Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
June 2016, 23(3): 51–56
www.sciencedirect.com/science/journal/10058885
The Journal of China Universities of Posts and Telecommunications
http://jcupt.bupt.edu.cn

Secrecy outage analysis on underlay cognitive radio using selection combining

Tan Youyu, Pan Gaofeng (✉), Zhao Hui

School of Electronic and Information Engineering, Southwest University, Chongqing 400715, China.

Abstract

Secure data transmission in future high-capacity high-coverage multi-tier hierarchical networks, for which cognitive radio (CR) has emerged as an essential recipe, is of utmost importance. This paper investigates the secrecy outage performance of selection combining (SC) in CR networks (CRNs) over Rayleigh fading channels. In a single-input multiple-output (SIMO) wiretap channel, a secondary user transmits confidential messages to another secondary user, which is equipped with $n_B\,(n_B \geqslant 1)$ antennas. Meanwhile, a passive eavesdropper, which is equipped with $n_E\,(n_E \geqslant 1)$ antennas, intends to overhear the messages. Both the legal receiver and the eavesdropper adopt SC scheme to process the received multiple signals. The secondary transmitter uses the underlay strategy to guarantee the quality of service of the primary user without spectrum sensing. Compared to the work proposed by Maged Elkashlan et al. in Ref. [1], we present an alternative method to derive the closed-form expression for the secrecy outage probability (SOP) and develop a simplified SOP when the maximal transmit power at the secondary user is sufficiently high. Our results reveal the impact of the primary network on the secondary network with a multi-antenna wiretap channel and simulations are conducted to validate the accuracy of our proposed analytical models.

Keywords secrecy outage probability, cognitive radio, selection combining, underlay

1 Introduction

Due to the broadcast nature of wireless links, security concerns have drawn considerable attention and have taken on an increasingly important role in spectrum sharing networks. Physical layer security has been widely considered as an effective technology to protect the confidential messages from being intercepted [2]. The wiretap channel, in which a source communicates with a receiver through a discrete memoryless channel (DMC) and a wire-tapper observes the output of this channel via another DMC, has been introduced by Wyner [3], which was characterized as the fundamental framework over the secure communications. Refs. [4–6] studied the secrecy performance over independent/correlated Rayleigh/lognormal/Rayleigh-log-normal fading channels, respectively.

Received date: 30-10-2015
Corresponding author: Pan Gaofeng, E-mail: gfpan@swu.edu.cn
DOI: 10.1016/S1005-8885(16)60032-8

Triggered by the rapidly-developing multi-antenna technique for 4G and beyond to attain better secrecy performance in wiretap channels, multi-antenna diversity technology has attracted a growing quantity of scholars' attention [7–10]. [7] considered single-input multi-output wiretap channel and derived the SOP with maximal ratio combing (MRC) at both the legitimate receiver and the eavesdropper. [8] extended the considered model of [7] to multiple eavesdroppers scenario. In addition, transmit antenna selection was introduced to attain the diversity at the transmitter in Refs. [9–10].

Security is an important requirement for future 5G systems, and CR is no exception. As a promising solution to the inadequacy of spectrum, CR has received great attention [11]. Underlay is an easy way to realize spectrum sharing, as the secondary user only needs to adjust its transmit power within a threshold that the primary user can tolerate [12], and it has been investigated in several works [13–15]. In underlay cognitive spectrum sharing networks,

the primary network and the secondary network are allowed to transmit concurrently in the same spectrum [16–17]. Ref. [18] has studied the SOP and the probability of non-zero secrecy capacity over Nakagami-*m* fading channels. Ref. [19] derived the SOP of the proposed three scheduling schemes in the presence of the coordinated and uncoordinated eavesdroppers in the multi-user multi-eavesdropper CR system.

However, very few researches have considered the secrecy performance of SIMO systems, which is one of the most effect technologies to improve the transmission rate in CRNs. Some previous works have laid a solid foundation to understand the role of physical layer security in CRNs, while the impact of multi-antenna wiretap channels on cognitive spectrum sharing networks with passive eavesdropping is less well understood. Refs. [20,1] investigated the secrecy outage performance of SIMO system using MRC/SC in CRNs. However, Ref. [20] only considered that the eavesdropper is equipped with a single antenna and the restriction of transmit power at the secondary transmitter is incomplete. Further, it is easy to see that the research method proposed by Ref. [1] is very complicated to understand the secrecy outage performance in CRNs. MRC has better combining performance than SC, while the hardware cost of implementing MRC is normally higher than that of implementing SC. Thus, SC is also a common combining technology in practical applications. In recent years, SC has been widely adopted to improve the secrecy performance in physical layer [1,10].

Motivated by the above observations, this paper investigates the secrecy outage performance of SC scheme in underlay CRNs over Rayleigh fading channels. We consider a secondary user Alice (A) transmits confidential messages to another secondary user Bob (B) equipped with $n_{\mathrm{B}}\left(n_{\mathrm{B}}\geqslant 1\right)$ antennas where SC scheme is adopted, while an eavesdropper equipped with $n_{\mathrm{E}}\left(n_{\mathrm{E}}\geqslant 1\right)$ antennas also adopts SC scheme to overhear the information. Passive eavesdropping is considered, where the knowledge of the eavesdropper's channel is unavailable at the secondary transmitter. A adopts the underlay strategy to guarantee the quality of service of the primary user without spectrum sensing. We present an alternative method to derive the closed-form expression for the SOP considered by Elkashlan et al. in Ref. [1]. Further, we also develop a simplified SOP when the maximal transmit power of the secondary user is sufficiently high.

2 System model and problem formulation

2.1 System model

In a cognitive wiretap radio network, as illustrated in Fig. 1, the secondary transmitter Alice (A) communicates with the secondary receiver Bob (B) under the malicious attempt of the eavesdropper Eve (E). We assume a cognitive network with underlay spectrum sharing which allows concurrent transmissions from PU and A in the same spectrum band. The eavesdropping is passive, which means that the channel state information (CSI) of the eavesdropper's channel is unknown at A. Under this condition, when A intends to send confidential data to B, A has no choice but to encode the confidential messages into the transmitted codeword $x=\left[x(1),\ldots x(l),\ldots x(L)\right]$, where L is the length of x, which is subject to the average power constraint $\frac{1}{L}\sum_{l=1}^{L}E\left[\left|x(l)\right|^2\right]\leqslant P_A$, where P_A is the transmit power at A. B and E are equipped n_{B} and n_{E} antennas, respectively, and adopt SC scheme to process the received signals. Both A and PU are equipped with a single antenna. All channels considered in this work are assumed to follow independent identically distributed (i.i.d.) Rayleigh fading, and the channel gains $\{h_{1i}\}_{i=1}^{n_{\mathrm{B}}}$, $\{h_{2j}\}_{j=1}^{n_{\mathrm{E}}}$ and h_0 are complex Gaussian random variables (RVs) with zero mean and variances Ω_1, Ω_2 and Ω_0, respectively. We assume that the main channel from A to B and the eavesdropper's channel from A to E are independent of each other, and all channels in Fig. 1 suffer from additive white Gaussian noise (AWGN) with variance of N_0.

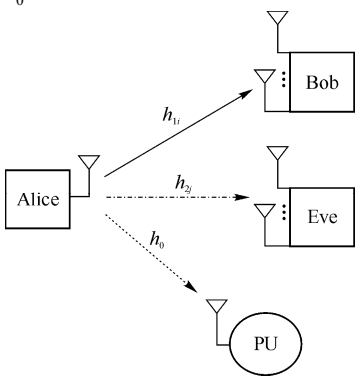

Fig. 1 A cognitive wiretap radio network

2.2 Problem formulation

In such cognitive wiretap channel, we must address