JJEE
Jordan Journal of Electrical Engineering
Volume 7, Number 4, December 2021
Pages 360-376
ISSN (Print): 2409-9600, ISSN (Online): 2409-9619

Secrecy Performance for Underlay Cooperative Cognitive Radio Network with Energy Harvesting and Transmit Antenna Selection Using MIMO Over Nakagami-m Fading Channels

Mahmoud A. Khodeir [1*], Saja M. Alquran [2]

[1, 2] Electrical Engineering Department, Jordan University of Science and Technology, Irbid, Jordan
E-mail: makhodeir@just.edu.jo

Received: March 13, 2021 *Revised: June 09, 2021* *Accepted: June 15, 2021*

***Abstract*—** This paper introduces underlay multiple input multiple output (MIMO) cooperative communication involving source, destination, eavesdropper, primary nodes and decode and forward (DF) relay. To improve the energy and spectral efficiencies, the source and relay are powered by the energy, harvested from the primary transmitter. All the channel state information (CSI) is assumed to be available at the source and relay. Here, transmit antenna selection/maximal ratio combining (TAS/MRC) is also implemented at the secondary relay. Moreover, to enhance the security performance, MRC technique is utilized at both the destination and the eavesdropper. Precise closed-form secrecy outage performance for the secondary relay with an active eavesdropper is derived over Nakagami-*m* fading channel. The obtained results indicate that when the number of antennas - at the intermediate relay and/or destination - increases, the secrecy outage performance - of the proposed system model over Nakagami-*m* fading channel - enhances for large average channel gain in the main channel. The secrecy outage probability (SOP) is used in this work as a performance metric. It is found to be equal to 0.1 when setting $m = 1$ for the Rayleigh fading channel, and greater than 0.01 when setting $m = 2$ for the Nakagami-*m* fading channel.

***Keywords*—** Underlay cooperative cognitive radio network; Secrecy performance; Energy harvesting; Transmit antenna selection scheme; MIMO; Nakagami-*m* fading channel.

1. INTRODUCTION

The increase in demand for mobile data traffic has led to an increase in the demand for more spectrum to achieve high data rates, enhance coverage and develop global internet access. Spectrum and energy are two indispensable resources that need to be allocated and controlled reasonably in wireless networks. In particular, two approaches are taken to resolve the issues of spectrum scarcity and energy limitation, namely cognitive radio (CR) and energy harvesting (EH).

EH can be implemented by allowing the secondary transmitter to harvest energy from the radio frequency (RF) signals that are close to the RF sources (i.e., primary users, cellular base stations and other surrounding RF sources). Then, one can convert the harvested energy from electromagnetic fields to electrical voltages and/or currents to supply different wireless equipment [1, 2]. In this paper, the interference signals emitted from the primary transmitter (PT) to the secondary users (i.e., source and relay) are also exploited to harvest energy to save more energy and spectrum [3, 4].

The physical layer security (PLS) technology can provide a secure connection to transmit data between two nodes through the time change of a wireless channel without sharing a secret key [5]. Commonly, metrics are applied to estimate secrecy performance such as average secrecy capacity (ASC), secrecy outage probability (SOP) and probability of non-zero secrecy capacity (PNSC). The SOP is the probability that the difference between the

* Corresponding author
Article's DOI: 10.5455/jjee.204-1615665316

capacity for the main channel and that for the wiretap channel (i.e., the channel used by the eavesdropper to obtain data from the source) in the system is lower than the secrecy data rate. This technique is used in this paper as a performance metric. In particular, the SOP is more fundamental and helpful than the secrecy throughput and the outage probability in terms of evaluating the security capability.

According to the underlay cognitive radio network (CRN), the simplest mode is achieved when the primary and secondary users can utilize the same wireless spectrum simultaneously under a predefined interference power threshold to guarantee reliable communication at the primary users. Yang et al. investigated secure communications against eavesdropping in an underlay cognitive radio network and derived the exact secrecy outage performance [6]. In addition, to achieving secure communications and saving both energy and spectrum, the authors in [7] employed the EH technique for underlay cognitive systems.

In [8], the authors studied the security performance of CRNs with energy harvesting under the interference power constraint, the primary interference, and the maximum transmitted power constraint under Nakagami-m fading channel. The analysis of the security capability for underlay cognitive relaying networks with energy harvesting (UCRNwEH) is paramount before manufacturing practical systems. Therefore, the authors in [9] performed the analysis on the security performance of URCNwEH over independent Rayleigh fading channels.

Furthermore, the multiple antennas technique is considered an effective method to increase the security performance for wireless wiretap channels as shown in [10]. In [11], the authors studied the SOP of an energy harvesting aided underlay single input multiple output CRN for multiple eavesdroppers over Nakagami-m fading channels. In particular, two eavesdroppers' scenarios were considered, namely colluding eavesdropping and noncolluding eavesdropping. Based on that, the authors derived closed-form expressions for the SOP of the proposed networks.

In general, one can improve the coverage of the area by using cooperative communication. In [12], the authors employed a decode and forward (DF) relay between the source and the destination, where the power of this relay depends on the harvested energy from the source. Particularly, the authors derived the security performance over Nakagami-m fading channels for the underlay CRNs to guarantee that the direct path between the source and the destination is under deep fading and/or shadowing. Moreover, the authors in [13] analyzed the physical-layer security of dual-hop energy RF-powered CRN system with an intermediate relay located at the middle to harvest energy from the source based on the power-splitting energy harvesting strategy and re-encoded data before relaying it to the destination. Here, both independent and identically distributed (i.i.d.) and independent but not-identically distributed (i.n.i.d.) flat Rayleigh fading channels are considered.

Many authors have also suggested the idea of adding multiple relays between the source and the destination to improve general network performance against the wiretap channel and to provide cooperative diversity. In this domain, several schemes with relay selection have been examined by Lei et al. [14]. Also, the authors in [15] employed the relay selection method with energy harvesting in cognitive networks. They derived the intercept outage probability for the proposed relay selection method and peak transmit power where interference power constrained is considered over Rayleigh distribution.

To the best of the authors' knowledge, no open literature has addressed the secrecy performance for underlay cooperative cognitive multiple input multiple output (MIMO) systems with EH and transmit antenna selection (TAS) schemes over Nakagami-m fading channels, which are utilized to: i) provide a good matching with various measurement data obtained empirically and ii) to model wireless fading channels including Rayleigh ($m = 1$) and one-sided Gaussian distribution ($m = 0.5$) as special cases. However, in [7] the authors investigated the secrecy performance of an underlay MIMO CRNs with EH and TAS and derived the closed-form expression for the SOP without relay over Rayleigh fading channel.

Moreover, a secondary DF relay is added between the source and destination in this paper. This relay is employed to ensure secure communications between the secondary transmitter and the destination in case that the direct communication - between the source and destination - is not available to transmit data. The power of this relay and the source depend on harvesting energy from the primary transmitter to achieve more energy and spectral efficiencies. Also, it is strictly constrained by the maximum tolerated interference power at the primary receiver (PR) and the maximum transmit power constraint. Furthermore, the secondary relay utilizes multiple antennas to get the advantages of the transmit antenna selection/maximal ratio combining (TAS/MRC) scheme.

Finally, in this paper, we investigate the secrecy performance to the secondary relay and a closed-form expression for SOP is derived for multiple antenna cooperative underlay CR over Nakagami-m fading channel. Also, all the channel state information (CSI) for both the main and the wiretap channels are available at the source and relay (active eavesdropping scenario). Here, one can achieve secrecy if the main channel is better than the wiretap channel. If such CSI is not available at the source and relay, this scenario is called passive eavesdropper . For such scenario, it is not possible to evaluate the secrecy capacity, so perfect secrecy cannot be guaranteed. The proposed model is assumed to operate with the existence of an active eavesdropper to achieve higher channel capacity as compared with the case of transmission without CSI. Here, the eavesdropper will try to overhear the confidential information that is transmitted from the relay to the destination through the wiretap channel.

The rest of this paper is organized as follows: in section 2, the proposed system model is presented. In section 3, the secrecy performance is analyzed. Section 4 presents and discusses the numerical results. Finally, the conclusions and future work are discussed in section 5.

2. SYSTEM MODEL

This section presents the proposed system model shown in Fig. 1. This model contains a typical CRN operating in underlay mode with PT, PR, source (S), relay (R), destination (D), and an active eavesdropper (E).

All the PT, PR, and S are equipped with a single antenna, while D, E, and R are equipped with $N_D \geq 1$, $N_E \geq 1$ and $N_R \geq 1$ antennas. In particular, the proposed work assumed that both D and E employed MRC as a combining diversity technique. This technique coherently combines the received signals when multiple RF chains are implemented, then better performance is achieved as compared with other schemes due to improving the signal to noise ratio (SNR). There are no direct links between S and D as well as S and E due to deep fading and shadowing. This data communication can be implemented using the DF intermediate relay. Here, S and R depend on the energy harvested from RF

signals emitted by the PT, while E will try to overhear the confidential information that is transmitted from R to D through the wiretap channel.

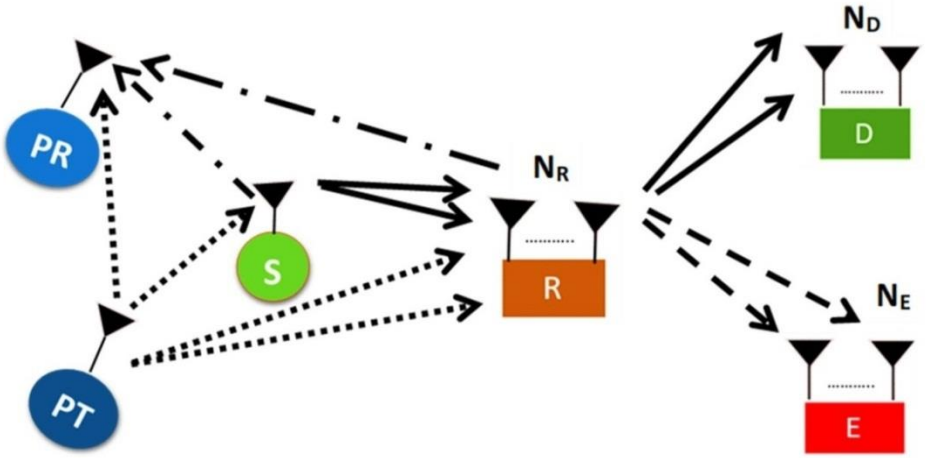

Fig. 1. System model with one relay.

This system model can be studied over i.i.d. quasi-static Nakagami-m fading channel with fading parameters m_τ. The average channel power gains of each group is Ω_τ, the instantaneous channel fading coefficients for each group is h_τ, where $\tau \in$ {PT-S, PT-R, S-PR, R-PR, S-R, R_i-D, R_i-E}. For simplification, we assume $m_{PT-S} = m_t$, $m_{PT-R} = m_A$, $m_{S-PR} = m_S$ and $m_{R-PR} = m_P$. Moreover, the thermal noise is added at each receiver and modeled as an additive white Gaussian noise (AWGN) with variance σ^2. The optimal antenna selection (OAS) scheme is used at the secondary relay with available CSI at both S and R.

In general, the exchange of data between S and D requires three-time phase; the first time phase, β, (where $0 \le \beta \le 1$) is dedicated for EH. The second and third time phases, $(1-\beta)/2$, are dedicated to the data transmission of the secondary source and the relay to D/E. In the second part, S will send the message to R which will try to decode the received signal and after that, R will decode data coming to D. Here, E can overhear the messages from R.

The energy of the secondary nodes is depending on harvested RF signals received from PT that is stored in an infinite capacity buffer to simplify the analysis. In particular, the harvested energy is stored in an energy buffer of infinite capacity to increase the lifetime of the battery, which leads to simplifying the analysis. However, if the energy storage device has a limited capacity, this will reduce the lifetime of the battery. The harvested energy at S can be expressed as:

$$E_S = \eta\beta P_t Y_t \tag{1}$$

where $0 \le \eta \le 1$ implies the EH efficiency [16], P_t is the transmit power at the PT, $Y_t = |h_{PT-S}|^2$, and h_{PT-S} is the instantaneous channel fading coefficients between PT and S.

The probability density function (PDF) and cumulative distribution function (CDF) of the channel gain Y_t can be written, respectively, as [17]:

$$f_{Y_t}(y) = \frac{{\lambda_t}^{m_t}}{\Gamma(m_t)} y^{m_t-1} e^{-\lambda_t y} \tag{2}$$

$$F_{Y_t}(y) = 1 - \frac{\Gamma(m_t, \lambda_t y)}{\Gamma(m_t)} \tag{3}$$

where $\lambda_t = \frac{m_t}{\Omega_t}$, $\Gamma(.)$ is the Gamma function as defined by Eq. (8.310.1) of [18] and $\Gamma(.,.)$ is the upper incomplete Gamma function as defined by Eq. (8.350.2) of [18].

Based on Eq. (1), the maximal transmit power at S can be given as:

$$P_{max1} = \frac{E_S}{(1-\beta)/2} = \frac{\eta\beta P_t Y_t}{(1-\beta)/2} \tag{4}$$

where $(1-\beta)/2$ is expended for transmission information from the S to R.

Accordingly, for the underlay spectrum sharing technique, S and R are allowed to use the same licensed spectrum if the interference due to PR is lower than a certain threshold and the transmitting power does not exceed the maximum transmitted power. Due to these power restrictions, the transmit power at S can be expressed as [19, 20]:

$$P_S = min\left(P_{max1}, \frac{P_I}{Y_S}\right) \tag{5}$$

where P_I is the maximum tolerated interference power at PR, $Y_S = |h_{S-PR}|^2$, and h_{S-PR} is the instantaneous channel fading coefficient between S and PR.

The PDF and CDF of the channel gain, Y_S, can be expressed, respectively, as [17]:

$$f_{Y_S}(y) = \frac{{\lambda_S}^{m_S}}{\Gamma(m_S)} y^{m_S-1} e^{-\lambda_S y} \tag{6}$$

$$F_{Y_S}(y) = 1 - \frac{\Gamma(m_S, \lambda_S y)}{\Gamma(m_S)} \tag{7}$$

where $\lambda_S = \frac{m_S}{\Omega_s}$.

The harvested energy at R can be expressed as:

$$E_R = \eta\beta P_t Y_A \tag{8}$$

where $Y_A = \sum_{j=1}^{N_R} \left|h_{PT-R_j}\right|^2$, and h_{PT-R_j} is the instantaneous channel fading coefficients between the PT and the j-th antenna at the R. The PDF and the CDF of the channel gain, Y_A, can be written, respectively, as [17]:

$$f_{Y_A}(y) = \rho_A y^{T_A-1} e^{-\lambda_A y} \tag{9}$$

$$F_{Y_A}(y) = 1 - \frac{\Gamma(T_A, \lambda_A y)}{\Gamma(T_A)} \tag{10}$$

where $\lambda_A = \frac{m_A}{\Omega_A}$, $T_A = m_A N_R$ and $\rho_A = \frac{1}{\Gamma(T_A)} (\lambda_A)^{T_A}$.

Based on Eq. (8), the maximal transmit power at R can be written as:

$$P_{max2} = \frac{E_R}{(1-\beta)/2} = \frac{\eta\beta P_t Y_A}{(1-\beta)/2} \tag{11}$$

where the time $(1-\beta)/2$ is expended for data transmission between R and D.

The transmit power at R is strictly constrained as follows [18, 19]:

$$\widehat{P_R} = min\left(P_{max2}, \quad \frac{P_I}{Y_P}\right) \tag{12}$$

where $Y_P = \left|h_{R_{\bar{b}}-PR}\right|^2$, $\bar{b}$ denotes the optimal selected antenna at R and $h_{R_{\bar{b}}-PR}$ is the channel fading coefficients between R and PR. The PDF and the CDF of the channel gain, Y_p, can be written, respectively, as follows [17]:

$$f_{Y_P}(y) = \frac{{\lambda_p}^{m_p}}{\Gamma(m_p)} y^{m_P-1} e^{-\lambda_p y} \tag{13}$$

$$F_{Y_P}(y) = 1 - \frac{\Gamma(m_P, \lambda_P y)}{\Gamma(m_P)} \tag{14}$$

where $\lambda_P = \frac{m_P}{\Omega_P}$.

In the second time phase, the channel capacity between S and R can be expressed as:

$$C_{SR} = \frac{1-\beta}{2}\ln\left(1+\frac{P_S}{\sigma^2}Y_{SR}\right), (\text{nat/s/Hz}) \tag{15}$$

where $Y_{SR} = \sum_{j=1}^{N_R}\left|h_{SR_j}\right|^2$, h_{SR_j} is the instantaneous channel fading coefficient between S and the j-th antenna at R. The CDF of the channel gain, Y_{SR}, can be written as:

$$F_{Y_{SR}}(y) = 1 - \frac{\Gamma(m_{SR}, \lambda_{SR} y)}{\Gamma(m_{SR})} \tag{16}$$

where $T_{SR} = m_{SR}N_R$ and $\lambda_{SR} = \frac{m_{SR}}{\Omega_{SR}}$.

Based on [21, 22], R can successfully decode the received signal in the second phase when C_{SR} is greater than the target data rate $R_d > 0$. Otherwise, R cannot recover the signal from S. Therefore, the probability that the relay can decode successfully is given by:

$$\begin{aligned}
P_{suc} &= pr(C_{SR} > R_d) \\
&= pr\left(\frac{1-\beta}{2}\ln\left(1+\frac{P_S}{\sigma^2}Y_{SR}\right) > R_d\right) \\
&= pr\left(Y_{SR} > \frac{(\theta-1)\sigma^2}{P_S}\right) \\
&= pr\left(Y_{SR} > \frac{(\theta-1)\sigma^2}{P_S}, P_s = P_{max1}\right) + pr\left(Y_{SR} > \frac{(\theta-1)\sigma^2}{P_S}, P_s = \frac{P_I}{Y_S}\right) \\
&= \underbrace{pr\left(Y_{SR} > \frac{(\theta-1)\sigma^2}{P_{max1}}, Y_s \le \frac{P_I}{P_{max1}}\right)}_{k_1} + \underbrace{pr\left(Y_{SR} > \frac{(\theta-1)\sigma^2 Y_s}{P_I}, Y_s > \frac{P_I}{P_{max1}}\right)}_{k_2}
\end{aligned} \tag{17}$$

where $\theta = exp(2R_d/(1-\beta))$.

Substituting Eqs. (2), (4), (7) and (16) into Eq. (17), then using Eqs. (3.471.9) and (8.352.7) in [18], K_1 can be written as:

$$\begin{aligned}
K_1 &= pr\left(Y_{SR} > \frac{\varsigma_1}{Y_t}, Y_s \le \frac{\xi_1}{Y_t}\right) \\
&= \int_0^\infty \left(1 - F_{Y_{SR}}\left(\frac{\varsigma_1}{x}\right)\right) F_{Y_S}\left(\frac{\xi_1}{x}\right) f_{Y_t}(x)dx \\
&= \sum_{l=0}^{T_{SR}-1} \frac{(\lambda_t)^{m_t}(\lambda_{SR}\varsigma_1)^l}{\Gamma(m_t)l!}\left(\int_0^\infty x^{m_t-l-1}\, e^{-\lambda_t x - \lambda_{SR}\frac{\varsigma_1}{x}}dx\right. \\
&\quad \left. - \sum_{k=0}^{m_S-1}\frac{(\lambda_s\xi_1)^k}{k!}\int_0^\infty x^{m_t-l-k-1}\, e^{-\lambda_t x - \lambda_{SR}\frac{\varsigma_1}{x} - \lambda_S\frac{\xi_1}{x}}dx\right) \\
&= \sum_{l=0}^{T_{SR}-1} \frac{(\lambda_t)^{m_t}(\lambda_{SR}\varsigma_1)^l}{\Gamma(m_t)l!}\left(2\left(\frac{\lambda_{SR}\varsigma_1}{\lambda_t}\right)^{\frac{m_t-l}{2}} K_{m_t-l}\left(2\sqrt{\lambda_t\lambda_{SR}\varsigma_1}\right)\right. \\
&\quad \left. - \sum_{k=0}^{m_S-1}\frac{2(\lambda_s\xi_1)^k}{k!}\left(\frac{\lambda_{SR}\varsigma_1+\lambda_S\xi_1}{\lambda_t}\right)^{\frac{m_t-l-k}{2}} \times K_{m_t-l-k}\left(2\sqrt{\lambda_t(\lambda_{SR}\varsigma_1+\lambda_S\xi_1)}\right)\right)
\end{aligned} \tag{18}$$

where $\varsigma_1 = \frac{(\theta-1)\sigma^2(1-\beta)}{2\eta\beta P_t}$, $\xi_1 = \frac{P_I(1-\beta)}{2\eta\beta P_t}$ and $K_v(x)$ is the modified Bessel function of order v, as defined by Eq. (8.407.1) of [18].

Now, by substituting Eqs. (3), (4), (6) and (16) into Eq. (17), then utilizing Eqs. (3.471.9) and (8.352.7) of [18], K_2 can be written as:

$$\begin{aligned} K_2 &= pr\left(Y_{SR} > \omega_1 Y_S, Y_t > \frac{\xi_1}{Y_S}\right) \\ &= \int_0^{\infty} \left(1 - F_{Y_{SR}}(\omega_1 x)\right)\left(1 - F_{Y_t}\left(\frac{\xi_1}{x}\right)\right) f_{Y_S}(x)dx \\ &= \sum_{n=0}^{m_t-1}\sum_{l=0}^{T_{SR}-1} \frac{(\lambda_S)^{m_S}(\lambda_t\xi_1)^n\left(\lambda_{SR_i}\omega_1\right)^l}{\Gamma(m_s)l!\,n!} \\ &\quad \times\left(\int_0^{\infty} x^{m_s+l-n-1}e^{-\lambda_S x-\lambda_{SR}\omega_1 x-\lambda_t\frac{\xi_1}{x}}dx\right) \\ &= \sum_{n=0}^{m_t-1}\sum_{l=0}^{T_{SR}-1} \frac{2(\lambda_S)^{m_S}(\lambda_t\xi_1)^n(\lambda_{SR}\omega_1)^l}{\Gamma(m_s)l!\,n!} \\ &\quad \times\left(\frac{\lambda_t\xi_1}{\lambda_S+\lambda_{SR}\omega_1}\right)^{\frac{m_s-n+l}{2}} K_{m_s-n+l}\left(2\sqrt{\lambda_t\xi_1(\lambda_S+\lambda_{SR}\omega_1)}\right) \end{aligned} \tag{19}$$

where $\omega_1 = \frac{(\theta-1)\sigma^2}{P_I}$.

In the third time phase, one can denote the successful decoding relay. Then, the channel capacity between R and D/E can be expressed as:

$$C_{R_iD} = \frac{1-\beta}{2}\ln\left(1+\frac{P_R}{\sigma^2}Y_{R_iD}\right), \text{ (nat/s/Hz)} \tag{20}$$

where $Y_{R_iD} = \sum_{j=1}^{N_D}\left|h_{R_iD_j}\right|^2$, $h_{R_iD_j}$ is the channel fading coefficient between the i-th antenna at R and the j-th antenna at D. The CDF of the channel gain Y_{R_iD} can be expressed as [17]:

$$F_{Y_{R_iD}}(y) = 1 - \frac{\Gamma\left(T_D, \lambda_{R_iD}y\right)}{\Gamma(T_D)} \tag{21}$$

where $\lambda_{R_iD} = \frac{m_{R_iD}}{\Omega_{R_iD}}$ and $T_D = m_{R_iD}N_D$.

Correspondingly, the channel capacity between R and E can be written as:

$$C_{R_iE} = \frac{1-\beta}{2}\ln\left(1+\frac{P_R}{\sigma^2}Y_{R_iE}\right), \text{ (nat/s/Hz)} \tag{22}$$

where $Y_{R_iE} = \sum_{j=1}^{N_E}\left|h_{R_iE_j}\right|^2$, $h_{R_iE_j}$ is the channel fading coefficient between the i-th antenna at R and the j-th antenna at E. The PDF of Y_{R_iE} can be expressed as [17]:

$$f_{Y_{R_iE}}(y) = \rho_E y^{T_E-1}e^{-\lambda_{RE}y} \tag{23}$$

where $\lambda_{R_iE} = \frac{m_{R_iE}}{\Omega_{R_iE}}$, $T_E = m_{R_iE}N_E$ and $\rho_E = \frac{1}{\Gamma(T_E)}\left(\lambda_{R_iE}\right)^{T_E}$.

Here, full CSI is considered to be available for both the main and the wiretap channels at S and R (i.e., active eavesdropping) [23]. The antenna at R is selected to maximize the achievable secrecy rate in the secondary relay which is used to transmit signals to D [19, 23]. In general, the metrics of the chosen antenna in the OAS scheme is shown as follows:

$$b = arg\max_{1\le i\le N_R} C_i, \tag{24}$$

where C_i is the achievable secrecy rate via the i-th antenna at R. Thus, the instantaneous secrecy capacity at R is the capacity difference between the main channel (i.e., R to D) and the wiretap channel (i.e., R to E), which can be written as:

$$C_S = \max_{1\le i\le N_R} C_i = \max_{1\le i\le N_R} \left[C_{R_iD} - C_{R_iE}\right]^+ \tag{25}$$

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

3. EXACT SECRECY OUTAGE PROBABILITY

Next, we derive the secrecy performance of the proposed system model by finding the exact closed-form expressions for SOP. The SOP is defined as the probability that the instantaneous secrecy capacity does not exceed the target secrecy rate, $R_S \geq 0$ [24]. Using Eq. (21), the security performance can be calculated by exploiting the following equation:

$$\begin{aligned} P_{out} &= Pr(C_S \le R_s) \\ &= \Pr(C_{SR} \le R_d) + Pr(C_{SR} > R_d)\ \underbrace{Pr(C_S \le R_S)}_{Q} \end{aligned} \tag{26}$$

To analytically evaluate P_{out}, the term Q must be first computed as:

$$\begin{aligned} Q &= Pr(C_S \le R_S) \\ &= Pr\left(\max_{1\le i\le N_R} \left[C_{R_iD} - C_{R_iE}\right]^+ \le R_S\right) \\ &= \prod_{i=1}^{N_R} Pr\left(C_{R_iD} - C_{R_iE} \le R_S\right) = (P_{out}^{OAS})^{N_R} \end{aligned} \tag{27}$$

Substituting Eqs. (20) and (22) into Eq. (27), we obtain:

$$\begin{aligned} P_{out}^{OAS} &= Pr\left(C_{R_iD} - C_{R_iE} \le R_S\right) \\ &= Pr\left(Y_{R_iD} \le \epsilon Y_{R_iE} + \frac{(\epsilon-1)\sigma^2}{\widehat{P_R}}\right) \end{aligned} \tag{28}$$

where $\epsilon = exp(2R_s/(1-\beta))$.

Now, by substituting Eq. (11) into Eq. (28), we get:

$$\begin{aligned} P_{out}^{OAS} &= Pr\left(Y_{R_iD} \le \epsilon Y_{R_iE} + \frac{(\epsilon-1)\sigma^2}{\widehat{P_R}}\right) \\ &= Pr\left(Y_{R_iD} \le \epsilon Y_{R_iE} + \frac{(\epsilon-1)\sigma^2}{\widehat{P_R}}, \widehat{P_R} = P_{max2}\right) \\ &\quad + pr\left(Y_{R_iD} \le \epsilon Y_{R_iE} + \frac{(\epsilon-1)\sigma^2}{\widehat{P_R}}, \widehat{P_R} = \frac{P_I}{Y_P}\right) \\ &= \underbrace{pr\left(Y_{R_iD} \le \epsilon Y_{R_iE} + \frac{(\epsilon-1)\sigma^2}{P_{max2}}, Y_P \le \frac{P_I}{P_{max2}}\right)}_{I_1} \\ &\quad + \underbrace{pr\left(Y_{R_iD} \le \epsilon Y_{R_iE} + \frac{(\epsilon-1)\sigma^2 Y_P}{P_I}, Y_P > \frac{P_I}{P_{max2}}\right)}_{I_2} \end{aligned} \tag{29}$$

Next, by substituting Eq. (12) into Eq. (29), I_1 (i.e., when $\widehat{P_R} = P_{max2}$) can be written as:

$$\begin{aligned} I_1 &= Pr\left(Y_{R_iD} \le \epsilon Y_{R_iE} + \frac{\delta_1}{Y_A}, Y_P \le \frac{\varphi_1}{Y_A}\right) \\ &= \int_0^\infty f_{Y_A}(x) F_{Y_P}\left(\frac{\varphi_1}{x}\right) H_1(x) dx \end{aligned} \tag{30}$$

where $\delta_1 = \frac{(\epsilon-1)(1-\beta)\sigma^2}{2\eta\beta P_t}$, $\varphi_1 = \frac{P_I(1-\beta)}{2\eta\beta P_t}$, and $H_1(x) = \int_0^\infty F_{Y_{R_iD}}\left(\epsilon y + \frac{\delta_1}{x}\right) f_{Y_{R_iE}}(y) dy$.

By substituting Eqs. (21) and (23) into $H_1(x)$, then using Eqs. (8.352.7) and (3.326.2) of [18], we can write $H_2(x)$ as:

$$\begin{aligned} H_1(x) &= \int_0^{\infty} F_{Y_{R_iD}}\left(\epsilon y + \frac{\delta_1}{x}\right) f_{Y_{R_iE}}(y)dy \\ &= 1 - \rho_E exp\left(-\frac{\lambda_{R_iD}\delta_1}{x}\right) \sum_{k=0}^{T_D-1} \sum_{l=0}^{k} \frac{{\lambda_{R_iD}}^k \epsilon^l}{k!} \binom{k}{l} \\ &\quad \times \left(\frac{\delta_1}{x}\right)^{k-l} \int_0^{\infty} y^{T_E+l-1} exp\big(-\big(\lambda_{R_iE} + \lambda_{R_iD}\epsilon\big)y\big)dy \\ &= 1 - \sum_{k,l} G_{k,l}\, exp\left(-\frac{\lambda_{R_iD}\delta_1}{x}\right)\left(\frac{\delta_1}{x}\right)^{k-l} \end{aligned} \tag{31}$$

where $\sum_{k,l} G_{k,l} = \sum_{k=0}^{T_D-1} \sum_{l=0}^{k} \binom{k}{l} \frac{\rho_E {\lambda_{R_iD}}^k \epsilon^l \Gamma(T_E+l)}{k!\left(\lambda_{R_iE}+\epsilon\lambda_{R_iD}\right)^{T_E+l}}$ and $\binom{k}{l} = \frac{K!}{l!(K-l)!}$.

By substituting Eqs. (9), (14) and (31) into Eq. (30), then using Eqs. (8.352.7) and (3.471.9) of [18], we can write I_1 as:

$$\begin{aligned} I_1 &= 1 + \sum_{t=0}^{m_P-1} \sum_{k,l} \frac{2(\lambda_A)^{T_A}(\lambda_P\varphi_1)^t {\delta_1}^{k-l} G_{k,l}}{(T_A-1)!\, t!} \\ &\quad \times \left(\frac{\lambda_{R_iD}\delta_1 + \lambda_P\varphi_1}{\lambda_A}\right)^{\frac{T_A+l-k-t}{2}} K_{T_A+l-k-t}\left(2\sqrt{\lambda_A\big(\lambda_{R_iD}\delta_1 + \lambda_P\varphi_1\big)}\right) \\ &\quad - \sum_{t=0}^{m_P-1} \frac{2(\lambda_A)^{T_A}(\lambda_P\varphi_1)^t}{(T_A-1)!\, t!}\left(\frac{\lambda_P\varphi_1}{\lambda_A}\right)^{\frac{T_A-t}{2}} K_{T_A-t}\big(2\sqrt{\lambda_A\lambda_P\varphi_1}\big) \\ &\quad - \sum_{k,l} \frac{2(\lambda_A)^{T_A}{\delta_1}^{k-l} G_{k,l}}{(T_A-1)!}\left(\frac{\lambda_{R_iD}\delta_1}{\lambda_A}\right)^{\frac{T_A+l-k}{2}} \times K_{T_A+l-k}\left(2\sqrt{\lambda_A\lambda_{R_iD}\delta_1}\right) \end{aligned} \tag{32}$$

By substituting Eq. (12) into Eq. (29), I_2 (i.e., when $\widehat{P_R} = \frac{P_I}{Y_P}$) can be expressed as follows:

$$\begin{aligned} I_2 &= Pr\left(Y_{R_iD} \le \epsilon Y_{R_iE} + \frac{(\epsilon-1)\sigma^2}{P_I} Y_P, Y_P > \frac{P_I}{P_{max2}}\right) \\ &= Pr\left(Y_{R_iD} \le \epsilon Y_{R_iE} + \frac{(\epsilon-1)\sigma^2}{P_I} Y_P, Y_A > \frac{\varphi_1}{Y_P}\right) \\ &= \int_0^{\infty} f_{Y_P}(x)\left(1 - F_{Y_A}\left(\frac{\varphi_1}{x}\right)\right) H_2(x)dx \end{aligned} \tag{33}$$

where $H_2(x) = \int_0^{\infty} F_{Y_{R_iD}}(\epsilon y + \gamma x) f_{Y_{R_iE}}(y)dy$ and $\gamma = \frac{(\epsilon-1)\sigma^2}{P_I}$.

Now, by substituting Eqs. (21) and (23) into $H_2(x)$, then using Eqs. (8.352.7) and (3.326.2) of [18], we find:

$$\begin{aligned} H_2(x) &= \int_0^{\infty} F_{Y_{R_iD}}(\epsilon y + \gamma x) f_{Y_{R_iE}}(y)dy \\ &= 1 - \rho_E exp\big(-\lambda_{R_iD}\gamma x\big) \sum_{k=0}^{T_D-1} \sum_{l=0}^{k} \frac{{\lambda_{R_iD}}^k \epsilon^l}{k!} \binom{k}{l} \\ &\quad \times (\gamma x)^{k-l} \int_0^{\infty} y^{T_E+l-1} exp\big(-\big(\lambda_{R_iE} + \lambda_{R_iD}\,\epsilon\big)y\big)dy \\ &= 1 - \sum_{k,l} G_{k,l}\,(\gamma x)^{k-l} e^{-\lambda_{R_iD}\gamma x} \end{aligned} \tag{34}$$

Then by substituting Eqs. (10), (13) and (34) into Eq. (33) to calculate I_2 (more details are shown in the Appendix A), we obtain:

$$I_2 = \sum_{t=0}^{T_A-1} \frac{2{\lambda_P}^{m_P}(\lambda_A\varphi_1)^t}{\Gamma(m_P)t!}\left(\frac{\lambda_A\varphi_1}{\lambda_P}\right)^{\frac{m_P-t}{2}} K_{m_P-t}\left(2\sqrt{\lambda_P\lambda_A\varphi_1}\right)$$
$$- \sum_{t=0}^{T_A-1}\sum_{k,l} \frac{2G_{k,l}{\lambda_P}^{m_P}(\lambda_A\varphi_1)^t\gamma^{k-l}}{\Gamma(m_P)t!}\left(\frac{\lambda_A\varphi_1}{\lambda_P+\lambda_{R_iD}\gamma}\right)^{\frac{k+m_P-t-l}{2}}$$
$$\times K_{k+m_P-t-l}\left(2\sqrt{(\lambda_P+\lambda_{R_iD}\gamma)\lambda_A\varphi_1}\right) \quad (35)$$

Finally, by substituting Eqs. (32) and (35) into Eq. (29) and then by using Eq. (27) to calculate Q, the SOP for R can be obtained by substituting Eqs. (27) and (17) into Eq. (26).

4. NUMERICAL RESULTS

In this section, numerical results are presented to verify the effect of changing some variables on improving the security performance for the proposed cooperative cognitive MIMO system. Monte-Carlo simulation results are presented as well. S and R are assumed to be able to harvest energy from PT and the OAS scheme is investigated at R. Here, the following parameters and considered: the EH efficiency is $\eta = 0.8$, the variance of AWGN is $\sigma^2 = 1$ and R_S/R_d is measured by unit nat/s/Hz. For simplicity, we define $m_{SR} = \mathrm{m}_R$, $m_{R_iD} = \mathrm{m}_D$, $m_{R_iE} = \mathrm{m}_E$, $m_p = m_S = m_R = m_t = m_D = m_E = m_A = m$, $\Omega_{SR} = \Omega_R$, $\Omega_{R_iD} = \Omega_D$ and $\Omega_{R_iE} = \Omega_E$. Table 1 also shows the description of some parameters.

Table 1. Notation of the considered parameters.

Symbols	Description
N_D	Number of the antenna at the Destination node
N_E	Number of the antenna at the Eavesdropper node
N_R	Number of the antenna at the Relay node
m	Fading shape parameter
Ω_τ	Average channel power gains for each group of τ, where $\tau \in$ {PT-S, PT-R, S-PR, R-PR, S-R, R_i-D, R_i-E}
σ^2	Variance of AWGN
β	Time factor for EH
η	EH efficiency
P_t	Transmit power at the PT.
P_I	Maximum tolerated interference power at PR
R_d	Target data rate
R_S	Target secrecy rate

The SOP versus Ω_D for different values of m is depicted in Fig. 2. In this case, one can significantly enhance the SOP by increasing Ω_D and m. In particular, Ω_D indicates the average SNR of the main channel (i.e., from R to D). For example, when $\Omega_D = 10$, the SOP equals 10^{-1} for the Rayleigh fading channel (i.e., by setting $m = 1$), while the achieved SOP is greater than 10^{-2} when setting $m = 2$. In general, for Nakagami-*m* fading channels (i.e., when $m > 1$), fluctuations in the signal strength are greatly reduced as compared to the

Rayleigh fading channel. Therefore, the security performance is improved. Here, the Nakagami-m fading channel is considered as a more generalized fading distribution to represent more flexible and accurate channel matching, with m is the fading severity parameter (i.e., $m = 1$ represents Rayleigh distribution as a special case). Finally, analysis results match the simulation results, which verify the analysis of security performance.

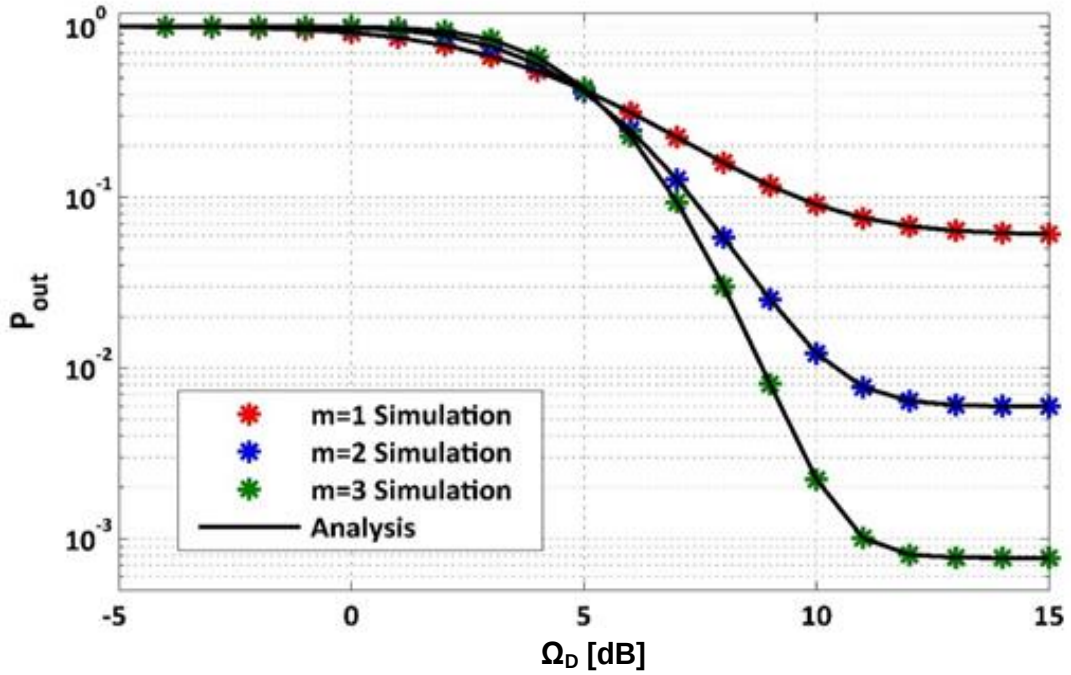

Fig. 2. SOP versus Ω_D with $R_S = R_d = 0.1$, $\beta = \frac{1}{3}$, $\Omega_E = 1$ dB, $\Omega_p = \Omega_S = \Omega_R = \Omega_t = \Omega_A = 5$ dB, $N_E = 4$, $N_D = N_R = 2$, $P_t = 1$ W and $P_I = 2$ W.

Fig. 3 shows the security performance against Ω_D for different values of the parameters N_D and m. For large Ω_D region, increasing Ω_D, N_D and m will enhance the security performance. In particular, Ω_D indicates the average SNR of the main channel (i.e., from R to D). Moreover, reducing the parameter m means that the channel fading is robust while increasing N_D will improve the MRC diversity gain at D. Moreover, one can observe that the security performance is enhanced by increasing m. For example, when $\Omega_D = 10$ and $N_D = 4$, the secrecy outage performance for $m = 3$ is smaller than that for $m = 2$. This means that increasing m refers to stronger received SNR and hence one can achieve higher secrecy diversity order for the same system model. However, for small Ω_D region (i.e., $\Omega_D = 5$ for $N_D = 2$ and $\Omega_D = 3$ for $N_D = 4$), the security performance can be enhanced for lower values of the parameters m.

Fig. 4 shows the SOP against P_t for different values of N_R and Ω_A. Here, one can enhance the SOP significantly by increasing Ω_A and N_R. In particular, higher Ω_A signifies better main channel quality - which is used to collect the energy from transmitting a signal between PT and R - while increasing the number of antennas at R, N_R, means that additional antennas can be picked for data transmission from R. Moreover, the SOP can be improved by increasing the transmit power, P_t, at the PT. This leads to maximizing the harvested energy by the secondary transmitter nodes (e.g., source and relay) to a certain point ($P_t = 15$ dBW). Hence, increasing P_t cannot enhance the SOP in an unlimited fashion.

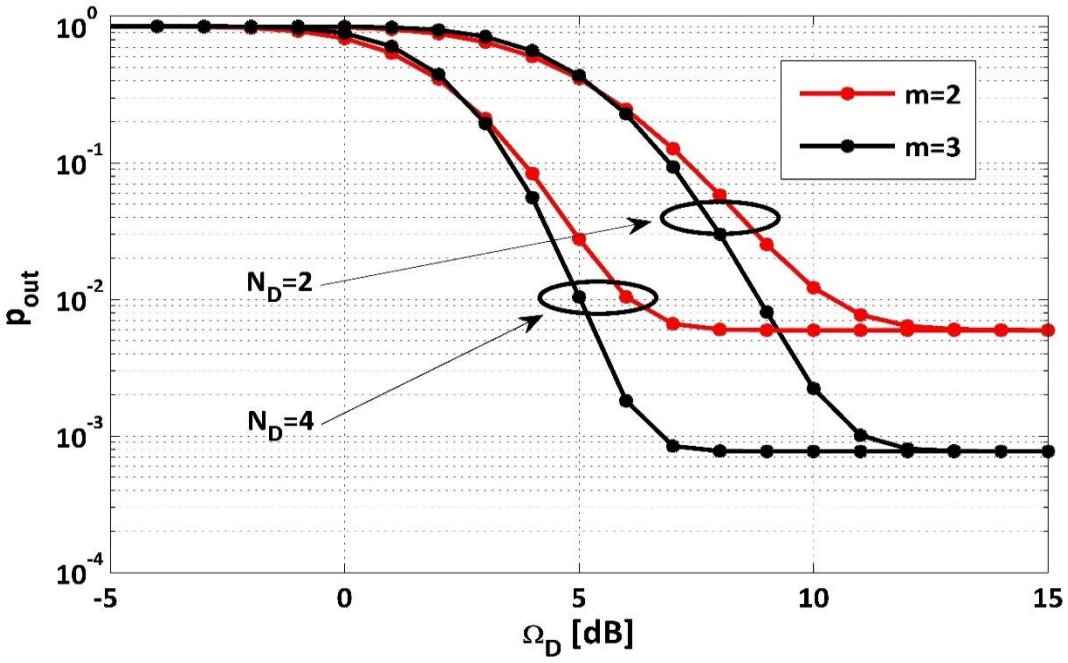

Fig. 3. SOP versus Ω_D with $R_S = R_d = 0.1$, $\beta = \frac{1}{3}$, $\Omega_E = 1$ dB, $\Omega_p = \Omega_S = \Omega_R = \Omega_t = \Omega_A = 5$ dB, $N_E = 4$, $N_R = 2$, $P_t = 1$ W and $P_I = 2$ W.

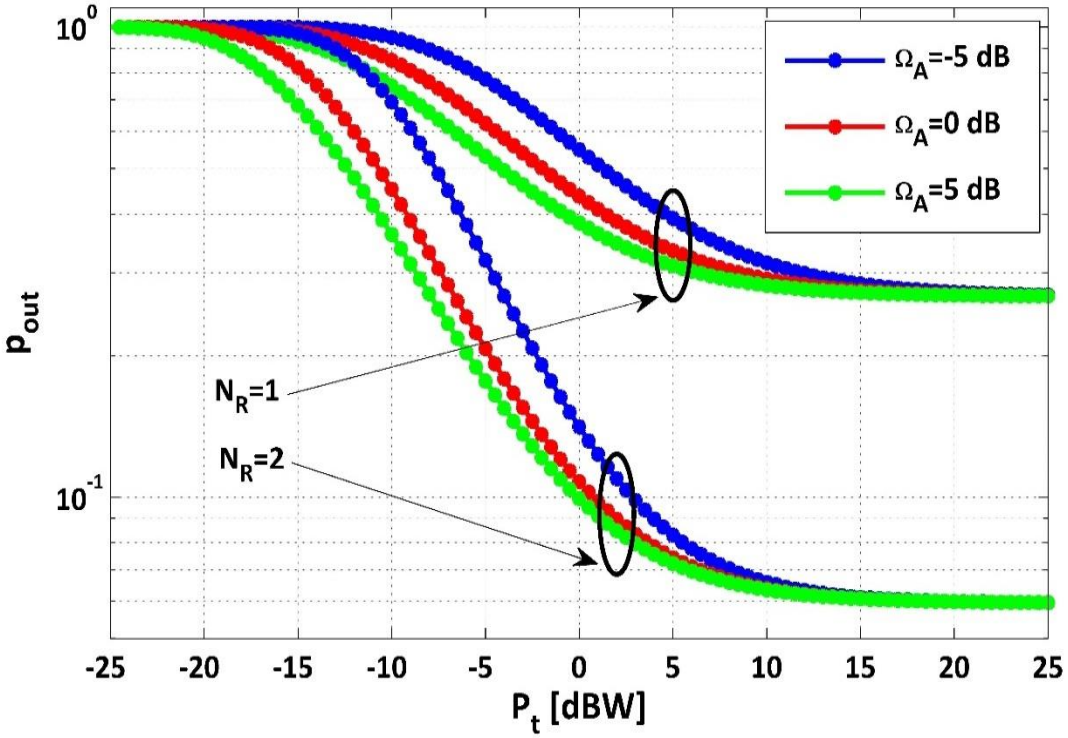

Fig. 4. SOP versus P_t with $R_S = R_d = 0.1$, $\beta = \frac{1}{3}$, $\Omega_E = 1$ dB, $\Omega_D = \Omega_p = \Omega_S = \Omega_R = \Omega_t = 5$ dB, $N_D = N_E = 3$, $m = 1$ and $P_I = 10$ dBW.

As shown in Fig. 5, the SOP can also be improved by decreasing the values of N_E and Ω_E, i.e., decreasing the number of the antennas at E signifies less diversity gain at E, while decreasing Ω_E will decrease the quality of the wiretap channel at E.

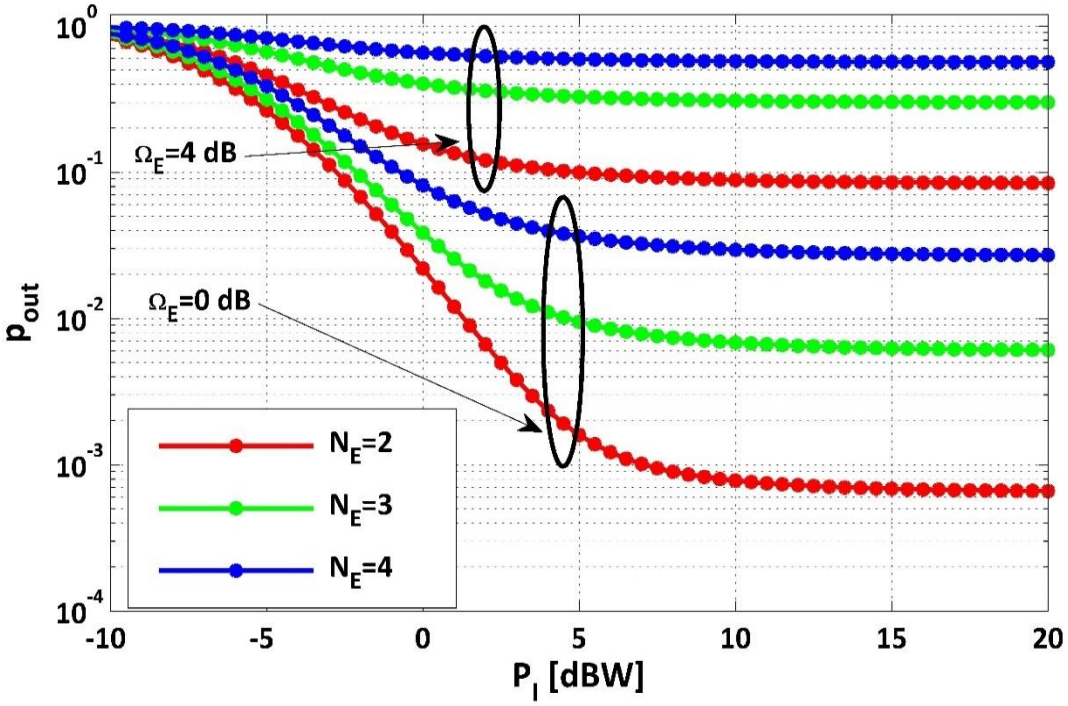

Fig. 5. SOP versus P_I with $R_S = R_d = 0.1$, $\beta = \frac{1}{3}$, $\Omega_D = \Omega_p = \Omega_S = \Omega_R = \Omega_t = \Omega_A = 5$ dB, $N_D = 3$, $N_R = 2$, $P_t = 10$ dBW and $m = 2$.

Fig. 6 shows the security performance against β for varying N_R. However, the exact value of β plays an important role in dividing the time between the energy harvesting phase and information transmission phase. Hence it is tedious to determine the exact value of β that achieves the lowest secrecy outage probability.

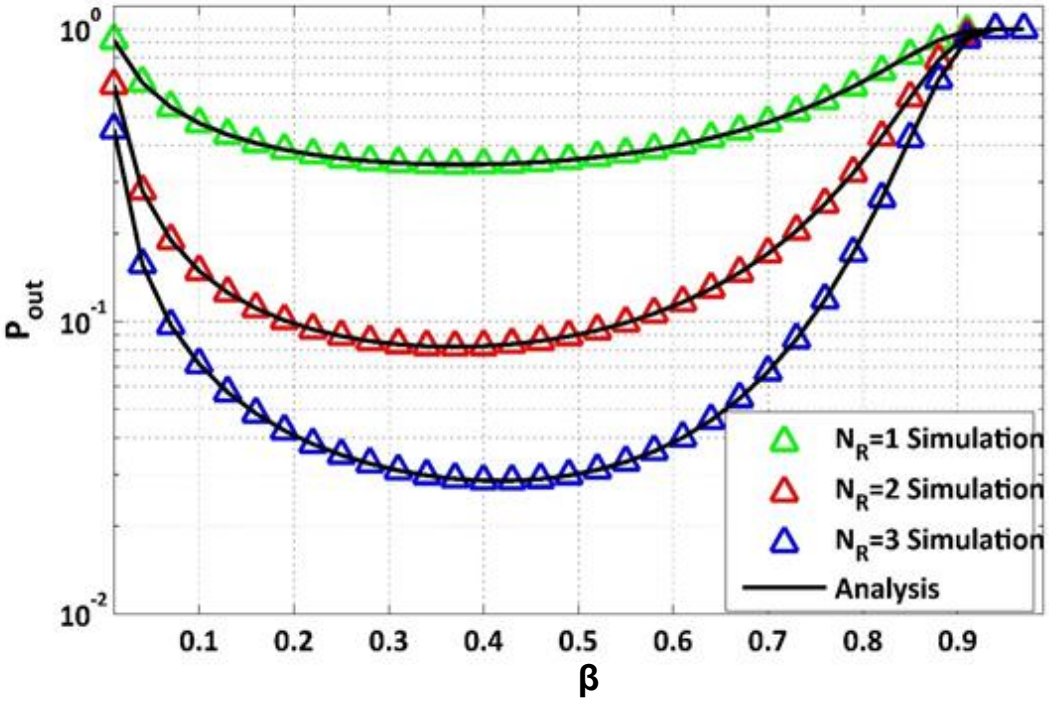

Fig. 6. SOP versus β with $R_S = R_d = 0.1$, $\Omega_E = 1$ dB, $\Omega_D = \Omega_p = \Omega_S = \Omega_R = \Omega_t = \Omega_A = 5$ dB, $N_D = N_E = 4$, $P_t = 0$ dBW, $P_I = 10$ dBW and $m = 1$.

Initially, the security performance can be enhanced by increasing β up to a certain point. Here, increasing β means that more energy can be harvested by both S and R. Nonetheless, increasing β reduces the time slot for the second and the third time phases. Finally, the security performance can also be enhanced by increasing the number of the antennas at R, N_R, i.e., more antennas can be selected for data transmission. Moreover, increasing the number of antennas at R will maximize β and improve the SOP. e.g., when $N_R = 1, \beta = 0.37$, the secrecy outage performance is greater than that for $N_R = 2, \beta = 0.37$ and for $N_R = 3, \beta = 0.43$, respectively.

Fig. 7 shows the security performance against β for different values of P_t. In particular, the SOP is enhanced by increasing the values of P_t and β. One can notice that increasing P_t will maximize the harvested energy at S and R. Moreover, increasing P_t will minimize β (i.e., this means that lower time will be allocated for the EH phase due to increasing the transmitted power from the PT); e.g., when $P_t = -5$ dBW, $\beta = 0.46$, the secrecy outage performance is greater than that for $P_t = 0$ dBW, $\beta = 0.37$ and for $P_t = 5$ dBW, $\beta = 0.25$, respectively.

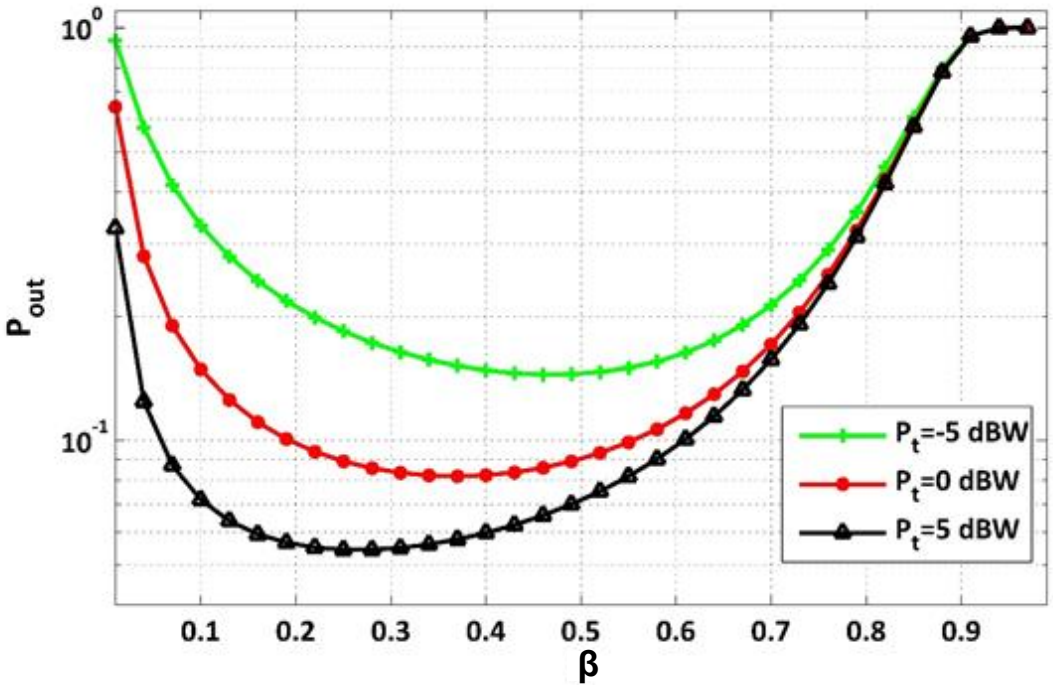

Fig. 7. SOP versus β with $R_S = R_d = 0.1$, $\Omega_E = 1$ dB, $\Omega_D = \Omega_p = \Omega_S = \Omega_R = \Omega_t = \Omega_A = 5$ dB, $N_D = N_E = 4$, $N_R = 2$, $P_I = 10$ dBW and $m = 1$.

Finally, Fig. 8 shows the security performance against β for different values of Ω_A. Here, the security performance can be enhanced by increasing β up to a certain point and increasing Ω_A. i.e., higher Ω_A signifies better main channel quality which is used to collect the energy signal from PT to R. Particularly, one can notice that increasing Ω_A will decrease β. This means lower time will be allocated for the EH phase (i.e., increasing Ω_A will maximize the harvested energy at R and will minimize β which will improve the SOP). Eventually, when $\Omega_A = -15$ dBW, $\beta = 0.55$, the secrecy outage performance is greater than that for $\Omega_A = -5$ dBW, $\beta = 0.4$ and for $\Omega_A = 5$ dBW, $\beta = 0.37$, respectively.

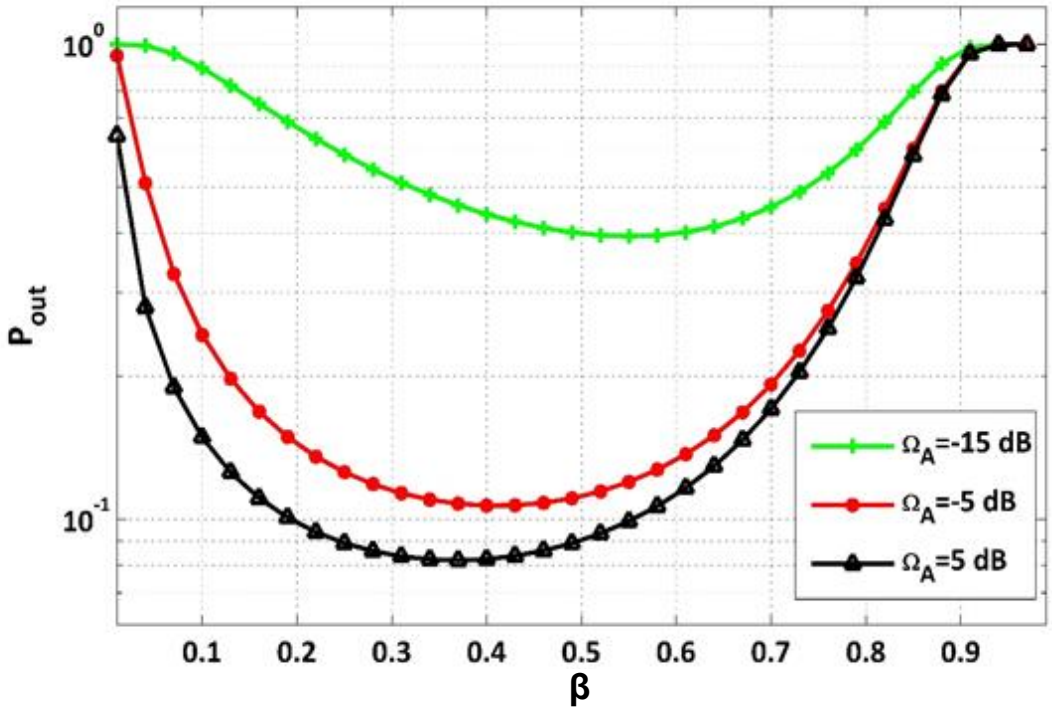

Fig. 8. SOP versus β with $R_S = R_d = 0.1$, $\Omega_E = 1$ dB, $\Omega_D = \Omega_p = \Omega_S = \Omega_R = \Omega_t = 5$ dB, $N_R = 2$, $N_D = N_E = 4$, $P_t = 0$ dBW, $P_I = 10$ dBW and $m = 1$.

5. CONCLUSIONS

A MIMO cooperative communication - that contains a source, destination, DF relay, and an active eavesdropper - was studied. A precise closed-form SOP for the secondary relay was derived over Nakagami-m fading channel. The energy harvesting approach was considered at the source, and relay. Moreover, transmit antenna selection with MRC technique is implemented at the secondary relay, while the MRC technique is employed at both the destination and the eavesdropper to enhance system security.

Numerical results showed that when the number of the antennas at the relay and/or the destination increases, the secrecy outage performance of the system is improved. It was indicated that the parameters between the relay and destination have a great impact on the secrecy outage probability. Furthermore, increasing the transmit power at the primary transmitter will effectively enhance the secrecy performance. Therefore, care must be taken to increase the power of the primary transmitter in order to enhance the energy efficiency at the source and relay.

In future works, multi relays can be add between the source and destination to enhance the security performance and to increase the coverage area by using optimal relay selection scheme to select the best relay to transmit data. Moreover, this model can be extended - in future work - for the case with passive eavesdropper that lacks both CSI and channel estimation errors.

Appendix:

By substituting Eqs. (10), (13) and (34) into Eq. (33), we obtain:

$$\begin{aligned} I_2 &= \int_0^{\infty} f_{Y_P}(x)\left(1 - F_{Y_A}\left(\frac{\varphi_1}{x}\right)\right) H_2(x)dx \\ &= \int_0^{\infty} \frac{{\lambda_p}^{m_p}\Gamma\left(T_A, \lambda_A\frac{\varphi_1}{x}\right)}{\Gamma(T_A)\Gamma(m_p)} x^{m_P-1}e^{-\lambda_p x}\left(1 - \sum_{k,l} G_{k,l}\,(\gamma x)^{k-l}e^{-\lambda_{R_iD}\gamma x}\right)dx \end{aligned} \tag{36}$$

Now, the above equation can be solved by using Eqs. (8.352.7) of [15], we achieve:

$$\Gamma\left(T_A, \lambda_A\frac{\varphi_1}{x}\right) = \Gamma(T_A)e^{-\lambda_A\frac{\varphi_1}{x}}\sum_{t=0}^{T_A-1}\frac{\left(\lambda_A\frac{\varphi_1}{x}\right)^t}{t!} \tag{37}$$

By substituting Eq. (37) into Eq. (36) and by utilizing Eq. (3.471.9) of [15] to solve the integral, I_2 can be expressed as follows:

$$\begin{aligned} I_2 &= \int_0^{\infty}\frac{{\lambda_p}^{m_p}}{\Gamma(m_p)}x^{m_P-1}e^{-\lambda_p x-\lambda_A\frac{\varphi_1}{x}}\sum_{t=0}^{T_A-1}\frac{\left(\lambda_A\frac{\varphi_1}{x}\right)^t}{t!}\times\left(1 - \sum_{k,l} G_{k,l}\,(\gamma x)^{k-l}e^{-\lambda_{R_iD}\gamma x}\right)dx \\ &= \sum_{t=0}^{T_A-1}\frac{{\lambda_p}^{m_p}(\lambda_A\varphi_1)^t}{\Gamma(m_p)t!}\int_0^{\infty}x^{m_P-t-1}e^{-\lambda_p x-\lambda_A\frac{\varphi_1}{x}}dx \\ &\quad - \sum_{t=0}^{T_A-1}\sum_{k,l}\frac{{\lambda_p}^{m_p}G_{k,l}(\lambda_A\varphi_1)^t\gamma^{k-l}}{\Gamma(m_p)t!}\int_0^{\infty}x^{m_P-t+k-l-1}e^{-\left(\lambda_p+\lambda_{R_iD}\gamma\right)x-\lambda_A\frac{\varphi_1}{x}}dx \\ &= \sum_{t=0}^{T_A-1}\frac{2{\lambda_P}^{m_P}(\lambda_A\varphi_1)^t}{\Gamma(m_P)t!}\left(\frac{\lambda_A\varphi_1}{\lambda_P}\right)^{\frac{m_P-t}{2}}K_{m_P-t}\left(2\sqrt{\lambda_P\lambda_A\varphi_1}\right) \\ &\quad - \sum_{t=0}^{T_A-1}\sum_{k,l}\frac{2G_{k,l}{\lambda_P}^{m_P}(\lambda_A\varphi_1)^t\gamma^{k-l}}{\Gamma(m_P)t!}\left(\frac{\lambda_A\varphi_1}{\lambda_P+\lambda_{R_iD}\gamma}\right)^{\frac{k+m_P-t-l}{2}} \\ &\qquad \times K_{k+m_P-t-l}\left(2\sqrt{\left(\lambda_P+\lambda_{R_iD}\gamma\right)\lambda_A\varphi_1}\right) \end{aligned} \tag{38}$$

REFERENCES

[1] R. Amirtharajah, A. Chandrakasan, "Self-powered signal processing using vibration-based power generation," *IEEE Journal of Solid-State Circuits,* vol. 33, no. 5, pp. 687–695, 1998.

[2] T. Soyata, L. Copeland, W. Heinzelman, "RF energy harvesting for embedded systems: a survey of tradeoffs and methodology," *IEEE Circuits and System Magazine,* vol. 16, no. 1, pp. 22–57, 2016.

[3] S. Park, H. Kim, D. Hong, "Cognitive radio networks with energy harvesting," *IEEE Transactions on Wireless Communications*, vol. 12, no. 3, pp. 1386–1397, 2013.

[4] S. Lee, R. Zhang, K. Huang, "Opportunistic wireless energy harvesting in cognitive radio networks," *IEEE Transactions on Wireless Communications,* vol. 12, no. 9, pp. 4788–4799, 2013.

[5] A. Hyadi, Z. Rezki, M. Alouini, "An overview of physical layer security in wireless communication systems with CSIT uncertainty," *IEEE Access,* vol. 4, pp. 6121–6132, 2016.

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

[7] L. Hongjiang, M. Xu, H. Zhang, G. Pan, I. Ansari, K. Qaraqe, "Secrecy outage performance for underlay MIMO CRNs with energy harvesting and transmit antenna selection," *IEEE Globecom Workshops*, pp. 1-6, 2016.

[8] T. Do-Dac, K. Ho-Van, "Energy harvesting cognitive radio networks: security analysis for Nakagami-m fading," *Wireless Networks*, vol. 10, pp. 1–12, 2019.

[9] K. Ho-Van, T. Do-Dac, "Security performance of underlay cognitive relaying networks with energy harvesting," *Wireless Personal Communications,* vol. 110, no. 2, pp. 829–46, 2020.

[10] A. Khisti, G. Wornell, "Secure transmission with multiple antennas—part II: the MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[11] K. Odeyemi, P. Owolawi, O. Olakanmi, "Secrecy outage probability in energy harvesting aided underlay cognitive radio network under eavesdroppers scenarios," *Transactions on Emerging Telecommunications Technologies*, vol. 110, no. 8, pp. e4041, 2020.

[12] K. Ho-Van, T. Do-Dac, "Security analysis for underlay cognitive network with energy-scavenging capable relay over Nakagami-m fading channels," *Wireless Communications and Mobile Computing*, vol. 2019, 2019.

[13] M. Bouabdellah, F. El Bouanani, P. Sofotasios, S. Muhaidat, D. Da Costa, K. Mezher, "Cooperative energy harvesting cognitive radio networks with spectrum sharing and security constraints," *IEEE Access,* vol. 7, no. 11, pp. 173329-173343, 2019.

[14] H. Lei, H. Zhang, I. Ansari, Z. Ren, D. Pan, K. Qaraqe, M. Alouini, "On secrecy outage of relay selection in underlay cognitive radio networks over Nakagami-m fading channels," *IEEE Transactions on Cognitive Communications and Networking,* vol. 3, no. 4, pp. 614–627, 2017.

[15] K. Ho-Van, T. Do-Dac, "Security enhancement for energy harvesting cognitive networks with relay selection," *Wireless Communications and Mobile Computing,* vol. 2020 , 2020.

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

[17] H. Zhao, Y. Tan, G. Pan, Y. Chen, N. Yang, "Secrecy outage on transmit antenna selection/maximal ratio combining in MIMO cognitive radio networks," *IEEE Transactions on Vehicular Technology,* vol. 65, no. 12, pp. 10236–10242, 2016.

[18] I. Gradshteyn, I. Ryzhik, *Table of Integrals, Series and Products*, San Diago, CA: Academia Press, 2007.

[19] H. Lei, H. Zhang, I. Ansari, C. Gao, Y. Guo, G. Pan, K. Qaraqe, "Secrecy outage performance for SIMO underlay cognitive radio systems with generalized selection combining over Nakagami-m channels," *IEEE Transactions on Vehicular Technology,* vol. 65, no. 12, pp. 10126–10132, 2016.

[20] H. Lei, C. Gao, I. Ansari, Y. Guo, Y. Zou, G. Pan, K. Qaraqe "Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-m channels," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2237–2250, 2016.

[21] X. Zhang, Y. Zhang, Z. Yan, J. Xing, W. Wang, "Performance analysis of cognitive relay networks over Nakagami-m fading channels," *IEEE Journal on Selected Areas in Communications,* vol. 33, no. 5, pp. 865–877, 2014.

[22] J. Zhu, Y. Zou, B. Champagne, W. Zhu, L. Hanzo, "Security–reliability tradeoff analysis of multirelay-aided decode-and-forward cooperation systems," *IEEE Transactions on Vehicular Technology,* vol. 65, no. 7, pp. 5825–5831, 2015.

[23] L. Wang, M. Elkashlan, J. Huang, R. Schober, R. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-m fading channels," *IEEE Transactions on Wireless Communications,* vol. 13, no. 11, pp. 6054–6067, 2014

[24] M. Bloch, J. Barros, M. Rodrigues, S. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory,* vol. 54, no. 6, pp. 2515–2534, 2008.