Secrecy Analysis of Reconfigurable Underlay Cognitive Radio Networks With SWIPT and Imperfect CSI

Anshu Thakur, *Student Member, IEEE*, Ashok Kumar, Nitin Gupta, *Senior Member, IEEE*, and Puspita Chatterjee, *Member, IEEE*

***Abstract*—In the present work, an underlay cognitive radio network (CRN) is considered to examine the secrecy performance for Simultaneous Wireless Information and Power Transfer (SWIPT) with imperfect channel state information (CSI). The eavesdropper as well as secondary receivers are considered to have energy harvesting potential. The eavesdropper is the malicious node that tries to sniff the information from the main link and degrades the performance of the system. The maximal ratio combining (MRC) technique is considered at all the nodes to optimize the signal from multiple antennas. Further, to deal with a more practical scenario, the path losses are also considered and therefore, the imperfect CSI is considered at all the receiving nodes. The main objective is to derive the exact, intercept and asymptotic secrecy outage probability for the Rayleigh fading channel. Moreover, the best antenna selection is also considered at the secondary transmitter for data transmission. The validation of the analytical result is done with the help of Monte-Carlo simulation.**

***Index Terms*—Outdated CSI, power splitter, secrecy outage probability, simultaneous wireless information and power transfer, underlay cognitive radio network.**

I. Introduction

THE communication techniques are rapidly changing with each passing day. A rapid increase in higher data throughput increases the demand of wireless broadband network. The high performance wireless networks have led to the spectrum scarcity issue [1]. The spectrum is a limited and precious resource, and therefore is unable to meet the today's need and also the tomorrow's users need of a band. The Federal Communication Commission (FCC) allocates the spectrum for particular services and provides the spectrum with particular fees [2]. The assigned, licensed spectrum is static in nature, which means that the spectrum is unavailable to other users even if it is not used by the owner. This leads to minimizing the usage of the spectrum and also leads to the spectrum shortage. The above mentioned factors have led to the changes in the spectrum regularities processes, because the present policies are not capable of meeting the requirements. This issue leads to the concept of re-configurable Cognitive Radio (CR). Re-configurability helps in adjusting adjusting operating parameters with the dynamic radio environment easily in real time without any changes in the hardware. These operating parameters include either changing of channel frequency, change in modulation scheme as per the channel conditions or adjustment of transmission power according to the permissible power limits [3].

The CRN is an encouraging technology to resolve the issue of spectrum scarcity by authorizing the unlicensed users also acknowledged as Secondary Users (SUs) to utilize and experience the same spectrum with licensed users or Primary Users (PUs) [4]. The way in which the SU can access the licensed spectrum is classified into underlay, interweave, and overlay systems. Among these, underlay CRN is of great importance as it makes the most of the interference tolerance ability of the PUs which enables the SUs to transmit along with the PUs. Further, CRN consists of a secondary transmitter that communicates with the secondary receiver. However, the broadcast nature of the CRN results in the information leakage. The Information Leakage is defined as the exposure of the information/data to the unintentional attackers. In this case, the information is unintentionally exposed to the attackers [11]. Earlier, conventionally the cryptography techniques were used to deal with the security issues. Computational complexity of these techniques often lead to tremendous consumption of energy. To deal with the issue, the physical layer security has been comes up as an alternative to secure the network by exploiting the characteristics of the channel [5]. In today's scenario, physical layer security is used for the secure transmission of the data without dealing with complications of cryptography [6]. The concept was created on Shannon's documentation of perfect secrecy [7] and was further expanded by Wyner in [8] and Csiszar et. al in [9], in which the classical three node model was discussed. The three node model consists of a source, destination and an eavesdropper. In CRN, the secondary transmitter can increase the transmitting power for

Manuscript received August 11, 2020; revised November 3, 2020; accepted November 18, 2020. Date of publication November 25, 2020; date of current version January 11, 2022. Recommended for acceptance by Dr. Uttam Ghosh. *(Corresponding author: Nitin Gupta.)*

Anshu Thakur and Ashok Kumar are with the Department of Electronics and Communication Engineering, National Institute of Technology, Hamirpur 177005, India (e-mail: anshuthakur@nith.ac.in; ashok@nith.ac.in).

Nitin Gupta is with the Department of Computer Science and Engineering, National Institute of Technology, Hamirpur 177005, India (e-mail: nitin3041@gmail.com).

Puspita Chatterjee is with the Department of Modeling, Simulation and Visualization Engineering, Old Dominion University, Norfolk, VA 23529 USA (e-mail: puspita.c@ieee.org).

Digital Object Identifier 10.1109/TNSE.2020.3040531

improving the received signal quality at the secondary receiver, However, this also leads to information leakage and is known as eavesdropping [10].

Recently, the SWIPT [12] has achieved tremendous recognition as a beneficial Energy Harvesting (EH)[13] solution to deal with the energy-limited communication systems. The SWIPT [14] uses the same electromagnetic waves for the transmission of information and energy. The concept of simultaneous transmission of energy and information was first introduced by Varshney et. al. in [15]. This work was further extended in [16], for frequency selective channels with addition to additive white Gaussian noise. The separate power receivers and hybrid power splitter receiver were introduced in [17], [18], respectively. The Time splitting (TS) and power splitting (PS) are two beneficent approaches of SWIPT for transferring the information and energy simultaneously to the destination [19]. The SWIPT [20] technique is naturally applicable to the physical layer security techniques. From the studies, it has been observed that with the increased signal to noise (SNR) ratio the secrecy capacity of the system decreases. To deal with this problem, MRC and multiple antenna consideration is an optimal solution as it utilizes all the diversity paths. The impact of the MRC scheme was studied in [21]. Till now a few work has been done for the secrecy analysis, however, to the best of knowledge, the present literature mostly works in secrecy performance with SWIPT and CRN, but limited to the perfect CSI. In the actual scenario, the perfect CSI is very hard to achieve due to inaccurate estimation of the signal, transmission delay, or wave spreading of the electromagnetic wave which leads to estimation error [22].

In the rest of the paper, In section II, related work is discussed followed by section III, which explains the system model. In section IV and V, Secrecy Outage Probability (SOP) and Asymptotic SOP of the considered system is derived respectively, followed by numerical analysis and the conclusion in section VI and VII respectively.

II. Related Works

In the literature, it has been found that use of the CRN raises security concern. To overcome this, authors in [23] considered the cognitive wiretap channel with multiple antennas for securing the transmission at the physical layer. The eavesdropper was considered to overhear the information that's being send from the secondary transmitter to the receiver. Further, the passive eavesdropping was considered and closed-form expressions for exact and asymptotic SOP were derived. The secrecy performance for underlay CRN over log-normal and Rayleigh fading in the presence of single eavesdropper was investigated in [24]. Zhao et. al. in [25] considered multiple-input multiple-output (MIMO) system with CRN to perform the secrecy outage in the presence of transmit antenna selection (TAS) scheme with selection combining (SC) and MRC. The MRC scheme is considered in MIMO system to optimize the received signal. The TAS is a less complicated and economic method to maximum avail the advantage of a MIMO system [26].

The dominant disadvantage of above discussed literature is that the CSI is considered to be perfectly known. Therefore, Zhu et. al. in [27] derived a sub-optimal antenna selection scheme (SAS) and optimal antenna selection (OAS) scheme depending upon the factor whether the global CSI is present on the source or not. Authors in in [28] proposed the resource allocation algorithm with downlink multiple input single output (MISO). This scheme was proposed to lower the net transmitted power in the presence of a potential and passive eavesdropper. Pei et. al. in [29] considered the multi-antenna for secure communication with imperfect CSI and CRN. The imperfect CSI and underlay CRN were also considered in [30], [31] to deal with secrecy performance of the system. However in our work, the SWIPT architecture is considered at the secondary transmitter as well as on eavesdropper and imperfect CSI is also considered at all the nodes.

The wireless networks are also having a bottleneck issue of limited network lifetime. These networks can be self sustaining with the help of radio frequency EH. Therefore, considering the fact, the CRN was discussed with EH technology in [32]. The throughput maximization analysis of CR based EH was done in [33]. In this model, the authors considered the secondary receiver with the finite battery while EH based receivers acted as an eavesdropper to represent the worst scenario. In [34] the output of a CRN having EH is achieved through a slotted mode. In this case, the SU sources are assumed to strengthen the EH with the use of natural resources.

The secrecy performance of SWIPT with multiple-input-single-output was discussed in [35]. Authors considered transmitter with multiple antennas that transmit information and energy simultaneously to the information receiver and multiple energy harvesting. Lei et. al. in [36] derived the SOP with OAS and SAS for considered MIMO and EH system. Further, the CRN with SWIPT architecture was investigated with a relay system in [37]. The joint optimal relay selection scheme and power allocation were discussed to minimize the consumption of energy and maximize the secrecy performance. The best relay selection scheme was also considered in [38] which proposed the dynamic power allocation and best relay selection scheme. Authors in [39] considered a MIMO system with an EH constraint to study the beamforming designs with partial CSI. In [40], the imperfect CSI was considered with SWIPT to improve the secrecy performance of the system. The imperfect CSI with transmit antenna selection (TAS) was studied by Lei at. al.in [41]. Authors in [23] considered the power constraint primary network. Authors applied the secondary network as well as eavesdropper with SC with multiple antennas. However, power constraint with imperfect CSI, MRC and SWIPT architecture is considered in our work. Distinct from all preceding works, The MRC technique with SWIPT architecture is proposed at the legitimate receiver for providing a protected transmission of data in Rayleigh fading. The considered MRC diversity combining technique, combines the signals coming from all the diversity paths and provides the coherent inclusion to maximize the signal to noise

TABLE I
MAIN NOTATIONS USED IN THE PAPER

Symbols/Notation	Definition
MRC	Maximal Ratio Combining
P_{avg}	Average Transmission Power
ρ	Power splitting factor
P_T	maximum power transmitted from secondary transmitter
P_I	Peak interference power
h_{main}	Channel gain estimated by main channel
h_E	Channel gain estimated by eavesdropper's channel
η	Estimation error
R_s	Data Rate
N_R	Antennas at secondary receiver
N_P	Antennas at primary users
N_T	Antennas at secondary transmitter
N_E	Antennas at eavesdropper
γ_{main}	Main channel's SNR
γ_E	SNR of the E channel
S_T	Secondary transmitter
S_R	Secondary receiver
E	Eavesdropper
PU	Primary users
P_{loss}^{total}	Path loss constant
C_{main}	Main channel capacity
C_E	Eavesdroppers channel capacity

ratio (SNR) at the receiver. The MRC diversity technique is used as its the optimal technique. Considering the above factors, the imperfect CSI with SWIPT and underlay CRN is propsed in this paper to represent a more practical scenario. The intercept, exact and asymptotic SOP is derived considering the best antenna selection scheme at the secondary transmitter. The TAS scheme is used to secure the communication over the Rayleigh fading. The Rayleigh model represents a statistical model considering the effect of the propagation environment on radio frequency signals.

A. Contribution

The main contributions of the present work are as follows:

(1) The secrecy performance of an underlay CRN is studied. The underlay CRN consists of SWIPT architecture and imperfect CSI over the Rayleigh fading environment with multiple antennas at the primary nodes, the secondary nodes and the eavesdropper. The closed form expression for exact and asymptotic SOP is derived. In comparison to [10] the SWIPT architecture is considered in our work having PS architecture at S_R and E.

(2) The intercept probability (the chances of occurring an intercept event) is also studied for the considered system model. Furthermore, the best antenna selection scheme is also opted at the secondary transmitter. Compared with [36] the imperfect CSI is considered having an underlay CRN with power constraint.

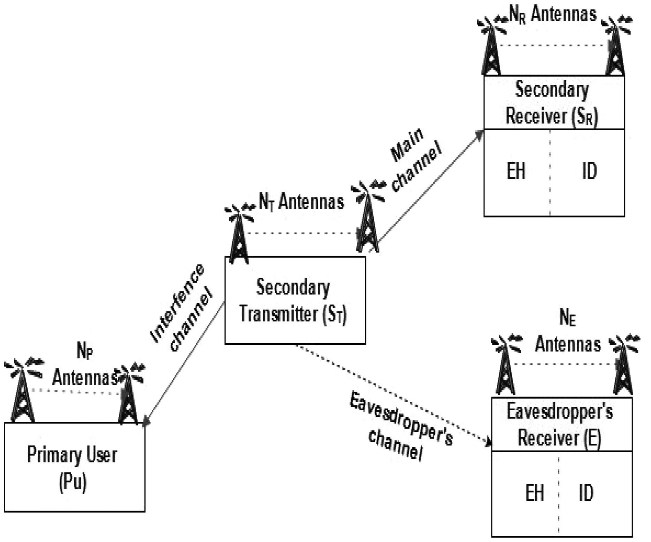

Fig. 1. System Model with primary user (PU), secondary transmitter (S_T), secondary receiver (S_R) and eavesdropper (E).

(3) The influence of power splitting factor ρ is also studied on the secrecy performance of the secondary networks with imperfect CSI. Moreover, the impact of the MRC technique on SOP is also characterized by SWIPT and imperfect CSI.

(4) In comparison to [23], [25] the imperfect CSI is considered in our work with SWIPT architecture to present a more practical and advance scenario.

III. System Model

The system model consists of a PU and cognitive radio transmitter (S_T) which communicates with the cognitive radio receiver (S_R) under the vicious attempt of an eavesdropper (E). The received message at S_R or E (due to eavesdropping) is having the capacity of information decoding (ID) and EH, as the SWIPT system is considered on these nodes. The main objective is secure transmission of the information from S_T to S_R by strictly meeting the interference constraint at the PU. All the nodes i.e. S_T, S_R, E, and PU are having $N_T \geq 1$, $N_R \geq 1$, $N_E \geq 1$, and $N_p \geq 1$ antenna respectively. Further, to ensure a practical scenario, all the nodes are considered to have the imperfect CSI. While considering the underlay CRN, the transmitted power at S_T should be controlled under a peak interference threshold power for reliable and secure communication at the PU. The main symbols/notations are discussed in Table I and system model is summarized in Fig. 1.

The transmitted power (P_T) of S_T can be given as follows [23]:

$$P_T = min\left(\frac{P_I}{|h_m|^2}, P_{avg}\right) \tag{1}$$

where, P_{avg} is the average transmission power at S_T, P_I denotes the peak interference power at the PU, h_m denotes the fading coefficient S_T to the PU having Ω_0 variance and zero mean. Considering that S_T transmit signal 't' with P_T power, the signal received at S_R can be written as:

$$Y_t^{total} = \left(\sqrt{\frac{P_T}{P_{loss}^{total}}}\hat{h}_{main}(t) + v_t\right) \tag{2}$$

where, $P_{loss}^{total} = (\frac{d_u^\alpha}{L_c})$ denotes the constant of path loss, d_u denotes the total distance, $(u \in (d_{main}, d_E))$, where d_{main} represents the distance between the S_T and S_R, while, the d_E represents the distance between the S_T and E. Further, L_c is the propagation loss constant, α represents the path loss exponent, $\hat{h}_{main}$ denotes the estimated channel gain, and v_t denotes the Additive White Gaussian Noise (AWGN) with zero mean and variance N_0. As, the power splitting (PS) architecture is adopted at S_R and E, the power splitter uses a factor $(0 \leq \rho \leq 1)$ for ID and remaining $(1 - \rho)$ for EH. Therefore, the signal received at S_R and E after applying the power splitting architecture is written as [42] :

$$Y_R = \sqrt{\rho_1}\left(\sqrt{\frac{P_T}{P_{loss}^t}}\hat{h}_t(t) + v_t\right) + z_t \tag{3}$$

where, $P_{loss}^t = (\frac{d_t^\alpha}{L_c})$ denotes the constant of path loss, d_t represents the distance between S_T to S_R, $\hat{h}_t$ denotes the estimated channel gain of main channel, ρ_1 is the power splitting factor at main channel and z_t represents the signal processing noise. The signal received at E after applying the SWIPT technique is given as [42]:

$$Y_e = \sqrt{\rho_2}\left(\sqrt{\frac{P_T}{P_{loss}^e}}\hat{h}_e(e) + v_e\right) + z_e \tag{4}$$

$\hat{h}_e$ denotes the channel gain of eavesdropper's channel, v_e denotes the AWGN and z_e is the processed signal noise, ρ_2 is the power splitting factor at eavesdropper's channel, and as mentioned before, the imperfect CSI is considered. Therefore, the channel estimation error at the receiver node is given as [21] :

$$\hat{h}_u = \sqrt{(1 - \eta_u^2)}h_u + \sqrt{\eta^2}n_u \tag{5}$$

where, $(u \in main, E, PU)$, and h_u represents the exact gain of the channel, n is a normal random variable distribution having zero mean and variance one. The parameter η_u represents the measure of accuracy of estimation, where $\eta_u = 0$ indicates the perfect CSI. Therefore, the main channel's instantaneous signal to noise (SNR) ratio can be expressed as [42]:

$$\gamma_{main} = \frac{\rho_1\zeta_t(1 - \eta_1^2)}{(\zeta_t\rho_1\eta_1^2 + \rho_1 N_0 + \sigma_t.^2)}\sum_{i=0}^{N_R}|h_{main}|^2 \tag{6}$$

and the SNR of eavesdroppers channel is expressed as [42] :

$$\gamma_E = \frac{\rho_2\zeta_e(1 - \eta_2^2)}{(\zeta_e\rho_2\eta_2^2 + \rho_2 N_0 + \sigma_e.^2)}\sum_{j=0}^{N_E}|h_E|^2 \tag{7}$$

where, $\zeta_t = \frac{P_T}{P_{loss}^t}$, $\zeta_e = \frac{P_T}{P_{loss}^e}$, h_{main}, h_E represents the channel gain of main channel and eavesdropper's channel respectively. Further, η_1, η_2 represents the estimation error of the main channel and eavesdroppers channel respectively, σ_t is the variance of main channel and σ_e is the variance of eavesdropper channel. Further, as the transmit power at S_T is strictly constrained and is denoted by the P_T at S_T from which the instantaneous SNR at S_R and E are represented as [23]:

$$\gamma_{main} = A_1\left(\frac{\gamma_I}{X}, \gamma_0\right)\sum_{i=0}^{N_R}|h_{main}|^2 \tag{8}$$

and the instantaneous SNR at eavesdropper channel is given as [23]:

$$\gamma_E = A_2\left(\frac{\gamma_I}{X}, \gamma_0\right)\sum_{j=0}^{N_E}|h_E|^2 \tag{9}$$

where, $\gamma_I = \frac{P_I}{N_0}$, $\gamma_0 = \frac{P_{avg}}{N_0}$, $A_1 = \frac{\rho_1\zeta_t(1-\eta_1^2)}{(\zeta_t\rho_1\eta_1^2+\rho_1 N_0+\sigma_t.^2)}$, $A_2 = \frac{\rho_2\zeta_e(1-\eta_2^2)}{(\zeta_e\rho_2\eta_2^2+\rho_2 N_0+\sigma_e.^2)}$ and $X = |h_u|^2$ represent the channel gain of main and eavesdropper channel i.e. $(u \in (main, e))$.

IV. Secrecy Outage Probability

The secrecy capacity C_s of the system is defined as [23] :

$$C_s = \begin{cases} C_{main} - C_E = log_2\left(\frac{1+\gamma_{main}}{1+\gamma_E}\right) & \text{if } \gamma_{main} \geq \gamma_E \\ 0 & \text{if } \gamma_{main} \leq \gamma_E \end{cases} \tag{10}$$

where, $C_{main} = log_2(1 + \gamma_{main})$ denotes the capacity of the main channel and $C_E = log_2(1 + \gamma_E)$ represents the capacity of the malicious eavesdropper channel. SOP is defined as a condition in which the data rate is greater than the channel capacity of the system i.e. $(R_s \geq C_s)$. In such a situation the theoretical security of the system is compromised. The notation of SOP is P_{out} and is defined as [23]:

$$\begin{aligned} P_{out} = Pr(R_s < C_s) &= Pr(\gamma_{main} \geq \gamma_E) \\ &+ Pr(\gamma_{main} \leq \gamma_E)Pr(C_s < R_s\ \gamma_{main} > \gamma_E) \end{aligned} \tag{11}$$

This can further be resolved as [23]:

$$\begin{aligned} P_{out} = \textstyle\int_0^\infty \int_0^\infty F_{\gamma main(X=x)}(\varepsilon\gamma_E)f_{\gamma_{ER_x|(X=x)}}(\gamma_E) \\ f_x(x)d\gamma_E dx \end{aligned} \tag{12}$$

Here, $f_{\gamma_{E|(X=x)}}$ denotes the probability distribution function (PDF) of γ_E conditioned on X and $f_x(x)$ is the PDF of the PU channel, $F_{\gamma_{main(X=x)}}(\varepsilon\gamma_E)$ represents the cumulative distributive function (CDF) of γ_{main} conditioned on X. Further,

$$(\varepsilon\gamma_E) = 2^{R_s}(1 + \gamma_E) - 1$$

The main channel's average SNR is given by $\gamma_1 = \Omega_1 \gamma_0$ and the average SNR of E channel is $\gamma_2 = \Omega_2 \gamma_0$. The Ω_1 and Ω_2 represents the variance of main channel and eavesdropper's channel respectively, having value equal to 1. The MRC technique is adopted in the present analysis with outdated CSI for the primary channel. Therefore, the PDF of primary channel is given as [42]:

$$f_x(X) = e^{-\frac{xA_3}{\Omega_0}} \frac{(A_3)^{N_p-1} x^{N_p-1}}{{\Omega_0}^{N_p}(N_p-1)!} \tag{13}$$

where, $A_3 = \frac{(1-\eta_3^2)}{(\eta_3^2+N_0+1)}$, η_3 is channel estimation error of the PU and N_0 denotes the mean of the system. However, the eavesdropper and main channels are having the SWIPT system with PS technique with outdated CSI. Therefore, in such a situation the PDF and CDF for eavesdropper's channel and main channel respectively are as follows [42]:

$$f_{\gamma_E|X=x}(\gamma_E) = \begin{cases} e^{-\frac{\gamma_E A_2}{\gamma_0}} \frac{(A_2)^{N_E} {\gamma_E}^{N_E-1}}{{\gamma_0}^{N_E}(N_E-1)!} & \text{if } X \geq \frac{\gamma_I}{\gamma_0} \\ e^{-\frac{\gamma_E A_2 X}{\gamma_E}} \frac{(A_2)^{N_E} {\gamma_E}^{N_E-1} X^{N_E-1}}{{\gamma_I}^{N_E}(N_E-1)!} & \text{if } X \leq \frac{\gamma_I}{\gamma_0} \end{cases} \tag{14}$$

and the CDF of the main channel is given as follows [42]:

$$F_{\gamma main|X=x}(\varepsilon\gamma_E) = \begin{cases} 1 - \left(exp^{-\frac{A_1 \epsilon \gamma_E}{\gamma_0}} \sum_{k=0}^{N_R-1} \frac{1}{k!} (\frac{A_1 \varepsilon \gamma_E}{\gamma_0})^k \right) & \text{if } X \geq \frac{\gamma_I}{\gamma_0} \\ 1 - \left(exp^{-\frac{A_1 \varepsilon \gamma_E X}{\gamma_p}} \sum_{k=0}^{N_R-1} \frac{1}{k!} (\frac{A_1 \varepsilon \gamma_E x}{\gamma_p})^k \right) & \text{if } X \leq \frac{\gamma_I}{\gamma_0} \end{cases} \tag{15}$$

Now, substituting the value of equation (12),(13) and (14) into equation (12) to derive the exact SOP. The closed form expression for exact SOP is as follows:

$$P_{out} = \int_0^\infty \int_0^\infty \Bigg[e^{-\frac{\gamma_E A_2}{\gamma_2}} \frac{(A_2)^{N_E} {\gamma_E}^{N_E-1}}{{\gamma_2}^{N_E}(N_E-1)!} - \Bigg(exp^{-\frac{A_1 \epsilon \gamma_E}{\gamma_1}} \sum_{k=0}^{N_R-1} \frac{1}{k!} \left(\frac{A_1 \varepsilon \gamma_E}{\gamma_1} \right)^k \times e^{-\frac{\gamma_E A_2}{\gamma_2}} \frac{(A_2)^{N_E} {\gamma_E}^{N_E-1}}{{\gamma_2}^{N_E}(N_E-1)!} \Bigg) \Bigg] e^{-\frac{xA_3}{\Omega_0}} \frac{(A_3)^{N_p-1} x^{N_p-1}}{{\Omega_0}^{N_p}(N_p-1)!} \tag{16}$$

Now, dividing the equation in parts

$$P_{out} = \int_0^\infty \int_0^\sigma \Bigg[e^{-\frac{\gamma_E A_2}{\gamma_2}} \frac{(A_2)^{N_E} {\gamma_E}^{N_E-1}}{{\gamma_2}^{N_E}(N_E-1)!} - \Bigg(exp^{-\frac{A_1 \epsilon \gamma_E}{\gamma_1}} \sum_{k=0}^{N_R-1} \frac{1}{k!} \left(\frac{A_1 \varepsilon \gamma_E}{\gamma_1} \right)^k \times e^{-\frac{\gamma_E A_2}{\gamma_2}} \frac{(A_2)^{N_E} {\gamma_E}^{N_E-1}}{{\gamma_2}^{N_E}(N_E-1)!} \Bigg) \Bigg] e^{-\frac{xA_3}{\Omega_0}} \frac{(A_3)^{N_p-1} x^{N_p-1}}{{\Omega_0}^{N_p}(N_p-1)!} + \int_0^\infty \int_\sigma^\infty e^{-\frac{\gamma_E A_2 X}{\gamma_E}} \frac{(A_2)^{N_E} {\gamma_E}^{N_E-1} X^{N_E-1}}{{\gamma_I}^{N_E}(N_E-1)!} - \Bigg(exp^{-\frac{A_1 \varepsilon \gamma_E X}{\gamma_p}} \sum_{k=0}^{N_R-1} \frac{1}{k!} \left(\frac{A_1 \varepsilon \gamma_E x}{\gamma_p} \right)^k e^{-\frac{\gamma_E A_2 X}{\gamma_E}} \frac{(A_2)^{N_E} {\gamma_E}^{N_E-1} X^{N_E-1}}{{\gamma_I}^{N_E}(N_E-1)!} e^{-\frac{xA_3}{\Omega_0}} \frac{(A_3)^{N_p-1} x^{N_p-1}}{{\Omega_0}^{N_p}(N_p-1)!} \Bigg) \tag{17}$$

Further, solving the equation (17) the expression is as follows:

$$P_{out} = \left(1 - \sum_{k=0}^{N_R-1} \sum_{h=0}^{k} \binom{k}{h} \frac{exp^{-\iota}(A_1)^k \kappa}{\gamma_1^k k!(N_E-1)!} \frac{(N_E+h-1)!}{\phi^{N_E+h}} \times \frac{(A_2)^{N_E}}{(\gamma_2)^{N_E}} \right) \times \left(1 - \sum_{u=0}^{N_p-1} \frac{A_3^{N_p}}{{\gamma_0}^{N_p} u!} \frac{\sigma^u}{(\frac{A_3}{\gamma_0})^{M_2}} \right) + \Bigg(\sum_{k=0}^{N_R-1} \times \sum_{h=0}^{k} \sum_{f=0}^{M_1} \frac{\kappa A_1^k}{k! \sigma \gamma_1^k} \frac{\phi_2(\sigma)^{-(N_E+h)}}{(N_E-1)!(N_p-1)!} \frac{(N_E+h-1)!}{(\sigma\gamma_2)^{N_E} f! {\gamma_0}^{N_p}} \times \frac{M_1!(A_2)^{N_E} {A_3}^{N_p} \sigma^f e^{\sigma\phi_2}}{\phi_2^{M_1+1} {\gamma_0}^{N_p}} \Bigg) \tag{18}$$

where, $\phi_1 = (\frac{\iota}{\sigma} + \frac{A_2}{\sigma\gamma_2})$, $\phi_2 = (\frac{(2^{R_s}-1)A_1}{\sigma\gamma_1} + \frac{A_3}{\gamma_0})$, $M_1 = (K + N_p - h - 1)$, $M_2 = (N_p - u)$, $\iota = \frac{2^{R_s} A_1}{\gamma_1}$ and $\kappa = (2^{R_s}-1)^{k-h}(2^{R_s})^h$

A. Antenna Selection Scheme

In a practical situation, it is not possible to co-phase the transmitted signals from variant antennas. Therefore, to avoid the complications, one of the feasible solutions is to opt for the best antenna for the information transmission. The SOP for antenna selection scheme is defined as [22]:

$$P_{out}^{TAS} = P(\underset{l=1..N_T}{max} C_{s_l} \leq R_s) = (P_{out})^{N_T} \tag{19}$$

After considering the equation (19), the S_T is fed with the best channel. As, it is economic option to transmit on the channel having the best SNR to avoid the destructive interference.

B. Intercept Probability

An intercept probability is a condition in which the eavesdropper's channel capacity is more than the main channel capacity, it can also be defined as [22]: $P_{in} = (C_{main} \leq C_E)$. Comparing the equation (18) with equation (10), one can observe that if $R_s = 0$, as mentioned in section (3) the $\varepsilon\gamma_E = 2^{R_s}(1+\gamma_E) - 1$. Putting this value in equation (15) and further solving this, the $\varepsilon\gamma_E$ will become equal to γ_E. The CDF of main channel will become:

$$F_{\gamma main|X=x}(\varepsilon\gamma_E) = 1 - \left(exp^{-\frac{A_1\gamma_E}{\gamma_1}} \sum_{k=0}^{N_R-1} \frac{1}{k!} \left(\frac{A_1\gamma_E}{\gamma_1} \right)^k \right) \tag{20}$$

using equation (20), (13) and (14) in equation (12), the intercept probability for $N_P = 1$ is calculated as follows:

$$P_{in} = \sum_{k=0}^{N_R-1} \frac{1}{(N_E-1)!} \left(\frac{A_1 A_2}{\gamma_1 \gamma_2} \right)^t \frac{(N_E+k-1)!}{\left[\frac{A_1}{\gamma_1} + \frac{A_2}{\gamma_2} \right]^t} \tag{21}$$

where, $t = (N_E + k)$. This equation (21) represents the case in which E is close to S_T and leads to $R_S = 0$. This event occurs when the eavesdropper's link is better than the main link. The

E will successfully decode the source message and easily intercept the information.

V. Asymptotic Secrecy Outage Probability

The asymptotic SOP expressions are derived for the higher SNR region of operations. The asymptotic SOP curve approximates the exact SOP at higher SNR region. Here, considering the higher SNR region means the S_R is assumed to be closer to S_T and therefore, the SNR of the region become higher and assumed to be infinity. Therefore the CDF of main channel is rewritten as:

$$F_{MRC}^{\infty} = \frac{(A_1 \epsilon \gamma_E)^{N_R}}{\gamma_1} + O(x) \tag{22}$$

The above mentioned expression is derived by applying taylor series expansion to equation (15). The Taylor expansion is [21].

$$\sum_{r=0}^{k-1} \frac{(x)^r}{r!} = e^x - \frac{x^k}{k!} + O(x^k)$$

The $O(x)$ represents the higher order terms. Using $(\varepsilon\gamma_E) = 2^{R_s}(1+\gamma_E) - 1$ and $(a+b)^n = \sum_{k=0}^{n} \binom{k}{h} (a)^k + (b)^{n-k}$ in equation (22), and further putting equation (22), (13) and (14) in equation (12) we get the expression as:

$$\begin{aligned} P_{out}^{\infty} = & \int_0^{\infty}\int_o^{\infty} \frac{(A_1)^{N_t}}{\gamma_1} \sum_{k=0}^{N_R} ((2^{R_s}\gamma_E)^k)(2^{R_s}-1)^{N_R-k} \\ & e^{-\frac{xA_3}{\Omega_0}} \frac{(A_3)^{N_p-1} x^{N_p-1}}{{\Omega_0}^{N_p}(N_p-1)!} e^{-\frac{\gamma_E A_2}{\gamma_0}} \frac{(A_2)^{N_E}{}^{N_E-1}}{{\gamma_0}^{N_E}} \\ & \frac{\gamma_E}{(N_E-1)!} \end{aligned} \tag{23}$$

Further solving the expression, for asymptotic SOP is derived as [21] :

$$P_{out}^{\infty} = (G_A \gamma_1)^{-G_D} + O(\gamma_1^{-G_D}) \tag{24}$$

Here, the G_D denotes the diversity order and G_A is the array gain of the system and the value of $G_D = 1$.

$$\begin{aligned} P_{out} = & \Bigg[\Bigg(1 - \sum_{k=0}^{N_R-1}\sum_{h=0}^{k} \frac{(A_1)^{N_R}\kappa}{N_R!(N_E-1)!} \frac{(A_2)^{N_E}}{(\gamma_2)^{N_E}}\Bigg) \\ & \times \Bigg(1 - \sum_{u=0}^{N_p-1} \frac{A_3^{N_p}}{\gamma_0^{N_p} u!} \frac{\sigma^u}{(\frac{A_3}{\gamma_0})^{M_2}}\Bigg) + \Bigg(\sum_{k=0}^{N_R-1}\sum_{f=0}^{M_1} \\ & \frac{\kappa A_1^k}{N_R!} \frac{(A_2)^{N_E}}{(\sigma\gamma_2)^{N_E}(N_E-1)!} \frac{(N_E+k-1)!}{\phi_3} \\ & \frac{(A_3)^{N_p} e^{-\frac{\sigma A_3}{\gamma_0}}}{(\gamma_0)^{N_p}(N_p-1)!} \frac{M_1!(\sigma)^f}{f!\frac{A_3}{\gamma_0}^{M_3}}\Bigg)\Bigg]^{-1} \end{aligned} \tag{25}$$

where, $M_3 = N_R + N_p - k$.

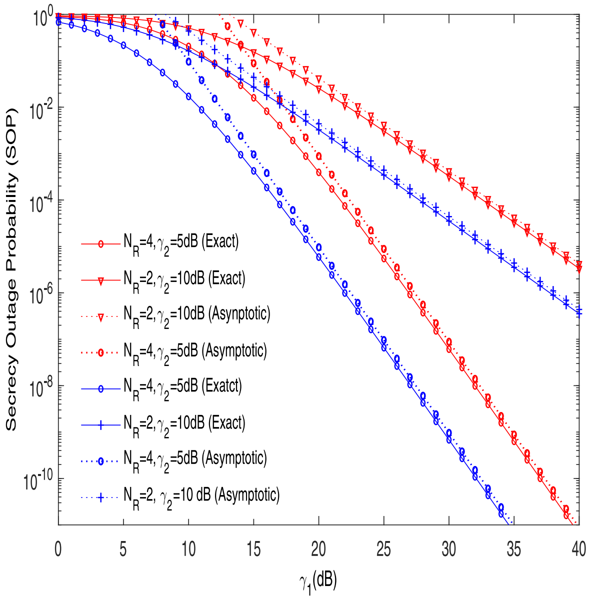

Fig. 2. SOP with γ_1 for $N_p = N_E = N_T = 2$, $\rho_1 = \rho_2 = 0.5$ and $\sigma = 1$.

VI. Numerical Analysis

This section provides the impact of SWIPT, imperfect CSI, and antenna selection scheme over underlay CRN. The main purpose is to study the effect of η_1, ρ_1, and N_T on the secrecy performance of the system. The main parameters used for the analysis are $R_s = 1nat/sec/Hz$, and α which represents the path loss having range from 2.7 to 3.5. Further, the values of $d_1 = d_2 = 10\ m$, $\sigma = 1$ and $\eta_3 = 0.5$ are considered throughout the analysis. Further, MRC technique is adopted at all channels to optimize the performance. The impact of intercept, exact and asymptotic SOP is further studied for SWIPT system with imperfect CSI and best antenna selection at S_T. In Fig. 2 the SOP is plotted against γ_1 for different values of N_R and γ_2. The parallel slope of asymptotic SOP with respect to exact SOP reveals that it is independent of γ_2 and N_R. The secrecy of the system increases with increasing value of N_R and also decreases with increasing value of γ_2. This is because the secrecy of the system is an increasing function of N_R and decreasing function with γ_2. Next, in Fig. 3, it is analyzed that the increasing value of γ_1 increases the SOP of system. The increased value of γ_1 concludes a stronger channel link between S_T and S_R in comparison to S_T to E.

The secrecy decreases with increasing value of ρ_1. This is due to the fact that more power is present for the ID and with the increasing value of ρ_1, the system also become more vulnerable to eavesdropping. Next, the Fig. 4 represents the SOP with increasing value of ρ_1 shows the more power is present for ID of the signal. The more the number of antennas i.e. N_R, the better is the security of system. Further, as the CSI tends towards perfect where $\eta = 0$ represents the perfect secrecy, the security of the system increases. At last, the Fig. 5 represents the intercept probability and SOP for the different number of transmitter antennas. An improved SOP and intercept probability can

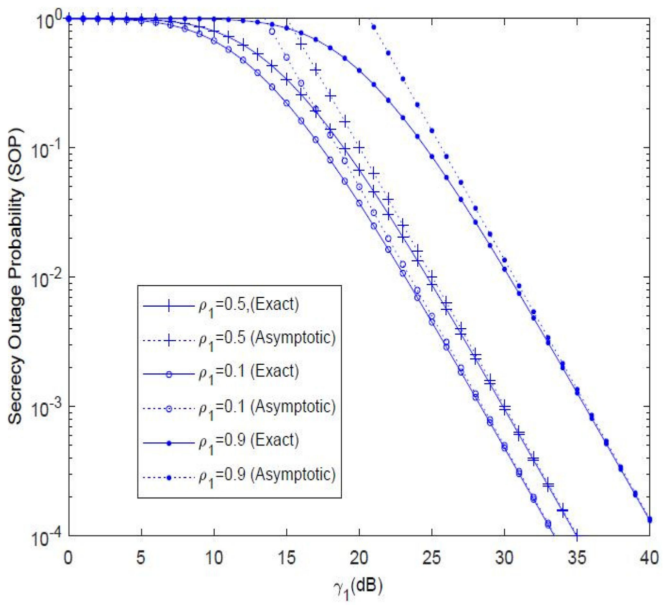

Fig. 3. SOP with γ_1 for $N_p = N_E = N_T = 2,$, $\eta_1 = \eta_2 = \eta_3 = \rho_2 = 0.5$, and $\sigma = 1$.

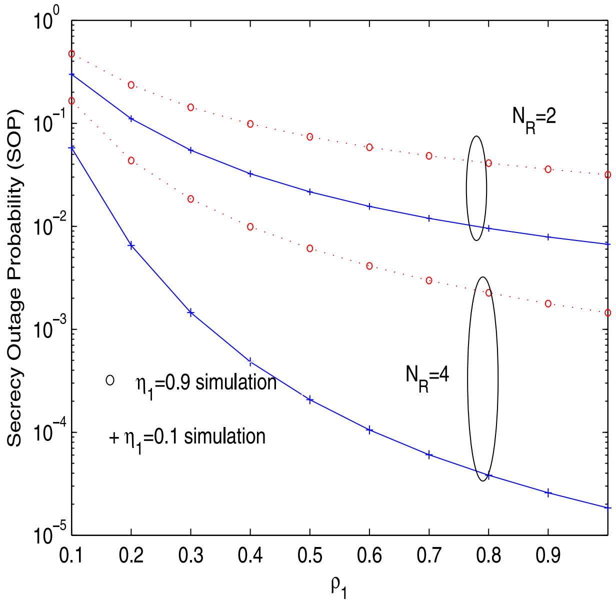

Fig. 4. SOP with ρ_1 for $N_p = N_E = N_T = 2, \rho_2 = 0.5, \eta_2 = \eta_3 = 0.5$ and $\sigma = 1$.

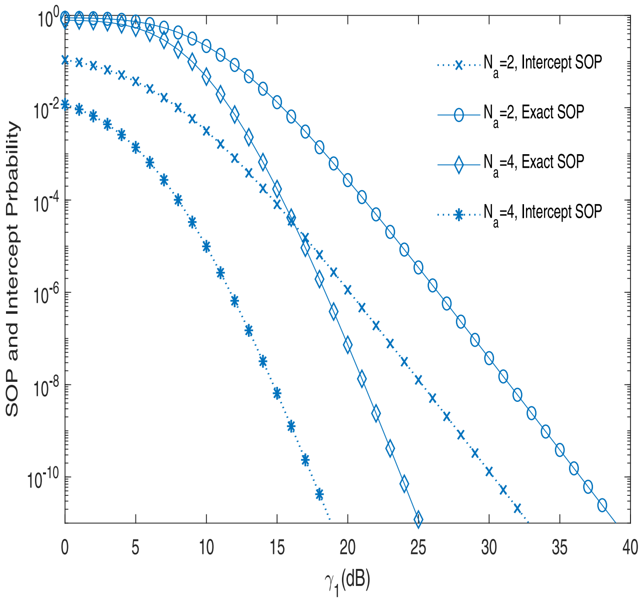

Fig. 5. SOP with γ_1 for $N_p = N_E = 2, \rho_1 = \rho_2 = 0.5$, and $\eta_1 = \eta_2 = \eta_3 = 0.5$.

be attained by adding the number of antennas as adding more antennas provide power gain to the S_T through receiving diversity, and the E will be unable to obtain this. Moreover, the security of intercept and SOP increases with an increasing number of antennas at the transmitter. In Monte-Carlo simulation 100 number of trials are considered having γ_1 from 0:40 (dB). The considered value of γ_2 is 5 dB. The R_s considered for the exact and asymptotic SOP is 1. whereas, for intercept SOP $R_s = 0$. The distance between main channel i.e. d_1 and eavesdropper's channel is 5 m. In this paper, the impact of the SWIPT architecture is studied on the security performance of the underlay CRN in a Rayleigh fading situation. The compact expressions and graphs reveals that secrecy increases with increasing number of antennas and is reciprocal for the value of ρ. The low value of ρ means that less signal is used for ID and more for EH. This affects the secrecy of the system also as the system tends towards the perfect CSI i.e η_0 the secrecy of the system increases..

VII. Conclusion

In this work, the intercept and secrecy outage probability is studied for underlay CRN with SWIPT and imperfect CSI. The analysis is studied in the presence of multiple antennas at all the nodes and to opt for the best antenna selection scheme at the transmitter. The present results reveal that the secrecy improves with increasing number of antennas and decreases with the SNR of the channel. Furthermore, the imperfect CSI has a negative impact on the system performance. The present analysis can be helpful to design practical CRN system with channel estimation errors and EH system.

References

[1] M. Matinmikko *et al.*, "Cognitive radio: An intelligent wireless communication system," *VTT Tech. Res. Centre Finland, Tech. Rep*, 2008.

[2] X. Zhou, M. Sun, G. Y. Li, and B.-H. F. Juang, "Intelligent wireless communications enabled by cognitive radio and machine learning," *China Commun.*, vol. 15, no. 12, pp. 16–48, 2018.

[3] N. Gupta, S. K. Dhurandher, and B. Kumar, "Cognitive radio networks: A comprehensive review," in *Proc. Handbook Res. IoT, Cloud Comput., Wireless Netw. Optim.* IGI Global, 2019, pp. 491–518.

[4] N. Gupta and S. K. Dhurandher, "Cross-layer perspective for channel assignment in cognitive radio networks: A survey," *Int. J. Commun. Syst.*, 2019.

[5] Z. Xiang, W. Yang, G. Pan, Y. Cai, and Y. Song, "Physical layer security in cognitive radio inspired noma network," *IEEE J. Sel. Top. Signal Proc.*, vol. 13, no. 3, pp. 700–714, Jun. 2019.

[6] Z. Ali, Y. Rao, W. U. Khan, and G. A. S. Sidhu, “Joint user pairing, channel assignment and power allocation in NOMA based CR systems,” *Appl. Sci.*, vol. 9, no. 20, 2019.

[7] C. E. Shannon, “Communication theory of secrecy systems,” *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[8] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[9] I. Csiszár and J. Korner, “Broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[10] A. Thakur, A. Kumar, N. Gupta, and A. Singh, “Secrecy outage performance analysis of MIMO underlay cognitive radio networks with delayed CSI and transmitter antenna selection,” *Int. J. Commun. Syst.*, 2019.

[11] I. Issa, A. B. Wagner, and S. Kamath, “An operational approach to information leakage,” *IEEE Trans. Inf. Theory*, vol. 66, no. 3, pp. 1625–1657, Mar. 2020.

[12] F. Jameel, W. U. Khan, Z. Chang, T. Ristaniemi, and J. Liu, “Secrecy analysis and learning-based optimization of cooperative NOMA swipt systems,” in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops).*, 2019, pp. 1–6.

[13] P. Mekikis, A. S. Lalos, A. Antonopoulos, L. Alonso, and C. Verikoukis, “Wireless energy harvesting in two-way network coded cooperative communications: A stochastic approach for large scale networks,” *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 1011–1014, Jun. 2014.

[14] G. Dong, H. Zhang, and D. Yuan, “Downlink achievable rate of massive MIMO enabled swipt systems over rician channels,” *IEEE Commun. Lett.*, vol. 22, no. 3, pp. 578–581, Mar. 2018.

[15] L. R. Varshney, “Transporting information and energy simultaneously,” in *Proc. IEEE Int. Symp. Inf. Theory.*, 2008, pp. 1612–1616.

[16] P. Grover and A. Sahai, “Shannon meets tesla: Wireless information and power transfer,” in *Proc. IEEE Int. Symp. Inf. theory.*, 2010, pp. 2363–2367.

[17] 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.

[18] 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.

[19] P.-V. Mekikis, A. Antonopoulos, E. Kartsakli, A. S. Lalos, L. Alonso, and C. Verikoukis, “Information exchange in randomly deployed dense wsns with wireless energy harvesting capabilities,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 3008–3018, Apr. 2016.

[20] H. Lei, Z. Dai, K.-H. Park, W. Lei, G. Pan, and M.-S. Alouini, “Secrecy outage analysis of mixed RF-FSO downlink swipt systems,” *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6384–6395, Dec. 2018.

[21] H. Lei, J. Zhang, K.-H. Park, I. S. Ansari, G. Pan, and M.-S. Alouini, “Secrecy performance analysis of SIMO underlay cognitive radio systems with outdated CSI,” *IET Commun.*, vol. 11, no. 12, pp. 1961–1969, 2017.

[22] R. Zhao, H. Lin, Y.-C. He, D.-H. Chen, Y. Huang, and L. Yang, “Secrecy performance of transmit antenna selection for MIMO relay systems with outdated CSI,” *IEEE Trans. Commun.*, vol. 66, no. 2, pp. 546–559, 2017.

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

[24] H. Liu *et al.*, “Physical-layer secrecy outage of spectrum sharing CR systems over fading channels,” *Sci. China Inf. Sci.*, vol. 59, no. 10, 2016.

[25] 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. 10 236–10 242, Dec. 2016.

[26] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, “Performance of transmit antenna selection physical layer security schemes,” *IEEE Signal Proc. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.

[27] 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.

[28] 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.

[29] Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, “Secure communication in multiantenna cognitive radio networks with imperfect channel state information,” *IEEE Trans. Signal Proc.*, vol. 59, no. 4, pp. 1683–1693, Apr. 2011.

[30] K. Shim, N. T. Do, B. An, and S.-Y. Nam, “Outage performance of physical layer security for multi-hop underlay cognitive radio networks with imperfect channel state information,” in *Proc. Int. Conf. Electron., Inf., Commun. (ICEIC).*, 2016, pp. 1–4.

[31] N. Mokari, S. Parsaeefard, H. Saeedi, and P. Azmi, “Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users,” *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 1058–1073, Feb. 2014.

[32] 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.

[33] 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.

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

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

[36] 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.

[37] X. Lu, W. Xu, S. Li, Z. Liu, and J. Lin, “Simultaneous wireless information and power transfer for cognitive two-way relaying networks,” in *Proc. IEEE 25th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC).*, 2014, pp. 748–752.

[38] L. Jiang and H. Tian, “Energy-efficient relay selection scheme for physical layer security in cognitive radio networks,” *Math. Problems Eng.*, vol. 2015, 2015.

[39] C. Xing, N. Wang, J. Ni, Z. Fei, and J. Kuang, “MIMO beamforming designs with partial CSI under energy harvesting constraints,” *IEEE Signal Proc. Lett.*, vol. 20, no. 4, pp. 363–366, Apr. 2013.

[40] R. Feng, Q. Li, Q. Zhang, and J. Qin, “Robust secure transmission in miso simultaneous wireless information and power transfer system,” *IEEE Trans. Veh. Tech.*, vol. 64, no. 1, pp. 400–405, Jan. 2015.

[41] H. Lei *et al.*, “On secure mixed RF-FSO systems with TAS and imperfect CSI,” *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4461–4475, Jul. 2020.

[42] G. Pan *et al.*, “On secrecy performance of MISO swipt systems with tas and imperfect CSI,” *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3831–3843, Sep. 2016.

Anshu Thakur (Student Member, IEEE) received the M.Tech. degree in electronics and communication systems from the Jaypee University of Information Technology, Waknaghat, India, in 2016. Since January 2017, she has been working toward the Ph.D. degree in electronics and communication engineering with the National Institute of Technology Hamirpur, Hamirpur, India. Her research interest includes secrecy analysis in wireless communication systems.

Ashok Kumar received the Ph.D. degree from the National Institute of Technology Hamirpur, Hamirpur, India. He is currently the Head of Department and an Associate Professor with the Department of Electronics and Communication Engineering, National Institute of Technology Hamirpur. He has authored/coauthored more than 50 research papers international/national journals and conferences on the topics of his research interests and also guided three Ph.D. students and, currently guiding four Ph.D. students in these research areas, which include wireless communication and wireless sensor networks. He is a Life Member of ISTE.

Nitin Gupta (Senior Member, IEEE) has been an Assistant Professor with the Department of Computer Science and Engineering, National Institute of Technology Hamirpur (Under Government of India), Hamirpur, India, since 2007. He has authored/coauthored various research papers in international journals such as IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE SYSTEMS JOURNAL, and conferences of repute such as IEEE International Conference on Communications and IEEE Global Communications Conference. His research interests include next generation wireless networks, especially cognitive radio networks. He is a Member of IEEE Communication Society, and a Member of ACM. He is also a Member of the Executive Committee of the IEEE Communication Society—Delhi Chapter. He is a Reviewer of various reputed journals such as IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS and IEEE SYSTEMS JOURNAL.

Pushpita Chatterjee (Member, IEEE) received the M.S. degree in computer and information science and the M.Tech. degree in computer engineering from the University of Calcutta, Kolkata, India, in 2002 and 2004, respectively, and the Ph.D. degree from the Indian Institute of Technology Kharagpur, Kharagpur, India, in 2012. She has been a Research Consultant with Old Dominion University (ODU), Norfolk, VA, USA, since 2016. Prior to joining ODU, she was a Senior Research Lead with the SRM Institute of Science and Technology (a Unit of SRM University, Chennai), Bangalore, India. She was responsible for leading a group of more than 20 researchers who were working for OpenFlow and software-defined networking and deep learning related application research with NEC, Japan, and NTT, Japan. She has a good number of publications to her credit in international journals, conferences, and books. Her research interests include smart health, machine learning, distributed and trust computing, wireless networks, and software-defined networking.