Secrecy Performance for Underlay Cooperative Cognitive Radio Network with EH and TAS Using MIMO over Nakagami-m Fading Channels

Saja Mohd Alquran and Mahmoud A. Khodeir

March 9, 2021

Secrecy performance for Underlay Cooperative Cognitive Radio Network with EH and TAS Using MIMO over Nakagami-m Fading Channels

SAJA MOH'D ALQURAN, and Mahmoud A. Khodeir
Electrical Engineering Department
Jordan University of Science and Technology
Irbid, Jordan
Smalquran16@eng.just.edu.jo, makhodeir@just.edu.jo

***Abstract*— This paper introduces underlay Multiple Input Multiple Output (MIMO) cooperative communication involving source, destination, eavesdropper, primary nodes and Decode and Forward (DF) relay, where the source and relay are powered by harvested energy from the primary transmitter to improve both energy efficiency and spectral efficiency. Here, the power of secondary nodes is strictly constrained by interference power and maximum transmit power. In particular, the unlicensed transmitter will forward the message of the unlicensed sender to the unlicensed recipient by using an intermediate relay. Here, the direct path is considered to be unreliable. Moreover, the secrecy outage performance will be studied over Nakagami-m fading channel, closed-form secrecy outage performance for secondary relay is derived with an active eavesdropper, where all the Channel State Information (CSI) is assumed to be available at source and relay. Here, Transmit Antenna Selection/Maximal Ratio Combining (TAS/MRC) is implemented at the secondary relay. Also, Maximal Ratio Combining (MRC) technique will utilize at both the destination and the eavesdropper to enhance the security performance. The secrecy performance for the secondary relay and the closed-form expression is derived for multiple antenna cooperative cognitive radios. The mathematical results indicate that when the number of antenna at the relay and/or destination increases, the secrecy outage performance of the system can be enhanced.**

Keywords—Cooperative decode-and-forward relay, Energy Harvesting, Transmit Antenna Selection scheme, maximal ratio combining, MIMO, physical layer security, Nakagami-m fading

I. Introduction

The increase in demand for mobile data traffic, which 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).

Energy harvesting can be implemented by allowing SUs to harvest energy from the Radio Frequency (RF) signals that are close to the RF sources (i.e., PUs, 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 equipments [1], [2]. Interference signals emitted from the primary transmitter 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 capacity for the main channel and that for the wiretap channel in the system is lower than the secrecy data rate. (i.e., this technique is used in this paper as a performance of metrics). To achieve secure communications and to save both energy and spectrum, the authors in [6] employed the EH technique for underlay cognitive systems. In [7], the authors studied the security performance of Cognitive Radio Networks (CRNs) with energy harvesting under interference power constraint, maximum transmit power constraint under Nakagami-m fading channel. Furthermore, the multiple antennas technique is considered as an effective method to increase the security performance for wireless wiretap channels as shown in [8].

We can improve the coverage of the area by using cooperative communication. In [9] the authors employed a DF relay between the source and the destination, and the power sources of this relay relies on harvesting energy from utilizing the RF signals. Particularly, the author calculates the security performance for the underlay CRNs to guarantee that the direct path between the source and the destination node is under deep fading and/or shadowing. Moreover, the authors in [10] analyzed the PLS of a Cognitive Radio Networks (CRN) system with an intermediate relay at the middle to harvest energy and re-encoded data before relaying it to the destination. Here, both Independent 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 also to provide cooperative diversity. In this domain, several schemes with relay selection have been examined in [11], the authors used an optimal relay selection scheme to improve the security of cooperative wireless communication against the wiretap channel.

Finally, the secrecy performance to the secondary relay will be studied over Nakagami-*m* fading channel with an active eavesdropper, where all CSI is assumed to be available at the secondary nodes (i.e., source and relay), while eavesdropper will try to overhear the confidential information that is transmitted from the relay to the destination through the wiretap channel. Here, the secondary nodes are powered by energy that is harvested from the primary transmitter. Also, TAS/MRC scheme is assumed active at the relay and the MRC technique will employ at the destination and the eavesdropper to enhance the performance system security.

The rest of this paper is organized as follows. In section II, we will describe the system model of our work. In section III is analyzed the secrecy performance. Section IV presents and discusses the numerical results. Finally, we conclude the paper in section V.

II. System Model

In this section, a cognitive radio network typical operating in underlay mode which contains Primary Transmitter (PT), Primary Receiver (PR), Source (S), Relays (R), Destination (D), and an Eavesdropper (E) is considered as shown in Figure 1.

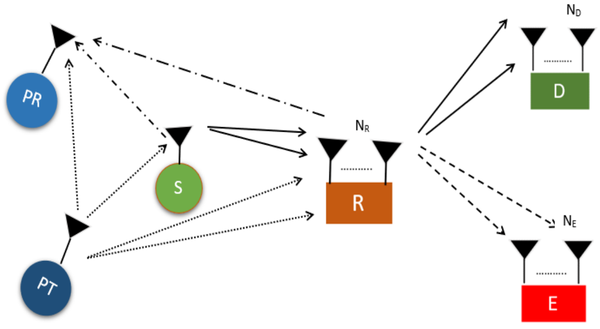

Fig. 1: System model with one relay.

All the PT, PR, and S are equipped with a single antenna, but D, E, and R are equipped with $N_D \geq 1$, $N_E \geq 1$ and $N_R \geq 1$ antennas. Also, the MRC diversity scheme is implemented at D and E. There are no direct links between the source to the destination and to the eavesdropper due to deep fading and shadowing and communication can be deployed using an intermediate relay. The intermediate relay is selected to be DF 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.

This system model can be studied over independent and identically distributed (i.i.d.) quasi-static Nakagami-*m* fading channel with fading parameters m_S, m_R, m_D, m_E and the average channel power gains Ω_S, Ω_R, Ω_D and Ω_E. Moreover, the thermal noise is added at each receiver is modeled as an AWGN with variance σ^2. The Optimal Antenna Selection (OAS) scheme is used at the secondary relay, where all the CSI is assumed to be available at S and R.

Also, the exchange of data from S to D requires three-time phase, the first portion of the time β ($0 \leq \beta \leq 1$) is dedicated for EH. The second and third portion of the time $(1-\beta)/2$ are dedicated to secondary source and relay transmission to the D/E. In the second part, S will send the message to the relay (i.e., this relay will try to decode the received signal). In the third part, the relay will be decoded data coming to D. Here, E can overhear the messages from the relay.

The energy of the secondary nodes is depending on harvested the RF signals received from PT that is stored in an infinite capacity buffer. The harvested energy at S can be expressed as

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

where $0 \leq \eta \leq 1$ implies the EH efficiency [12], P_t is the transmit power at the PT, $Y_t = \left| h_{PT-S} \right|$, and h_{PT-S} is the instantaneous channel fading coefficient 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 [13]:

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

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

where $\lambda_t = \frac{m_t}{\Omega_t}$, $\Gamma(.)$ is the Gamma function as defined by (8.310.1) of [14] and $\Gamma(.,.)$ is the Upper incomplete Gamma function as defined by (8.350.2) of [14].

Based on (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 source to the relay.

Accordingly, to the underlay spectrum sharing technique, S and R are allowed to use the same licensed spectrum if the interference due to PR lower than a certain threshold and the transmitting power does not exceed the maximum transmitted power. Due to these restriction power, the transmit power at *S* can be expressed [15], [16]:

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

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 follows [13]:

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

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

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 PT and j-th antenna at the R.

The PDF and the CDF of the channel gain Y_A can be shown, respectively, as [13]:

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

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

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 (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 transmission information from R to D.

The transmit power at R is strictly constrained as follows [15], [16]:

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

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 [13]:

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

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

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

In the second time phase, the channel capacity between S and the relay 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 the S and j-th antenna at Relay.

The CDF of the channel gain Y_{SR} can be written as:

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

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

Based on [17] and [18], the relay 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 R can successfully decode depending on (15), can be expressed as:

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

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

Substituting (4),(2),(7) and (16) into (17), then using (3.471.9) and (8.352.7) in [14], K_1 can be written as:

$$\begin{aligned}
K_1 &= pr\left(Y_{SR} > \frac{\varsigma}{Y_t}, Y_s \le \frac{\xi}{Y_t}\right) \\
&= \int_0^\infty \left(1 - F_{Y_{SR}}\left(\frac{\varsigma}{x}\right)\right) F_{Y_S}\left(\frac{\xi}{x}\right) f_{Y_t}(x) dx \\
&= \sum_{l=0}^{T_{SR}-1} \frac{(\lambda_t)^{m_t} (\lambda_{SR}\varsigma)^l}{\Gamma(m_t) l!} \left(\int_0^\infty x^{m_t-l-k-1} e^{-\lambda_t x - \lambda_{SR}\frac{\varsigma}{x}} dx \right. \\
&\quad \left. - \sum_{l=0}^{m_S-1} \frac{(\lambda_S \xi)^k}{k!} \int_0^\infty x^{m_t-l-k-1} e^{-\lambda_t x - \lambda_{SR}\frac{\varsigma}{x}} dx \right) \\
&= \sum_{l=0}^{T_{SR}-1} \frac{(\lambda_t)^{m_t} (\lambda_{SR}\varsigma)^l}{\Gamma(m_t) l!} \left(2\left(\frac{\lambda_{SR}\varsigma}{\lambda_t}\right)^{\frac{m_t-l}{2}} K_{m_t-l}\left(2\sqrt{\lambda_t \lambda_{SR} \varsigma}\right) \right. \\
&\quad \left. - \sum_{k=0}^{m-1} \frac{2(\lambda_S \xi)^k}{k!} \left(\frac{\lambda_{SR}\varsigma + \lambda_S \xi}{\lambda_t}\right)^{\frac{m_t-l}{2}} K_{m_t}\left(22\sqrt{\lambda_t \lambda_{SR}\varsigma + \lambda_S \xi}\right) \right)
\end{aligned} \tag{18}$$

where $\varsigma = \frac{(\theta-1)\sigma^2(1-\beta)}{2\eta\beta P_t}$ and $\xi = \frac{P_I(1-\beta)}{2\eta\beta P_t}$. and $K_v(x)$ is the modified Bessel function of order v, as defined by (8.407.1) of [14].

Now, by substituting (3),(4),(6) and (16) into (17), then utilizing (3.471.9) and (8.352.7) of [14], K_2 can be written as:

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

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

In the third time phase, one can denote the successful decoding relay. Then, the channel capacity between the 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 *j*-th antenna at D.

The CDF of the channel gain Y_{R_iD} can be expressed as [13]:

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

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

Correspondingly, the channel capacity from the relay 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 the relay and the *j*-th antenna at E.

The PDF of Y_{R_iE} can be expressed as [13]:

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

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

We consider that the full CSI of both the main and the wiretap channels is available at source and relay, which is called active eavesdropping [19]. The antenna at R is selected to maximizes the achievable secrecy rate in the secondary relay which is used to transmit signals to D [16], [20]. In general, the metrics of the chosen antenna in the OAS scheme is showed as:

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

where C_i is the achievable secrecy rate via the *i*-th antenna at *R*. Thus, the instantaneous secrecy capacity at the relay is the capacity difference between the main channel (i.e., R to D) and the wiretap channel (i.e., R to E) 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 $[x]^+ = max(x, 0)$,

III. Exact Secrecy Outage Probability

We evaluate the secrecy performance of this system model by deriving the exact closed-form expressions for SOP in this section. The SOP has defined the probability that the instantaneous secrecy capacity does not exceed the target secrecy rate, $R_S \geq 0$ [20]. using (21), the security performance can be calculated by using this equation:

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

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

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

Substituting (20) and (22) into (27), one obtains:

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

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

Now, by substituting (11) and (12) into (28), one obtains:

$$P_{out}^{OAS} = Pr\left(Y_{R_iD} \le \epsilon Y_{R_iE} + \frac{(\epsilon-1)\sigma^2}{\widehat{P_R}}\right)$$
$$= Pr\left(Y_{R_iD} \le \epsilon Y_{R_iE} + \frac{(\epsilon-1)\sigma^2}{\widehat{P_R}}, \widehat{P_R} = P_{max2}\right)$$
$$+pr\left(Y_{R_iD} \le \epsilon Y_{R_iE} + \frac{(\epsilon-1)\sigma^2}{\widehat{P_R}}, \widehat{P_R} = \frac{P_I}{Y_P}\right)$$

$$= \underbrace{pr\left(Y_{R_iD} \le \epsilon Y_{R_iE} + \frac{(\epsilon-1)\sigma^2}{P_{max2}}, Y_P \le \frac{P_I}{P_{max2}}\right)}_{I_1}$$
$$+ \underbrace{pr\left(Y_{R_iD} \le \epsilon Y_{R_iE} + \frac{(\epsilon-1)\sigma^2 Y_P}{P_I}, Y_P > \frac{P_I}{P_{max2}}\right)}_{I_2} \quad (29)$$

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

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

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 (21) and (23) into $H_1(x)$, then using (8.352.7) and (3.326.2) of [14], one achieves:

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

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 (9), (14) and (31) into (30), then using (8.352.7) and (3.471.9) of [14], one obtains:

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

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

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

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

By substituting (21) and (23) into $H_2(x)$, then using (8.352.7) and (3.326.2) of [14], one finds:

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

By substituting (10), (13) and (34) into (33), then utilizing (8.352.7) and (3.471.9) of [14], one obtains:

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

In the end, the SOP for the relay is obtained by substituting (32) and (35) into (29) and in (27) and (26) and (17).

IV. Numerical Results

In this section, the numerical results are present and study the effect of changing values of variable on the security performance for a cooperative cognitive MIMO system under the effect of a relay and source are harvested energy from the primary transmitter. Also, the OAS scheme is investigated at the relay. 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 $m_{SR} = m_R, m_{R_iD} = m_D, m_{R_iE} = m_E$, $m_S = m_R = m_t = m_A = m_D = m_E = m$, $\Omega_{SR} = \Omega_R$, $\Omega_{R_iD} = \Omega_D$ and $\Omega_{R_iE} = \Omega_E$.

Fig. 2 shows the security performance against Ω_D for different values of the parameters N_D and m. By increasing Ω_D, N_D and m, the security performance can be enhanced. In particular, Ω_D indicates the average SNR of the main channel (i.e., from the relay to the destination). Moreover, reducing the parameter *m* means that the channel fading is robust the MRC diversity gain at D can be improved by increasing N_D. Finally, one can notice that the security performance can be enhanced for lower values of the parameters *m* and small Ω_D region.

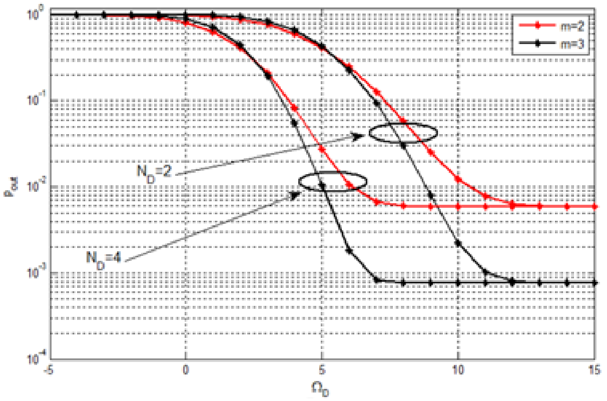

Fig. 2: SOP versus Ω_D with $R_S = R_d = 0.1$, $\beta = \frac{1}{2}$, $\Omega_E = 1$ dB, $\Omega_p = \Omega_S = \Omega_R = \Omega_t = \Omega_A = 5$ dB, $N_E = 4$, $N_R = 2$, $P_t = 1$ W and $P_I = 2$ W.

Fig. 3 shows the SOP against P_t for different values for 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 signal from PT to the relay. While increasing the number of antennas at the relay, N_R, means additional antennas can be picked for data transmission from R.

Finally, the SOP can be improved by increasing the value of the transmit power, P_t, at the PT (i.e., higher transmit power at the primary transmitter leads to maximize the harvested energy by the secondary transmitter nodes e.g., source and relay) to a certain point ($P_t = 15$ dBW). This means that increasing P_t cannot enhance the SOP in an unlimited fashion.

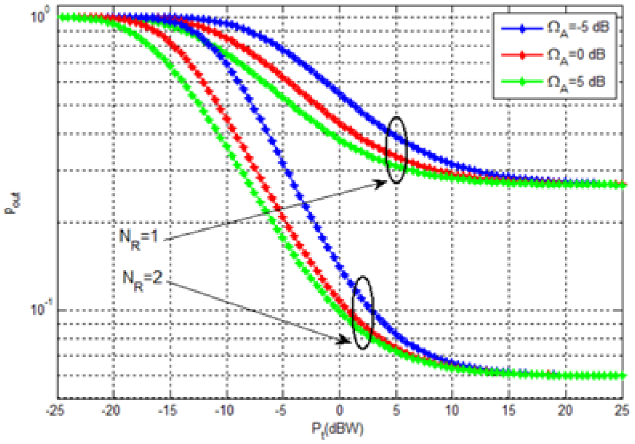

Fig. 3: SOP versus P_t with $R_S = R_d = 0.1$, $\beta = \frac{1}{2}$, $\Omega_E = 1$ dB, $\Omega_D = \Omega_p = \Omega_S = \Omega_R = \Omega_t = 5$ dB, $N_D = N_E = 3$, $m = 1$ and $P_I = 10$ dBW.

Also, the SOP can 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. Also, decreasing Ω_E will decrease the quality of the wiretap channel at E as shown in Fig. 4.

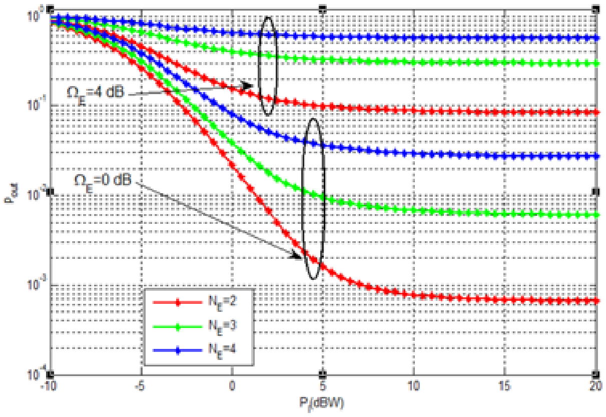

Fig. 4: SOP versus P_I with $R_S = R_d = 0.1$, $\beta = \frac{1}{2}$, $\Omega_D = \Omega_p = \Omega_S = \Omega_R = \Omega_t = \Omega_A = 5$ dB, $N_D = 3$, $N_R = 2$, $P_t = 10$ dBW and $m = 2$.

Fig. 5 shows the security performance against β for a different value of N_R . In the beginning, the security performance can be enhanced by increasing the value of β up to a certain point. Here, increasing the value of β means more energy can be harvested by S and R. Finally, the security performance is enhanced by increasing the number of the antennas N_R at R i.e., more antennas can be selected for transmitting information. Moreover, increasing the number of antennas at R leads to 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.

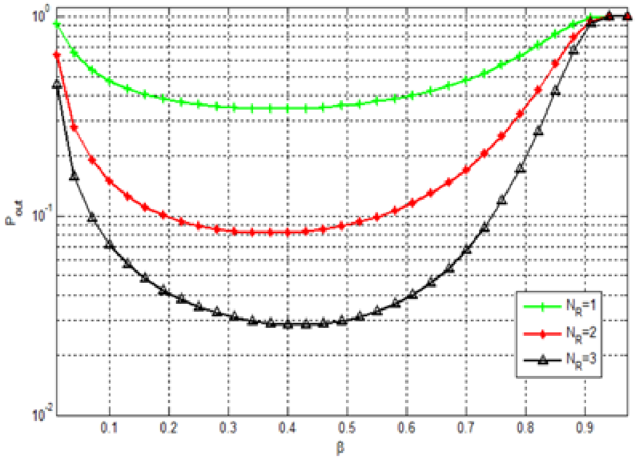

Fig. 5: SOP versus β with $R_S = R_d = 0.1$, $\Omega_E = 1$ dB, $\Omega_D = \Omega_p = \Omega_S = \Omega_R = \Omega_t = \Omega_A = 5$ dB, $N_D = N_E = 4$, $P_t = 0$ dBW, $P_I = 10$ dBW and $m = 1$.

Fig. 6 shows the security performance against β for different values of P_t. Here, the SOP is enhanced by increasing P_t at the PT. This means lower time will be allocated for the

EH phase (i.e., increasing P_t will maximize the harvested energy at S and R). Moreover, increasing P_t will minimize β and improve the SOP. 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.

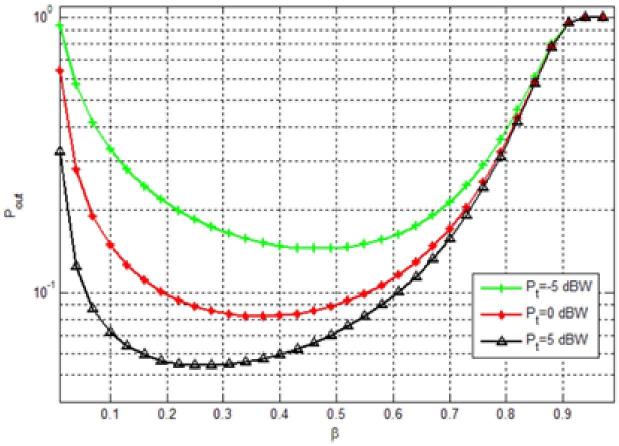

Fig. 6: SOP versus β with $R_S = R_d = 0.1$, $\Omega_E = 1$ dB, $\Omega_D = \Omega_p = \Omega_S = \Omega_R = \Omega_t = \Omega_A = 5$ dB, $N_D = N_E = 4$, $N_R = 2$, $P_I = 10$ dBW and $m = 1$.

Fig. 7 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. Particularly, one can notice that increasing Ω_A will decrease β. i.e., higher Ω_A signifies better main channel quality which is used to collect the energy signal from PT to R. 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. e.g., 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).

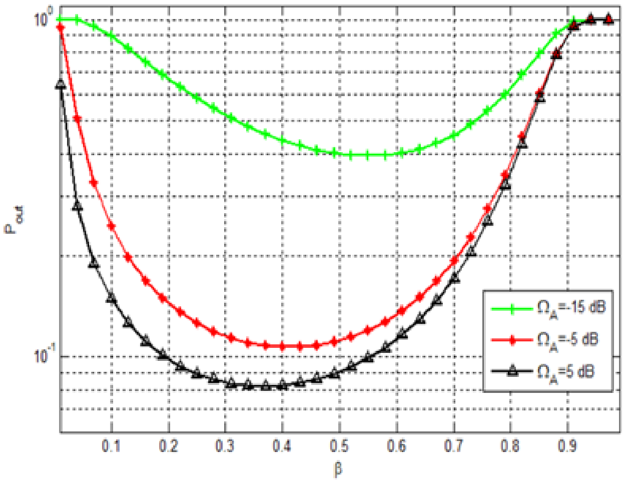

Fig. 7: SOP versus β with $R_S = R_d = 0.1$, $\Omega_E = 1$ dB, $\Omega_D = \Omega_p = \Omega_S = \Omega_R = \Omega_t = 5$ dB, $N_R = 2$, $N_D = N_E = 4$, $P_t = 0$ dBW, $P_I = 10$ dBW and $m = 1$.

V. Conclusion

In this paper, we realize MIMO cooperative communication with the source, destination, eavesdropper, and DF relay. Here, we derived precise closed-form SOP for the secondary relay over Nakagami-*m* fading channel for the approach of EH is considered, active eavesdropper, and TAS/MRC scheme is active at the relay. Also, the MRC scheme is employed at the destination and the eavesdropper to enhance system security.

Finally, the numerical results show that when the number of the antenna at R and/or D increases, the secrecy outage performance of the system can be improved. It is indicated that the parameters between R and D have a great impact on the SOP, and when increasing the power of the primary transmitter is very effective in enhancing secrecy performance. Then, care must be taken to increase the power of the primary transmitter to enhance energy efficiency at the source and relay.

In future works will add multi relays between source and destination to enhance security performance, increase the coverage area, and we will select one relay to send data by using an optimal relay selection scheme.

References

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

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

[3] S. Park, H. Kim, and D. Hong, “Cognitive radio networks with energy harvesting,” *IEEE Trans. Wirel. Commun.*, vol. 12, no. 3, pp. 1386–1397, 2013.

[4] S. Lee, R. Zhang, and K. Huang, “Opportunistic wireless energy harvesting in cognitive radio networks,” *IEEE Trans. Wirel. Commun.*, vol. 12, no. 9, pp. 4788–4799, 2013.

[5] A. Hyadi, Z. Rezki, and M.-S. 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, SA. Vorobyov, J. Chen, H. Zhang, “Secure communications in underlay cognitive radio networks: User scheduling and performance analysis”. IEEE Commun Lett, vol. 20, pp. 1191–1194, 2016.

[7] T. Do-Dac, K. Ho-Van, “Energy harvesting cognitive radio networks: security analysis for Nakagami-m fading”. Wirel Networks, vol. 10, pp. 1–12, 2019.

[8] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[9] K. Ho-Van and T. Do-Dac, “Security Analysis for Underlay Cognitive Network with Energy-Scavenging Capable Relay over Nakagami-m Fading Channels,” *Wirel. Commun. Mob. Comput.*, vol. 2019, 2019.

[10] M. Bouabdellah, F. El Bouanani, PC. Sofotasios, S. Muhaidat, DB. 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.

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

[12] Y. Jiang, J. Zhu, and Y. Zou, “Secrecy outage analysis of multi-user multi-eavesdropper cellular networks in the face of cochannel interference,” *Digit. Commun. Networks*, vol. 1, no. 1, pp. 68–74, 2015.

[13] H. Zhao, Y. Tan, G. Pan, Y. Chen, and N. Yang, “Secrecy outage on transmit antenna selection/maximal ratio combining in MIMO cognitive

radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10236–10242, 2016.

[14] I. S. Gradshteyn and I. M. Ryzhik, "Table of Integrals, Series and Products,(; Elsevier, 2007)," *Reprod. with Permis. Copyr. owner. Furth. Reprod. prohibited without Permis.*

[15] H. Lei, H. Zhang, IS. Ansari, C. Gao, Y. Guo, G. Pan and K. A. Qaraqe, "Secrecy outage performance for SIMO underlay cognitive radio systems with generalized selection combining over Nakagami-*m* channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10126–10132, 2016.

[16] H. Lei, C Gao, IS Ansari, Y Guo, Y. Zou, G. Pan and K. A. Qaraqe "Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-*m* channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2237–2250, 2016.

[17] X. Zhang, Y. Zhang, Z. Yan, J. Xing, and W. Wang, "Performance analysis of cognitive relay networks over Nakagami-*m* fading channels," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 5, pp. 865–877, 2014.

[18] J. Zhu, Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Security–reliability tradeoff analysis of multirelay-aided decode-and-forward cooperation systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5825–5831, 2015.

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

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