POWER ALLOCATION FOR ENERGY-CONSTRAINED COGNITIVE RADIOS IN THE PRESENCE OF AN EAVESDROPPER

Sina Maleki, Ashkan Kalantari, Symeon Chatzinotas and Björn Ottersten

Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg
e-mail:{sina.maleki,ashkan.kalantari,symeon.chatzinotas,bjorn.ottersten}@uni.lu

ABSTRACT

Reliable and agile spectrum sensing as well as secure communication are key requirements of a cognitive radio system. In this paper, secrecy throughput of a cognitive radio is maximized in order to determine the sensing threshold, the sensing time, and the transmission power. Constraints of the problem are defined as a lower-bound on the detection probability, an upper-bound on the average energy consumption per time-frame, and the maximum transmission power of the cognitive radio. We show that the problem can be solved by an on-off strategy where the cognitive radio only performs sensing and transmits data if the cognitive channel gain is greater than the average eavesdropper channel gain. The problem is then solved by a line-search over sensing time. Eventually, the secrecy throughput of the cognitive radio is evaluated employing the IEEE 802.15.4/ZigBee standard.

Index Terms— Secrecy capacity, secrecy throughput, power allocation, resource allocation, cognitive radio

1. INTRODUCTION

Cognitive radios are proposed as a solution to the spectrum scarcity problem [1]. Interweave cognitive radio is a category of cognitive radio systems where each cognitive radio listens to the wireless spectrum in periodic sensing slots, and the cognitive radio gains spectrum access if the primary user is deemed to be inactive [2]. Therefore, increasing the throughput of the cognitive radio, while protecting the primary user from harmful interference of the cognitive user is a critical issue. Similar to any other wireless communication system, cognitive radios are also vulnerable to inadequate security due to the presence of an eavesdropper. Therefore, it is also important to make sure that confidential messages of a cognitive transmitter are secure.

Optimization of the cognitive radio throughput subject to the constraint on the amount of interference to the primary user is considered thoroughly in the literature, e.g. [3], [4]. Joint optimization of the cognitive transmission power and spectrum sensing while maximizing the throughput is another problem which is considered in [5, 6, 7] for example. However, there are only few works which consider resource allocation in the presence of an eavesdropper. The authors in [8] consider a scenario where one or more eavesdroppers listen to an underlay multiple-input multiple-output (MIMO) cognitive radio system. Underlay cognitive radios are another type of cognitive systems where the cognitive transmitter gains access to the spectrum concurrently with the primary use, while keeping the interference below a specific threshold [2]. A MISO underlay cognitive scenario is considered in [9]. The authors show that while concurrent secondary transmission with the primary user may reduce the primary channel capacity, it can potentially improve the secrecy rate of the primary user. Recently, Zhang et al. [10] studied an overlay cognitive scenario where the primary user gains a higher security rate by leveraging cooperation with cognitive users. Overlay cognitive radios are another category of cognitive systems where cognitive users are aware of the primary channel and codebook messages [2]. None of these works consider optimization of the secrecy capacity for interweave cognitive radios. Further, the constraint on the energy consumption, which is a critical issue in a cognitive sensor network [3], has not been investigated in the context of physical layer security for cognitive radios.

In this paper, secrecy throughput of an interweave cognitive radio system is maximized subject to a constraint on the probability of detection, maximum transmission power, and maximum energy consumption per time-frame, in order to obtain the sensing threshold, the sensing time, and the transmission power. The constraint on the probability of detection protects the primary receiver from harmful interference of the cognitive transmitter, while the other constraints are inherent limitations of a low-power sensor network. Further, we assume that the cognitive radio is only aware of the average channel gain to the eavesdropper and thus instead of the instantaneous secrecy capacity, the average secrecy capacity is considered for optimization. Given the sensing threshold and the sensing time, the average secrecy capacity optimization problem is shown to be non-concave in the transmission power P_c, and thus instead, a lower-bound on the average secrecy capacity is maximized. This way, we show that the power allocation problem reduces to an on-off strategy, where the cognitive radio performs sensing and eventually accesses the spectrum upon the absence of the primary transmitter, only if the cognitive channel gain is better than the average eavesdropper channel gain. It is shown that the problem can be solved by a line-search over the sensing time, when this condition is satisfied.

The remainder of the paper is organized as follows. We present the system model and problem formulation in Section 2. In this section, we further analyze the problem and provide a sub-optimal solution. The secrecy throughput of the cognitive radio system in the presence of an eavesdropper is evaluated in Section 3, and finally we draw our conclusions in Section 4.

2. ANALYSIS AND PROBLEM FORMULATION

We consider a cognitive radio system which consists of a cognitive transmitter and receiver pair as shown in Fig. 1. The cognitive transmitter senses the spectrum in periodic sensing slots by receiving N observation samples denoted by r_i. Denoting w_i, s_i and h_p to be the noise, the signal and the channel gain between the primary user

This work is partially supported by the National Research Fund, Luxembourg under the project CO2SAT : Cooperative & Cognitive Architectures for Satellite Networks, and AFR grant (Reference 5798109) for the project Physical Layer Security in Satellite Communications.

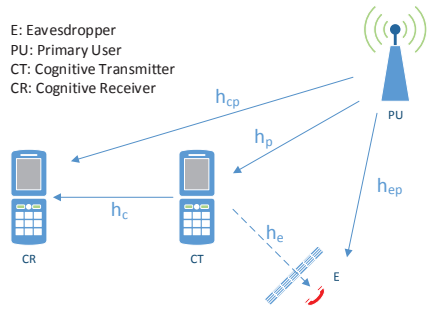

Fig. 1. Graphical representation of the system model

and the cognitive transmitter, in order to detect the presence (or absence) of the primary user, the cognitive transmitter solves a binary hypothesis testing problem as follows

$$\begin{aligned}\mathcal{H}_0 &: r_i = w_i, i = 1, \ldots, N, \\ \mathcal{H}_1 &: r_i = h_p s_i + w_i, i = 1, \ldots, N,\end{aligned} \tag{1}$$

where $\mathcal{H}_0$ and $\mathcal{H}_1$ denote the respective absence and the presence of the primary user, w_i is the Additive White Gaussian Noise (AWGN) with zero mean and variance σ_w^2, s_i is the primary user signal which follows an i.i.d. random Gaussian distribution with zero mean and variance σ_s^2, and the channel gain h_p is assumed to be constant during each sensing period. The average received SNR of the primary user signal at the cognitive transmitter is thus $\gamma = \frac{|h_p|^2\sigma_s^2}{\sigma_w^2}$, where γ denotes the SNR. An energy detector is employed by the cognitive transmitter in order to solve (1). The energy detector calculates accumulated energy of N samples and compares the result with a threshold denoted by λ, as follows

$$\mathcal{E} = \frac{1}{\sigma_w^2}\sum_{i=1}^{N}|r_i|^2 \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \lambda, \tag{2}$$

where $|\cdot|$ denotes the absolute value. Based on the model parameters described under (1), $\mathcal{E}$ follows a chi-square distribution with $2N$ degrees of freedom under $\mathcal{H}_0$ and $\mathcal{H}_1$ [11]. This way, the probabilities of false alarm and detection are obtained by

$$P_f = Pr(\mathcal{E} \geq \lambda|\mathcal{H}_0) = \frac{\Gamma(N, \frac{\lambda}{2\sigma_w^2})}{\Gamma(N)}, \tag{3}$$

$$P_d = Pr(\mathcal{E} \geq \lambda|\mathcal{H}_1) = \frac{\Gamma(N, \frac{\lambda}{2(1+\gamma)})}{\Gamma(N)}, \tag{4}$$

where $\Gamma(a)$ is the gamma function and $\Gamma(a,x)$ is the upper-incomplete gamma function.

The cognitive transmitter gains access to the sensing band, if the primary user is deemed to be inactive. A hidden eavesdropper is listening to the cognitive radio data transmission with a non-line-of-sight (NLOS) Rayleigh fading channel denoted by h_e as depicted in Fig. 1. Denoting P_c to be the transmission power of the cognitive transmitter, and h_c to be the channel gain between the pair of cognitive transmitter and receiver, the secrecy capacity of the cognitive radio is obtained as follows

$$\mathcal{C}_{s,\mathcal{H}_0} = \mathbb{E}_{|h_e|^2}\left[\log_2\left(1+\frac{|h_c|^2P_c}{\sigma_w^2}\right) - \log_2\left(1+\frac{|h_e|^2P_c}{\sigma_w^2}\right)\right], \tag{5}$$

$$\begin{aligned}\mathcal{C}_{s,\mathcal{H}_1} =& \mathbb{E}_{|h_e|^2}\left[\log_2\left(1+\frac{|h_c|^2P_c}{\sigma_w^2+|h_{cp}|^2P}\right)\right. \\ &\left. - \log_2\left(1+\frac{|h_e|^2P_c}{\sigma_w^2+|h_{ep}|^2P}\right)\right],\end{aligned} \tag{6}$$

where $\mathcal{C}_{s,\mathcal{H}_0}$ and $\mathcal{C}_{s,\mathcal{H}_1}$ represent the secrecy capacity when the primary user is deemed to be inactive and active, i.e., when absence of the primary user is correctly detected or detection of the primary user presence is missed, respectively. Further, P is the transmission power of the primary user, h_{ep} the channel between the primary user and the eavesdropper, h_{cp} the channel between the primary user and the cognitive receiver, and $\mathbb{E}[\cdot]$ denotes the expected value. Note that here we assume that the instantaneous h_c is known but the instantaneous h_e is not known, and we only know the $\mathbb{E}_{|h_e|^2}[|h_e|^2]$.

Periodic time-frames of T units are assigned to the cognitive radio, where the cognitive radio performs spectrum sensing in the beginning of each time-frame. The cognitive transmitter starts sending data to the cognitive receiver, if the outcome of sensing leads to the absence of the primary user. Denoting T_s to be the sensing time and f_s to be the sampling frequency, $T_s = \frac{N}{f_s}$. This way, the cognitive transmitter can access to the spectrum during the remaining $T - T_s$ units. The cognitive radio secrecy throughput in each time-frame, denoted by $\mathcal{R}_s$ is thus defined as follows

$$\begin{aligned}\mathcal{R}_s =& \pi_0(1-P_f)Pr(success|\mathcal{H}_0)\frac{T-T_s}{T}\mathcal{C}_{s,\mathcal{H}_0} \\ &+ \pi_1(1-P_d)Pr(success|\mathcal{H}_1)\frac{T-T_s}{T}\mathcal{C}_{s,\mathcal{H}_1},\end{aligned} \tag{7}$$

where π_0 and π_1 are a priori probabilities of the primary user absence and presence, and $Pr(success|\mathcal{H}_0)$ and $Pr(success|\mathcal{H}_1)$ are the probabilities of successful transmission under $\mathcal{H}_0$ and $\mathcal{H}_1$. In [3], it is discussed that since the received data at the cognitive receiver is free of the interference under $\mathcal{H}_0$, $Pr(success|\mathcal{H}_0) \to 1$. On the other hand, since the received signal at the cognitive receiver is interfered with the primary user signal under $\mathcal{H}_1$, $Pr(success|\mathcal{H}_1) \to 0$. Therefore, (7) approximately becomes

$$\mathcal{R}_s \approx \pi_0(1-P_f)\frac{T-T_s}{T}\mathcal{C}_{s,\mathcal{H}_0}. \tag{8}$$

As mentioned earlier, a cognitive radio gains spectrum access by avoiding harmful interference to the primary user. Therefore, a constraint on the probability of detection is considered in this paper and current standards, such as IEEE 802.22 [12], which protects the primary user from harmful interference of the cognitive transmitter. This constraint is defined as a lower-bound on the probability of detection, denoted by α.

Moreover, cognitive radios are often low-power sensors with limited battery capacity. To incorporate this limitation in our problem formulation, we let the the average energy consumption per time-frame to be less than a specific threshold denoted by $E_{\max}$. Each cognitive radio consumes energy in two folds: a) some energy is spent on sensing, and b) if the primary user is deemed to be inactive, some energy is also consumed on data transmission. This way, denoting P_s and P_c to be the sensing and transmission power, the average energy consumption of the cognitive radio per time-frame becomes $P_sT_s + \big[\pi_0(1-P_f) + \pi_1(1-P_d)\big]P_c(T-T_s)$. Note that here we assume the idle energy due to the non data transmission is negligible, and the cognitive radio always has data available for transmission. No data transmission occurs when the primary user is correctly detected or a false alarm occurs. However, as shall be

shown later, due to inadequate security, in some cases the cognitive radio should not transmit any data even if the primary user is deemed to be absent. In such scenarios, performing spectrum sensing becomes irrelevant and thus some energy can be saved for future communications. We should also note that each radio in general has a peak power constraint which needs to be taken into account. Here, the maximum transmission power is denoted by $P_{c,\max}$.

Our goal is to assign the sensing threshold, the sensing time, and cognitive transmission power so as to maximize the cognitive radio secrecy throughput subject to the probability of detection constraint and the maximum energy consumption per time-frame, as follows

$$\begin{aligned}&\max_{\lambda,T_s,P_c}\ \pi_0(1-P_f)\frac{T-T_s}{T}\mathcal{C}_{s,\mathcal{H}_0}\\&\text{s.t. } P_d\geq\alpha,\\&\quad P_sT_s+\big[\pi_0(1-P_f)+\pi_1(1-P_d)\big]P_c(T-T_s)\leq E_{\max},\\&\quad P_c\leq P_{c,\max},\\&\quad 0<T_s\leq T.\end{aligned}\tag{9}$$

Note that here the available channel side information includes the cognitive channel gain, h_c and the average eavesdropper channel gain denoted by ζ_e. For a given λ and T_s in the feasible set of (9), we can rewrite (9) as follows

$$\begin{aligned}&\max_{P_c}\ \mathbb{E}_{|h_e|^2}\left[\log_2\left(1+\frac{|h_c|^2P_c}{\sigma_w^2}\right)-\log_2\left(1+\frac{|h_e|^2P_c}{\sigma_w^2}\right)\right]\\&\text{s.t } P_c\leq\min\left\{P_{c,\max},\frac{E_{\max}-P_sT_s}{\big[\pi_0(1-P_f)+\pi_1(1-P_d)\big](T-T_s)}\right\}.\end{aligned}\tag{10}$$

The problem (10) in the current shape is not concave in P_c. However, since a log function is concave, using Jensen's inequality, we can write

$$\begin{aligned}&\mathbb{E}_{|h_e|^2}\left[\log_2\left(1+\frac{|h_c|^2P_c}{\sigma_w^2}\right)-\log_2\left(1+\frac{|h_e|^2P_c}{\sigma_w^2}\right)\right]\\&=\log_2\left(1+\frac{|h_c|^2P_c}{\sigma_w^2}\right)-\mathbb{E}_{|h_e|^2}\left[\log_2\left(1+\frac{|h_e|^2P_c}{\sigma_w^2}\right)\right]\\&\geq\log_2\left(1+\frac{|h_c|^2P_c}{\sigma_w^2}\right)-\log_2\mathbb{E}_{|h_e|^2}\left[\left(1+\frac{|h_e|^2P_c}{\sigma_w^2}\right)\right]\\&=\log_2\left(1+\frac{|h_c|^2P_c}{\sigma_w^2}\right)-\log_2\left(1+\frac{\mathbb{E}_{|h_e|^2}\big[|h_e|^2\big]P_c}{\sigma_w^2}\right).\end{aligned}\tag{11}$$

Therefore, instead of solving (10), we solve the following problem which is the lower-bound of (10),

$$\begin{aligned}&\max_{P_c}\ \log_2\big(1+aP_c\big)-\log_2\big(1+bP_c\big)\\&\text{s.t } P_c\leq\min\left\{P_{c,\max},\frac{E_{\max}-P_sT_s}{\big[\pi_0(1-P_f)+\pi_1(1-P_d)\big](T-T_s)}\right\},\end{aligned}\tag{12}$$

where $a=|h_c|^2/\sigma^w$, and $b=\zeta_e/\sigma_w^2$ where $\zeta_e=\mathbb{E}\Big[|h_e|^2\Big]$. We know that $\log_2\big(1+aP_c\big)-\log_2\big(1+bP_c\big)=\log_2\left(\frac{1+aP_c}{1+bP_c}\right)$. Again since log is a concave function, the optimal solution of (12) is the one which maximizes $\left(\frac{1+aP_c}{1+bP_c}\right)$. We note that if $a\leq b$, $\log_2\left(\frac{1+aP_c}{1+bP_c}\right)\leq 0$ and thus the optimal solution of (12) becomes $P_c^*=0$. Therefore, in case $|h_c|\leq\sqrt{\zeta_e}$, the cognitive radio should not transmit, even if the primary user is perceived to be absent. Consequently, performing spectrum sensing when $|h_c|\leq\sqrt{\zeta_e}$ becomes irrelevant. This way, the cognitive radio may lose some transmission opportunities, but the lifetime of the cognitive radio increases, and data transmission security is also assured. Further, in case we are dealing with a real-time system, the quality of the cognitive channel can be improved with respect to the eavesdropper channel by adding artificial noise to the eavesdropper through the cooperation of friendly jammers [13, 14, 15].

Considering the fact that if $a>b$, $\left(\frac{1+aP_c}{1+bP_c}\right)$ is a monotonic increasing function in P_c, the optimal solution of (12) becomes the maximum P_c in the feasible set of the problem which is $P_c^*=\min\left\{P_{c,\max},\frac{E_{\max}-P_sT_s}{\big[\pi_0(1-P_f)+\pi_1(1-P_d)\big](T-T_s)}\right\}$ when $|h_c|>\sqrt{\zeta_e}$.

So far, we have considered solving (9) for a given λ and T_s. Now, we solve the problem for a given P_c. This way, (9) becomes as follows

$$\begin{aligned}&\max_{\lambda,T_s}\ \pi_0(1-P_f)\frac{T-T_s}{T}\\&\text{s.t. } P_d\geq\alpha,\\&\quad P_sT_s+\big[\pi_0(1-P_f)+\pi_1(1-P_d)\big]P_c(T-T_s)\leq E_{\max},\\&\quad 0<T_s<T.\end{aligned}\tag{13}$$

For a given T_s, the optimal solution to (13) is obtained by the minimum P_f in the feasible set of the problem. Since P_d is a monotonic increasing function of P_f [16], the minimum P_d in the feasible set of the problem, is the optimal solution. Note that P_d is a one-to-one function of λ, and thus finding the optimal P_d is equivalent to finding λ. The minimum P_d is obtained by $P_d^*=\max\Big\{\alpha,P_d(E_{\max})\Big\}$, where $P_d(E_{\max})$ is the minimum P_d for which the second constraint in (13) is satisfied with equality.

Inserting P_d^* in (13) and P_c^* when $|h_c|>\sqrt{\zeta_e}$, (9) can be solved by the following algorithm,

$$\begin{aligned}&|h_c|\leq\sqrt{\zeta_e}:\mathcal{R}_s^*=\ 0,\\&|h_c|>\sqrt{\zeta_e}:\mathcal{R}_s^*=\ \underset{T_s}{\text{argmax}}\ \pi_0\Big(1-P_f(P_d^*)\Big)\mathcal{C}_{s,\mathcal{H}_0}(P_c^*(P_d^*))\\&\qquad\qquad\text{s.t. } 0<T_s\leq T,\end{aligned}\tag{14}$$

where $\mathcal{R}_s^*$ denotes the maximum secrecy throughput. Note that, in this paper, a Rayleigh fading model is considered for the eavesdropper channel. However, the algorithm in (14) is independent from the type of the channel and can be applied to any model as far as the average eavesdropper channel gain is known.

3. NUMERICAL RESULTS

In this section, we evaluate the secrecy throughput of the cognitive radio in different scenarios. A Chipcon 2420 transceiver based on IEEE 802.15.4/ZigBee is employed to model the cognitive radio. Based on this model, the sensing power is approximately $P_s\simeq 40$ mW and the maximum transmission power is $P_{c,\max}\simeq 20$ mW [3]. For both the cognitive and eavesdropper channel, a Rayleigh fading channel model is considered. Further, we assume $T=100$ ms, $\sigma_w^2=1$, and the received SNR from the primary user $\gamma=0$ dB.

Fig. 2 depicts the average maximum secrecy throughput versus average cognitive channel gain denoted by ζ_c, for different values of π_0. In this figure, we assume $E_{\max}=6000$ μJ, $\zeta_e=1$,

$\pi_0 = 0.2, 0.5, 0.8$, and we let ζ_c to change from 1 to 10. It is shown that by increasing the ratio ζ_c/ζ_e, the secrecy throughput improves. This verifies that improving the quality of the cognitive channel with respect to the eavesdropper channel can potentially enhance the secrecy throughput of the cognitive radio. Further, the secrecy outage probability defined by $Pr(|h_c| \leq \zeta_e)$ can be reduced with increasing ζ_c/ζ_e. We can also see that as the probability of primary user absence increases, the secrecy throughput of the cognitive radio also increases. This is due to the higher chance of transmission when the primary user is absent.

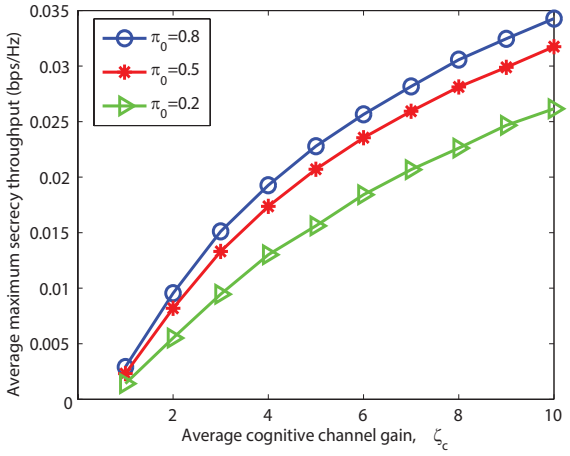

Fig. 2. Average maximum secrecy throughput versus average cognitive channel gain for different values of π_0, and for $\zeta_e = 1$, $P_s = 40$ mW, $P_{c,\max} = 20$ mW, $\gamma = 0$ dB, and $E_{\max} = 6000$ μJ.

The average maximum secrecy throughput versus ζ_c is shown in Fig. 3 for different values of E_{max}. In this figure, we assume $\zeta_e = 1$, $\pi_0 = 0.5$, $E_{\max} = 60, 600, 6000$ μJ, and again we let ζ_c to change from 1 to 10. As is depicted, the most important result of this figure is that as the energy constraint of the cognitive radio becomes stricter, we may reach a point where even by improving the ratio ζ_c/ζ_e, the secrecy throughput of the cognitive radio can not be improved significantly. In such a situation, small channel estimation errors may lead to a non-secure cognitive transmission. The only feasible solution in such scenarios is to increase the available energy of the system, for example by incorporating some energy harvesting techniques.

To evaluate the tightness of the bound in (11), in Fig. 4, the sub-optimal secrecy capacity obtained by the Jensen's inequality is compared with the optimal one obtained by exhaustive search, with respect to the cognitive channel gain. Without loss of generality, we assume $E_{\max} \to \infty$, and thus the power constraint in (12) reduces to $P_c \leq P_{c,\max}$. Further, $\zeta_e = 1$, and we let ζ_c to change from 1 to 10. Note that here we are only interested in the tightness of the bound, and thus we only consider the secrecy capacity and not the effect of λ and T_s. As we can see the sub-optimal solution is very close to the optimal one. This shows that the bound used in this paper is very tight at least for low values of the power.

4. CONCLUSION

We considered power allocation in a cognitive radio system in the presence of an eavesdropper. The underlying problem was defined

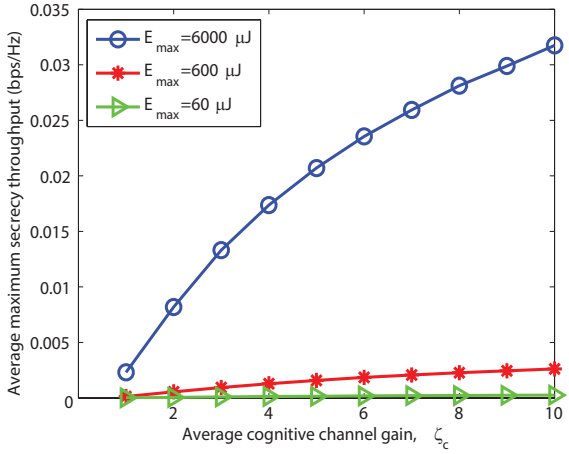

Fig. 3. Average maximum secrecy throughput versus average cognitive channel gain for different values of $E_{\max}$, and for $\zeta_e = 1$, $P_s = 40$ mW, $P_{c,\max} = 20$ mW, $\gamma = 0$ dB, and π_0=0.5.

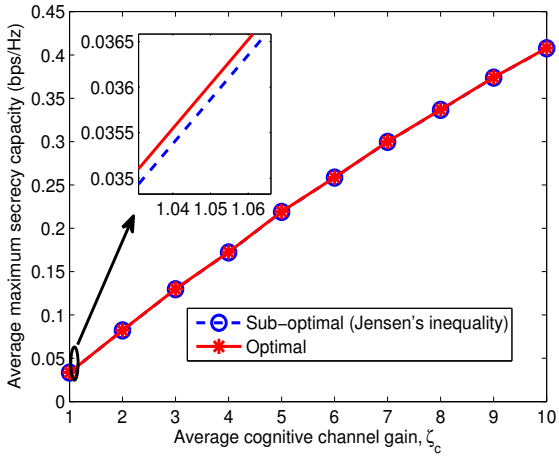

Fig. 4. Average maximum secrecy capacity versus average cognitive channel gain for $\zeta_e = 1$, $E_{\max} \to \infty$, and $P_{c,\max} = 20$ mW.

so as to maximize the secrecy throughput in order to determine the sensing threshold, and to allocate resources including the sensing time and the transmission power. To solve the problem efficiently, a lower-bound on the secrecy capacity was optimized and consequently, it was shown that the sub-optimal strategy is to neither sense, nor transmit when the cognitive channel gain is less than the average eavesdropper channel gain. The secrecy throughput of the cognitive radio was evaluated by employing the IEEE 802.15.4/ZigBee standard. It was shown that although improving the quality of the cognitive channel with respect to the eavesdropper channel can potentially improve the secrecy throughput, but as the maximum available energy per time-frame reduces, we may reach a point that the secrecy throughput of the system can not be improved, even with improving the cognitive channel gain. Further, it was shown that the solution obtained by the lower-bound on the secrecy capacity is very close to the optimal one obtained from exhaustive search.

5. REFERENCES

[1] D. Cabric, I. D. O'Donnell, M. S. W. Chen, and R. W. Brodersen, "Spectrum sharing radios," *IEEE Circuits and Systems Magazine*, vol.6, no.2, pp.30,45, 2006.

[2] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking Spectrum Gridlock With Cognitive Radios: An Information Theoretic Perspective," *Proceedings of the IEEE*, vol.97, no.5, pp.894,914, May 2009.

[3] S. Maleki, S. P. Chepuri, and G. Leus, "Optimization of hard fusion based spectrum sensing for energy-constrained cognitive radio networks", *Physical Communication*, vol.9, pp.193-198, December 2013.

[4] Y-C. Liang, Y. Zeng, E. C. Y. Peh, and A. T. Hoang, "Sensing-Throughput Tradeoff for Cognitive Radio Networks," *IEEE Transactions on Wireless Communications*, vol.7, no.4, pp.1326,1337, April 2008.

[5] Y. Pei, Y-C. Liang, K. C. Teh, and K. H. Li, "How much time is needed for wideband spectrum sensing?," *IEEE Transactions on Wireless Communications*, vol.8, no.11, pp.5466,5471, November 2009.

[6] S. Stotas, and A. Nallanathan, "Optimal Sensing Time and Power Allocation in Multiband Cognitive Radio Networks," *IEEE Transactions on Communications*, vol.59, no.1, pp.226,235, January 2011.

[7] G. Scutari, J-S. Pang, "Joint Sensing and Power Allocation in Nonconvex Cognitive Radio Games: Nash Equilibria and Distributed Algorithms," *IEEE Transactions on Information Theory*, vol.59, no.7, pp.4626,4661, July 2013.

[8] L. Zhang, R. Zhang, Y-C. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," *IEEE Transactions on Communications*, vol.58, no.6, pp.1877,1886, June 2010.

[9] T. Kwon, V. M. S. Wong, and R. Schober, "Secure MISO cognitive radio system with perfect and imperfect CSI," *2012 IEEE Global Communications Conference (GLOBECOM)*, pp.1236,1241, 3-7 Dec. 2012.

[10] N. Zhang, N. Lu, N. Cheng, J. W. Mark, and X. S. Shen, "Cooperative Spectrum Access Towards Secure Information Transfer for CRNs," *IEEE Journal on Selected Areas in Communications*, vol.31, no.11, pp.2453,2464, November 2013.

[11] S. Kay, "Fundamentals of Statistical Signal Processing, Volume II:Detection Theory", Prentice-Hall 1998.

[12] Functional requirements for the 802.22 WRAN standard. IEEE 802.22-05/0007r46, September 2006.

[13] X. Zhou, and M. R. McKay, "Secure Transmission With Artificial Noise Over Fading Channels: Achievable Rate and Optimal Power Allocation," *IEEE Transactions on Vehicular Technology*, vol.59, no.8, pp.3831,3842, Oct. 2010.

[14] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving Physical Layer Secrecy Using Full-Duplex Jamming Receivers," *IEEE Transactions on Signal Processing*, vol.61, no.20, pp.4962,4974, Oct.15, 2013.

[15] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. Bloch, S. Ulukus, and A. Yener, "Cooperative Security at the Physical Layer: A Summary of Recent Advances," *IEEE Signal Processing Magazine*, vol.30, no.5, pp.16,28, Sept. 2013.

[16] P. Varshney, "Distributed detection and data fusion", Springer 1997.