On Physical Layer Security for Reactive DF Cognitive Relay Networks

Louis Sibomana, Hans-Jürgen Zepernick, Hung Tran

IEEE Global Communications Conference

2014 Austin, USA

On Physical Layer Security for Reactive DF Cognitive Relay Networks

Louis Sibomana[1], Hans-Jürgen Zepernick[1], and Hung Tran[2]
[1]Blekinge Institute of Technology, SE-371 79 Karlskrona, Sweden
E-mail: {lsm, hjz}@bth.se
[2]Information Technology Faculty, NIEM, 31-Phan Dinh Giot, Hanoi, Vietnam
E-mail: {tranhungemail}@gmail.com

***Abstract*—This paper analyzes the physical layer security for cognitive relay networks under the peak interference power constraint of the primary user receiver. In particular, a secondary user (SU) transmitter communicates with an SU receiver through the help of multiple secondary relays (SRs) using a decode-and-forward (DF) protocol. There exist multiple eavesdroppers (EAVs) who illegally listen to the secondary network communication. We consider a reactive DF scheme, and only the SRs that satisfy a decoding threshold participate in the relay selection. Analytical expressions of the probability of existence of secrecy capacity and secrecy outage probability are obtained. Numerical results are provided to evaluate the impact of the number of SRs, number of EAVs and channel mean powers on the secondary system security. We also investigate the effect of the interference from the primary network to the secondary network performance. Moreover, the performance of proactive DF is analyzed for the purpose of comparison.**

I. Introduction

Recently, cooperative relaying has been introduced in cognitive radio networks (CRNs) to enhance the secondary network coverage and to improve radio spectrum utilization [1]–[4]. In particular, secondary relays (SRs) assist the secondary user transmitter (SU-Tx) to forward the message to the SU receiver (SU-Rx) using the licensed frequency band of the primary user (PU). In this context, the secondary system capacity [5] and outage probability [6] have been analyzed for reactive decode and forward (R-DF) and proactive DF (P-DF) schemes considering either peak interference power (PIP) or outage constraints at the PU receiver (PU-Rx).

In addition, information theoretic security has received much attention [7]–[10] where physical layer properties such as multiple antennas and cooperative networks are exploited to achieve secure transmission in wireless communications. In [10]–[13], different relay selection strategies have been studied for conventional cooperative wireless networks in the presence of eavesdroppers (EAVs) that intercept the legitime message transmission. Moreover, CRN technology is also prone to eavesdropping attacks as discussed in [14]. Cognitive relay physical layer security has been considered in [15] where the SU asymptotic secrecy rate and secrecy outage probability have been analyzed. However, the work in [15] ignored the effect of the PU transmitter (PU-Tx) interference to the secondary network and thus, the analysis does not depict a realistic scenario. Further, the analysis in [10], [12], [13], [15] assumed high signal-to-noise ratio (SNR) and hence, all relays are able to successfully decode the message from the source. This assumption is not valid for practical systems that often operate in the low to medium SNR regimes. It is noted that the secondary network operates in low to medium SNR to satisfy the PU interference power constraint. Therefore, it is important to evaluate the secondary system security at all SNRs and by considering the interference from the PU-Tx to the secondary network.

In this paper, we study the physical layer security for a secondary relay network with multiple SRs in the presence of multiple EAVs and consider the interference from the primary network to the secondary network. We consider an R-DF scheme, i.e., only the SRs that satisfy the decoding threshold participate in the relay selection. In particular, we derive the cumulative distribution function (CDF) and probability density function (PDF) of the end-to-end signal-to-interference-plus-noise ratio (SINR). Accordingly, analytical expressions of the probability of existence of non-zero secrecy capacity and secrecy outage probability are obtained. Moreover, we investigate the impact of the number of SRs, number of EAVs and interference from the PU-Tx to SU-Rx and EAV on the secondary network security. For the purpose of comparison, the performance of proactive DF is also analyzed.

The rest of the paper is organized as follows. Section II describes the system model. In Section III, we present the performance analysis of the considered system. Section IV provides numerical results and discussions. Finally, conclusions are presented in Section V.

II. System model

A. Underlay cognitive relay network model

Fig.1 shows an underlay cognitive relay network where an SU-Tx sends confidential messages to the SU-Rx through the assistance of N trusted SRs in the presence of a PU-Tx communicating with a PU-Rx. There exist K passive EAVs intercepting signals from the SR to the SU-Rx. We assume that the direct links from the SU-Tx to the SU-Rx and EAV are not available due to severe shadowing [12], [13]. The secondary network communication occurs in two phases. In the first phase, the SU-Tx broadcasts the information to all SRs. Then, one SR is selected to forward

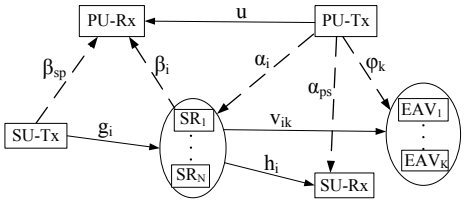

Fig. 1. Model of the considered cognitive relay network in the presence of multiple eavesdroppers. (Dashed lines: Interference links; Solid lines: Communication links).

the message to the SU-Rx in the second phase based on R-DF or P-DF protocols. The channel power gains of the links PU-Tx→PU-Rx, SU-Tx→SR$_i$, SR$_i$→SU-Rx and SR$_i$→EAV$_k$ are, respectively, denoted by u, g_i, h_i, $i \in \{1, 2, \ldots, N\}$ and v_{ik}, $k \in \{1, 2, \ldots, K\}$. Further, β_{sp}, β_i, α_i, α_{ps} and φ_k represent the channel power gains of the SU-Tx→PU-Rx, SR$_i$→PU-Rx, PU-Tx→SR$_i$, PU-Tx→SU-Rx and PU-Tx→EAV$_k$ links, respectively. We assume that all channels are subject to independent Rayleigh fading and the channel power gains are exponentially distributed random variables (RVs). Accordingly, the channel mean powers are defined as $\Omega_u, \Omega_{g_i}, \Omega_{h_i}, \Omega_{v_{ik}}, \Omega_{sp}, \Omega_{\beta_i}, \Omega_{\alpha_i}, \Omega_{ps}$ and Ω_{φ_k}.

For the underlay approach, the interference from the SU transmitting nodes (SU-Tx, SR$_i$) to the PU-Rx should be managed to be below a predefined threshold [2], [3] such that

$$P_s \beta_{sp} \leq Q \tag{1}$$

$$P_{r_i} \beta_i \leq Q \tag{2}$$

where Q is the maximum acceptable level of interference that the PU-Rx can tolerate. Further, P_s and P_{r_i} are, respectively, the SU-Tx and ith SR instantaneous transmit powers. Note that the transmit power cannot be infinite or very large in practice. As such, $P_s \leq P_{s,\max}$ and $P_{r_i} \leq P_{r,\max}$ where $P_{s,\max}$ and $P_{r,\max}$ denote the SU-Tx and ith SR maximum transmit power limits, respectively. We can see from (1) that perfect channel state information (CSI) of the PU is required at the SU-Tx to maintain the PU-Rx PIP constraint, i.e., perfect knowledge of β_{sp} at the SU-Tx. In practice, it is hard for the SU to obtain perfect CSI of the PU and is costly in terms of feedback. To overcome the limitation of PU perfect CSI, we can tolerate a certain amount of error for the SU transmit power control [4]. Accordingly, the interference power constraint at the PU-Rx is reformulated as

$$\Pr\{P_s \beta_{sp} > Q\} \leq \epsilon \tag{3}$$

where ϵ is the tolerated error to satisfy (1). As a consequence, the SU-Tx and ith SR transmit powers are obtained as

$$P_s = \min\left\{\frac{Q}{\Omega_{sp} \ln\left(1/\epsilon\right)}, P_{s,\max}\right\} \tag{4}$$

$$P_{r_i} = \min\left\{\frac{Q}{\Omega_{\beta_i} \ln\left(1/\epsilon\right)}, P_{r,\max}\right\} \tag{5}$$

Note that this case happens when statistical information about the PU channel is available at the SUs, i.e., Ω_{sp} and Ω_{β_i} are relatively stable and can be estimated at the SU transmitting nodes [3].

B. R-DF scheme and secrecy capacity

We define $C_{s,i}$, $C_{i,d}$ and $C_{i,k}$ as the instantaneous channel capacity at the SR$_i$, SU-Rx and EAV$_k$ nodes, respectively. Taking account for the PU-Tx interference, we have

$$C_{s,i} = \frac{W}{2} \log_2\left(1 + \frac{\gamma_s g_i}{\gamma_p \alpha_i + 1}\right) \tag{6}$$

$$C_{i,d} = \frac{W}{2} \log_2\left(1 + \frac{\gamma_{r_i} h_i}{\gamma_p \alpha_{ps} + 1}\right) \tag{7}$$

$$C_{i,k} = \frac{W}{2} \log_2\left(1 + \frac{\gamma_{r_i} v_{ik}}{\gamma_p \varphi_k + 1}\right) \tag{8}$$

where W is the system bandwidth. Further, $\gamma_s = P_s/N_0$, $\gamma_{r_i} = P_{r_i}/N_0$ and $\gamma_p = P_p/N_0$ are, respectively, the SU-Tx, SR$_i$ and PU-Tx transmit SNRs with N_0 being the noise power. Moreover, $\gamma_{s,\max} = P_{s,\max}/N_0$ and $\gamma_{r,\max} = P_{r,\max}/N_0$ denote the maximum transmit SNR of the SU-Tx and SR$_i$, respectively. We also define $\gamma_Q = Q/N_0$ as the PU PIP SNR.

For the DF protocol, each SR first decodes the received signal from the SU-Tx and then re-encodes and transmits its decoded outcome to the SU-Rx. In the opportunistic R-DF scheme, the best SR among the set of SR candidates that successfully decoded the message from the SU-Tx [5], [6] is selected to forward the message to the SU-Rx as

$$\mathbf{b} = \arg\max_{i \in \mathcal{R}_j} \{\gamma_{i,d}\}, \quad \mathcal{R}_j = \{j \mid \gamma_{s,i} \geq \gamma_{th}, \forall i \in \mathcal{N}\} \tag{9}$$

where $\mathcal{N} = \{1, 2, \ldots, N\}$, $\gamma_{i,d} = (\gamma_{r_i} h_i)/(\gamma_p \alpha_{ps} + 1)$ and $\gamma_{s,i} = (\gamma_s g_i)/(\gamma_p \alpha_i + 1)$. Further, $\gamma_{th} = 2^{\frac{2R_s}{W}} - 1$ is the decoding threshold with R_s being the SU-Tx→SR$_i$ link target transmission rate and $\mathcal{R}_j$ is a set of j SRs that decoded the message. Accordingly, the SINR at the SU-Rx is given by

$$\gamma_{\text{R-DF}} = \max_{i \in \mathcal{R}_j} \{\gamma_{i,d}\} \tag{10}$$

During the second phase, K EAVs independently overhear the transmission from SR$_i$ to the SU-Rx. The secrecy rate at the SU-Rx can be achieved by considering the EAV with the highest SINR as

$$\gamma_{\mathbf{b},E} = \max_{k \in \mathcal{K}} \left\{\frac{\gamma_r v_{\mathbf{b},k}}{\gamma_p \varphi_k + 1}\right\}, \quad \mathcal{K} = \{1, 2, \ldots, K\} \tag{11}$$

Given (10) and (11), and in view of (7) and (8), we have $C_{\text{R-DF}} = (W/2)\log_2\left(1+\gamma_{\text{R-DF}}\right)$ and $C_{\mathbf{b},E} = (W/2)\log_2\left(1+\gamma_{\mathbf{b},E}\right)$. The secrecy capacity is defined as the difference between the capacity of the main link and that of a wiretap link [8]. The SU achievable secrecy capacity is expressed as

$$C_{\text{sec}} = \max\{0, C_{\text{R-DF}} - C_{\mathbf{b},E}\} \tag{12}$$

For further analysis, we define the RV $Y = aX_1/(bX_2 + c)$ where X_1 and X_2 are independent exponentially distributed RVs with mean Ω_1 and Ω_2, respectively. Further, a, b and c are positive constants. The CDF of Y is given by [6]

$$F_Y(y) = 1 - \frac{a\Omega_1}{a\Omega_1 + b\Omega_2 y} \exp\left(-\frac{cy}{a\Omega_1}\right) \tag{13}$$

By differentiating (13) with respect to y, the PDF of Y is

$$f_Y(y) = \frac{ab\Omega_1\Omega_2 \exp\left(-\frac{cy}{a\Omega_1}\right)}{(a\Omega_1 + b\Omega_2 y)^2} + \frac{ac\Omega_1 \exp\left(-\frac{cy}{a\Omega_1}\right)}{a\Omega_1 + b\Omega_2 y} \quad (14)$$

III. Performance analysis

In this section, analytical expressions of the probability of non-zero secrecy capacity and secrecy outage probability are derived. We first consider the presence of a single EAV and then, extend the results to multiple EAVs. In addition, we assume that all SRs are close to each other to form a cluster [4] and thus, $\Omega_{g_i} = \Omega_g$, $\Omega_{h_i} = \Omega_h$, $\Omega_{\beta_i} = \Omega_\beta$, $\Omega_{\alpha_i} = \Omega_\alpha$ and $\gamma_{r_i} = \gamma_r$, $\forall i \in \mathcal{N}$. The same assumption is also applied to the K EAVs and hence, $\Omega_{\varphi_k} = \Omega_\varphi$ and $\Omega_{v_{\mathbf{b},k}} = \Omega_v$, $\forall k \in \mathcal{K}$.

A. Presence of a Single EAV

Let $F_{\gamma_{\text{R-DF}}}(y)$ and $f_{\gamma_{\mathbf{b},E}}(y)$ denote, respectively, the CDF of $\gamma_{\text{R-DF}}$ and PDF of $\gamma_{\mathbf{b},E}$. From (10), we have

$$F_{\gamma_{\text{R-DF}}}(y) = \sum_{j=0}^{N} \underbrace{\Pr\{\gamma_{\text{R-DF}} < y \mid \mathcal{R}_j\}}_{P_1} \Pr\{\mathcal{R}_j\} \quad (15)$$

where $\Pr\{\mathcal{R}_j\}$ represents the probability of exact j SRs satisfying the decoding threshold and is obtained as

$$\Pr\{\mathcal{R}_j\} = \binom{N}{j} A^{N-j}(1-A)^j \quad (16)$$

In (16), A is determined with the help of (13) as

$$A = \Pr\left\{\frac{\gamma_s g_i}{\gamma_p \alpha_i + 1} \le \gamma_{th}\right\} = 1 - \frac{\exp\left(-B_0\gamma_{th}\right)}{1 + B\gamma_{th}} \quad (17)$$

where $B_0 = 1/(\gamma_s\Omega_g)$ and $B = B_0\gamma_p\Omega_\alpha$. We consider that the events $\mathcal{R}_j$ and $\gamma_{\text{R-DF}} < y$ are independent [6] and therefore,

$$\begin{aligned} P_1 &= \int_0^\infty \Pr\left\{\max_{i\in\mathcal{R}_j}\left\{\frac{\gamma_r h_i}{\gamma_p x + 1}\right\} < y\right\} f_{\alpha_{ps}}(x)dx \\ &= \int_0^\infty \left\{1 - \exp\left[-\frac{y(\gamma_p x + 1)}{\gamma_r \Omega_h}\right]\right\}^j \frac{\exp\left(-\frac{x}{\Omega_{ps}}\right)}{\Omega_{ps}} dx \\ &= \sum_{m=0}^{j} \binom{j}{m} (-1)^m \frac{\exp\left(-B_2 y\right)}{1 + B_1 y} \end{aligned} \quad (18)$$

where $B_1 = B_2\gamma_p\Omega_{ps}$ and $B_2 = m/(\gamma_r\Omega_h)$. Substituting (18) and (16) into (15), we obtain

$$\begin{aligned} F_{\gamma_{\text{R-DF}}}(y) = \sum_{j=0}^{N}\sum_{n=0}^{N-j}\sum_{m=0}^{j} \binom{N}{j}\binom{N-j}{n}\binom{j}{m}(-1)^{m+n} \\ \times \frac{\exp\left\{-\left[(n+j)B_0\gamma_{th} + B_2 y\right]\right\}}{(1 + B\gamma_{th})^{n+j}(1 + B_1 y)} \end{aligned} \quad (19)$$

Further, the PDF of $\gamma_{\mathbf{b},E}$ is obtained using (14) as

$$f_{\gamma_{\mathbf{b},E}}(y) = \frac{G\exp(-Gy)}{(1 + G_1 y)} + \frac{G_1\exp(-Gy)}{(1 + G_1 y)^2} \quad (20)$$

where $G = 1/(\gamma_r\Omega_v)$ and $G_1 = G\gamma_p\Omega_\varphi$.

1) Existence of non-zero secrecy capacity: According to [8], [13], the probability of existence of a non-zero secrecy capacity denoted by $P^{\text{ex}}_{\text{R-DF}}$ is given by

$$P^{\text{ex}}_{\text{R-DF}} = \Pr\{C_{\text{sec}} > 0\} = 1 - \int_0^\infty F_{\gamma_{\text{R-DF}}}(y) f_{\gamma_{\mathbf{b},E}}(y)dy \quad (21)$$

Then, substituting (19) and (20) into (21), we have

$$\begin{aligned} P^{\text{ex}}_{\text{R-DF}} = 1 - \sum_{j=0}^{N}\sum_{n=0}^{N-j}\sum_{m=0}^{j} \binom{N}{j}\binom{N-j}{n}\binom{j}{m}(-1)^{m+n} \\ \times \frac{\exp\left[-(n+j)B_0\gamma_{th}\right]}{\left(1 + B\gamma_{th}\right)^{n+j}} I_1 \end{aligned} \quad (22)$$

where $\lambda = B_2 + G$ and

$$I_1 = \int_0^\infty \frac{\exp(-\lambda y)}{1 + B_1 y}\left[\frac{G}{1 + G_1 y} + \frac{G_1}{(1 + G_1 y)^2}\right] dy \quad (23)$$

To solve (23), two cases are considered: If $B_1 \neq G_1$, I_1 is obtained in (24) where $\Psi(z) = \exp(z)\text{Ei}(-z)$ with $\text{Ei}(z) = -\int_{-z}^{\infty}\frac{\exp(-t)}{t}dt$ being the exponential integral function. If $B_1 = G_1$, I_1 is given by

$$I_1 = \frac{G}{B_1} + \frac{1}{2} - \frac{\lambda}{2B_1} + \frac{\lambda}{B_1^2}\left(G - \frac{\lambda}{2}\right)\Psi\left(\frac{\lambda}{B_1}\right) \quad (25)$$

Note that (24) and (25) are solved with the help of [16, eq. (3.352.4)], [16, eq. (3.353.3)] and [16, eq. (3.353.2)].

2) Secrecy outage probability: For delay-constrained applications and without perfect CSI of the EAV channel, the secondary network must set a secrecy target rate R. The secrecy outage probability is formulated as

$$P^{\text{out}}_{\text{sec, R-DF}} = \sum_{j=0}^{N} \underbrace{\Pr\{C_{\text{sec}} < R \mid \mathcal{R}_j\}}_{P_2} \Pr\{\mathcal{R}_j\} \quad (26)$$

The secondary system is in outage whenever the transmitted message is neither secure nor reliable [13]. By recalling that $\gamma_{\text{R-DF}}$ and $\mathcal{R}_j$ are independent and using the total probability theorem, P_2 is given by

$$\begin{aligned} P_2 = \underbrace{\Pr\{C_{\text{sec}} < R | \gamma_{\text{R-DF}} > \gamma_{\mathbf{b},E}\}}_{P_3} \Pr\{\gamma_{\text{R-DF}} > \gamma_{\mathbf{b},E}\} \\ + \underbrace{\Pr\{C_{\text{sec}} < R | \gamma_{\text{R-DF}} \le \gamma_{\mathbf{b},E}\}}_{P_4} \underbrace{\Pr\{\gamma_{\text{R-DF}} \le \gamma_{\mathbf{b},E}\}}_{P_5} \end{aligned} \quad (27)$$

where $P_5 = \int_0^\infty F_{\gamma_{\text{R-DF}}}(y) f_{\gamma_{\mathbf{b},E}}(y)dy$ and P_3 is obtained as

$$\begin{aligned} P_3 &= \Pr\{\gamma_{\text{R-DF}} < \rho(1 + \gamma_{\mathbf{b},E}) - 1 | \gamma_{\text{R-DF}} > \gamma_{\mathbf{b},E}\} \\ &= \int_0^\infty \frac{F_{\gamma_{\text{R-DF}}}\left[\rho(1+y) - 1\right] - F_{\gamma_{\text{R-DF}}}(y)}{\Pr\{\gamma_{\text{R-DF}} > \gamma_{\mathbf{b},E}\}} f_{\gamma_{\mathbf{b},E}}(y)dy \end{aligned} \quad (28)$$

where $\rho = 2^{\frac{2R}{W}}$. Since $R > 0$, we have $P_4 = 1$. Substituting (28) into (27), we obtain

$$P_2 = \int_0^\infty F_{\gamma_{\text{R-DF}}}\left[\rho(1+y) - 1\right] f_{\gamma_{\mathbf{b},E}}(y)dy \quad (29)$$

$$I_1 = \frac{GB_1}{B_1-G_1}\int_0^\infty \frac{\exp(-\lambda y)}{1+B_1y}dy - \frac{GG_1}{B_1-G_1}\int_0^\infty \frac{\exp(-\lambda y)}{1+G_1y}dy + \frac{G_1B_1^2}{(G_1-B_1)^2}\int_0^\infty \frac{\exp\big(-\lambda y\big)}{1+B_1y}dy - \frac{B_1G_1^2}{(G_1-B_1)^2}$$
$$\times \int_0^\infty \frac{\exp\big(-\lambda y\big)}{1+G_1y}dy + \frac{G_1^2}{G_1-B_1}\int_0^\infty \frac{\exp\big(-\lambda y\big)}{(1+G_1y)^2}dy$$
$$= \frac{G}{B_1-G_1}\left[\Psi\Big(\frac{\lambda}{G_1}\Big) - \Psi\Big(\frac{\lambda}{B_1}\Big)\right] + \frac{\lambda}{G_1-B_1}\Psi\Big(\frac{\lambda}{G_1}\Big) + \frac{G_1}{G_1-B_1} + \frac{B_1G_1}{\big(G_1-B_1\big)^2}\left[\Psi\Big(\frac{\lambda}{G_1}\Big) - \Psi\Big(\frac{\lambda}{B_1}\Big)\right] \quad (24)$$

where $F_{\gamma_{\text{R-DF}}}[\rho(1+y)-1]$ can be obtained from (18). Further, (26) is obtained by considering (16), (20) and (29) as

$$P_{\text{R-DF}}^{\text{out}} = \sum_{j=0}^{N}\sum_{n=0}^{N-j}\sum_{m=0}^{j}\binom{N}{j}\binom{N-j}{n}\binom{j}{m}(-1)^{m+n} \times \frac{\exp\{-[(n+j)B_0\gamma_{th} + B_2(\rho-1)]\}}{[1+B_1(\rho-1)]\big(1+B\gamma_{th}\big)^{n+j}} I_2 \quad (30)$$

where $A_3 = (B_1\rho)/[1+B_1(\rho-1)]$, $\delta = B_2\rho + G$ and

$$I_2 = \frac{1}{2} + \frac{G}{G_1} - \frac{\delta}{2G_1} + \left[\frac{G\delta}{G_1^2} - \frac{\delta^2}{2G_1^2}\right]\Psi\Big(\frac{\delta}{G_1}\Big) \quad (31)$$

$$I_2 = \frac{G}{A_3-G_1}\left[\Psi\Big(\frac{\delta}{G_1}\Big) - \Psi\Big(\frac{\delta}{A_3}\Big)\right] + \frac{\delta}{G_1-A_3}\Psi\Big(\frac{\delta}{G_1}\Big) + \frac{G_1}{G_1-A_3} + \left[\Psi\Big(\frac{\delta}{G_1}\Big) - \Psi\Big(\frac{\delta}{A_3}\Big)\right]\frac{A_3G_1}{\big(G_1-A_3\big)^2} \quad (32)$$

It is noted that (31) for $A_3 = G_1$ and (32) for $A_3 \neq G_1$ are obtained using the same integration as in (24) and (25).

B. Presence of multiple EAVs

1) Existence of non-zero secrecy capacity: In the presence of multiple EAVs, the PDF of $\gamma_{\mathbf{b},E}$ is obtained from (11) and by using (14) as

$$f_{\gamma_{\mathbf{b},E}}(y) = K\sum_{l=0}^{K-1}\binom{K-1}{l}(-1)^l\exp[-(l+1)Gy] \times \left[\frac{G}{(1+G_1y)^{l+1}} + \frac{G_1}{(1+G_1y)^{l+2}}\right] \quad (33)$$

Then, $P_{\text{R-DF}}^{\text{ex}}$ is obtained considering (19) and (33) as

$$P_{\text{R-DF}}^{\text{ex}} = 1 - K\sum_{j=0}^{N}\sum_{n=0}^{N-j}\sum_{m=0}^{j}\sum_{l=0}^{K-1}\binom{N}{j}\binom{N-j}{n}\binom{j}{m} \times \frac{\binom{K-1}{l}(-1)^{m+l+n}}{(1+B\gamma_{th})^{n+j}}\exp[-(n+j)B_0\gamma_{th}]\,I_3 \quad (34)$$

where $\mu = B_2 + (l+1)G$ and

$$I_3 = \frac{A_1}{(l+1)!}\left[\sum_{t=1}^{l+1}(t-1)!\Big(\frac{1}{B_1}\Big)^{-t}(-\mu)^{l+1-t} - (-\mu)^{l+1}\Psi\Big(\frac{\mu}{B_1}\Big)\right] + \frac{A_2}{(l+2)!}\left[\sum_{t=1}^{l+2}(t-1)! \times\Big(\frac{1}{B_1}\Big)^{-t}(-\mu)^{l+2-t} - (-\mu)^{l+2}\Psi\Big(\frac{\mu}{B_1}\Big)\right] \quad (35)$$

Further, $A_1 = G/\big(B_1\big)^{l+2}$ and $A_2 = 1/\big(B_1\big)^{l+2}$. Note that (35) is obtained for a particular case where $B_1 = G_1$ and using [16, eq. (3.353.2)]. If $B_1 \neq G_1$, I_3 is given by

$$I_3 = \int_0^\infty \frac{\exp(-\mu y)}{1+B_1y}\left[\frac{G}{(1+G_1y)^{q_1}} + \frac{G_1}{(1+G_1y)^{q_2}}\right]dy \quad (36)$$

where $q_1 = l+1$ and $q_2 = l+2$. It is difficult to obtain a closed-form solution for (36) and hence, it is solved numerically.

2) Secrecy outage probability: For multiple EAVs and by substituting (29) and (33) into (26), $P_{\text{R-DF}}^{\text{out}}$ is given in (37) where $A_0 = (n+j)B_0\gamma_{th}$, $\xi = B_2\rho + (l+1)G$, $G_2 = G/(G_1)^{l+2}$ and $G_3 = 1/(G_1)^{l+2}$. If $A_3 \neq G_1$, we have

$$I_4 = \int_0^\infty \frac{\exp(-\xi y)}{1+A_3y}\left[\frac{G}{\big(1+G_1y\big)^{q_1}} + \frac{G_1}{\big(1+G_1y\big)^{q_2}}\right]dy \quad (39)$$

3) P-DF scheme: When the P-DF scheme is used, the best SR is selected to maximize the minimum of the SINR between the source-relay and relay-destination [5], [6] as

$$\gamma_{\text{P-DF}} = \max_{i\in\{1,2,\ldots,N\}}\left\{\min\left\{\frac{\gamma_s g_i}{\gamma_p\alpha_i+1}, \frac{\gamma_{r_i}h_i}{\gamma_p\alpha_{ps}+1}\right\}\right\} \quad (40)$$

As such, the CDF of $\gamma_{\text{P-DF}}$, i.e., $\Pr\{\gamma_{\gamma_{\text{P-DF}}} < y\}$ is obtained as

$$F_{\gamma_{\text{P-DF}}}(y) = \int_0^\infty \frac{\exp\big(-\frac{x}{\Omega_{ps}}\big)}{\Omega_{ps}}\prod_{i=1}^{N}\left[1 - \frac{\exp\big(-B_0y\big)}{1+By} \times \exp\big[-D\big(\gamma_p x+1\big)y\big]\right]dx = \sum_{j=0}^{N}\binom{N}{j}(-1)^j\frac{\exp(-j\eta y)}{\big(1+By\big)^j\big(1+D_1y\big)} \quad (41)$$

where $\eta = B_0+D$, $D = 1/\gamma_r\Omega_h$ and $D_1 = Dj\gamma_p\Omega_{ps}$. For the case of multiple EAVs, $P_{\text{P-DF}}^{\text{ex}}$ is given in (42) and is solved numerically.

IV. Numerical results

This section provides numerical examples based on Monte-Carlo simulations to verify our analysis conducted in the previous section. In all simulations, we set the system bandwidth $W = 5$ MHz, PU-Rx tolerable error $\epsilon = 0.01$ and target transmission rate of the SU-Tx→SR link $R_s = 64$ kbps.

Fig. 2 shows that the probability of non-zero secrecy capacity generally increases with respect to the increase of PU PIP SNR γ_Q. This is due to the fact that increasing

$$P_{\text{R-DF}}^{\text{out}} = \sum_{j=0}^{N}\sum_{n=0}^{N-j}\sum_{m=0}^{j}\sum_{l=0}^{K-1}\binom{N}{j}\binom{N-j}{n}\binom{j}{m}\binom{K-1}{l}(-1)^{m+l+n}\frac{K\exp\{-[A_0+B_2(\rho-1)]\}}{[1+B_1(\rho-1)]\,(1+B\gamma_{th})^{n+j}}I_4 \tag{37}$$

$$I_4 = \frac{G_2}{(l+1)!}\left[\sum_{t=1}^{l+1}(t-1)!\Big(\frac{1}{G_1}\Big)^{-t}(-\xi)^{l+1-t} - (-\xi)^{l+1}\Psi\Big(\frac{\xi}{G_1}\Big)\right] + \frac{G_3}{(l+2)!}\left[\sum_{t=1}^{l+2}(t-1)!\Big(\frac{1}{G_1}\Big)^{-t}\right.$$
$$\left.\times(-\xi)^{l+2-t} - (-\xi)^{l+2}\Psi\Big(\frac{\xi}{G_1}\Big)\right], \quad A_3 = G_1 \tag{38}$$

$$P_{\text{P-DF}}^{\text{ex}} = 1 - K\sum_{j=0}^{N}\sum_{l=0}^{K-1}\binom{N}{j}\binom{K-1}{l}(-1)^{j+l}\int_0^{\infty}\frac{\exp\{-[j\eta+(l+1)G]\,y\}}{(1+By)^{j}(1+D_1y)}\left[\frac{G}{(1+G_1y)^{l+1}}+\frac{G_1}{(1+G_1y)^{l+2}}\right]dy \tag{42}$$

γ_Q allows an increase of the SU transmit SNR according to (4) and (5). Moreover, it is shown that this probability increases when the number N of SRs increases. For example, by increasing $N = 1$ to $N = 4$, the secondary network security is improved. This shows how exploiting opportunistic relay selection in cooperative networks contributes to security enhancement, i.e., increasing the possibility that more SRs participate in relay selection. On the other hand, the secondary network security performance is degraded when the number K of EAVs increases, e.g., from $K=1$ to $K=2$. In this case, the probability of intercepting the message increases. Further, the probability of existence of secrecy capacity is also reduced by increasing the PU-Tx transmit SNR γ_p, e.g., $\gamma_p = 5$ dB to $\gamma_p = 10$ dB. Here, the PU-Tx transmit power becomes a stronger interference source to the secondary receiving nodes.

It is observed in Fig. 3 that the probability of non-zero secrecy capacity decreases as the number K of EAVs becomes high for all scenarios. In addition, we can see that the secondary network security is enhanced by increasing the channel mean power Ω_φ of the PU-Tx→EAV link, i.e., $\Omega_\varphi=0.5$ (Case 1) to $\Omega_\varphi=2$ (Case 2). Here, the PU-Tx is close to the EAV, and thus, the EAV channel capacity is degraded by the PU-Tx interference. As expected, when the EAV is far away from the SR, the probability of non-zero secrecy capacity is high, e.g., $\Omega_v=1$ (Case 3) compared to $\Omega_v=2$ (Case 2).

Fig. 4 shows the secrecy outage probability. As discussed for the probability of non-zero secrecy capacity in Figs. 2 and 3, we can see that the number K of EAVs and channel mean power Ω_φ of the PU-Tx→EAV link have the same impact on the secrecy outage probability. For example, increasing $\Omega_\varphi=2$ to $\Omega_\varphi = 4$, the secondary system security is improved. The effect of the SU secrecy target rate is also observed in Fig. 4 where the secrecy outage probability is high for $R=128$ kbps compared to $R=64$ kbps.

Fig. 5 compares the probability of non-zero secrecy capacity for the P-DF and R-DF schemes. In general, the R-DF scheme outperforms the P-DF scheme as the PU PIP SNR γ_Q increases. This is due to the fact that when γ_Q increases, the decoding threshold is satisfied in the first phase. Accordingly, more relay selection diversity is achieved. However, at low values of γ_Q, e.g., at $\gamma_Q<-2$ dB in Case 4, P-DF provides a better performance than R-DF. Again, the probability of non-zero secrecy capacity is high when the interference from PU-Tx→EAV increases, e.g., $\Omega_\varphi=2$ (Case 5) to $\Omega_\varphi=4$ (Case 6). In addition, the secondary network security is degraded when K increases, e.g., $K=1$ in Case 5 to $K=2$ in Case 6.

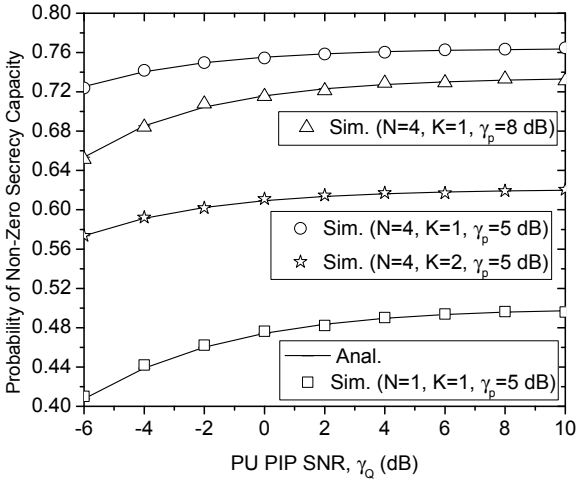

Fig. 2. Probability of existence of non-zero secrecy capacity versus PU PIP SNR, γ_Q with SU maximum transmit SNR $\gamma_{s,\max}=\gamma_{r,\max}=12$ dB, $\Omega_g=\Omega_h=\Omega_v=2$ and $\Omega_\alpha=\Omega_\beta=\Omega_\varphi=\Omega_{sp}=\Omega_{ps}=0.5$.

V. Conclusion

In this paper, we have studied the physical layer security for cognitive relay networks with multiple SRs in the presence of a single EAV and multiple EAVs. Analytical expressions of the probability of existence of non-zero secrecy capacity and secrecy outage probability have been derived under the PU PIP constraint and SU maximum transmit power limit. The effect of the number N of SRs, number K of EAVs and channel mean powers on the secondary security performance has been evaluated. Further, the impact of the interference from primary network to the secondary network has been investigated. The numerical examples indicate that the secondary system security is improved by exploiting relay selection diversity.

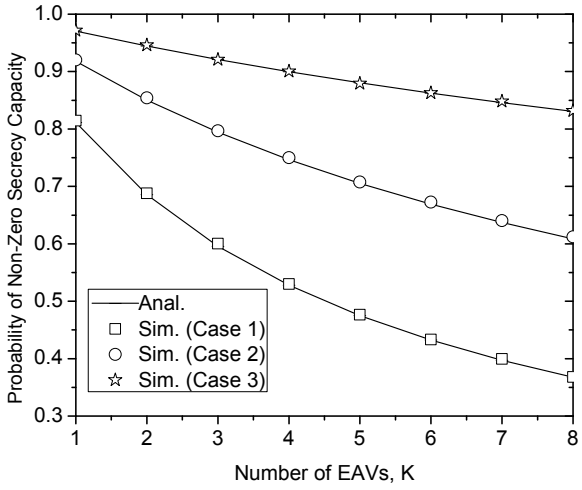

Fig. 3. Probability of existence of non-zero secrecy capacity versus number K of EAVs with $N=6$, $\gamma_Q=10$ dB, $\gamma_p=5$ dB, $\gamma_{s,\max}=\gamma_{r,\max}=12$ dB and $\Omega_g=\Omega_h=2$.
Case 1: $\Omega_v=2$, $\Omega_\alpha=\Omega_\beta=\Omega_\varphi=\Omega_{sp}=\Omega_{ps}=0.5$;
Case 2: $\Omega_v=2$, $\Omega_\alpha=\Omega_\beta=\Omega_{sp}=\Omega_{ps}=0.5$, $\Omega_\varphi=2$;
Case 3: $\Omega_v=1$, $\Omega_\alpha=\Omega_\beta=\Omega_{sp}=\Omega_{ps}=0.5$, $\Omega_\varphi=2$.

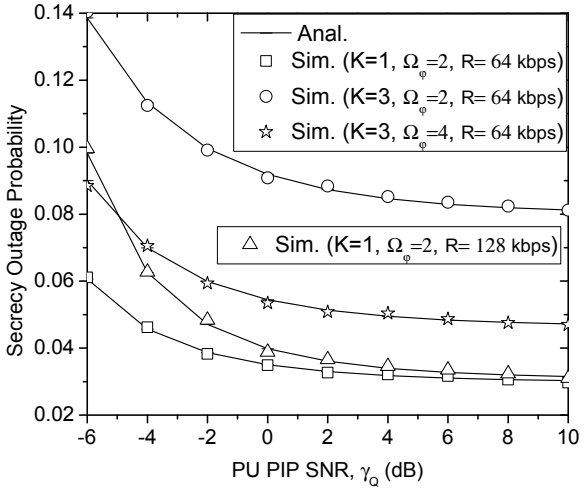

Fig. 4. Secrecy outage probability with $N=6$, $\gamma_p=5$ dB, $\gamma_{s,\max}=\gamma_{r,\max}=12$ dB, $\Omega_g=\Omega_h=2$, $\Omega_v=1$ and $\Omega_\alpha=\Omega_\beta=\Omega_{sp}=\Omega_{ps}=0.5$.

The results also show that the secondary network security is enhanced by increasing the channel mean power of the PU-Tx→EAV link.

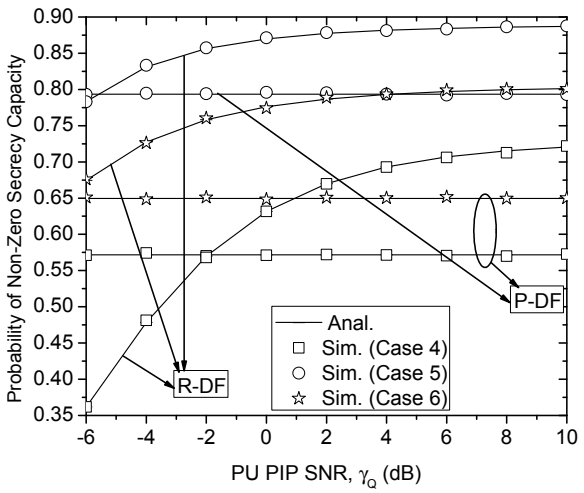

Fig. 5. Probability of existence of non-zero secrecy capacity with $N=4$, $\gamma_{s,\max}=\gamma_{r,\max}=12$ dB, $\gamma_p=5$ dB and $\Omega_g=\Omega_h=\Omega_v=2$.
Case 4: $K=1$, $\Omega_\alpha=\Omega_\beta=\Omega_{sp}=\Omega_{ps}=\Omega_\varphi=2$;
Case 5: $K=1$, $\Omega_\alpha=\Omega_\beta=\Omega_{sp}=\Omega_{ps}=1$, $\Omega_\varphi=4$;
Case 6: $K=2$, $\Omega_\alpha=\Omega_\beta=\Omega_{sp}=\Omega_{ps}=1$, $\Omega_\varphi=4$.

REFERENCES

[1] Z. Qian, J. Juncheng, and Z. Jin, "Cooperative relay to improve diversity in cognitive radio networks," *IEEE Commun. Mag.*, vol. 47, no. 2, pp. 111–117, Feb. 2009.

[2] J. Lee, H. Wang, J. G. Andrews, and D. Hong, "Outage probability of cognitive relay networks with interference constraints," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 390–395, Feb. 2011.

[3] Y. Zou, J. Zhu, B. Zheng, and Y.-D. Yao, "An adaptive cooperation diversity scheme with best relay selection in cognitive radio networks," *IEEE Trans. Signal Process.*, vol. 58, no. 10, pp. 5438–5445, Oct. 2010.

[4] K. Tourki, K. A. Qaraqe, and M.-S. Alouinin, "Outage analysis for underlay cognitive networks using incremental regenerative relaying," *IEEE Trans. Veh. Technol.*, vol. 62, no. 2, pp. 721–734, Feb. 2013.

[5] S. Sagong, J. Lee, and D. Hong, "Capacity of reactive DF scheme in cognitive relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3133–3138, Oct. 2011.

[6] H. Tran, H.-. Zepernick, and H. Phan, "Cognitive proactive and reactive DF relaying schemes under joint outage and peak transmit power constraints," *IEEE Commun. Lett.*, vol. 17, no. 8, pp. 1548–1551, Aug. 2013.

[7] R. F. Schaefer and H. Boche, "Physical layer service integration in wireless networks: Signal processing challenges," *IEEE Signal Process. Mag.*, vol. 31, no. 3, pp. 147–156, May 2014.

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

[9] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[10] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–188, Mar. 2010.

[11] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical layer security in cooperative wireless networks," *IEEE J. S. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[12] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Commun.*, vol. 4, no. 15, pp. 1787–1791, Oct. 2010.

[13] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6076–6085, Dec. 2013.

[14] A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu, and V. C. M. Leung, "A survey of security challenges in cognitive radio networks: solutions and future research directions," *Proc. IEEE*, vol. 100, no. 12, pp. 3172–3186, Dec. 2012.

[15] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Commun.*, vol. 6, no. 16, pp. 2676–2687, Nov. 2012.

[16] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series and Products*, 7th ed. Elsevier, 2007.