EasyChair Preprint

№ 5123

Realistic Secrecy Outage Performance for Underlay Cognitive Radio Networks Using MIMO Systems with EH and TAS

Saja Alquran and Mahmoud A. Khodeir

March 9, 2021

Realistic Secrecy Outage Performance for Underlay Cognitive Radio Networks Using MIMO Systems with EH and TAS

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*— In this paper, the physical layer secrecy outage performance of Multiple Input Multiple Output (MIMO) secondary nodes is studied. The proposed model is assumed to operate in underlay Cognitive Radio Network (CRN) that contains a primary node with a single antenna. Active eavesdropper is also assumed to present in our model. Furthermore, Transmit Antenna Selection (TAS) scheme is applied at the secondary transmitter that has a suitable battery to charge the collected Radio Frequency (RF) energy broadcasted from the primary transmitter to improve both energy and spectral efficiencies. We achieved the secrecy outage performance of the secondary system and derived exact closed-form expression for the secrecy outage performance. The numerical results show that when the number of the antenna at source and/or destination increases, the secrecy outage performance of the system can be improved.**

***Index Terms*— Cognitive Radio Networks (CRNs), Energy Harvesting (EH), Optimal Antenna Selection (OAS), Maximal Ratio Combining (MRC), Secrecy Outage Probability (SOP), Nakagami-*m* fading.**

I. INTRODUCTION

The power source in wireless communications often has a significant impact on network lifetime [1]. Usually, the wireless nodes depends on a batteries as power supplies while have limited capacity and need physical charge or frequent change. These days, energy-saving in wireless nodes can be attained through a technology that uses RF to harvest energy.

This main target here is to provide both spectrum and energy efficiency using RF to harvest energy in CRN for wireless networking [2], [3]. In general, networks that deploy this kind of technology have two groups of users the Primary Users (PUs) with licensed spectrum and the Secondary Users (SUs) that are allowed to access the licensed spectrum for the PUs based on dynamic spectrum access approaches. Here, the security issue in an underlay mode becomes more complex.

Many researchers investigated the physical layer security technique in order to enhance the performance of wireless channels against eavesdropper users by developing the physical characteristics of wireless communication channels. i.e., In [4], the authors derived exact and asymptotic closed-form expression for SOP with MIMO underlay spectrum and passive eavesdropper.

In RF energy, the SUs are allowed to harvest energy from the RF signals that are close to the RF sources (i.e., PUs, cellular base stations, and other surrounding RF sources). Then the harvested energy is converted into electricity to operate the wireless equipment [5], [6].

Thus, the CRNs with EH technology becomes a focus in recent years. The authors in [3] first suggested the idea of using RF signals from the primary transmitter to power the secondary devices.

The outage and capacity performance for Multiple Input Single Output (MISO) Simultaneous Wireless Information and Power Transfer (SWIPT) system under two schemes Time Splitting (TS) and Power Splitting (PS) over Nakagami-*m* fading channels was derived in [7]. Also, in [8] the authors investigated the SOP of an energy harvesting aided underlay Single Input Multiple Output (SIMO) cognitive radio network under the multiple eavesdroppers over Nakagami-*m* fading channels.

The TAS schemes are considered to be low-cost and low-complex alternative to achieve many of the benefits of MIMO systems. The authors in [9] derived the closed-form expressions of exact and asymptotic SOP over Nakagami-*m* channels with Generalized Selection Combining (GSC) for various schemes of antenna selection and compare it with the space-time transmission (STT) scheme under MIMO cognitive wiretap system.

To the best of the author's knowledge, no open literature addresses the secrecy performance for underlay cognitive MIMO systems with EH and TAS schemes over Nakagami-*m* fading channels. Based on [10-11], the secondary transmitter in the proposed work will be operated using a power by collected from RF signals. In particular, these RF signals are harvested from the primary transmitter to achieve more energy and spectral efficiencies. We investigate the secrecy outage performance of the secondary system and closed-form expression for SOP is derived for multiple antenna at the destination and the eavesdropper with an active eavesdropper.

The rest of this paper is organized as follows. In section II, we will describe the system model of our work. In section III, an SOP analysis is performed. Section IV presents and discusses the numerical results. Finally, we conclude the paper

in section V.

II. SYSTEM MODEL

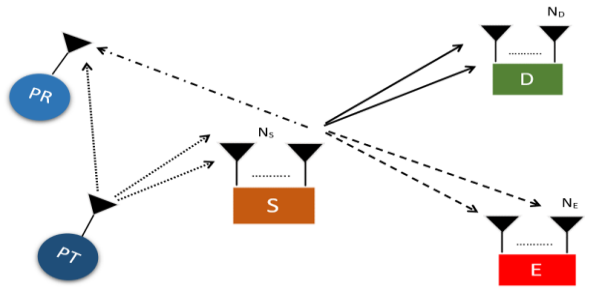

Figure 1: A system model.

The proposed model is shown in Figure 2.1. Here, we study the underlay MIMO cognitive network where the secondary network is allowed to utilize the same spectrum licensed to the primary network. Furthermore, the transmit power of the Source (S) is strictly constrained by both of the maximum transmitted power and the interference power at the primary receiver. In this model an active Eavesdropper (E) exists near the Destination (D) is trying to overhear the transmitting signal (i.e., transmitted in the main channel) via wiretap channels.

The primary nodes contain a primary transmitter (PT) and a primary receiver (PR). Here, the two primary nodes contain one antenna, while all the nodes in the secondary network are equipped with $N_S \geq 1, N_D \geq 1$ and $N_E \geq 1$ antennas. However, S is supplied with a battery to collect the RF energy broadcasted from PT.

We assumed that all channels experience independent and identically distributed (i.i.d.) quasi-static Nakagami-m fading channel with fading parameters m_S, m_R, m_D and m_E, and the average channel power gains Ω_S, Ω_R, Ω_D and Ω_E. Also, the thermal noise is added at each receiver is modeled by Additive White Gaussian Noise (AWGN) with variance σ^2. Additionally, we adopted the MRC scheme at D and E. Finally, the exchange of data and energy from S to D requires two-time phases, the first portion of time β $(0 \leq \beta \leq 1)$ is dedicated for EH and the second portion of time $1-\beta$ is dedicated for Information Transmissions (IT) [12]. In particular, in the first phase (i.e., EH), S collects the energy from the RF signal emitted from PT by using all antennas at S and utilizing it as the power to transmit data that is stored in an infinite capacity buffer. The harvested energy at S is given by:

$$E_S = \eta\beta P_t Y_S \quad (1)$$

where $0 \leq \eta \leq 1$ signifies the EH efficiency [13], P_t is the transmit power of PT, $Y_S = \sum_{i=1}^{N_S} \left|h_{PT\_S_i}\right|^2$, and $h_{PT\_S_i}$ is the channel gain coefficient between PT and the i-th antenna at S.

The probability density function (PDF) and Cumulative Distribution Function (CDF) of the channel gain Y_S can be written as [14]:

$$f_{Y_S}(y) = \rho_S y^{T_S-1} e^{-\lambda_S y} \quad (2)$$

$$F_{Y_S}(y) = 1 - \frac{\Gamma(T_S, \lambda_S y)}{\Gamma(T_S)} \quad (3)$$

where $\lambda_S = \frac{m_S}{\Omega_S}$, $T_S = m_S N_S$, and $\rho_S = \frac{1}{\Gamma(T_S)}(\lambda_S)^{T_S}$, $\Gamma(.)$ is the Gamma function as defined by (8.310.1) in [15] and $\Gamma(.,.)$ is the upper incomplete Gamma function as defined by (8.350.2) of [15].

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

$$P_{max} = \frac{E_S}{1-\beta} = \frac{\eta\beta P_t Y_S}{1-\beta} \quad (4)$$

In the second time phase, S will send the confidential information to D by only selecting the optimal antenna for transmitting this information. This allows utilizing the underlay mode using the same spectrum if the interference due to PR is lower than a certain threshold and the transmitting power does not exceed P_{max}. Due to these restriction power, the transmit power at S can be expressed as [16]:

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

where P_I is the maximum tolerated interference power at PR, $Y_R = \left|h_{S_bR}\right|^2$, b denotes the optimal selected antenna at S, and h_{S_bR} is the instantaneous channel fading coefficient between bth antenna at S and PR.

The PDF and the CDF of the channel gain Y_R can be written as:

$$f_{Y_R}(y) = \frac{{\lambda_R}^{m_R}}{\Gamma(m_R)} y^{m_R-1} e^{-\lambda_R y} \quad (6)$$

$$F_{Y_R}(y) = 1 - \frac{\Gamma(m_R, \lambda_R y)}{\Gamma(m_R)} \quad (7)$$

where $\lambda_R = \frac{m_R}{\Omega_R}$

The channel capacity at D is expressed as follow:

$$C_{S_iD} = \ln\left(1 + \frac{P_S}{\sigma^2} Y_{S_iD}\right), \text{nat/sec/Hz} \quad (8)$$

where $Y_{S_iD} = \sum_{j=1}^{N_D} \left|h_{S_iD_j}\right|^2$, $h_{S_iD_j}$ is the instantaneous channel fading coefficient between the i-th antenna at S and the j-th antenna at D.

The CDF of the channel gain Y_{S_iD} can be written as [14]:

$$F_{Y_{S_iD}}(y) = 1 - \frac{\Gamma(T_D, \lambda_D y)}{\Gamma(T_D)} \quad (9)$$

where $\lambda_D = \frac{m_D}{\Omega_D}$ and $T_D = m_D N_D$.

Similarly, the channel capacity E can be written as:

$$C_{S_iE} = \ln\left(1 + \frac{P_S}{\sigma^2} Y_{S_iE}\right) \text{nat/sec/Hz} \quad (10)$$

where $Y_{S_iE} = \sum_{j=1}^{N_E} \left|h_{S_iE_j}\right|^2$, $h_{S_iE_j}$ is the instantaneous channel fading coefficients between the i-th antenna at S and the j-th antenna at E.

The PDF of the channel gain Y_{S_iE} can be written as [14]:

$$f_{Y_{S_iE}}(y) = \rho_E y^{T_E-1} e^{-\lambda_E y} \quad (11)$$

where $\lambda_E = \frac{m_E}{\Omega_E}, T_E = m_E N_E$ and $\rho_E = \frac{1}{\Gamma(T_E)}(\lambda_E)^{T_E}$.

If CSI of the main channel and the eavesdropper channel is available at S this scheme is called the OAS. Here, the antenna at S is chosen to maximize the usable secrecy rate in the secondary system. Also, the selected antenna is used to transmit signals to D [16],[17].

In general, the metrics of the chosen antenna in the OAS scheme is given as:

$$b = arg \max_{1\le i\le N_S} C_i \tag{12}$$

where C_i is the achievable secrecy rate via the i-th antenna at S. Hence, the instantaneous secrecy capacity (i.e., the difference between Shannon capacity of the main channel and wiretap channel) can be written as:

$$\begin{aligned} C_S &= \max_{1\le i\le N_S} C_i \\ &= \max_{1\le i\le N_S} \left[C_{S_iD} - C_{S_iE}\right]^+ \end{aligned} \tag{13}$$

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

III. Secrecy Outage Probability Analysis

The SOP has defined the probability that the instantaneous secrecy capacity does not exceed the target secrecy rate, $R_S \ge 0$, which can be written as follows [16]:

$$\begin{aligned} P_{out} &= Pr(C_S \le R_S) \\ &= Pr\left(\max_{1\le i\le N_S}\left[C_{S_iD} - C_{S_iE}\right]^+ \le R_S\right) \\ &= \prod_{i=1}^{N_S} Pr\left(C_{S_iD} - C_{S_iE} \le R_S\right) \\ &= (P_{out}^{OAS})^{N_S} \end{aligned} \tag{14}$$

where $P_{out}^{OAS} = Pr\left(C_{S_iD} - C_{S_iE} \le R_S\right)$ demonstrates the security performance with a single antenna at S while D and E are equipped with $N_D \ge 1$ and $N_E \ge 1$ antennas, respectively [14]. Making use of (5), (8), and (10), one can obtain P_{out}^{OAS} which can be written as follows:

$$\begin{aligned} P_{out}^{OAS} &= Pr\left(C_{S_iD} - C_{S_iE} \le R_S\right) \\ &= Pr\left(Y_{S_iD} \le \theta Y_{S_iE} + \tfrac{(\theta-1)\sigma^2}{P_S}, P_S = P_{max}\right) \\ &+ Pr\left(Y_{S_iD} \le \theta Y_{S_iE} + \tfrac{(\theta-1)\sigma^2}{P_S}, P_S = \tfrac{P_I}{Y_R}\right) \\ &= \underbrace{Pr\left(Y_{S_iD} \le \theta Y_{S_iE} + \tfrac{(\theta-1)\sigma^2}{P_{max}}, Y_R \le \tfrac{P_I}{P_{max}}\right)}_{I_1} \\ &+ \underbrace{Pr\left(Y_{S_iD} \le \theta Y_{S_iE} + \tfrac{(\theta-1)\sigma^2}{P_I} Y_R, Y_R > \tfrac{P_I}{P_{max}}\right)}_{I_2} \end{aligned} \tag{15}$$

where $\theta = exp(R_S)$.

Substituting (4) into (15), I_1 can be expressed as:

$$\begin{aligned} I_1 &= Pr\left(Y_{S_iD} \le \theta Y_{S_iE} + \frac{\varsigma}{Y_S}, Y_R \le \frac{\xi}{Y_S}\right) \\ &= \int_0^\infty f_{Y_S}(x) F_{Y_R}\left(\frac{\xi}{x}\right) H_1(x) dx \end{aligned} \tag{16}$$

where $\varsigma = \frac{(\theta-1)(1-\beta)\sigma^2}{\eta\beta P_t}$, $\xi = \frac{P_I(1-\beta)}{\eta\beta P_t}$, and $H_1(x) = \int_0^\infty F_{Y_{S_iD}}\left(\theta y + \frac{\varsigma}{x}\right) f_{Y_{S_iE}}(y) dy$.

Substituting (9) and (11) into $H_1(x)$, then using (8.352.7) and (3.326.2) in [15], one achieves:

$$\begin{aligned} H_1(x) &= \int_0^\infty F_{Y_{S_iD}}\left(\theta y + \frac{\varsigma}{x}\right) f_{Y_{S_iE}}(y) dy \\ &= 1 - \rho_E exp\left(-\frac{\lambda_D \varsigma}{x}\right) \sum_{k=0}^{T_D-1} \sum_{l=0}^{k} \frac{{\lambda_D}^k \theta^l}{k!} \binom{k}{l} \\ &\times \left(\frac{\varsigma}{x}\right)^{k-l} \int_0^\infty y^{T_E+l-1} exp(-(\lambda_E \\ &+ \lambda_D\theta)y) dy \\ &= 1 - \sum_{k,l} E_{k,l}\, exp\left(-\frac{\lambda_D \varsigma}{x}\right)\left(\frac{\varsigma}{x}\right)^{k-l} \end{aligned} \tag{17}$$

where $\sum_{k,l} E_{k,l} = \sum_{k=0}^{T_D-1} \sum_{l=0}^{k} \binom{k}{l} \frac{\rho_E \lambda_D{}^k \theta^l \Gamma(T_E+l)}{k!(\lambda_E+\lambda_D\theta)^{T_E+l}}$, $\binom{k}{l} = \frac{k!}{l!(k-l)!}$

By substituting (2), (7), and (17) into (16), then using (8.352.7) and (3.471.9) in [15], one achieves:

$$\begin{aligned} I_1 &= 1 + \sum_{t=0}^{m_R-1} \sum_{k,l} \frac{2\rho_S(\lambda_R\xi)^t \varsigma^{k-l} E_{k,l}}{t!} \left(\frac{\lambda_D\varsigma + \lambda_R\xi}{\lambda_S}\right)^{\frac{T_S+l-k-t}{2}} \\ &\times K_{T_S+l-k-t}\left(2\sqrt{\lambda_S(\lambda_D\varsigma + \lambda_R\xi)}\right) \\ &- \sum_{t=0}^{m_R-1} \frac{2\rho_S(\lambda_R\xi)^t}{t!} \left(\frac{\lambda_R\xi}{\lambda_S}\right)^{\frac{T_S-t}{2}} K_{T_S-t}\left(2\sqrt{\lambda_S\lambda_R\xi}\right) \\ &- \sum_{k,l} 2\rho_S \varsigma^{k-l} E_{k,l} \left(\frac{\lambda_D\varsigma}{\lambda_S}\right)^{\frac{T_S+l-k}{2}} K_{T_S+l-k}\left(2\sqrt{\lambda_S\lambda_D\varsigma}\right) \end{aligned} \tag{18}$$

where $K_v(x)$ is the modified Bessel function of order v as defined by (8.407.1) in [15].

By substituting (4) into (15), I_2 can be written as:

$$\begin{aligned} I_2 &= Pr\left(Y_{S_iD} \le \theta Y_{S_iE} + \frac{(\theta-1)\sigma^2}{P_I} Y_R, Y_R > \frac{P_I}{P_{max}}\right) \\ &= Pr\left(Y_{S_iD} \le \theta Y_{S_iE} + \frac{(\theta-1)\sigma^2}{P_I} Y_R, Y_S > \frac{\xi}{Y_R}\right) \\ &= \int_0^\infty f_{Y_R}(x)\left(1 - F_{Y_S}\left(\frac{\xi}{x}\right)\right) H_2(x) dx \end{aligned} \tag{19}$$

where $H_2(x) = \int_0^\infty F_{Y_{S_iD}}(\theta y + \omega x) f_{Y_{S_iE}}(y) dy$ and $\omega = \frac{(\theta-1)\sigma^2}{P_I}$.

By substituting (9) and (11) into $H_2(x)$, then using (8.352.7) and (3.326.2) of [15], one achieves:

$$\begin{aligned} H_2(x) &= \int_0^\infty F_{Y_{S_iD}}(\theta y + \omega x) f_{Y_{S_iE}}(y) dy \\ &= 1 - \sum_{k,l} E_{k,l}\, exp(-\lambda_D \omega x)(\omega x)^{k-l} \end{aligned} \tag{20}$$

Now, by substituting (3), (6), and (20) into (19), then using (8.352.7) and (3.471.9) in [15], one achieves:

$$\begin{aligned} I_2 &= \sum_{t=0}^{T_S-1} \frac{2{\lambda_R}^{m_R}(\lambda_S\xi)^t}{\Gamma(m_R)t!} \left(\frac{\lambda_S\xi}{\lambda_R}\right)^{\frac{m_R-t}{2}} \times K_{m_R-t}\left(2\sqrt{\lambda_R\lambda_S\xi}\right) \\ &- \sum_{t=0}^{T_S-1} \sum_{k,l} \frac{2E_{k,l}{\lambda_R}^{m_R}(\lambda_S\xi)^t \omega^{k-l}}{\Gamma(m_R)t!} \left(\frac{\lambda_S\xi}{\lambda_R + \lambda_D\omega}\right)^{\frac{k+m_R-t-l}{2}} \\ &\times K_{k+m_R-t-l}\left(2\sqrt{(\lambda_R + \lambda_D\omega)\lambda_S\xi}\right) \end{aligned} \tag{27}$$

where $K_v(x)$ is the modified Bessel function of order v and defined by (8.407.1) in [15].

Then, P_{out}^{OAS} can be obtained by substituting (18) and (21) into (15). Finally, we obtain the exact security outage performance with the OAS scheme by replacing (15) into (14).

IV. Numerical Results

Numerical results are given to verify the exact closed-form expressions for the cognitive MIMO system that appears in Figure 1. Here, the following parameters and considered the EH efficiency is $\eta = 0.8$, the variance of AWGN is $\sigma^2 = 1$, and the R_S is measured by unit nat/s/Hz. For simplicity, assume $m_S = m_R = m_D = m_E = m$. Figure 2 and 3 show the SOP against P_I when N_S, P_t, and N_E are varying respectively. Here, the shape parameter $m = 2$. In particular, the security performance is improved by increasing P_I, up to a certain point after which no more improvement appears. Accordingly, when P_I is large, the transmit power at S reaches its maximum power, P_{max}, therefore, since the proposed system is located in a non-cognitive model. The total interference from the secondary transmitter is ignored.

Next, one can notice that the security performance is enhanced by increasing the number of the antennas at the source, N_S, (i.e., more diversity gain is achieved at the source). Moreover, when increasing the value of the transmit power at the source, P_t, or by decreasing the number of the antennas at the eavesdropper, N_E, (i.e., This signifies less diversity gain at E).

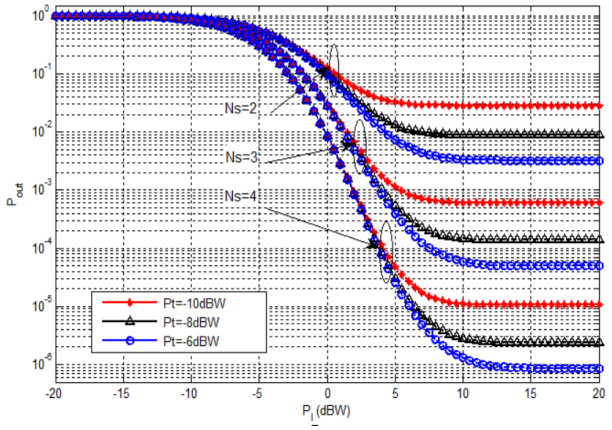

Figure 2: SOP versus P_I with $\Omega_S = \Omega_E = 1$ dB, $\Omega_R = \Omega_D = 10$ dB, $N_D = N_E = 4$, $R_S = 1$, $\beta = 0.5$ and $m = 2$.

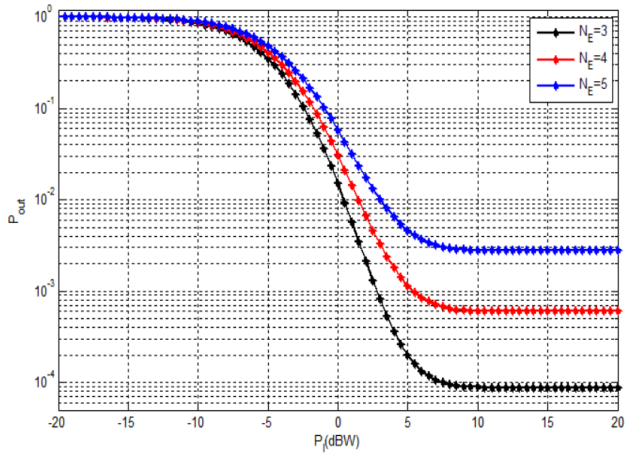

Figure 3: SOP versus P_I with $P_t = -10$ dBW, $\Omega_S = \Omega_E = 1$ dB, $\Omega_R = \Omega_D = 10$ dB, $N_D = 4$, $N_S = 3$, $R_S = 1$, $\beta = 0.5$ and $m = 2$.

The SOP versus P_t when N_S and Ω_S are varying is demonstrated in Figure 4. This figure showed that one can enhance the security performance by increasing P_t or Ω_S. In particular, higher Ω_S signifies better main channel quality which is used to collect the energy signal from PT and a higher transmit power, P_t, at the primary transmitter (i.e., higher transmit power at the primary transmitter this leads to maximum harvested energy at the source). Finally, the SOP can be improved by increasing N_S that enhance the EH ability of S and improves the chance of choosing an antenna to transmit information from source to destination.

Moreover, one can observe that when $\Omega_S = 5$ dB for different values of N_S, the security performance is enhanced by increasing the transmit power at the source to a certain point (i.e., $P_t = 0$ dBW) the SOP remains constant. This means that increasing the transmit power of the source cannot enhance the SOP in an unlimited manner. i.e., when $N_S = 2$ and $P_t = -5$ dBW one can improve the SOP by increasing Ω_S. However, one can observe that at $\Omega_S = -5$ dB, when increasing P_t will affect the performance of the system to a certain point is 10 dBW. When $\Omega_S = 5$ dB, increasing P_t will affect the overall performance of the system to a certain level of the P_t (i.e., $P_t = 0$ dBW).

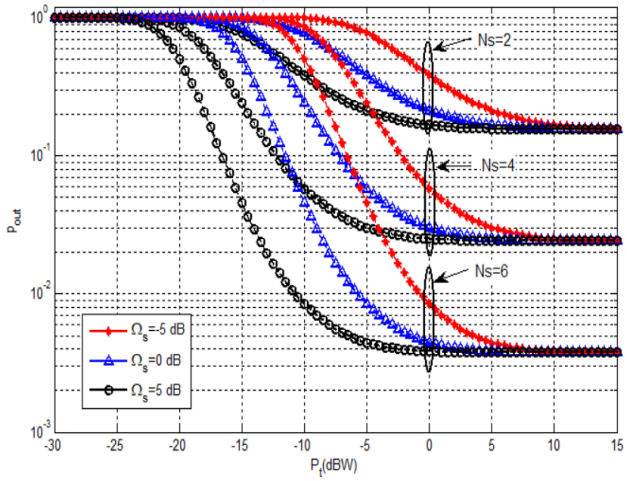

Figure 4: SOP versus P_t with $R_S = 1$, $\Omega_D = 6$ dB, $\Omega_R = \Omega_E = 1$ dB, $N_D = N_E = 4$, $\beta = 0.5$, $m = 2$ and $P_I = 10$ dBW.

Figure 5 shows the security performance against Ω_D for different values of N_D and m. Here, one can enhance the security performance significantly by increasing Ω_D, N_D and m. In particular, Ω_D indicates the average SNR of the main channel and reducing the parameter m means that the channel fading is robust and can improve the MRC diversity gain at D 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.

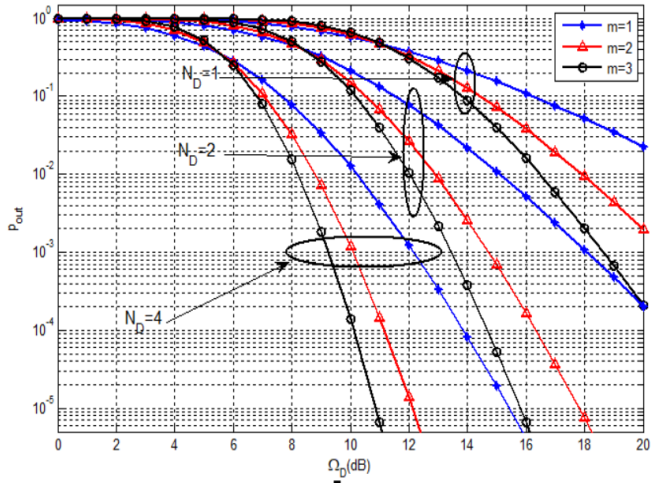

Figure 5: SOP versus Ω_D with $\Omega_S = \Omega_R = \Omega_E = 1$ dB, $P_t = P_I = 1$ W, $R_S = 1$, $N_S = 2$, $N_E = 4$ and $\beta = 0.5$.

Figure 6 shows the security performance against β with a different value of N_S. The security performance can be improved by increasing the value of β. This means more energy can be harvested by the secondary transmitter. Moreover, the value of $1-\beta$ will decrease, then smaller time slot will be allocated for the information transmission phase.
Accordingly, it is hard to determine the exact value of β to achieves the lowest SOP, where the proper value of β plays an important role in dividing the time between the harvested energy in the first phase and the information transmission in the second phase. In particular, by increasing the value of β, the reliability of the cognitive systems will decrease as the system needs more time to harvest energy. Here, one can notice a floor in the higher region, similar to the one shown in Figure 2. i.e., increasing the power at S will not enhance the secrecy performance in an unlimited manner. From the figure, one can notice that by increasing the number of the antennas at the source will effectively improve the SOP. e.g., for $\beta = 0.5$, the secrecy outage performance for $N_S = 7$ is smaller than that for $N_S = 3$ and $N_S = 5$.

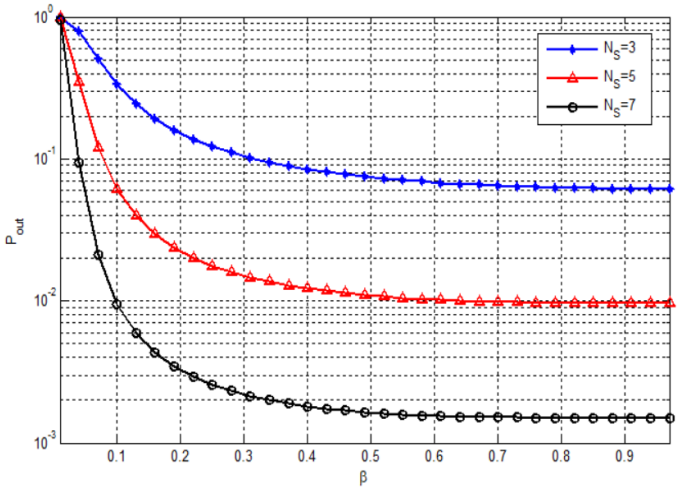

Figure 6: SOP versus β with $\Omega_D = 6$ dB, $\Omega_S = \Omega_R = \Omega_E = 1$ dB, $N_D = N_E = 4, R_S = 1, P_t = 0$ dBW, $m = 2$ and $P_I = 10$ dBW.

V. Conclusion

In this paper, we realize the physical layer secrecy outage performance of MIMO secondary nodes operates in the underlay spectrum for the CRN system consisting of a single antenna primary node. Exact closed-form expressions for security performance with OAS and EH schemes are derived over Nakagami-*m* fading channels. The numerical results show that when the number of the antenna at the source and/or the destination increases, the secrecy outage performance of the system can be improved. In our future works will add relay between the secondary nodes to enhance security performance and increase the coverage area.

REFERENCES:

[1] Hasan, Ziaul, Hamidreza Boostanimehr, and Vijay K. Bhargava. "Green cellular networks: A survey, some research issues and challenges." IEEE Communications surveys & tutorials 13.4 (2011): 524-540.

[2] Park, Sungsoo, Hyungjong Kim, and Daesik Hong. "Cognitive radio networks with energy harvesting." IEEE Transactions on Wireless communications 12.3 (2013): 1386-1397.

[3] Lee, Seunghyun, Rui Zhang, and Kaibin Huang. "Opportunistic wireless energy harvesting in cognitive radio networks." IEEE Transactions on Wireless Communications 12.9 (2013): 4788-4799.

[4] Elkashlan, Maged, et al. "On the security of cognitive radio networks." *IEEE Transactions on Vehicular Technology* 64.8 (2014): 3790-3795.

[5] Amirtharajah, Rajeevan, and Anantha P. Chandrakasan. "Self-powered signal processing using vibration-based power generation." *IEEE journal of solid-state circuits* 33.5 (1998): 687-695.

[6] Soyata, Tolga, Lucian Copeland, and Wendi Heinzelman. "RF energy harvesting for embedded systems: A survey of tradeoffs and methodology." *IEEE Circuits and Systems Magazine* 16.1 (2016): 22-57.

[7] Pan, Gaofeng, et al. "On secrecy performance of MISO SWIPT systems with TAS and imperfect CSI." *IEEE Transactions on Communications* 64.9 (2016): 3831-3843.

[8] Odeyemi, Kehinde O., Pius A. Owolawi, and Oladayo O. Olakanmi. "Secrecy outage probability in energy harvesting aided underlay cognitive radio network under eavesdroppers scenarios." *Transactions on Emerging Telecommunications Technologies* 31.8 (2020): e4041.

[9] Lei, Hongjiang, et al. "Secrecy outage performance for SIMO underlay cognitive radio systems with generalized selection combining over Nakagami-$ m $ channels." *IEEE Transactions on Vehicular Technology* 65.12 (2016): 10126-10132.

[10] Zhang, Jun, et al. "Large system secrecy rate analysis for SWIPT MIMO wiretap channels." IEEE Transactions on Information Forensics and Security 11.1 (2015): 74-85.

[11] Singh, Ajay, Manav R. Bhatnagar, and Ranjan K. Mallik. "Secrecy outage of a simultaneous wireless information and power transfer cognitive radio system." IEEE Wireless Communications Letters 5.3 (2016): 288-291.

[12] Hadzi-Velkov, Zoran, et al. "Wireless networks with energy harvesting and power transfer: Joint power and time allocation." *IEEE Signal Processing Letters* 23.1 (2015): 50-54.

[13] Zhou, Xun, Rui Zhang, and Chin Keong Ho. "Wireless information and power transfer: Architecture design and rate-energy tradeoff." *IEEE Transactions on communications* 61.11 (2013): 4754-4767.

[14] Zhao, Hui, et al. "Secrecy outage on transmit antenna selection/maximal ratio combining in MIMO cognitive radio networks." *IEEE Transactions on Vehicular Technology* 65.12 (2016): 10236-10242

[15] Jeffrey, Alan, and Daniel Zwillinger, eds. *Table of integrals, series, and products*. Elsevier, 2007.

[16] Lei, Hongjiang, et al. "Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-$ m $ channels." *IEEE Transactions on Vehicular Technology* 66.3 (2016): 2237-2250.

[17] Zhu, Jia, et al. "On secrecy performance of antenna-selection-aided MIMO systems against eavesdropping." *IEEE Transactions on Vehicular Technology* 65.1 (2015): 214-225.