Physical Communication 22 (2017) 32–41

Contents lists available at ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom

Full length article

Cognitive radio network with secrecy and interference constraints

Hung Tran [a,*], Georges Kaddoum [b], François Gagnon [b], Louis Sibomana [c]

[a] School of Innovation, Design and Engineering, Malardalen University, Sweden
[b] University of Québec, ETS Engineering School, LACIME Laboratory, Montreal, Canada
[c] School of Computing, Blekinge Institute of Technology, Karlskrona, Sweden

ARTICLE INFO

Article history:
Received 28 April 2016
Received in revised form
4 October 2016
Accepted 6 December 2016
Available online 14 December 2016

Keywords:
Cognitive radio networks
Physical layer security
Power allocation
Security constraint

ABSTRACT

In this paper, we investigate the physical-layer security of a secure communication in single-input multiple-output (SIMO) cognitive radio networks (CRNs) in the presence of two eavesdroppers. In particular, both primary user (PU) and secondary user (SU) share the same spectrum, but they face with different eavesdroppers who are equipped with multiple antennas. In order to protect the PU communication from the interference of the SU and the risks of eavesdropping, the SU must have a reasonable adaptive transmission power which is set on the basis of channel state information, interference and security constraints of the PU. Accordingly, an upper bound and lower bound for the SU transmission power are derived. Furthermore, a power allocation policy, which is calculated on the convex combination of the upper and lower bound of the SU transmission power, is proposed. On this basis, we investigate the impact of the PU transmission power and channel mean gains on the security and system performance of the SU. Closed-form expressions for the outage probability, probability of non-zero secrecy capacity, and secrecy outage probability are obtained. Interestingly, our results show that the strong channel mean gain of the PU transmitter to the PU's eavesdropper in the primary network can enhance the SU performance.

1. Introduction

Cognitive radio networks (CRNs) have been widely considered as an effective approach to solve the problems of low spectrum utilization for next generation of wireless networks [1]. The key idea behind the CRNs is to let the unlicensed users, known as secondary users (SUs), and licensed users, named as primary users (PUs), share the same frequency band provided that the SUs transmission do not cause harmful interference to the PUs. Based on this concept, two main spectrum access approaches, namely as interweave and underlay, have been proposed [2,3]. In the interweave approach, the SUs need to find the spectrum holes for their own communication. This approach highly depends on the spectrum detection technique, thus any missed detection of the SUs may cause severe interference to the PUs. In addition, in the dense areas, almost spectrum is often occupied by the PUs, and hence this approach is not efficient due to the lack of spectrum holes. On the other hand, in the underlay approach, the SUs can concurrently access the licensed spectrum of the PUs as long as the interference from the SUs to the PUs is maintained below a given threshold. This approach has been obtained a great attention as the SUs can operate in the dense areas where the number of spectrum holes are limited [4–10]. Further, the SU can utilize the interference of the PU as an active jamming signal to enhance its security.

There is a fact that the wireless networks face many new security challenges from all aspects of the networking architecture, including the spectrum sensing, spectrum access, and spectrum management due to the natural broadcast property of wireless signals. This becomes more severe in the spectrum underlay approach where the SUs and PUs coexist in the same frequency band, and they may cause mutual interference to each other. To protect the communications confidentiality against the eavesdroppers, the physical layer security has emerged as a promising solution [11–17]. Further, to quantify the security of a wireless system, the secrecy capacity metric was formulated as the maximum achievable rate from the transmitter to the legitimate receiver minus the one listening by the eavesdropper over the illegitimate channel. Following this approach, Wayner showed that if the main channel is better than the illegitimate channel, the transmitter can exchange the secure messages with the intended receiver at a non-zero secrecy rate [11]. As an extension of [11], the works in

* Corresponding author.
E-mail addresses: tran.hung@mdh.se (H. Tran), georges.kaddoum@etsmtl.ca (G. Kaddoum), francois.gagnon@etsmtl.ca (F. Gagnon), lsm@bth.se (L. Sibomana).

http://dx.doi.org/10.1016/j.phycom.2016.12.001
1874-4907/

[18–23] have studied the physical layer security for various fading models. Face to the same security concerns in the conventional wireless systems, the security policies to against the eavesdroppers become more difficult in the CRN where both SUs and PUs are vulnerable and easy to be eavesdropped due to the mutual interference. However, in some cases, the secondary transmitter (S-Tx) can take the advantages of fading channel to become an active jammer who can severely degrade the eavesdropper (EAV) capacity in the illegitimate channel, i.e., the PUs secure information may be protected from the EAV by the interference caused by the SUs to the EAV. In the light of this idea, the security concern of the PUs in the CRN has been interpreted into constraints to the SUs, i.e., the SUs are allowed to utilize the licensed spectrum of the PUs as long as the secure criteria and quality of service (QoS) of the PUs are satisfied [24–33]. Particularly, in [25,29], authors have applied game theory cooperation strategies to study the security for a simple CRN scenario where a pair of the SU and a pair of the PU share the same spectrum in the presence of a single EAV. Power allocation and bandwidth assignment strategies have been proposed to enhance the security of the PUs communication.

Regarding the effectiveness of multiple antennas on the security of the CRN, the security problems in the multiple-input single-out (MISO) CRNs have been considered in [24,26,28]. Authors in [28] have investigated the case where the S-Tx uses the beamforming technique to maximize the PU's secrecy capacity under the SU's QoS constraints. In [26] and [24], the SU also uses the beamforming technique to maximize the secrecy rate of the SU while keeping the interference at the PU below a predefined threshold. In [30], the physical layer security with multiple user scheduling for CRNs in terms of ergodic secrecy capacity and probability of non-zero secrecy capacity has been examined. More recently, *Wang* et al. have proposed two secure transmission schemes, named as nonadaptive and adaptive secure transmission strategies, to maximize the throughput for MISO CRN over slow fading channel [32]. An approximation for the optimal rate parameters of the nonadaptive secure transmission strategy has been obtained at the high signal-to-noise ratio (SNR) regime. However, a power allocation policy for the SU as well as performance analysis of the SU under both the statistical outage and security constraints of the PU has not been studied.

Motivated by all above works, in this paper, we study the performance of a single-input multiple-output (SIMO) CRN under joint constraint of the interference and security of the PU. More specifically, we consider that the two eavesdroppers, named as EAV_1 and EAV_2, equipped with multiple antennas try to overhear the information from the PU and SU in the same spectrum. To guarantee the desired security and performance of the PU, the S-Tx must control its transmission power to meet the peak transmission power of the SU, and both the outage probability constraint and probability of secrecy constraint of the PU. Given these settings, the analysis for the considered secondary network is investigated in two folds, namely system performance and security performance. Main contributions in this paper are summarized as follows:

- An upper bound and lower bound for the transmission power of the S-Tx are derived. Then, a power allocation policy under the convex combination of the upper and the lower transmission power for the S-Tx is proposed.
- To analyze the performance of the SU, a closed-form expression for the outage probability is derived.
- To evaluate the security of the SU, closed-form expressions for the probability of non-zero secrecy capacity and outage secrecy capacity are derived.
- More interestingly, the results show that a strong channel mean gain of the primary transmitter (P-Tx)→EAV_1 wiretap link can enhance the performance of the SU by using our proposed power allocation policy.

The remainder of this paper is presented as follows. In Section 2, the system model, assumptions, and problem statement for the SIMO CRN are introduced. In Section 3, the upper bound, lower bound of the S-Tx transmission power, and the power allocation policy for the S-Tx are obtained. Further, closed-form expressions for the outage probability, probability of non-zero secrecy capacity, and outage secrecy capacity are derived. In Section 4, the numerical results and discussions are provided. Finally, conclusions are given in Section 5.

Symbols	Meaning
$N_s, N_p, N_{e_1}, N_{e_2}$	Number of antennas at the secondary receiver (S-Rx), primary receiver (P-Rx), EAV_1, EAV_2
$h = (h_1, h_2, \ldots, h_{N_p})$	Channel gain of the P-Tx→P-Rx communication link
$g = (g_1, g_2, \ldots, g_{N_s})$	Channel gain of the S-Tx→S-Rx communication link
$f = (f_1, f_2, \ldots, f_{N_{e_1}})$	Channel gain of the P-Tx→EAV_1 illegitimate link
$k = (k_1, k_2, \ldots, k_{N_{e_2}})$	Channel gain of the S-Tx→EAV_2 illegitimate link
$\beta = (\beta_1, \beta_2, \ldots, \beta_{N_s})$	Channel gain of the P-Tx→S-Rx interference link
$\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{N_{e_1}})$	Channel gain of the S-Tx→EAV_1 interference link
$\rho = (\rho_1, \rho_2, \ldots, \rho_{N_{e_2}})$	Channel gain of the P-Tx→EAV_2 interference link
$\varphi = (\varphi_1, \varphi_2, \ldots, \varphi_{N_p})$	Channel gain of the S-Tx→P-Rx interference link
R_p, R_s	Target rates of the P-Tx and S-Tx
R_δ	Secrecy target rate of the P-Tx under the eavesdropping of EAV_1
$\gamma_{SU}, \gamma_{PU}, \gamma_{e_1}, \gamma_{e_2}$	Signal-to-interference-plus-noise ratios (SINRs) of the S-Rx, P-Rx, EAV_1, and EAV_2
θ, ϵ	Outage probability threshold and outage secrecy threshold of the PU
N_0	Noise power (a product of noise power spectral density ($\mathcal{N}_0$) and system bandwidth (B), i.e., $N_0 = B\mathcal{N}_0$)
$P_{S\text{-}Tx}, P_{P\text{-}Tx}$	Transmission power of the S-Tx, P-Tx
P_u, P_l	Upper bound and lower bound of the transmission power of the S-Tx
$P_{S\text{-}Tx}^{\max}$	Peak transmission power of the S-Tx
$\gamma_{P\text{-}Tx} = \frac{P_{P\text{-}Tx}}{N_0}$	Transmission SNR of the P-Tx
$\gamma_{S\text{-}Tx} = \frac{P_{S\text{-}Tx}}{N_0}$	Transmission SNR of the S-Tx
$\gamma_u = \frac{P_u}{N_0}$	Upper bound of the transmission SNR of the S-Tx
$\gamma_l = \frac{P_l}{N_0}$	Lower bound of the transmission SNR of the S-Tx

2. System model

In this section, we introduce the system model, channel assumptions, and spectrum sharing constraints.