. Zhang, and K.-C. Chua, "Wireless information and power transfer: A dynamic power splitting approach," *IEEE Trans. Commun.*, vol. 61, no. 9, pp. 3990–4001, Sep. 2013.

[6] 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, Sep. 2013.

[7] S. Yin, Z. Qu, and S. Li, "Achievable throughput optimization in energy harvesting cognitive radio systems," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 3, pp. 407–422, Mar. 2015.

[8] J. P. J, S. S. Kalamkar, and A. Banerjee, "Energy harvesting cognitive radio with channel-aware sensing strategy," *IEEE Commun. Lett.*, vol. 18, no. 7, pp. 1171–1174, Jul. 2014.

[9] 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.

[10] 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.

[11] 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.

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

[13] H. Lei, M. Xu, I. S. Ansari, G. Pan, K. A. Qaraqe, and M.-S. Alouini, "On secure underlay MIMO cognitive radio networks with energy harvesting and transmit antenna selection," *IEEE Trans. Green Commun. Netw.*, vol. 1, no. 2, pp. 192–203, Jun. 2017.

[14] H. Lei, H. Zhang, I. S. Ansari, Z. Ren, G. Pan, K. A. Qaraqe, and M.-S. Alouini, "On secrecy outage of relay selection in underlay cognitive radio networks over Nakagami-*m* fading channels," *IEEE Trans. Cogn. Commun. Netw.*, vol. 3, no. 4, pp. 614–627, Dec. 2017.

[15] H. Lei, C. Gao, I. S. Ansari, Y. Guo, Y. Zou, G. Pan, and K. A. 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.

[16] H. Lei, H. Zhang, I. S. Ansari, C. Gao, Y. Guo, G. Pan, and K. A. 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.

[17] M. Gans, "The effect of Gaussian error in maximal ratio combiners," *IEEE Trans. Commun.*, vol. TCOMM-19, no. 4, pp. 492–500, Aug. 1971.

[18] A. P. Liavas, "Tomlinson-Harashima precoding with partial channel knowledge," *IEEE Trans. Commun.*, vol. 53, no. 1, pp. 5–9, Jan. 2005.

[19] 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.

[20] 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, Sep. 2016.

[21] 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, Sep. 2015.

[22] V. U. Prabhu and M. R. D. Rodrigues, "On wireless channels with M-antenna eavesdroppers: Characterization of the outage probability and outage secrecy capacity," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 853–860, Sep. 2011.

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

[24] S. Sanayei and A. Nosratinia, "Asymptotic capacity analysis of transmit antenna selection," in *Proc. IEEE Int. Symp. Inf. Theory*, Chicago, IL, USA, Jun./Jul. 2004, p. 242.

[25] 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.

[26] A. Singh, M. R. Bhatnagar, and R. K. Mallik, "Physical layer security of a multiantenna–based CR network with single and multiple primary users," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 11011–11022, Dec. 2017.

[27] 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.

[28] N. Sadeque, I. Land, and R. Subramanian, "Average secrecy rate under transmit antenna selection for the multiple-antenna wiretap channel," in *Proc. IEEE 24th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, London, U.K., Sep. 2004, pp. 238–242.

[29] K. Shim, H. Oh, T. N. Do, and B. An, "A physical layer security–based transmit antenna selection scheme for NOMA systems," in *Proc. 10th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Prague, Czech Republic, Jul. 2018, pp. 597–602.

[30] Y. Deng, M. Elkashlan, P. L. Yeoh, N. Yang, and R. K. Mallik, "Cognitive MIMO relay networks with generalized selection combining," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4911–4922, Sep. 2014.

[31] A. Papoulis and S. U. Pillai, *Probability, Random Variables, and Stochastic Processes*, 4th ed. New York, NY, USA: McGraw-Hill, 2002.

AJAY SINGH (Member, IEEE) received the B.Tech. degree from Kurukshetra University, Kurukshetra, India, in 2003, and the M.E. degree from Panjab University, Chandigarh, India, in 2007, both in electronics and communication engineering, and the Ph.D. degree from the Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi, India, in 2012. From May 2013 to January 2016, he was with the Faculty of the Department of Electronics and Communication Engineering, National Institute of Technology Raipur, India. From January 2016 to March 2018, he was with the Faculty of the Department of Electronics and Communication Engineering, National Institute of Technology Hamirpur, India. Since March 2018, he has been with the Faculty of the Department of Electrical Engineering, Indian Institute of Technology Jammu, India, where he is currently an Assistant Professor. His current research interest includes physical layer security of wireless communications systems.

MANAV R. BHATNAGAR (Senior Member, IEEE) received the M.Tech. degree in communications engineering from the Indian Institute of Technology Delhi, New Delhi, India, in 2005, and the Ph.D. degree in wireless communications from the Department of Informatics, University of Oslo, Oslo, Norway, in 2008.

From 2008 to 2009, he was a Postdoctoral Research Fellow with the University Graduate Center (UNIK), University of Oslo. He held visiting appointments at the Wireless Research Group, Indian Institute of Technology Delhi, the Signal Processing in Networking and Communications (SPiNCOM) Group, University of Minnesota Twin Cities, Minneapolis, MN, USA, the Alcatel-Lucent Chair, SUPELEC, France, the Department of Electrical Computer Engineering, Indian Institute of Science, Bangalore, India, UNIK, University of Oslo, the Department of Communications and Networking, Aalto University, Espoo, Finland, and the INRIA/IRISA Laboratory, University of Rennes, Lannion, France. He is currently a Professor with the Department of Electrical Engineering, IIT Delhi, New Delhi, India, where he is also a Brigadier Bhopinder Singh Chair Professor. His research interests include signal processing for multiple-input-multiple-output systems, cooperative communications, non-coherent communication systems, distributed signal processing for cooperative networks, multiuser communications, ultrawideband-based communications, free-space optical communication, cognitive radio, software-defined radio, power line communications, molecular communications, and satellite communications.

Dr. Bhatnagar is a Fellow of the Institution of Engineering and Technology (IET), U.K., the Indian National Academy of Engineering (INAE), the National Academy of Sciences, India (NASI), the Institution of Electronics and Telecommunication Engineers (IETE), India, and the Optical Society of India (OSI). He has received the NASI-Scopus Young Scientist Award for engineering category in 2016, the Shri Om Prakash Bhasin Award in the field of Electronics and Information Technology for the year 2016, and the Hari Om Ashram Prerit Dr. Vikram Sarabhai Research Award, in 2017. He was selected as an Exemplary Reviewer of the IEEE Communications Letters, from 2010 to 2012, and an Exemplary Reviewer of the IEEE Transactions on Communications, in 2015. He was an Editor of the IEEE Transactions on Wireless Communications, from 2011 to 2014.

RANJAN K. MALLIK (Fellow, IEEE) received the B.Tech. degree in electrical engineering from the Indian Institute of Technology Kanpur in 1987 and the M.S. and Ph.D. degrees in electrical engineering from the University of Southern California, Los Angeles, in 1988 and 1992, respectively.

From August 1992 to November 1994, he was a Scientist with the Defence Electronics Research Laboratory, Hyderabad, India, working on missile and EW projects. From November 1994 to January 1996, he was a Faculty Member with the Department of Electronics and Electrical Communication Engineering, Indian Institute of Technology Kharagpur. From January 1996 to December 1998, he was with the Faculty of the Department of Electronics and Communication Engineering, Indian Institute of Technology Guwahati. Since December 1998, he has been with the Faculty of the Department of Electrical Engineering, Indian Institute of Technology Delhi, where he is currently a Professor. His research interest includes diversity combining and channel modeling for wireless communications, space-time systems, cooperative communications, multiple-access systems, power line communications, difference equations, and linear algebra. He is a member of the Eta Kappa Nu, a member of the IEEE Communications, Information Theory, and Vehicular Technology Societies, American Mathematical Society, and International Linear Algebra Society, a Fellow of the Indian National Academy of Engineering, the Indian National Science Academy, The National Academy of Sciences, India, Allahabad, the Indian Academy of Sciences, Bangalore, The World Academy of Sciences-for the advancement of science in developing countries (TWAS), The Institution of Engineering and Technology, U.K., The Institution of Electronics and Telecommunication Engineers, India, and The Institution of Engineers (India), and a Life Member of the Indian Society for Technical Education. He was a recipient of the Hari Om Ashram Prerit Dr. Vikram Sarabhai Research Award in the field of electronics, telematics, informatics, and automation, the Shanti Swarup Bhatnagar Prize in engineering sciences, the Khosla National Award, and the J. C. Bose Fellowship. He has served as an Area Editor and an Editor for the IEEE Transactions on Wireless Communications, and as an Editor for the IEEE Transactions on Communications.

• • •