Achievable Secrecy Capacity in an Underlay Cognitive Radio Network

Louis Sibomana, Hans-Jürgen Zepernick, Hung Tran

IEEE Conference on Communications and Network Security

2014 San Francisco, USA

Achievable Secrecy Capacity in an Underlay Cognitive Radio Network

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, Vietnam, E-mail: {tranhungemail}@gmail.com

***Abstract*—In this paper, we consider a spectrum sharing cognitive radio network where a secondary user (SU) transmitter (SU-Tx) communicates with multiple SU receivers (SU-Rxs). There exist multiple eavesdroppers (EAVs) who illegally listen to the secondary network communication. Further, the primary network consists of a primary user (PU) transmitter serving multiple PU receivers. In particular, the SU-Tx transmit power is subject to the joint constraint of PU outage and SU maximum transmit power limit. Moreover, we investigate the secondary network physical layer security in terms of average secrecy capacity for both cases of known and unknown channel information of the EAV at the SU-Tx. Numerical results are provided to evaluate the impact of the number of PU-Rxs, number of EAVs, number of SU-Rxs, and channel mean powers among users on the SU average secrecy capacity.**

I. Introduction

Cognitive radio network (CRN) technology has been proposed as a promising solution to the radio spectrum shortage and inefficiency in its utilization [1], [2]. In particular, an underlay CRN improves the spectrum usage by allowing the secondary users (SUs) to access the frequency bands of the primary users (PUs) given that the received interference at the PU receiver (PU-Rx) remains below a predefined threshold. To limit harmful interference to the PU-Rx, various interference constraints, e.g., outage constraint, peak or average interference power constraints and SU power allocation strategies have been studied [3]–[7]. Further, different performance metrics such as ergodic capacity [4], [6], [8], [9], outage capacity [4] and outage probability [9] have been considered for the secondary network performance analysis.

On the other hand, security is becoming a critical issue in wireless systems due to the broadcast nature of wireless communications [10]. Different from cryptographic techniques at the upper layers, physical layer security techniques utilize physical layer properties to secure transmission of confidential information [10]–[12]. In particular, the physical layer security provides the theoretical analysis about how much information can be safely transmitted in the presence of an eavesdropper (EAV). In [13]–[16], the security problem for conventional wireless data transmission has been studied from an information theoretic point of view.

Like any other wireless communication technology, CRN is also subject to security challenges [17], [18]. In this context, the PU secrecy capacity and outage probability of secrecy capacity have been analyzed in [18]. An information secrecy cooperative game was considered in [19] where the PU and SU cooperate to maximize the PU secrecy rate. Further, [20] studied the probability of existence of non-zero secrecy capacity of PU. While the works [18]–[20] focused on the primary network security, it is challenging to provide secondary network security in addition to the PU protection requirements and mutual interference between primary and secondary networks.

The secondary network physical layer security has been studied in [21]–[23]. The SU secrecy capacity of the multiple-input single-output (MISO) channel has been analyzed in [21] with perfect knowledge of channel state information (CSI) of both the SU transmitter (SU-Tx) to the SU receiver (SU-Rx) and SU-Tx→EAV links. In practice, the EAVs are not willing to provide their CSI to the legitimate party. The case where CSI is not perfectly known at the SU-Tx has been considered in [22] for the MISO channel. However, the implementation of multiple antennas is limited due to resource constraints such as cost and size in today's mobile nodes. An alternative approach to enhance physical layer security is to exploit opportunistic scheduling (OS) in a multiuser environment. In [23], an SU-Rx that maximizes the achievable secrecy rate was scheduled for transmission in order to improve the secondary network security under perfect CSI of all channels.

Moreover, the effect of the interference from the primary network to the secondary network was ignored in [21]–[23]. However, different to existing wireless networks where interference is undesired, interference can be beneficial to improve the secure transmission when used to degrade the performance of the EAV channel. For example, a device-to-device (D2D) communication has been introduced in [24] to improve the security in cellular network where D2D generates interference to the EAV to reduce the achievable data rate of the EAV link. Different to [21]–[23], in this work, we consider the interference from the PU transmitter (PU-Tx) to the SU-Rx and EAV, and evaluates its impact on the secondary network security.

In addition, the SU secrecy capacity in [21], [22] has been obtained by considering only a single EAV and single SU-Rx under the SU transmit power limit and interference temperature limit at the PU. Further, [23] examined the presence of multiple EAVs considering only a single PU-Rx and a peak interference power constraint at the PU. To address a more realistic scenario, we consider the interference from the

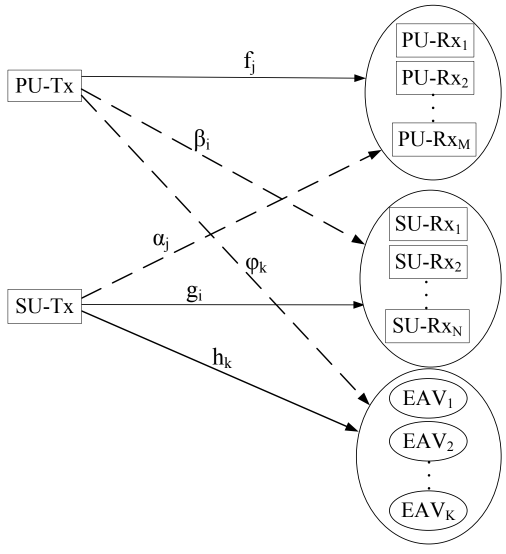

Fig. 1. A CRN underlay model in the presence of multiple eavesdroppers. (Dashed lines: Interference links; Solid lines: Communication links).

primary network to the secondary network, the presence of multiple PU-Rxs, multiple EAVs and multiple SU-Rxs, and the SU maximum transmit power limit.

In this paper, we analyze the SU achievable secrecy capacity for both availability of full CSI and the case of absence of EAV CSI at the SU-Tx. In particular, the SU-Tx transmit power under the joint outage constraint of multiple PUs and SU-Tx maximum transmit power limit is obtained. Further, we exploit OS where the SU-Rx with best channel condition is scheduled for transmission. Given these settings, the probability density function (PDF) of the received signal-to-interference-plus-noise ratio (SINR) at the SU-Rx and EAV, respectively, is derived to evaluate the SU average secrecy capacity. Moreover, the impact of the number of PU-Rxs, number of SU-Rxs, number of EAVs, the SU maximum transmit power limit and the channel mean powers among users on the SU average secrecy capacity is investigated.

The rest of the paper is organized as follows. Section II describes the system model and spectrum sharing constraints. In Section III, the SU average secrecy capacity is analyzed. Section IV provides numerical results and discussions. Finally, conclusions are presented in Section V.

II. System model and spectrum sharing constraints

A. System model

We consider an underlay CRN system model as depicted in Fig.1 where the secondary network consists of an SU-Tx communicating with N SU-Rxs whereas the primary network consists of a PU-Tx serving M PU-Rxs. Further, there exist K EAVs who intercept the secondary network communication and the eavesdropping nodes are assumed to be passive, i.e., they only listen. We assume that the shared bandwidth is normalized to unity and all nodes are equipped with a single antenna. Note that the considered system model represents a realistic scenario where the PU-Tx can act as a macro primary base station of any cellular network while SU-Tx operates as a femtocell access point [25].

Let f_j, $j = 1, 2, \ldots, M$ and g_i, $i = 1, 2, \ldots, N$ denote the channel gains of the communication links PU-Tx→PU-Rx$_j$ and SU-Tx→SU-Rx$_i$. The channel gains of SU-Tx→EAV$_k$, $k = 1, 2, \ldots, K$, are represented by h_k. Furthermore, the channel gains of the interference links SU-Tx→PU-Rx$_j$, PU-Tx→SU-Rx$_i$ and PU-Tx→EAV$_k$ are, respectively, defined by α_j, β_i and φ_k. Moreover, all channels are assumed to be subject to independent Rayleigh fading. In addition, we define a set $\mathcal{E} = (f_j, g_i, h_k, \alpha_j, \beta_i, \varphi_k)$ of channel gains $e \in \mathcal{E}$ that are exponentially distributed random variables with channel mean power Ω_e. It should be noted that we do not require that the channel mean powers Ω_e to be the same for all links and thereby representing a realistic scenario.

In an underlay CRN, an SU is allowed to transmit as long as the transmission from the secondary network does not cause harmful interference to the PU-Rx. In the aforementioned related works [21]–[23], it is assumed that the SU has perfect knowledge of CSI of the SU-Tx→PU-Rx link. However, it is hard to obtain perfect knowledge of CSI since the collaboration between PU and SU may be limited [7]. In this paper, we assume that the SU-Tx has statistical channel knowledge of the PU. The SU can estimate the average channel gains of the PU based on system parameters such as transmission distance and transmit/receive antenna gain which are considered to be relatively stable [5]. In addition, the average channel gain estimated at the SU can also reduce the feedback burden for the PU, i.e., save feedback channel resources.

B. Spectrum sharing constraints

In the considered system model, the SU-Tx must control its transmit power to ensure that the interference inflicted to the PU-Rx is kept below a predetermined threshold [5]–[7]. Here, we translate the PU interference power constraint in terms of a minimum target rate that should be satisfied with a desired outage probability. Moreover, an additional constraint is considered as the transmit power cannot be infinite or very large in practice. These constraints can be formulated as

$$P_{\text{out,p}} = \Pr\left\{\theta_{p,j} < \theta_{th,j}\right\} \leq \xi_{p,j} \tag{1a}$$

$$P_s \leq P_{\max} \tag{1b}$$

where $\Pr\{\cdot\}$ denotes the probability, $\theta_{th,j} = 2^{R_{p,j}} - 1$, and $P_{\max}$ is the SU maximum transmit power limit. Further, $R_{p,j}$, $\xi_{p,j}$ and $\theta_{p,j}$ are the PU target transmission rate, PU outage threshold and instantaneous SINR at the jth PU-Rx, respectively.

1) PU outage probability: We consider a homogenous primary network and therefore $\forall j$: $\xi_{p,j} = \xi_p$, $R_{p,j}$=R_p, $\theta_{th,j} = \theta_{th}$, $\Omega_{f_j} = \Omega_f$ and $\Omega_{\alpha_j} = \Omega_\alpha$. In order to guarantee that no harmful interference is caused to any of the M PU-Rxs, the PU outage probability is derived based on the lowest-instantaneous SINR at the PU-Rx among all PU-Rxs. In this case, the SINR at the jth PU-Rx is defined as

$$\theta_p = \min_{j=1,2,\ldots,M} \left\{ \frac{P_p f_j}{P_s \alpha_j + N_0} \right\} \tag{2}$$

where N_0 is the noise power, P_p denotes the PU transmit power and P_s is the SU instantaneous transmit power.

From (2) and (1a), the PU outage probability is derived as follows:

$$\begin{aligned} P_{\text{out},p} &= 1 - \Pr\left\{ \min_{j=1,2,\ldots,M} \left\{ \frac{P_p f_j}{P_s \alpha_j + N_0} \right\} \geq \theta_{th} \right\} \\ &= 1 - \prod_{j=1}^{M} \int_0^{\infty} \Pr\left\{ f_j \geq \frac{\theta_{th}\Big(P_s x + N_0\Big)}{P_p} \right\} f_{\alpha_j}(x) dx \\ &= 1 - \left[\frac{P_p \Omega_f}{\theta_{th} P_s \Omega_\alpha + P_p \Omega_f} \exp\left(- \frac{\theta_{th} N_0}{P_p \Omega_f} \right) \right]^M \end{aligned} \tag{3}$$

where $f_{\alpha_j}(x) = (1/\Omega_\alpha)\exp(-x/\Omega_\alpha)$ is the PDF of α_j since the channels are modeled as Rayleigh fading.

2) SU-Tx transmit power policy: The SU should adapt its transmit power within the instantaneous and maximum transmit power limit to ensure that no harmful interference is caused to the primary network, i.e, to satisfy the PU outage constraint. Using (3) and considering (1a) and (1b), and then after some manipulations, we obtain an expression of the SU-Tx transmit power policy in terms of transmit signal-to-noise ratio (SNR) as

$$\gamma_s = \min\left\{ \frac{\gamma_p \Omega_f}{\theta_{th}\Omega_\alpha} \Gamma^+, \gamma_{\max} \right\} \tag{4}$$

where

$$\Gamma^+ = \max\left\{ 0, \frac{1}{\sqrt[M]{1-\xi_p}} \exp\left(- \frac{\theta_{th}}{\gamma_p \Omega_f} \right) - 1 \right\}$$

and $\gamma_p = P_p/N_0$ is the PU transmit SNR. Further, $\gamma_s = P_s/N_0$ and $\gamma_{\max} = P_{\max}/N_0$ are, respectively, the transmit SNR of the SU instantaneous transmit power and maximum transmit power limit.

III. SU AVERAGE SECRECY CAPACITY

The SU secrecy capacity is defined as the maximum transmission rate at which a message can be reliably received by the SU-Rx and kept perfectly secret from the EAV. Moreover, the SU capacity can be enhanced by exploiting OS transmission [8]. It is also shown in [23] that the secondary network physical layer security is improved by selecting the SU-Rx with the best channel condition. Recall that [21]–[23] did not consider the interference form the primary network to secondary network. Using OS and considering PU-Tx→SU-Rx link, the SINR of the selected ith SU-Rx is given by

$$\gamma_{\text{OS}} = \max_{i=1,2,\ldots,N} \left\{ \frac{\gamma_s g_i}{\gamma_p \beta_i + 1} \right\} \tag{5}$$

and the corresponding instantaneous capacity is defined as

$$C_s = \log_2 \Big(1 + \gamma_{\text{OS}}\Big) \tag{6}$$

In the considered model, K EAVs independently try to listen to the SU communication. The maximum channel gain among all EAVs is defined as

$$\gamma_e = \max_{k=1,2,\ldots,K} \left\{ \frac{\gamma_s h_k}{\gamma_p \varphi_k + 1} \right\} \tag{7}$$

and the achievable capacity at the kth EAV is given by

$$C_e = \log_2 \Big(1 + \gamma_e\Big) \tag{8}$$

According to [13], [14], the achievable secrecy rate of the SU can be formulated as

$$C_{\text{sec}} = C_s - C_e \tag{9}$$

A. Average secrecy capacity with full CSI

If the SU-Tx has perfect CSI of both SU-Tx→SU-Rx and SU-Tx→EAV links, the secondary network can achieve optimal secure transmission by allowing transmission only when $\gamma_{\text{OS}} > \gamma_e$. In this case, the SU achievable average secrecy rate, i.e, ergodic secrecy capacity [14] is given by

$$C_{\text{global CSI}} = \int_0^{\infty} \int_y^{\infty} C_{\text{sec}}(x,y) f_{\gamma_{\text{os}}}(x) f_{\gamma_e}(y) dx dy \tag{10}$$

where $f_{\gamma_{\text{os}}}(x)$ and $f_{\gamma_e}(y)$ are the PDF of γ_{os} and γ_e, respectively. Furthermore, using (5), the cumulative distribution (CDF) of γ_{OS} is obtained as

$$\begin{aligned} F_{\gamma_{\text{OS}}}(x) &= \Pr\left\{\gamma_{\text{OS}} < x\right\} \\ &= \prod_{i=1}^{N} \int_0^{\infty} \Pr\left\{ g_i \leq \frac{x\Big(\gamma_p u + 1\Big)}{\gamma_s} \right\} \\ &\times \quad f_{\beta_i}(u) du \\ &= \left[1 - \frac{\exp\big(-Bx\big)}{\Big(1 + Ax\Big)} \right]^N \end{aligned} \tag{11}$$

where $f_{\beta_i}(u) = (1/\Omega_\beta)\exp\big(-u/\Omega_\beta\big)$, $A = \gamma_p \Omega_\beta/(\gamma_s \Omega_g)$ and $B = 1/(\gamma_s \Omega_g)$. Then, differentiating (11) with respect to x and applying binomial expansion, we obtain

$$\begin{aligned} f_{\gamma_{\text{OS}}}(x) &= N \sum_{n=0}^{N-1} \binom{N-1}{n} (-1)^n \exp\left[-B\big(n+1\big)x\right] \\ &\times \left[\frac{B}{\Big(1+Ax\Big)^{n+1}} + \frac{A}{\Big(1+Ax\Big)^{n+2}} \right] \end{aligned} \tag{12}$$

Similarly, from (7), the PDF of γ_e is given by

$$\begin{aligned} f_{\gamma_e}(y) &= K \sum_{l=0}^{K-1} \binom{K-1}{l} (-1)^l \exp\left[-C\big(l+1\big)y\right] \\ &\times \left[\frac{C}{\Big(1+Dy\Big)^{l+1}} + \frac{D}{\Big(1+Dy\Big)^{l+2}} \right] \end{aligned} \tag{13}$$

where $C = 1/(\gamma_s \Omega_h)$ and $D = \gamma_p \Omega_\varphi/(\gamma_s \Omega_h)$. Furthermore, by substituting (12) and (13) into (10), we have

$$C_{\text{global CSI}} = NK \sum_{n=0}^{N-1} \sum_{l=0}^{K-1} \binom{N-1}{n} \binom{K-1}{l} (-1)^{n+l} \times \int_0^\infty \int_y^\infty \left[\log_2(1+x) - \log_2(1+y)\right] \times \exp\left\{-\left[B(n+1)x + C(l+1)y\right]\right\} \times \left[\frac{B}{(1+Ax)^{n+1}} + \frac{A}{(1+Ax)^{n+2}}\right] \times \left[\frac{C}{(1+Dy)^{l+1}} + \frac{D}{(1+Dy)^{l+2}}\right] dxdy \qquad (14)$$

B. Average secrecy capacity without EAV CSI

When the SU-Tx has only perfect CSI of the SU-Rx link channel, the SU average secrecy capacity is given by

$$C_{\text{without EAV CSI}} = NK \sum_{n=0}^{N-1} \sum_{l=0}^{K-1} \binom{N-1}{n} \binom{K-1}{l} (-1)^{n+l} \times \int_0^\infty \int_0^\infty \left[\log_2\left(1+x\right) - \log_2\left(1+y\right)\right]^+ \times \exp\left\{-\left[B(n+1)x + C(l+1)y\right]\right\} \times \left[\frac{B}{(1+Ax)^{n+1}} + \frac{A}{(1+Ax)^{n+2}}\right] \times \left[\frac{C}{(1+Dy)^{l+1}} + \frac{D}{(1+Dy)^{l+2}}\right] dxdy \qquad (15)$$

where $[z]^+ = \max\{z, 0\}$ [14]. Note that the SU average secrecy capacity without EAV CSI accounts also for the information accumulated at the EAV, i.e., $\gamma_{\text{OS}} > \gamma_e$ and $\gamma_{\text{OS}} \leq \gamma_e$ scenarios different to the secrecy capacity with full CSI where information is transmitted when the legitime channel is more reliable than the EAV channel, $\gamma_{\text{OS}} > \gamma_e$.

Obtaining closed-form solutions for the expressions in (14) and (15) is difficult due to the integral complexity. However, (14) and (15) can easily be solved numerically.

IV. Numerical results

In this section, we study the impact of primary network parameters, number N SU-Rxs, number K of EAVs, SU maximum transmit power limit and the channel mean powers among users on the SU average secrecy capacity. Specifically, analyticals results are presented along with Monte-Carlo simulations to validate our analysis.

Fig. 2 compares the SU average secrecy capacity with global CSI and without EAV CSI at the SU-Tx. It is observed that the SU average secrecy capacity with full CSI is higher than the secrecy capacity without EAV CSI for all scenarios. Hence, the secrecy capacity with full CSI is an upper bound for the secrecy capacity when only the CSI of the SU-Tx→SU-Rx link is known. This is due to the fact that when the SU-Tx has full CSI of both legitime and EAV links, transmission occurs only if $\gamma_{\text{os}} > \gamma_e$, i.e., when the SU-Tx→SU-Rx channel is stronger than the SU-Tx→EAV channel. It is also shown that as the number of EAVs increases, $K = 1$ to $K = 3$, the SU average secrecy capacity is significantly reduced. If $K \to \infty$, it is hard to obtain a non-zero secrecy capacity, i.e., $\Pr\{C_s > 0\} \to 0$. However, a non-zero secrecy capacity of the SU can be obtained for $K < N$ in the case of unknown EAV CSI.

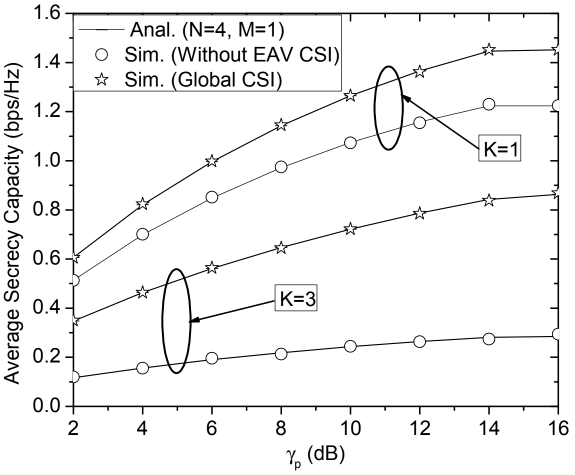

Fig. 2. SU average secrecy capacity versus PU transmit SNR, γ_p, with SU maximum transmit SNR $\gamma_{\max} = 14$ dB, $\Omega_e = 2$ $\forall e \in \mathcal{E}$, $\xi_p = 0.01$ and $R_p = 0.02$ bps/Hz (i.e., LTE user spectral efficiency requirement).

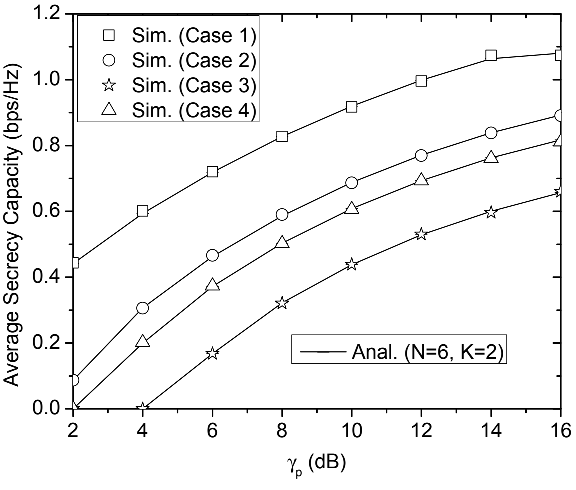

Fig. 3. SU average secrecy capacity without EAV CSI versus γ_p with $\gamma_{\max} = 14$ dB and $\Omega_e = 2$. Case 1: $M = 1$, $R_p = 0.02$ bps/Hz, $\xi_p = 0.01$; Case 2: $M = 2$, $R_p = 0.02$ bps/Hz, $\xi_p = 0.01$; Case 3: $M = 2$, $R_p = 0.04$ bps/Hz, $\xi_p = 0.01$; Case 4: $M = 2$, $R_p = 0.02$ bps/Hz, $\xi_p = 0.008$.

Fig. 3 illustrates the impact of the primary network parameters on the SU average secrecy capacity without EAV CSI at the SU-Tx. It is observed that the SU average secrecy capacity becomes low as the number of PU-Rxs increases in Case 2 where $M = 2$ compared to Case 1 with $M = 1$. Further, the SU average secrecy capacity also decreases when the PU target rate R_p becomes high, e.g, $R_p = 0.04$ bps/Hz in Case 3 referred to Case 2. We can see that when $R_p = 0.04$ bps/Hz, the PU outage constraint is not satisfied. In this case, the SU-Tx is allowed to transmit at $\gamma_p \geq 4$ dB compared to the scenario where $R_p = 0.02$ bps/Hz (Case 2). In addition, the secondary network performance is degraded as the PU outage threshold ξ_p becomes low, i.e., Case 4 where $\xi_p = 0.008$ compared to Case 2 where $\xi_p = 0.01$. The results in Fig. 3 are explained by the SU transmit SNR policy in (4). That is, when the PU outage constraint is not satisfied, the SU transmit power must be reduced to not cause harmful interference at the PU-Rx.

Moreover, the effect of the number of SU-Rxs, SU maximum transmit SNR $\gamma_{\max}$ and channel mean power of the SU-Tx→PU-Rx link on the SU average secrecy capacity is observed in Fig. 4. The SU average secrecy capacity increases with respect to the increase of the number of SU-Rxs. Thus, exploiting the OS transmission can enhance the secondary network security. The impact of $\gamma_{\max}$ is observed at $\gamma_p \geq 12$ dB for $\gamma_{\max} = 8$ dB where the secrecy capacity decreases, i.e., the SU transmit SNR becomes saturated at $\gamma_p \geq 12$ dB for $\gamma_{\max} = 8$ dB compared to the scenario $\gamma_{\max} = 14$ dB. Further, the SU average secrecy capacity decreases as Ω_α become high (from $\Omega_\alpha = 2$ to $\Omega_\alpha = 3$). Again, this case is in accordance with the SU transmit power policy in (4), i.e., the SU transmit SNR is decreased to reduce the interference to the PU-Rx.

Fig. 5 shows the impact of the channel mean powers among users on the SU average secrecy capacity. In particular, when the channel mean power of the PU-Tx→SU-Rx link increases ($\Omega_\beta = 2$ to 4), the secondary network performance is degraded. In this case, the PU-Tx becomes an interference source to the ith SU-Rx. Moreover, we can see that the SU performance is significantly improved when the channel mean power of the PU-Tx→EAV link increases ($\Omega_\varphi = 2$ to 4). It is noted that the results in [20] also indicate that the primary network security is improved by increasing the interference from the SU to the EAV. Therefore, a high security in spectrum sharing can be achieved when the PU and SU cooperate to combat the EAV attacks.

In addition, it is also observed that the channel mean power of the PU-Tx→ PU-Rx link has an important impact on the secondary network performance. For example, by increasing $\Omega_f = 2$ to 3 in Fig. 5, the SU average secrecy capacity increases. In this case, the PU outage probability decreases as Ω_f increases leading to an increase of the SU transmit SNR.

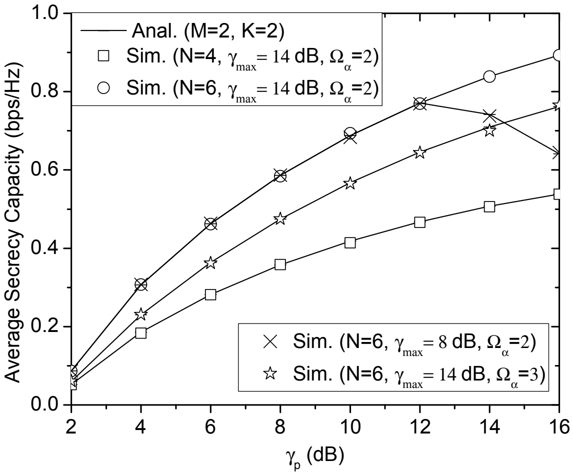

Fig. 4. SU average secrecy capacity without EAV CSI versus γ_p with $R_p = 0.02$ bps/Hz, $\xi_p = 0.01$ and $\Omega_\beta = \Omega_\varphi = \Omega_h = \Omega_f = \Omega_g = 2$.

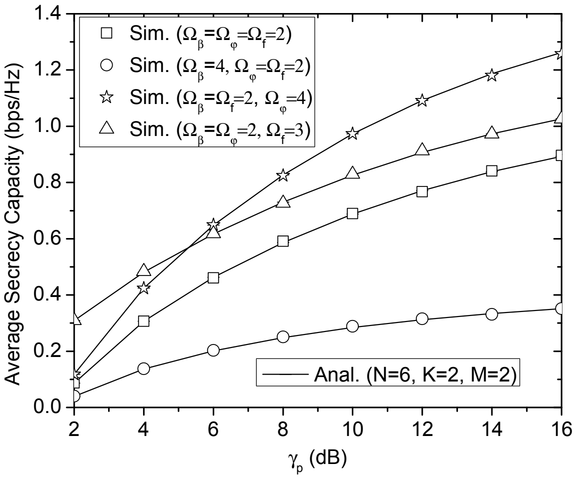

Fig. 5. SU average secrecy capacity without EAV CSI versus γ_p with $\gamma_{\max} = 16$ dB, $R_p = 0.02$ bps/Hz, $\xi_p = 0.01$ and $\Omega_\alpha = \Omega_h = \Omega_g = 2$.

V. Conclusion

In this paper, we have investigated the physical layer security of secondary network in the presence of multiple EAVs. Analytical expressions of the SU average secrecy capacity for both full CSI and absence of CSI of the EAV are obtained under the joint outage constraint of multiple PU-Rxs and SU maximum transmit power limit. Further, we have studied the impact of the primary network parameters, number of PU-Rxs, number of SU-Rxs, number of EAVs, SU maximum transmit power limit and channel mean powers among users on the SU average secrecy capacity. The numerical examples indicate that the SU average secrecy capacity for global CSI serves as an upper bound for the case of unknown CSI of the EAV link. The results also show that the secondary network performance strongly depends on the SU-Tx transmit power policy and channel condition of the PU-Tx→EAV link. Moreover, the secondary network security is improved by increasing the interference from the PU-Tx to the EAV. It is shown that multiuser diversity scheduling improves the secondary network security. It should also be noted that the considered performance metric, i.e., average secrecy capacity, is applicable to delay tolerant applications. For the case of delay-limited applications, the secrecy outage probability is the appropriate metric and will be examined in our future work.

REFERENCES

[1] S. Haykin, “Cognitive radio: Brain-empowered wireless communications,” *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[2] I. Akyildiz, W. Lee, M. Vuran, and S. Mohanty, “Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey,” *Computer Network*, vol. 50, no. 13, pp. 2127–2159, Sep. 2006.

[3] A. Ghasemi and E. Soussa, “Fundamental limits of spectrum sharing in fading environments,” *IEEE Trans. Wireless Commun.*, vol. 6, no. 2, pp. 649–658, Feb. 2007.

[4] R. Zhang, “On peak versus average interference power constraints for protecting primary users in cognitive radio networks,” *IEEE Trans. Wireless Commun.*, vol. 8, no. 4, pp. 2112–2120, Apr. 2009.

[5] 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 Processing*, vol. 58, no. 10, pp. 5438–5445, Oct. 2010.

[6] X. Kang, R. Zhang, Y. Liang, and H. Krishna, “Optimal power allocation strategies for fading cognitive radio channels with primary user outage constraint,” *IEEE J. Sel. Areas Commun.*, vol. 29, no. 2, pp. 374–383, Feb. 2011.

[7] P. J. Smith, P. A. Domochowski, H. A. Suraweera, and M. Shafi, “The effects of limited channel konwledge on cognitive radio system capacity,” *IEEE Trans. Vehic. Techn.*, vol. 62, no. 2, pp. 927–933, Feb. 2013.

[8] T. W. Ban, W. Choi, B. C. Jung, and D. K. Sung, “Multiuser diversity in a spectrum sharing system,” *IEEE Trans. Wireless Commun.*, vol. 8, no. 1, pp. 102–106, Jan. 2009.

[9] H. Tran, M. Hagos, M. Mohamed, and H.-J. Zepernick, “Impact of primary networks on the performance of secondary networks,” in *Proc. IEEE ComManTel, Ho Chi Minh City, Vietnam*, Jan. 2013, pp. 1–6.

[10] R. F. Schaefer and H. Boche, “Physical layer service integration in wireless networks,” *IEEE Signal Processing Mag.*, vol. 31, no. 3, pp. 147–156, Apr. 2014.

[11] 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.

[12] J. Barros and M. R. Rodrigues, “Secrecy capacity of wireless channels,” in *Proc. IEEE ISIT, Seattle, Washington, USA*, Jul. 2006, pp. 1–5.

[13] 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.

[14] P. K. Gopala, L. Lai, and H. E. Gamal, “On the secrecy capacity of fading channels,” *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Jan. 2008.

[15] F. Oggier and B. Hassibi, “Secrecy capacity of the MIMO wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 75, no. 8, pp. 4961–4972, Aug. 2011.

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

[17] 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.

[18] Z. Shu, Y. Qian, and S. Ci, “On physical layer security for cognitive radio networks,” *IEEE Network*, vol. 7, no. 3, pp. 28–33, Jun. 2013.

[19] Y. Wu and K. Liu, “An information secrecy game in cognitive radio networks,” *IEEE Trans. on Inf. Forensics and Security*, vol. 6, no. 3, pp. 831–842, Sep. 2011.

[20] L. Sibomana, H. Tran, H.-J. Zepernick, and C. Kabiri, “On non-zero secrecy capacity and outage probability of cognitive radio networks,” in *Proc IEEE International Symposium Wireless Personal Multimedia Communications (WPMC), Atlantic City, USA*, Jun. 2013, pp. 1–6.

[21] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, “Secure communication over MISO cognitive radio channels,” *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.

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

[23] Y. Zou, X. Wang, and W. Shen, “Physical-layer security with multiuser scheduling in cognitive radio networks,” *IEEE Trans. Wireless Commun.*, vol. 61, no. 12, pp. 5103–5113, Dec. 2013.

[24] J. Yue, C. Ma, H. Yu, and W. Zhou, “Secrecy-based access control for device-to-device communication underlaying cellular networks,” *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2068–2071, Nov. 2013.

[25] S. Al-Rubaye, A. Al-Dulaimi, and J. Cosmas, “Cognitive femtocell: future wireless networks for indoor applications,” *IEEE Veh. Technol. Mag.*, pp. 44–51, Mar. 2011.