

RESEARCH

Open Access

Security-reliability trade-off for cognitive radio networks in the presence of eavesdropping attack

Jia Zhu

Abstract

In this paper, we consider a cognitive radio network that consists of one cognitive base station (CBS) and multiple cognitive users (CUs) in the presence of an eavesdropper. In the cognitive radio network, CBS first detects whether there is spectrum hole through spectrum sensing and then communicates with CUs over the detected spectrum hole. Due to the broadcast nature of wireless transmission, the eavesdropper can overhear the cognitive transmissions between CBS and CUs and attempts to decode its overheard signals for interception purpose. In order to effectively defend against the eavesdropping attack, we propose a multiuser scheduling scheme for cognitive transmissions, where a CU with the highest instantaneous capacity to CBS is selected and scheduled to communicate with CBS. We analyze the security-reliability trade-off performance of proposed multiuser scheduling scheme for cognitive transmissions with the imperfect spectrum sensing over Rayleigh fading channels, where the security and reliability are evaluated in terms of the intercept probability and the outage probability, respectively. Numerical results illustrate that as the intercept probability requirement loosens, the outage probability of proposed multiuser scheduling scheme decreases accordingly, showing the trade-off between security and reliability. In addition, as the number of CUs increases, numerical intercept probability and outage probability of the multiuser scheduling scheme significantly improve, implying the security and reliability benefits through multiuser scheduling.

Keywords: Security-reliability trade-off; Cognitive radio; Eavesdropping; Intercept probability; Outage probability

1 Introduction

Cognitive radio (CR) is emerging as a means to improve the spectrum resource utilization and allows unlicensed users (also called secondary user or cognitive user) to access the licensed spectrum in an opportunistic way [1-3]. Nowadays, most of radio spectrum is already licensed to particular wireless systems, e.g., the very high frequency (VHF) band from 174 to 216 MHz is allocated to broadcast television systems in North America, the ultra-high frequency (UHF) band from 880 to 915 MHz is allocated to the Global System for Mobile Communications (GSM), and so on. There is no available spectrum suited for developing new wireless communication systems. However, it has been reported by Federal

Communications Commission (FCC) that the utilization of licensed spectrum typically ranges from 15% to 85% with a high variance in time, showing that the licensed spectrum is underutilized [4]. This provides us with an opportunity to develop a cognitive radio system that opportunistically utilizes the licensed spectrum. More specifically, if the licensed spectrum band is detected as idle, i.e., the band is not occupied by a licensed user (referred to as primary user), the cognitive radio system can reuse such idle licensed spectrum for data transmission [5]. In view of the above observations, cognitive radio relies on the spectrum sensing that is responsible for detecting and identifying the idle spectrum (known as spectrum hole).

Spectrum sensing enables the cognitive users to be adapted to the radiofrequency (RF) environment by

Correspondence: christina825@163.com
School of Telecommunications and Information Engineering, Nanjing
University of Posts and Telecommunications, Nanjing 210003, People's
Republic of China

detecting spectrum holes, and the simplest way for spectrum hole detection is to detect whether the primary user is present (or absent). Specifically, the presence of primary user implies the unavailability of licensed spectrum and the absence of primary user implies an available spectrum hole. At present, there are three main signal detection approaches for the spectrum sensing, i.e., the energy detection [6], matched filter detection [7], and cyclostationary detection [8,9]. In general, the energy detection is sensitive to the background noise and unintended interference, which, however, has the advantage of simpler implementation than the matched filter detection and cyclostationary detection. In contrast, the matched filter detection is robust to the unintended interference, but requires some prior knowledge about the primary user signal such as the modulation type and signal waveform which may not be available in practice. As an alternative, the cyclostationary detection is presented through exploiting the cyclostationary feature of modulated signals, which typically requires long observation time to extract certain signal features. In addition, in order to combat the wireless fading effect, cooperative spectrum sensing [10-12] emerges by allowing cognitive users to cooperate with each other in detecting the presence of primary user. It is shown that the detection performance can be significantly improved through cooperative spectrum sensing.

It is pointed out that most existing work on cognitive radio is focused on the spectrum sensing and less attention has been paid to the cognitive radio security against eavesdropping attack. As is known, in cognitive radio networks, CUs first perform the spectrum sensing to identify spectrum holes and then communicate with each other over the detected spectrum holes [2,3]. However, due to the broadcast nature of wireless medium, an eavesdropping attacker within the transmit coverage of cognitive source node will be able to overhear the cognitive transmissions and may decode its overheard signals for the interception purpose. Traditionally, cryptographic techniques relying on secret keys are employed to protect the confidential transmissions from eavesdropping, which, however, is not secure when the eavesdropper is with sufficient computational capacity for exhaustive key search (also known as brute-force attack) [13,14]. To this end, physical layer security is now emerging as a means to secure wireless transmissions against the eavesdropping attack [15,16]. In [17], the authors have proposed the concept of security-reliability trade-off (SRT) for wireless communications and examined the opportunistic relay selection for improving SRT. It has been shown in [17] that as the number of cooperative relays increases, the SRT performance of wireless communications can be significantly improved.

In this paper, we investigate the security-reliability trade-off for cognitive radio transmissions with imperfect spectrum sensing, where mutual interference between primary and cognitive users should be taken in account in characterizing the SRT performance. This differs from [17] where no interference is considered in performing the SRT analysis. We consider a cognitive radio network consisting of one cognitive base station (CBS) and multiple cognitive users (CUs) in the presence of an eavesdropper, where CBS communicates with CUs over detected spectrum holes and the eavesdropper attempts to intercept the cognitive transmission. We propose a multiuser scheduling scheme to improve the security of cognitive transmission against eavesdropping attack and conduct the SRT analysis of proposed multiuser scheduling scheme in Rayleigh fading channels. Numerical results show that with an increasing number of CUs, the SRT performance of cognitive radio transmissions significantly improves, showing the advantage of proposed multiuser scheduling scheme against eavesdropping attack.

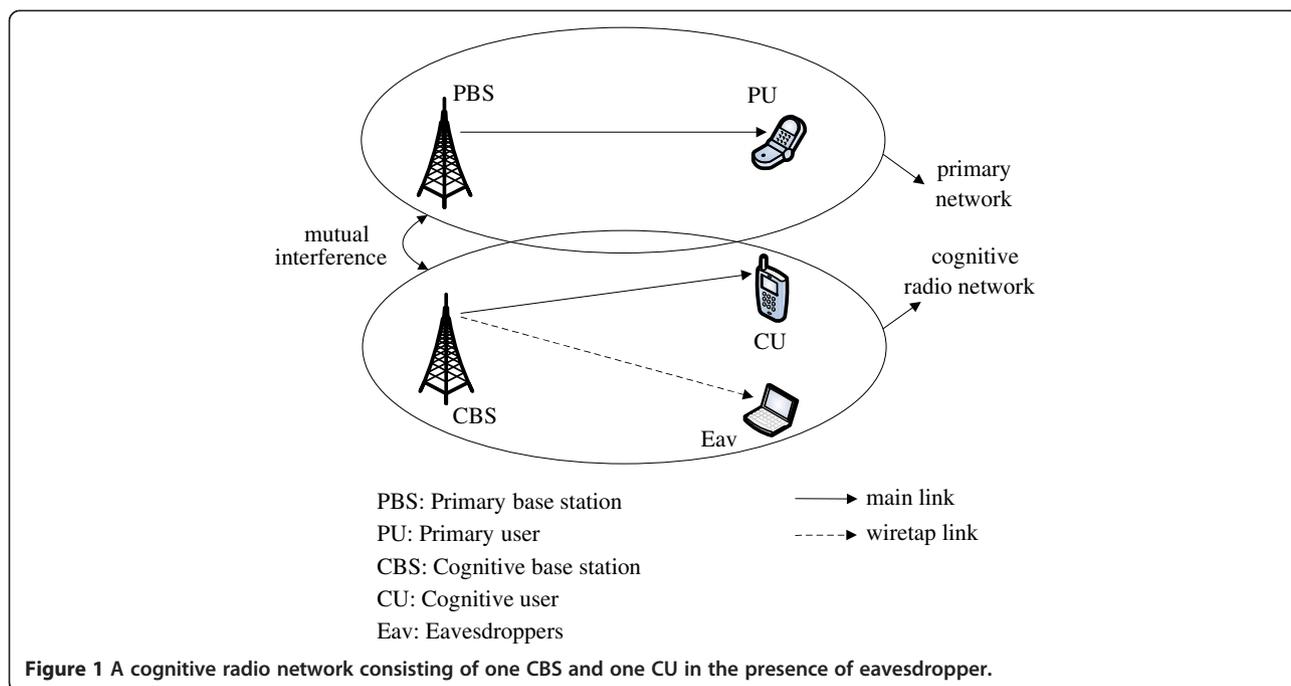
The rest of this paper is organized as follows. Section 2 presents the conventional direct transmission for cognitive radio in the presence of an eavesdropper and proposes the multiuser scheduling scheme to improve the cognitive transmission security against the eavesdropping attack. In Section 3, we perform the SRT analysis of traditional direct transmission and proposed multiuser scheduling schemes over Rayleigh fading channels. Next, in Section 4, the numerical SRT performance of proposed multiuser scheduling scheme is provided and compared with the traditional direct transmission. Finally, we give some concluding remarks in Section 5.

2 Proposed multiuser scheduling scheme in cognitive radio networks

In this section, we first describe the traditional direct transmission for cognitive radio in the presence of an eavesdropper and then propose the multiuser scheduling scheme to defend against eavesdropping attack.

2.1 Direct transmission

Figure 1 shows a cognitive radio network with one CBS and one CU, which is allowed to opportunistically access the spectrum licensed to the primary network that consists of one primary base station (PBS) and one primary user (PU). Specifically, if PBS and PU are communicating with each other over the licensed spectrum, CBS and CU are not allowed to transmit. If the licensed spectrum is detected as idle (i.e., the spectrum is not being used by PBS and PU), CBS and CU can reuse the detected idle spectrum (also referred to as spectrum hole) for data transmission. For notational convenience, let $H = H_0$ represent the case that the licensed spectrum is idle



and $H = H_1$ represent the other case of the spectrum being occupied by PBS and PU. The probability of the licensed spectrum being idle and available for CBS and CU is denoted by $P_a = \Pr(H = H_0)$. In addition, let $\hat{H} = H_0$ and $\hat{H} = H_1$ denote the licensed spectrum being detected as idle and busy, respectively, at cognitive users. Moreover, the probabilities of detection and false alarm of the presence of spectrum hole are represented by $P_d = \Pr\{\hat{H} = H_0 | H = H_0\}$ and $P_f = \Pr\{\hat{H} = H_0 | H = H_1\}$, respectively. In order to protect the quality of service (QoS) of primary transmissions, the detection probability and false alarm probability should be guaranteed to be above certain requirements. Throughout this paper, we consider the cognitive downlink transmission from CBS to CU. Notice that similar performance analysis and results can be obtained for the cognitive up-link transmission from CU to CBS.

Without loss of generality, let x_p and x_s denote the primary and secondary signals, respectively. Given the spectrum hole detected (i.e., $\hat{H} = H_0$), CBS starts transmitting its signal x_s to CU with power P_s and data rate R , thus the received signal at CU is written as

$$r_{CU} = \sqrt{P_s} h_{CBS-CU} x_s + \sqrt{\alpha P_p} h_{PBS-CU} x_p + n_{CU} \quad (1)$$

where h_{CBS-CU} and h_{PBS-CU} represent the fading coefficients of the channel from CBS to CU and that from PBS to CU, P_p is the transmit power of PBS, n_{CU} is the

additive white Gaussian noise (AWGN) with zero mean and variance N_0 , and α is defined as

$$\alpha = \begin{cases} 0, & H = H_0 \\ 1, & H = H_1 \end{cases} \quad (2)$$

where $H = H_0$ means that the licensed spectrum is unoccupied by primary users and thus PBS keeps silent, leading to $\alpha = 0$ in this case. Moreover, $\alpha = 1$ occurs when $H = H_1$, which is due to the fact that PBS is transmitting its signal x_p to PU in the case of $H = H_1$. Notice that due to the background noise and unintended interference, it is not possible to achieve the perfect spectrum sensing without missed detection and false alarm. In other words, the detected result $\hat{H} = H_0$ may happen even when there is actually no spectrum hole (i.e., $H = H_1$), which is referred to as false alarm of the presence of spectrum hole and causes mutual interference between primary and secondary users. Meanwhile, the broadcast nature of wireless transmission leads the cognitive transmission to be overheard and possibly intercepted by the eavesdropper. Thus, given that CBS transmits its signal x_s , we can express the signal overheard at eavesdropper (Eav) as

$$r_{Eav} = \sqrt{P_s} h_{CBS-Eav} x_s + \sqrt{\alpha P_p} h_{PBS-Eav} x_p + n_{Eav} \quad (3)$$

where $h_{CBS-Eav}$ and $h_{PBS-Eav}$ represent the fading coefficients of the channel from CBS to Eav and that from PBS to Eav, n_{Eav} is the zero-mean AWGN with variance N_0

received at Eav. Using Equation 1, we can easily obtain the capacity of main channel from CBS to CU as

$$C_m = \log_2 \left(1 + \frac{|h_{\text{CBS-CU}}|^2 P_s}{\alpha |h_{\text{PBS-CU}}|^2 P_p + N_0} \right) \quad (4)$$

where subscript ‘m’ denotes the main channel from CBS to CU. Also, using Equation 3, we can obtain the capacity of wiretap channel from CBS to Eav as

$$C_w = \log_2 \left(1 + \frac{|h_{\text{CBS-Eav}}|^2 P_s}{\alpha |h_{\text{PBS-Eav}}|^2 P_p + N_0} \right) \quad (5)$$

where subscript ‘w’ denotes the wiretap channel from CBS to Eav.

2.2 Multiuser scheduling scheme

In this subsection, we propose a multiuser scheduling scheme for cognitive radio security against eavesdropping attack. Figure 2 shows a cognitive radio network consisting of one CBS and multiple CUs in the presence of an Eav, where the multiple CUs are denoted by $U = \{\text{CU}_i | i = 1, 2, \dots, N\}$. If a spectrum hole is detected, CBS can transmit to multiple CUs by using various orthogonal multiplexing approaches, such as time-division multiplexing (TDM), orthogonal frequency division multiplexing (OFDM), and so on. Moreover, given an orthogonal subchannel, we can dynamically choose the best CU to access the subchannel against the eavesdropping attack. Following [13] and [14], we assume that the channel state information (CSI) of both the main link and wiretap link is available at CBS, which is a commonly used assumption in physical layer security literature.

Without loss of generality, we consider that CU_i is selected as the best user to access the detected spectrum hole. Assuming that CBS starts transmitting its signal x_s to CU_i with power P_s and data rate R , we can express the received signal at CU_i as

$$r_{\text{CU}_i} = \sqrt{P_s} h_{\text{CBS-CU}_i} x_s + \sqrt{\alpha P_p} h_{\text{PBS-CU}_i} x_p + n_{\text{CU}_i} \quad (6)$$

where $h_{\text{CBS-CU}_i}$ and $h_{\text{PBS-CU}_i}$ represent the fading coefficients of the channel from CBS to CU_i and that from PBS to CU_i , n_{CU_i} is the zero-mean AWGN with variance N_0 at CU_i , and α is given by Equation 2. Meanwhile, the received signal at Eav is written as

$$r_{\text{Eav}} = \sqrt{P_s} h_{\text{CBS-Eav}} x_s + \sqrt{\alpha P_p} h_{\text{PBS-Eav}} x_p + n_{\text{Eav}} \quad (7)$$

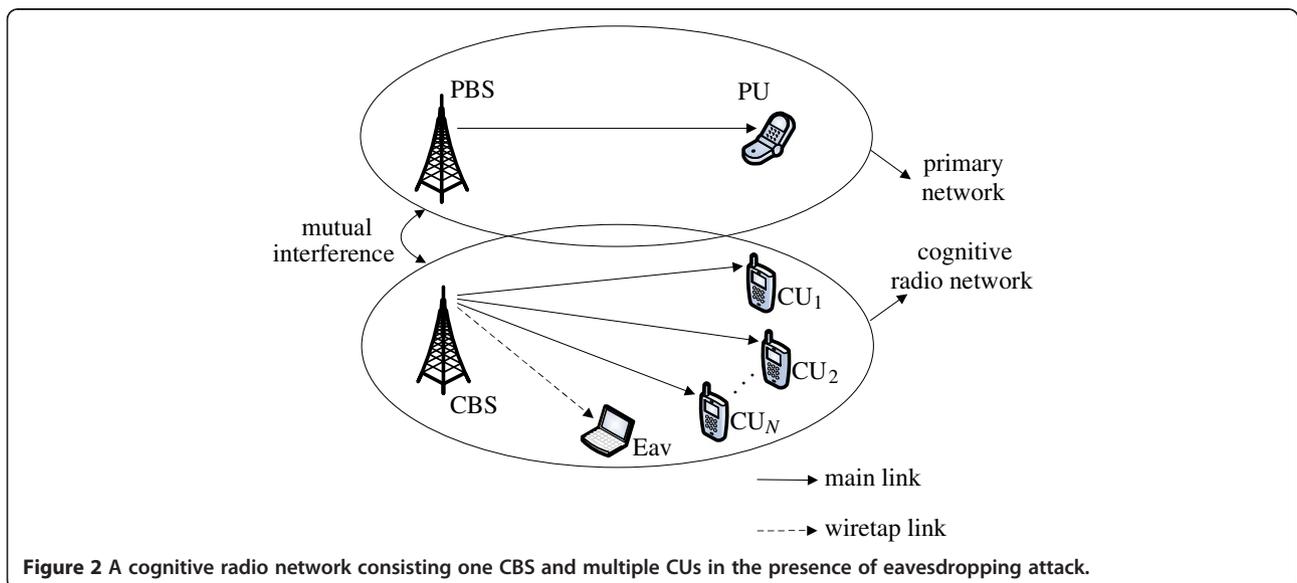
where $h_{\text{CBS-Eav}}$ and $h_{\text{PBS-Eav}}$ represent the fading coefficients of the channel from CBS to Eav and that from PBS to Eav, n_{Eav} is the zero-mean AWGN with variance N_0 received at Eav. Obviously, the capacity of main channel from CBS to CU_i is obtained from Equation 6 as

$$C_m^i = \log_2 \left(1 + \frac{|h_{\text{CBS-CU}_i}|^2 P_s}{\alpha |h_{\text{PBS-CU}_i}|^2 P_p + N_0} \right) \quad (8)$$

where superscript ‘i’ denotes CU_i . Similarly, the capacity of wiretap channel from CBS to Eav can be computed from Equation 7 as

$$C_w = \log_2 \left(1 + \frac{|h_{\text{CBS-Eav}}|^2 P_s}{\alpha |h_{\text{PBS-Eav}}|^2 P_p + N_0} \right) \quad (9)$$

which is determined by the fading coefficients of channels from CBS and PBS to Eav and has nothing to do with



CU_{*i*}. This means that the eavesdropper's CSI will not affect the multiuser scheduling policy. In general, a CU with the highest instantaneous capacity C_m^i is regarded as the best user. Therefore, the multiuser scheduling criterion can be given by

$$\text{Best CU} = \arg \max_{i \in U} C_m^i \quad (10)$$

where U represents the set of all CUs. Substituting C_m^i from Equation 8 to Equation 10 gives

$$\text{Best CU} = \arg \max_{i \in U} \frac{|h_{\text{CBS-CU}_i}|^2 P_s}{\alpha |h_{\text{PBS-CU}_i}|^2 P_p + N_0} \quad (11)$$

Using Equation 11, we can obtain the main channel capacity of proposed multiuser scheduling scheme as given in as

$$C_m^{\text{multiuser}} = \max_{i \in U} C_m^i = \max_{i \in U} \log_2 \left(1 + \frac{|h_{\text{CBS-CU}_i}|^2 P_s}{\alpha |h_{\text{PBS-CU}_i}|^2 P_p + N_0} \right). \quad (12)$$

So far, we have presented the conventional direct transmission for cognitive radio in the presence of eavesdropping attack and also proposed the multiuser scheduling scheme to enhance the cognitive transmission security.

3 Security-reliability trade-off analysis for cognitive transmissions over Rayleigh fading channels

In this section, we present the SRT analysis for the traditional direct transmission and proposed multiuser scheduling schemes in cognitive radio networks.

3.1 Direct transmission

This subsection analyzes the SRT analysis of conventional direct transmission over Rayleigh fading channels, where the security and reliability are characterized by the intercept probability at Eav and outage probability at CU, respectively. According to the Shannon's channel coding theorem, when the channel capacity falls below the data rate, the receiver is impossible to recover the source signal and an outage event occurs in this case. Otherwise, the receiver is able to succeed in decoding the source signal. Thus, given a spectrum hole detected (i.e., $\hat{H} = H_0$), the outage probability of direct transmission at CU is written as

$$P_{\text{out}}^{\text{direct}} = \Pr(C_m < R | \hat{H} = H_0) \quad (13)$$

where C_m is given by Equation 4 and R is the data rate. Substituting C_m from Equation 4 into Equation 13 yields

$$P_{\text{out}}^{\text{direct}} = \Pr \left(\frac{|h_{\text{CBS-CU}}|^2 P_s}{\alpha |h_{\text{PBS-CU}}|^2 P_p + N_0} < 2^R - 1 | \hat{H} = H_0 \right). \quad (14)$$

Using the law of total probability and Equation 2, we can rewrite Equation 14 as

$$\begin{aligned} P_{\text{out}}^{\text{direct}} &= \Pr \left(\frac{|h_{\text{CBS-CU}}|^2 P_s}{\alpha |h_{\text{PBS-CU}}|^2 P_p + N_0} < 2^R - 1, H = H_0 | \hat{H} = H_0 \right) \\ &\quad + \Pr \left(\frac{|h_{\text{CBS-CU}}|^2 P_s}{\alpha |h_{\text{PBS-CU}}|^2 P_p + N_0} < 2^R - 1, H = H_1 | \hat{H} = H_0 \right) \\ &= \Pr \left(\frac{|h_{\text{CBS-CU}}|^2 P_s}{N_0} < 2^R - 1 \right) \Pr(H = H_0 | \hat{H} = H_0) \\ &\quad + \Pr \left(\frac{|h_{\text{CBS-CU}}|^2 P_s}{|h_{\text{PBS-CU}}|^2 P_p + N_0} < 2^R - 1 \right) \\ &\quad \Pr(H = H_1 | \hat{H} = H_0). \end{aligned} \quad (15)$$

Using the Bayes' theorem, we can obtain $\Pr(H = H_0 | \hat{H} = H_0)$ as

$$\begin{aligned} \Pr(H = H_0 | \hat{H} = H_0) &= \frac{\Pr(H = H_0) \Pr(\hat{H} = H_0 | H = H_0)}{\sum_{i=0}^1 \Pr(H = H_i) \Pr(\hat{H} = H_0 | H = H_i)} \\ &= \frac{P_a P_d}{P_a P_d + (1 - P_a) P_f} \end{aligned} \quad (16)$$

where $P_a = \Pr(H = H_0)$ is the probability of licensed spectrum being idle and available for CBS, and $P_d = \Pr\{\hat{H} = H_0 | H = H_0\}$ and $P_f = \Pr\{\hat{H} = H_0 | H = H_1\}$ represent the probabilities of detection and false alarm of the presence of spectrum hole, respectively. Similarly, $\Pr(H = H_1 | \hat{H} = H_0)$ can be given by

$$\Pr(H = H_1 | \hat{H} = H_1) = \frac{(1 - P_a) P_f}{P_a P_d + (1 - P_a) P_f} \quad (17)$$

Denoting $|h_{\text{CBS-CU}}|^2 = x$, $|h_{\text{PBS-CU}}|^2 = y$, $\gamma_s = P_s / N_0$, $\gamma_p = P_p / N_0$, $\pi_0 = \Pr(H = H_0 | \hat{H} = H_0)$, and $\pi_1 = \Pr(H = H_0 | \hat{H} = H_0)$, we obtain

$$P_{\text{out}}^{\text{direct}} = \pi_0 \Pr(\gamma_s x < 2^R - 1) + \pi_1 \Pr(\gamma_s x - \gamma_p (2^R - 1) y < 2^R - 1) \quad (18)$$

From the Appendix, we can obtain

$$\Pr(\gamma_s x < 2^R - 1) = 1 - \exp \left(- \frac{2^R - 1}{\sigma_{\text{CBS-CU}}^2 \gamma_s} \right) \quad (19)$$

and

$$\begin{aligned} & \Pr(\gamma_s x - \gamma_p (2^R - 1)y < 2^R - 1) \\ &= 1 - \frac{\sigma_{\text{CBS-CU}}^2 \gamma_s}{\sigma_{\text{PBS-CU}}^2 \gamma_p (2^R - 1) + \sigma_{\text{CBS-CU}}^2 \gamma_s} \exp\left(-\frac{2^R - 1}{\sigma_{\text{CBS-CU}}^2 \gamma_s}\right) \end{aligned} \quad (20)$$

Thus, substituting Equations 19 and 20 into Equation 18, we can obtain the closed-form outage probability expression of direct transmission scheme as

$$\begin{aligned} P_{\text{out}}^{\text{direct}} &= \pi_0 \left[1 - \exp\left(-\frac{2^R - 1}{\sigma_{\text{CBS-CU}}^2 \gamma_s}\right) \right] \\ &+ \pi_1 \left[1 - \frac{\sigma_{\text{CBS-CU}}^2 \gamma_s}{\sigma_{\text{PBS-CU}}^2 \gamma_p (2^R - 1) + \sigma_{\text{CBS-CU}}^2 \gamma_s} \exp\left(-\frac{2^R - 1}{\sigma_{\text{CBS-CU}}^2 \gamma_s}\right) \right]. \end{aligned} \quad (21)$$

In addition, when the wiretap channel capacity becomes larger than the data rate, the eavesdropper will be able to succeed in decoding the source signal and an intercept event occurs [17]. Therefore, given a spectrum hole detected, the intercept probability of direct transmission at Eav is obtained as

$$P_{\text{intercept}}^{\text{direct}} = \Pr(C_w > R | \hat{H} = H_0) \quad (22)$$

where C_w is given by Equation 5. Substituting C_w from Equation 5 into Equation 22 yields

$$P_{\text{intercept}}^{\text{direct}} = \Pr\left(\frac{|h_{\text{CBS-Eav}}|^2 P_s}{\alpha |h_{\text{PBS-Eav}}|^2 P_p + N_0} > 2^R - 1 | \hat{H} = H_0\right) \quad (23)$$

Similar to Equation 15, we can rewrite Equation 23 as

$$\begin{aligned} P_{\text{intercept}}^{\text{direct}} &= \pi_0 \Pr\left(\frac{|h_{\text{CBS-Eav}}|^2 P_s}{N_0} > 2^R - 1\right) \\ &+ \pi_1 \Pr\left(\frac{|h_{\text{CBS-Eav}}|^2 P_s}{|h_{\text{PBS-Eav}}|^2 P_p + N_0} > 2^R - 1\right), \end{aligned} \quad (24)$$

where $\pi_0 = \Pr(H = H_0 | \hat{H} = H_0)$ and $\pi_1 = \Pr(H = H_1 | \hat{H} = H_0)$, which are given by Equations 16 and 17, respectively. Considering that random variables $|h_{\text{CBS-Eav}}|^2$ and $|h_{\text{PBS-Eav}}|^2$ follow independent exponential distributions with respective means $\sigma_{\text{CBS-Eav}}^2$ and $\sigma_{\text{PBS-Eav}}^2$, we obtain

$$\Pr\left(\frac{|h_{\text{CBS-Eav}}|^2 P_s}{N_0} > 2^R - 1\right) = \exp\left(-\frac{2^R - 1}{\sigma_{\text{CBS-Eav}}^2 \gamma_s}\right) \quad (25)$$

and

$$\begin{aligned} & \Pr\left(\frac{|h_{\text{CBS-Eav}}|^2 P_s}{|h_{\text{PBS-Eav}}|^2 P_p + N_0} > 2^R - 1\right) \\ &= \frac{\sigma_{\text{CBS-Eav}}^2 \gamma_s}{\sigma_{\text{PBS-Eav}}^2 \gamma_p (2^R - 1) + \sigma_{\text{CBS-Eav}}^2 \gamma_s} \exp\left(-\frac{2^R - 1}{\sigma_{\text{CBS-Eav}}^2 \gamma_s}\right) \end{aligned} \quad (26)$$

where $\gamma_s = P_s/N_0$ and $\gamma_p = P_p/N_0$. Substituting Equations 25 and 26 into Equation 24, we obtain a closed-form intercept probability expression of traditional direct transmission as

$$\begin{aligned} P_{\text{intercept}}^{\text{direct}} &= \pi_0 \exp\left(-\frac{2^R - 1}{\sigma_{\text{CBS-Eav}}^2 \gamma_s}\right) \\ &+ \frac{\pi_1 \sigma_{\text{CBS-Eav}}^2 \gamma_s}{\sigma_{\text{PBS-Eav}}^2 \gamma_p (2^R - 1) + \sigma_{\text{CBS-Eav}}^2 \gamma_s} \exp\left(-\frac{2^R - 1}{\sigma_{\text{CBS-Eav}}^2 \gamma_s}\right). \end{aligned} \quad (27)$$

One can see that the outage probability and intercept probability of direct transmission are, respectively, given by Equations 21 and 27, which characterize the trade-off between security and reliability.

3.2 Proposed multiuser scheduling scheme

In this subsection, we present the SRT analysis of proposed multiuser scheduling scheme in Rayleigh fading channels. Similar to Equation 13, the outage probability of proposed multiuser scheduling scheme can be obtained as

$$P_{\text{out}}^{\text{multiuser}} = \Pr(C_m^{\text{multiuser}} < R | \hat{H} = H_0) \quad (28)$$

where $C_m^{\text{multiuser}}$ is given by Equation 12. Substituting $C_m^{\text{multiuser}}$ from Equation 12 into Equation 28 gives

$$P_{\text{out}}^{\text{multiuser}} = \Pr\left(\max_{i \in U} \log_2\left(1 + \frac{|h_{\text{CBS-CU}_i}|^2 P_s}{\alpha |h_{\text{PBS-CU}_i}|^2 P_p + N_0}\right) < R | \hat{H} = H_0\right). \quad (29)$$

By using the law of total probability, Equation 29 is rewritten as

$$\begin{aligned} P_{\text{out}}^{\text{multiuser}} &= \Pr\left(\max_{i \in U} \log_2\left(1 + \frac{|h_{\text{CBS-CU}_i}|^2 P_s}{\alpha |h_{\text{PBS-CU}_i}|^2 P_p + N_0}\right) < R, H = H_0 | \hat{H} = H_0\right) \\ &+ \Pr\left(\max_{i \in U} \log_2\left(1 + \frac{|h_{\text{CBS-CU}_i}|^2 P_s}{\alpha |h_{\text{PBS-CU}_i}|^2 P_p + N_0}\right) < R, H = H_1 | \hat{H} = H_0\right) \\ &= \Pr\left(\max_{i \in U} \log_2\left(1 + \frac{|h_{\text{CBS-CU}_i}|^2 P_s}{N_0}\right) < R, H = H_0 | \hat{H} = H_0\right) \\ &+ \Pr\left(\max_{i \in U} \log_2\left(1 + \frac{|h_{\text{CBS-CU}_i}|^2 P_s}{|h_{\text{PBS-CU}_i}|^2 P_p + N_0}\right) < R, H = H_1 | \hat{H} = H_0\right), \end{aligned} \quad (30)$$

which can be further obtained as

$$\begin{aligned}
 P_{\text{out}}^{\text{multiuser}} &= \pi_0 \Pr \left(\max_{i \in \mathcal{U}} \log_2 \left(1 + \frac{|h_{\text{CBS-CU}_i}|^2 P_s}{N_0} \right) < R \right) \\
 &\quad + \pi_1 \Pr \left(\max_{i \in \mathcal{U}} \log_2 \left(1 + \frac{|h_{\text{CBS-CU}_i}|^2 P_s}{|h_{\text{PBS-CU}_i}|^2 P_p + N_0} \right) < R \right) \\
 &= \pi_0 \prod_{i=1}^N \Pr \left(\log_2 \left(1 + \frac{|h_{\text{CBS-CU}_i}|^2 P_s}{N_0} \right) < R \right) \\
 &\quad + \pi_1 \prod_{i=1}^N \Pr \left(\log_2 \left(1 + \frac{|h_{\text{CBS-CU}_i}|^2 P_s}{|h_{\text{PBS-CU}_i}|^2 P_p + N_0} \right) < R \right) \\
 &= \pi_0 \prod_{i=1}^N \Pr \left(\frac{|h_{\text{CBS-CU}_i}|^2 P_s}{N_0} < 2^{R-1} \right) \\
 &\quad + \pi_1 \prod_{i=1}^N \Pr \left(\frac{|h_{\text{CBS-CU}_i}|^2 P_s}{|h_{\text{PBS-CU}_i}|^2 P_p + N_0} < 2^{R-1} \right)
 \end{aligned} \tag{31}$$

where $\pi_0 = \Pr(H = H_0 | \hat{H} = H_0)$, $\pi_1 = \Pr(H = H_0 | \hat{H} = H_0)$, N is the number of CUs, and the second equation arises due to the fact that random variables $|h_{\text{CBS-CU}_i}|^2$ and $|h_{\text{PBS-CU}_i}|^2$ are independent for different CUs. Noting that $|h_{\text{CBS-CU}_i}|^2$ and $|h_{\text{PBS-CU}_i}|^2$ follow independent exponential distributions with respective means $\sigma_{\text{CBS-CU}_i}^2$ and $\sigma_{\text{PBS-CU}_i}^2$, we can obtain

$$\Pr \left(\frac{|h_{\text{CBS-CU}_i}|^2 P_s}{N_0} < 2^{R-1} \right) = 1 - \exp \left(- \frac{2^{R-1}}{\sigma_{\text{CBS-CU}_i}^2 \gamma_s} \right) \tag{32}$$

and

$$\begin{aligned}
 &\Pr \left(\frac{|h_{\text{CBS-CU}_i}|^2 P_s}{|h_{\text{PBS-CU}_i}|^2 P_p + N_0} < 2^{R-1} \right) \\
 &= 1 - \frac{\sigma_{\text{CBS-CU}_i}^2 \gamma_s}{\sigma_{\text{PBS-CU}_i}^2 \gamma_p (2^{R-1}) + \sigma_{\text{CBS-CU}_i}^2 \gamma_s} \exp \left(- \frac{2^{R-1}}{\sigma_{\text{CBS-CU}_i}^2 \gamma_s} \right).
 \end{aligned} \tag{33}$$

Hence, substituting Equations 32 and 33 into Equation 31, we obtain the closed-form outage probability expression of proposed multiuser scheduling scheme as

$$\begin{aligned}
 P_{\text{out}}^{\text{multiuser}} &= \pi_0 \prod_{i=1}^N \left[1 - \exp \left(- \frac{2^{R-1}}{\sigma_{\text{CBS-CU}_i}^2 \gamma_s} \right) \right] \\
 &\quad + \pi_1 \prod_{i=1}^N \left[1 - \frac{\sigma_{\text{CBS-CU}_i}^2 \gamma_s}{\sigma_{\text{PBS-CU}_i}^2 \gamma_p (2^{R-1}) + \sigma_{\text{CBS-CU}_i}^2 \gamma_s} \right. \\
 &\quad \quad \left. \exp \left(- \frac{2^{R-1}}{\sigma_{\text{CBS-CU}_i}^2 \gamma_s} \right) \right].
 \end{aligned} \tag{34}$$

In addition, similar to Equation 22, the intercept probability of proposed multiuser scheduling scheme is obtained as

$$P_{\text{intercept}}^{\text{multiuser}} = \Pr(C_w > R | \hat{H} = H_0) \tag{35}$$

where C_w is given by Equation 9. Substituting C_w from Equation 9 into Equation 35 yields

$$P_{\text{intercept}}^{\text{multiuser}} = \Pr \left(\frac{|h_{\text{CBS-Eav}}|^2 P_s}{\alpha |h_{\text{PBS-Eav}}|^2 P_p + N_0} > 2^{R-1} | \hat{H} = H_0 \right) \tag{36}$$

which can be further rewritten as

$$\begin{aligned}
 P_{\text{intercept}}^{\text{multiuser}} &= \pi_0 \Pr \left(\frac{|h_{\text{CBS-Eav}}|^2 P_s}{N_0} > 2^{R-1} \right) \\
 &\quad + \pi_1 \Pr \left(\frac{|h_{\text{CBS-Eav}}|^2 P_s}{|h_{\text{PBS-Eav}}|^2 P_p + N_0} > 2^{R-1} \right).
 \end{aligned} \tag{37}$$

Note that $|h_{\text{CBS-Eav}}|^2$ and $|h_{\text{PBS-Eav}}|^2$ follow independent exponentially distributed random variables with respective means $\sigma_{\text{CBS-Eav}}^2$ and $\sigma_{\text{PBS-Eav}}^2$. Thus, we obtain

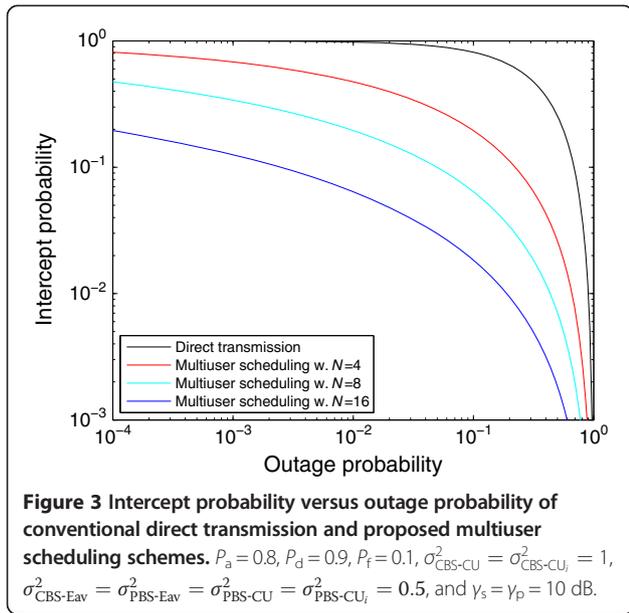
$$\begin{aligned}
 P_{\text{intercept}}^{\text{multiuser}} &= \pi_0 \exp \left(- \frac{2^{R-1}}{\sigma_{\text{CBS-Eav}}^2 \gamma_s} \right) \\
 &\quad + \frac{\pi_1 \sigma_{\text{CBS-Eav}}^2 \gamma_s}{\sigma_{\text{PBS-Eav}}^2 \gamma_p (2^{R-1}) + \sigma_{\text{CBS-Eav}}^2 \gamma_s} \exp \left(- \frac{2^{R-1}}{\sigma_{\text{CBS-Eav}}^2 \gamma_s} \right).
 \end{aligned} \tag{38}$$

which is the same as the intercept probability of conventional direct transmission. As shown in Equations 34 and 38, we have derived the closed-form expression of outage probability and intercept probability of proposed multiuser scheduling scheme in Rayleigh fading channels. So far, we have completed the SRT analysis of conventional direct transmission and proposed multiuser scheduling schemes in cognitive radio networks.

4 Numerical results and discussion

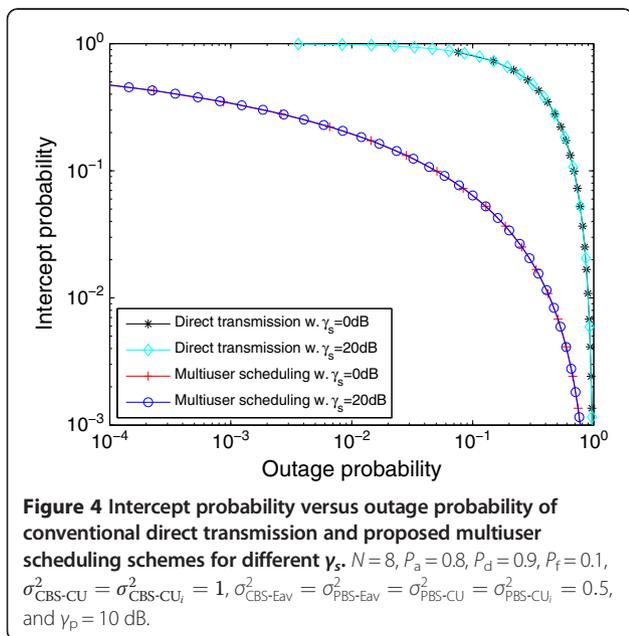
In the section, we present the numerical results of outage and intercept probabilities to show the trade-off between security and reliability for cognitive radio networks in the presence of eavesdropping attack. In cognitive radio networks, the detection probability and false alarm probability should be guaranteed to be above certain requirements in order to protect the QoS of primary transmissions. According to the IEEE 802.22 standard, the detection and false alarm probabilities are specified to $P_d = 0.9$ and $P_f = 0.1$ throughout this paper. Moreover, the probability of licensed spectrum being idle and available is set to $P_a = 0.8$.

Figure 3 shows the intercept probability versus outage probability of direct transmission and proposed multiuser scheduling schemes through using Equations 21, 27, 34, and 38 with $P_a = 0.8$, $P_d = 0.9$, $P_f = 0.1$, $\sigma_{\text{CBS-CU}}^2 = \sigma_{\text{CBS-CU}_i}^2 = 1$, $\sigma_{\text{CBS-Eav}}^2 = \sigma_{\text{PBS-Eav}}^2 = \sigma_{\text{PBS-CU}}^2 = \sigma_{\text{PBS-CU}_i}^2 = 0.5$, and $\gamma_s = \gamma_p = 10$ dB. One can see from Figure 3 that as the outage probability increases from 10^{-4} to 10^0 , the intercept probabilities of conventional direct transmission and proposed multiuser schemes both decrease from 10^0 to 10^{-3} , showing



that the security performance improves as the reliability requirement loosens. In addition, it is shown from Figure 3 that the SRT performance of multiuser scheduling scheme always outperforms the conventional direct transmission. Moreover, as the number of users increases from $N = 4$ to $N = 16$, the SRT performance of proposed multiuser scheduling scheme significantly improves, meaning the security and reliability benefit through multiuser scheduling.

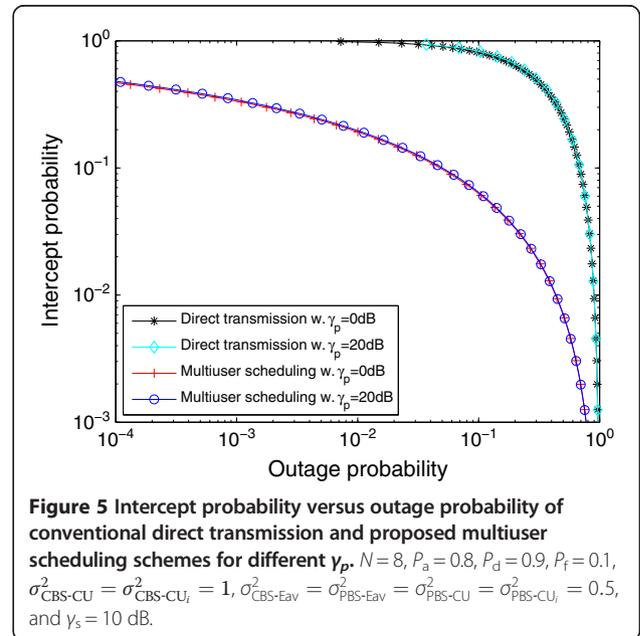
In Figure 4, we show the intercept probability versus outage probability of the conventional direct transmission and proposed multiuser scheduling schemes for different γ_s with $N = 8, P_a = 0.8, P_d = 0.9, P_f = 0.1, \sigma_{\text{CBS-CU}}^2 = \sigma_{\text{CBS-CU}_i}^2 = 1,$

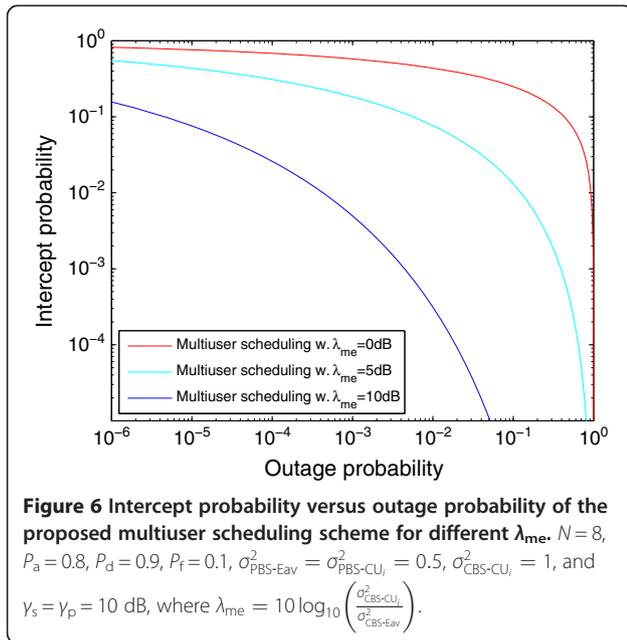


$\sigma_{\text{CBS-Eav}}^2 = \sigma_{\text{PBS-Eav}}^2 = \sigma_{\text{PBS-CU}}^2 = \sigma_{\text{PBS-CU}_i}^2 = 0.5,$ and $\gamma_p = 10$ dB. It is seen from Figure 4 that for both the direct transmission and multiuser scheduling scheme, the SRT performance corresponding to $\gamma_s = 0$ dB is almost identical to that corresponding to $\gamma_s = 20$ dB. This implies that increasing the transmit power of CBS cannot improve the SRT performance. Figure 4 also shows that for both cases of $\gamma_s = 0$ dB and $\gamma_s = 20$ dB, the proposed multiuser scheduling scheme always performs better than the direct transmission in terms of SRT performance.

Figure 5 illustrates the intercept probability versus outage probability of the conventional direct transmission and proposed multiuser scheduling schemes for different γ_p with $N = 8, P_a = 0.8, P_d = 0.9, P_f = 0.1, \sigma_{\text{CBS-CU}}^2 = \sigma_{\text{CBS-CU}_i}^2 = 1, \sigma_{\text{CBS-Eav}}^2 = \sigma_{\text{PBS-Eav}}^2 = \sigma_{\text{PBS-CU}}^2 = \sigma_{\text{PBS-CU}_i}^2 = 0.5,$ and $\gamma_s = 10$ dB. As is shown in Figure 5, as the primary signal-to-noise ratio γ_p increases from $\gamma_p = 0$ dB to $\gamma_p = 20$ dB, the SRT performance of both direct transmission and multiuser scheduling scheme almost keep unchanged. This means that the SRT for cognitive radio networks has nothing to do with the primary transmit power and background noise.

Figure 6 shows the intercept probability versus outage probability of the multiuser scheduling scheme for different λ_{me} with $N = 8, P_a = 0.8, P_d = 0.9, P_f = 0.1, \sigma_{\text{PBS-Eav}}^2 = \sigma_{\text{PBS-CU}_i}^2 = 0.5, \sigma_{\text{CBS-CU}_i}^2 = 1,$ and $\gamma_s = \gamma_p = 10$ dB, where λ_{me} is defined as $\lambda_{\text{me}} = 10 \log_{10} \left(\frac{\sigma_{\text{CBS-CU}_i}^2}{\sigma_{\text{CBS-Eav}}^2} \right)$ which is the ratio of average gain of main channel from CBS to CU to that of wiretap channel from CBS to Eav, which is called main-to-eavesdropper ratio (MER) throughout this paper. One can observe from Figure 6 that as the MER





increases from $\lambda_{me} = 0$ dB to $\lambda_{me} = 10$ dB, the SRT performance of proposed multiuser scheduling scheme improves significantly. This is due to the fact that with an increasing MER, the capacity of wiretap channel from PBS to Eav degrades and thus the probability of succeeding in intercepting the cognitive transmission at Eav decreases.

5 Conclusions

In this paper, we have investigated the security-reliability trade-off for cognitive radio networks in the presence of an eavesdropper. We have proposed a multiuser scheduling scheme to improve the SRT performance of cognitive radio transmission against eavesdropping attack. We have derived closed-form expressions of intercept probability and outage probability of the proposed multiuser scheduling scheme in cognitive radio networks with imperfect spectrum sensing. For the comparison purpose, we have also analyzed the SRT performance of traditional direct transmission in Rayleigh fading channels. Numerical results have shown that the proposed multiuser scheduling scheme strictly outperforms the conventional direct transmission in terms of SRT performance. In addition, with an increasing number of cognitive users, the SRT performance of proposed multiuser scheduling scheme significantly improves, showing the security and reliability benefits through multiuser scheduling.

Appendix

Proof of Equations 19 and 20

It is noticed that random variables $|h_{\text{CBS-CU}}|^2 = x$ and $|h_{\text{PBS-CU}}|^2 = y$ follow independent exponential distributions with respective means $\sigma_{\text{CBS-CU}}^2$ and $\sigma_{\text{PBS-CU}}^2$. Thus,

the joint probability density function (PDF) of (x, y) is given by

$$f(x, y) = \frac{1}{\sigma_{\text{CBS-CU}}^2 \sigma_{\text{PBS-CU}}^2} \exp\left(-\frac{x}{\sigma_{\text{CBS-CU}}^2} - \frac{y}{\sigma_{\text{PBS-CU}}^2}\right) \quad (39)$$

for $(x > 0, y > 0)$. Using the PDF of exponentially distributed random variable $|h_{\text{CBS-CU}}|^2 = x$ with mean $\sigma_{\text{CBS-CU}}^2$, we obtain

$$\begin{aligned} \Pr(\gamma_s x < 2^R - 1) &= \int_0^{\gamma_s} \frac{1}{\sigma_{\text{CBS-CU}}^2} \exp\left(-\frac{x}{\sigma_{\text{CBS-CU}}^2}\right) dx \\ &= 1 - \exp\left(-\frac{2^R - 1}{\sigma_{\text{CBS-CU}}^2 \gamma_s}\right) \end{aligned} \quad (40)$$

which is Equation 19. Using the joint PDF of (x, y) , we have

$$\begin{aligned} \Pr(\gamma_s x - \gamma_p (2^R - 1)y < 2^R - 1) &= \iint_{\Theta} \frac{1}{\sigma_{\text{CBS-CU}}^2 \sigma_{\text{PBS-CU}}^2} \exp\left(-\frac{x}{\sigma_{\text{CBS-CU}}^2} - \frac{y}{\sigma_{\text{PBS-CU}}^2}\right) dx dy \end{aligned} \quad (41)$$

where $\Theta = \{(x, y) | \gamma_s x - \gamma_p (2^R - 1)y < 2^R - 1\}$. From Equation 41, we obtain

$$\begin{aligned} \Pr(\gamma_s x - \gamma_p (2^R - 1)y < 2^R - 1) &= 1 - \int_0^{\infty} \frac{1}{\sigma_{\text{CBS-CU}}^2} \exp\left(-\frac{x}{\sigma_{\text{CBS-CU}}^2}\right) dx \int_0^{\frac{\gamma_s x - (2^R - 1)}{\gamma_p (2^R - 1)}} \frac{1}{\sigma_{\text{PBS-CU}}^2} \exp\left(-\frac{y}{\sigma_{\text{PBS-CU}}^2}\right) dy. \end{aligned} \quad (42)$$

Performing the double integral in Equation 42 yields

$$\begin{aligned} \Pr(\gamma_s x - \gamma_p (2^R - 1)y < 2^R - 1) &= 1 - \frac{\sigma_{\text{CBS-CU}}^2 \gamma_s}{\sigma_{\text{PBS-CU}}^2 \gamma_p (2^R - 1) + \sigma_{\text{CBS-CU}}^2 \gamma_s} \exp\left(-\frac{2^R - 1}{\sigma_{\text{CBS-CU}}^2 \gamma_s}\right). \end{aligned} \quad (43)$$

This completes the calculation of Equation 20.

Competing interest

The author declares that she has no competing interest.

Acknowledgements

This work was supported in part by the National Natural Science Foundation of China (grant no. 61302104) and the Scientific Research Foundation of Nanjing University of Posts and Telecommunications (grant no. NY213014).

Received: 13 May 2013 Accepted: 14 October 2013

Published: 6 November 2013

References

1. J. Mitola, G.Q. Maguire, Cognitive radio: making software radios more personal. *IEEE Pers Commun* **6**, 13–18 (1999)
2. Y. Zou, Y.-D. Yao, B. Zheng, Cooperative relay techniques for cognitive radio systems: spectrum sensing and secondary user transmissions. *IEEE Commun Mag* **50**, 4 (2012)
3. Y. Zou, Y.-D. Yao, B. Zheng, Cognitive transmissions with multiple relays in cognitive radio networks. *IEEE Trans Wireless Commun* **10**(2), 648–659 (2011)
4. Federal Communications Commission (FCC), Notice of proposed rule-making and order, 2003. Rep ET Docket (03-322)
5. S. Hu, Y. Yao, Z. Yang, *Cognitive medium access control protocols for secondary users sharing a common channel with time division multiple access primary users*, Wiley Wireless Commun. and Mobile Computing, 2012. doi:10.1002/wcm.2185
6. H. Urkowitz, Energy detection of unknown deterministic signals. *Proceedings of IEEE* **55**(4), 523–231 (1967)
7. A. Sahai, N. Hoven, R. Tandra, Some fundamental limits in cognitive radio, in *Proceedings of the 42nd Allerton Conference on Communication, Control and Computing*, Monticello, 2004
8. A. Fehske, J.D. Gaeddert, J.H. Reed, *A new approach to signal classification using spectral correlation and neural networks*, in *Proceedings of the Symposium on IEEE DySPAN*, Baltimore, 2005
9. K. Kim, I. Akbar, K. Bae, J. Um, C. Spooner, J. Reed, Cyclostationary approaches to signal detection and classification in cognitive radio, in *Proceedings of the Symposium on IEEE DySPAN*, Dublin, 17–20 April 2007
10. A. Ghasemi, E.S. Sousa, *Collaborative spectrum sensing for opportunistic access in fading environment* Proc, IEEE DYSPAN, 2005, 131–136
11. Y. Zou, Y.-D. Yao, B. Zheng, A selective-relay based cooperative spectrum sensing scheme without dedicated reporting channels in cognitive radio networks. *IEEE Trans. Wireless Commun.* **10**(4), 1188–1198 (2011)
12. J. Zhu, Y. Zou, B. Zheng, Cooperative detection for primary user in cognitive radio networks. *EURASIP J Wirel Commun Netw* **2009**(617320), 12 (2009)
13. M. Bloch, J.O. Barros, M. Rodrigues, S.W. McLaughlin, Wireless information-theoretic security. *IEEE Trans Inf Theory* **54**(6), 2515–2534 (2008)
14. Y. Zou, X. Wang, W. Shen, Optimal relay selection for physical-layer security in cooperative wireless networks. *IEEE J. Sel. Area Commun.* **31**(10), 2099–2111 (2013)
15. A. Khisti, G.W. Wornell, Secure transmission with multiple antennas: the MISOME wiretap channel. *IEEE Trans Inf Theory* **56**(7), 3088–3104 (2010)
16. F. Oggier, B. Hassibi, The secrecy capacity of the MIMO wiretap channel. *IEEE Trans Inf Theory* **57**(8), 4961–4972 (2011)
17. Y. Zou, X. Wang, W. Shen, L. Hanzo, *Security versus reliability analysis for opportunistic relaying* (IEEE Trans. Veh. Tech, in press)

doi:10.1186/1687-6180-2013-169

Cite this article as: Zhu: Security-reliability trade-off for cognitive radio networks in the presence of eavesdropping attack. *EURASIP Journal on Advances in Signal Processing* 2013 **2013**:169.

Submit your manuscript to a SpringerOpen[®] journal and benefit from:

- Convenient online submission
- Rigorous peer review
- Immediate publication on acceptance
- Open access: articles freely available online
- High visibility within the field
- Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com
