Secrecy Outage and Diversity Analysis of Cognitive Radio Systems

Yulong Zou, *Senior Member, IEEE,* Xuelong Li, *Fellow, IEEE,* and Ying-Chang Liang, *Fellow, IEEE*

***Abstract*—In this paper, we investigate the physical-layer security of a multi-user multi-eavesdropper cognitive radio system, which is composed of multiple cognitive users (CUs) transmitting to a common cognitive base station (CBS), while multiple eavesdroppers may collaborate with each other or perform independently in intercepting the CUs-CBS transmissions, which are called the coordinated and uncoordinated eavesdroppers, respectively. Considering multiple CUs available, we propose the round-robin scheduling as well as the optimal and suboptimal user scheduling schemes for improving the security of CUs-CBS transmissions against eavesdropping attacks. Specifically, the optimal user scheduling is designed by assuming that the channel state information (CSI) of all links from CUs to CBS, to primary user (PU) and to eavesdroppers are available. By contrast, the suboptimal user scheduling only requires the CSI of CUs-CBS links without the PU's and eavesdroppers' CSI. We derive closed-form expressions of the secrecy outage probability of these three scheduling schemes in the presence of the coordinated and uncoordinated eavesdroppers. We also carry out the secrecy diversity analysis and show that the round-robin scheduling achieves the diversity order of only one, whereas the optimal and suboptimal scheduling schemes obtain the full secrecy diversity, no matter whether the eavesdroppers collaborate or not. In addition, numerical secrecy outage results demonstrate that for both the coordinated and uncoordinated eavesdroppers, the optimal user scheduling achieves the best security performance and the round-robin scheduling performs the worst. Finally, upon increasing the number of CUs, the secrecy outage probabilities of the optimal and suboptimal user scheduling schemes both improve significantly.**

***Index Terms*—Cognitive radio, multi-user scheduling, secrecy outage probability, secrecy diversity, diversity order.**

I. Introduction

COGNITIVE radio is widely recognized as a dynamic spectrum access technique, which enables unlicensed users (also called secondary users or cognitive users) and licensed users (known as primary users) to share the same spectrum but with different priorities, where the primary users (PUs) have a higher priority than the cognitive users (CUs) in accessing the licensed spectrum [1]-[3]. In cognitive radio systems, CUs are typically allowed to detect whether or not the licensed spectrum is being used by PUs through spectrum sensing functionality and then to access the detected unused spectrum (referred to as spectrum hole) [4], [5]. Due to the dynamic nature of cognitive radio, various malicious devices may participate in the spectrum sensing and access, leading legitimate users to be exposed to both internal and external attacks [6]. For example, cognitive radio is supposed to be capable of adapting its operating parameters to any changes of its surrounding radio environment. However, a malicious attacker may intentionally modify the radio environment (e.g., by emitting interference) in which the cognitive radio operates, misleading legitimate CUs and even causing them to malfunction. Therefore, cognitive radio faces many new security challenges from all aspects of the networking architecture, including the spectrum sensing, spectrum access, and spectrum management.

Physical-layer security [7]-[9] is emerging as an effective means to protect the communications confidentiality against eavesdropping attacks by exploiting the physical characteristics (e.g., multipath fading, propagation delay, etc.) of wireless channels. It has been shown that if the wiretap channel (from source to eavesdropper) is inferior to the main channel (from source to destination), the source can reliably and securely transmit to the destination at a positive data rate (see [10] and reference therein). In [7], Wyner introduced the notation of secrecy capacity in a discrete memoryless wiretap channel and showed the secrecy capacity as the difference between the capacities of the main channel and wiretap channel. Later on, Wyner's results were extended to the Gaussian wiretap channel in [8] and wireless fading channels in [9] and [11], where the achievable rate-equivocation region was characterized from an information-theoretic perspective. It is noted that the secrecy capacity of wireless communications is limited and degraded due to the multipath fading effect. To this end, considerable research efforts were devoted to improving the wireless physical-layer security by employing the multiple-input multiple-output (MIMO) [12], artificial noise [13], [14] and beamforming techniques [15]-[17]. In addition, the joint artificial noise and beamforming design was investigated in [18] to enhance the wireless physical-layer security, where the artificial noise covariance and beamforming weights were jointly optimized with a target secrecy rate requirement. It was demonstrated that the joint artificial noise and beamforming approach further improves the wireless secrecy capacity.

As aforementioned, the physical-layer security is examined

Manuscript received December 20, 2013; revised April 25, 2014. This work was partially supported by the National Natural Science Foundation of China (Grant Nos. 61302104, 61271240, and 61125106), the Scientific Research Foundation of Nanjing University of Posts and Telecommunications (Grant Nos. NY213014 and NY214001), the 1311 Talent Program of Nanjing University of Posts and Telecommunications, the Natural Science Foundation of Jiangsu Province (Grant No. BK20140887), the Shaanxi Key Innovation Team of Science and Technology (Grant No. 2012KCT-04), and the Key Project of Natural Science Research of Higher Education Institutions of Jiangsu Province (Grant No. 14KJA510003).

Y. Zou is with the School of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, Jiangsu, P. R. China (e-mail: yulong.zou@njupt.edu.cn).

X. Li is with the Center for OPTical IMagery Analysis and Learning (OPTIMAL), State Key Laboratory of Transient Optics and Photonics, Xi'an Institute of Optics and Precision Mechanics, Chinese Academy of Sciences, Xi'an 710119, Shaanxi, P. R. China (e-mail: xuelong_li@opt.ac.cn).

Y.-C. Liang is with the Institute for Infocomm Research (I2R), Agency for Science, Technology & Research (A*STAR), Singapore (e-mail: liangyc@ieee.org). He is also with the University of Electronic Science and Technology of China (UESTC), Chengdu, China.

Digital Object Identifier 10.1109/JSAC.2014.141121.

extensively for conventional non-cognitive wireless networks [9]-[18], but is rarely studied for cognitive radio networks. The physical-layer security of cognitive transmissions was investigated in [19]-[21] where the achievable secrecy rates of the multiple-input single-output (MISO), MIMO and relay selection were developed for cognitive radio networks. More recently, in [22], we examined the physical-layer security with multi-user scheduling for cognitive radio networks in terms of the ergodic secrecy rate and intercept probability. In this paper, we explore the physical-layer security of a multi-user multi-eavesdropper (MUME) cognitive radio network, where the eavesdroppers may collaborate with each other or perform independently in intercepting the cognitive transmissions. This is different from the existing cognitive radio security works [19]-[22] in the following aspects. On the one hand, we examine the use of multi-user scheduling for improving the physical-layer security of cognitive transmissions, whereas multiple antennas or multiple relays are employed in [19]-[21] with the aid of antenna array design or relay selection. On the other hand, we are focused on the secrecy outage probability analysis of cognitive radio networks in the presence of both the uncoordinated and coordinated eavesdroppers, differing from our previous work [22], where the intercept probability of cognitive transmissions was analyzed for the uncoordinated eavesdroppers only. Notice that the intercept probability was defined in [22] as the probability that the capacity of the main channel falls below that of the wiretap channel. By contrast, the secrecy outage probability is the probability that the difference between the capacity of the main channel and that of the wiretap channel becomes less than a predefined secrecy rate (i.e., R_s). It can be observed that the intercept probability is just a special case of the secrecy outage probability with $R_s = 0$, showing that the secrecy outage probability to be studied in this paper is more general than the intercept probability analyzed in our previous work [22]. Technically speaking, it is much more challenging to obtain a closed-form expression of the secrecy outage probability than that of the intercept probability for cognitive radio networks, especially in the presence of coordinated eavesdroppers.

The following summarizes the main contributions of this paper. First, we propose the round-robin scheduling, optimal user scheduling and suboptimal user scheduling to protect the cognitive transmissions against the uncoordinated and coordinated eavesdroppers. The difference between the optimal and suboptimal scheduling schemes lies in that the optimal scheduling assumes the perfect CSI of all links from CUs to CBS, to PU and to eavesdroppers, whereas the suboptimal scheduling only needs the CSI of CUs-CBS links. Since the PU's and eavesdroppers' CSI is challenging to obtain at CUs in practical systems, the suboptimal user scheduling scheme is more attractive than the optimal user scheduling from this perspective, although the latter scheme may achieve a better security performance. Second, we derive closed-form expressions of the secrecy outage probability for the round-robin scheduling as well as the optimal and suboptimal user scheduling schemes with a PU's QoS constraint for both the uncoordinated and coordinated eavesdroppers. Last, we characterize the secrecy diversity orders of these three schemes through an asymptotic secrecy outage analysis and show that no matter whether the eavesdroppers collaborate or not, the round-robin scheduling achieves the diversity order of only one, whereas the optimal and suboptimal user scheduling schemes obtain the diversity order of M, where M is the number of CUs.

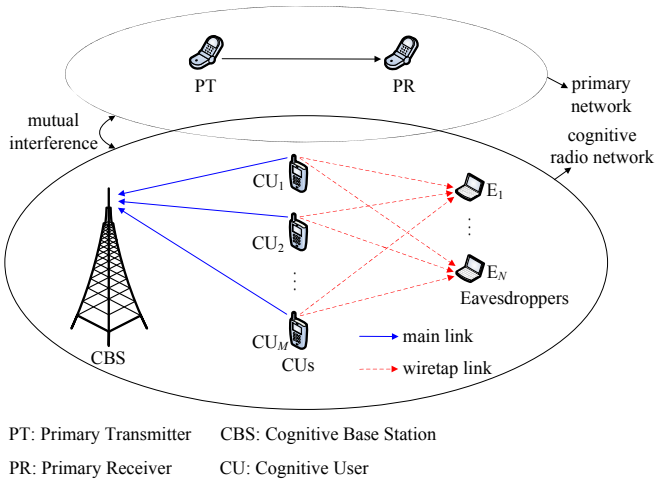

Fig. 1. A multi-user multi-eavesdropper (MUME) cognitive radio network coexists with a primary network.

The remainder of this paper is organized as follows. We first present the system model of a MUME cognitive radio network in Section II. Then, Section III proposes the round-robin scheduling, the optimal user scheduling and the suboptimal user scheduling in the presence of multiple uncoordinated and coordinated eavesdroppers. The closed-form secrecy outage expressions of various user scheduling schemes are also derived for both the uncoordinated and coordinated eavesdroppers. Next, in Section IV, we carry out the secrecy diversity analysis of the round-robin scheduling as well as the optimal and suboptimal scheduling schemes, followed by Section V, where numerical secrecy outage results of these three schemes are provided. Finally, some concluding remarks are drawn in Section VI.

II. System Model and Problem Formulation

As shown in Fig. 1, a multi-user multi-eavesdropper cognitive radio network consisting of one CBS, M CUs and N eavesdroppers shares the spectrum that is licensed to a primary network including one PT and one PR. Throughout this paper, we consider the use of underlay spectrum sharing, i.e., a CU and a PT are allowed to transmit simultaneously over the same spectrum, as long as the interference caused by CU is tolerable at PR and the quality of service (QoS) of PT-PR transmission is unaffected. We consider that PT transmits to PR without power control and a maximum interference power I is assumed to be tolerable at PR without affecting its QoS. This means that the interference received at PR from CU_i must be less than the maximum tolerable level I for the sake of protecting the primary QoS. Considering that CU_i transmits to CBS over the same spectrum band as the PT, we shall limit the transmit power of CU_i denoted by P_i as

$$P_i = \frac{I}{|h_{ip}|^2}, \tag{1}$$

where h_{ip} represents the fading coefficient of the CU_i-PR channel. It is pointed out that the simple power control model given by (1) is widely used in literature [23]-[25] for characterizing the underlay cognitive radio. As shown in (1), the transmit power of CU_i is a function of the random fading $|h_{ip}|^2$, which makes the closed-form secrecy outage probability analysis of the cognitive transmissions become more challenging. Considering a maximum power constraint P, the transmit power of CU_i may be modeled as $P_i = \min(\frac{I}{|h_{ip}|^2}, P)$. Since only a constant P is introduced in this model, it will not result in any additional challenges in the secrecy outage analysis and, moreover, no new insight into the secrecy outage probability will be provided, as compared to the power control model of (1). Thus, we consider the use of (1) in modeling the CU_i's transmit power throughout this paper. In Fig. 1, M CUs transmit their data packets to CBS, which is a typical uplink transmission scenario in cognitive radio networks [2]. Meanwhile, there are N eavesdroppers in the cognitive radio network, which attempt to intercept the packets transmitted from CUs to CBS. For notational convenience, we denote M CUs and N eavesdroppers by $\mathcal{U} = \{\mathrm{CU}_i | i = 1, 2, \cdots, M\}$ and $\mathcal{E} = \{\mathrm{E}_j | j = 1, 2, \cdots, N\}$, respectively.

In addition, when a CU and a PT simultaneously transmit to their respective destination nodes, PT also causes an interference to CBS in decoding the CU's signal. Following [23] and [26], the interference received at CBS from PT is considered to be a complex Gaussian random variable under an assumption that the primary signal may be generated by the random Gaussian codebook. Moreover, the thermal noise at CBS is also complex Gaussian distributed. Thus, the interference plus noise at CBS, denoted by n_b, can be modeled as a complex Gaussian random variable with zero mean and variance N_b, which is represented by $n_b \sim \mathcal{CN}(0, N_b)$. Similarly, we can also model the interference plus noise received at an eavesdropper E_j, denoted by n_{e_j}, as a complex Gaussian random variable i.e. $n_{e_j} \sim \mathcal{CN}(0, N_{e_j})$. In the cognitive radio network shown in Fig. 1, M CUs may access the licensed band and transmit to CBS using an orthogonal multiple access method e.g. the orthogonal frequency division multiple access (OFDMA). Generally speaking, the licensed band is first divided into multiple subchannels which are then assigned to M CUs. Given a subchannel, we may need to determine which CU should be selected to access the subchannel, which will be discussed in the following Section III. Without loss of generality, considering that CU_i transmits its signal x_i to CBS with power P_i, we can express the received signal at CBS as

$$y_{ib} = \sqrt{\frac{I}{|h_{ip}|^2}} h_{ib} x_i + n_b, \tag{2}$$

where h_{ib} is the fading coefficient of the channel from CU_i to CBS and $n_b \sim \mathcal{CN}(0, N_b)$ represents the interference and thermal noise received at CBS. Using the Shannon's channel capacity formula, the capacity of the main channel from CU_i to CBS can be obtained from (2) as

$$C_{ib} = \log_2(1 + \frac{I|h_{ib}|^2}{|h_{ip}|^2 N_b}). \tag{3}$$

Meanwhile, due to the broadcast nature of radio propagation, the CU_i-CBS transmission may also be overheard by N eavesdroppers. Thus, the signal received at an eavesdropper E_j can be written as

$$y_{ie_j} = \sqrt{\frac{I}{|h_{ip}|^2}} h_{ie_j} x_i + n_{e_j}, \tag{4}$$

where h_{ie_j} is the fading coefficient of the channel from CU_i to E_j and $n_{e_j} \sim \mathcal{CN}(0, N_{e_j})$ represents the interference and thermal noise received at eavesdropper E_j. Similarly to (3), the capacity of the wiretap channel from CU_i to E_j is obtained from (4) as

$$C_{ie_j} = \log_2(1 + \frac{I|h_{ie_j}|^2}{|h_{ip}|^2 N_{e_j}}). \tag{5}$$

In this paper, we consider two eavesdropping scenarios: 1) uncoordinated case, where the eavesdroppers are independent of each other in intercepting the CU_i-CBS transmission; and 2) coordinated case, where the eavesdroppers collaborate for intercepting the cognitive transmissions. In the uncoordinated case, the eavesdroppers perform the interception independently and the CU_i-CBS transmission is secure when all N eavesdroppers fail to decode the signal x_i. Thus, the overall capacity of the wiretap channel from CU_i to N eavesdroppers can be given by the maximum of individual achievable rates at N eavesdroppers, yielding

$$C_{ie} = \max_{e_j \in \mathcal{E}} C_{ie_j} = \max_{e_j \in \mathcal{E}} \log_2(1 + \frac{I|h_{ie_j}|^2}{|h_{ip}|^2 N_{e_j}}), \tag{6}$$

for the uncoordinated case, where $\mathcal{E}$ denotes the set of N eavesdroppers. In the coordinated case, N eavesdroppers first combine their received signals to obtain an enhanced version for the sake of improving the possibility of successfully decoding the signal x_i. Considering the maximal ratio combining (MRC) and using (4), we obtain a combined version of the received signals at N eavesdroppers as

$$y_{ie} = \sum_{e_j \in \mathcal{E}} \sqrt{\frac{I}{|h_{ip}|^2}} |h_{ie_j}|^2 x_i + \sum_{e_j \in \mathcal{E}} h^*_{ie_j} n_{e_j},$$

from which the overall capacity of the wiretap channel from CU_i to N eavesdroppers is given by

$$C_{ie} = \log_2[1 + \frac{I(\sum\limits_{e_j \in \mathcal{E}} |h_{ie_j}|^2)^2}{|h_{ip}|^2 \sum\limits_{e_j \in \mathcal{E}} (|h_{ie_j}|^2 N_{e_j})}], \tag{7}$$

for the coordinated case. As discussed in [8] and [9], the secrecy capacity of wireless transmissions is shown as the difference between the capacity of the main channel and that of the wiretap channel. Thus, we can obtain the secrecy capacity of CU_i-CBS transmission in the presence of N eavesdroppers as

$$C_i^s = C_{ib} - C_{ie}, \tag{8}$$

where C_{ib} is given by (3) and C_{ie} is characterized by (6) and (7) for the uncoordinated and coordinated cases, respectively. Additionally, all the wireless channels shown in Fig. 1 (i.e., h_{ip}, h_{ib} and h_{ie_j}) are characterized with the Rayleigh fading model. The average channel gains of $|h_{ip}|^2$, $|h_{ib}|^2$ and $|h_{ie_j}|^2$ are denoted by σ^2_{ip}, σ^2_{ib} and $\sigma^2_{ie_j}$, respectively. Moreover,

although only the Rayleigh fading model is considered in this paper, similar performance analysis can be obtained for other fading channel models (e.g., Nakagami model).

III. Multi-user Scheduling Schemes and Secrecy Outage Analysis

In this section, we present several multi-user scheduling schemes including the round-robin scheduling, the optimal user scheduling, and the suboptimal user scheduling in the presence of the uncoordinated and coordinated eavesdroppers. The optimal user scheduling is aimed to maximize the secrecy capacity of the cognitive transmissions from CUs to CBS, assuming that the CSIs of all CUs-CBS, CUs-PR, and CUs-E$_j$ links are available. By contrast, the suboptimal user scheduling only assumes that the CSIs of CUs-CBS links are known, attempting to address the multi-user scheduling without the PR's and eavesdroppers' CSI knowledge. The closed-form secrecy outage probability expressions of the round-robin scheduling as well as the optimal and suboptimal scheduling are also derived for both the uncoordinated and coordinated eavesdroppers.

A. Round-Robin Scheduling

This subsection presents the conventional round-robin scheduling as a benchmark. With the round-robin scheduling, M CUs take turns in accessing the licensed spectrum and thus each user has an equal chance to transmit its signal to CBS. As is known, a secrecy outage event occurs when the secrecy capacity drops below a predefined secrecy rate R_s. Thus, given that CU$_i$ transmits to CBS, the secrecy outage probability of CU$_i$-CBS transmission is obtained as

$$P_{out,i} = \Pr\left(C_i^s < R_s\right), \tag{9}$$

where C_i^s is given by (8). Substituting (3) and (6) into (8) and combining with (9) yield

$$P_{out,i} = \Pr\left(\max_{e_j\in\mathcal{E}} \frac{|h_{ie_j}|^2}{N_{e_j}} > \frac{1}{2^{R_s}N_b}|h_{ib}|^2 - \frac{2^{R_s}-1}{2^{R_s}I}|h_{ip}|^2\right), \tag{10}$$

for the uncoordinated case, which is further obtained as (see Appendix A)

$$P_{out,i} = \frac{\sigma_{ip}^2(2^{R_s}-1)N_b + \sum\limits_{n=1}^{2^N-1} \frac{(-1)^{|\mathcal{E}_n|+1}2^{R_s}N_bI}{\sigma_{ib}^{-2}2^{R_s}N_b + \sum\limits_{e_j\in\mathcal{E}_n}(\sigma_{ie_j}^{-2}N_{e_j})}}{\sigma_{ib}^2I + \sigma_{ip}^2(2^{R_s}-1)N_b}, \tag{11}$$

where N is the number of eavesdroppers, $\mathcal{E}_n$ represents the n-th non-empty subset of the elements of $\mathcal{E}$, and $|\mathcal{E}_n|$ is the cardinality of set $\mathcal{E}_n$. Additionally, it is observed from (7) that obtaining a general closed-form expression of the secrecy outage probability $P_{out,i}$ for the coordinated case is challenging. For simplicity, we assume that the fading coefficients of all CU$_i$-E$_j$ channels $|h_{ie_j}|^2$ are independent and identically distributed (i.i.d.) random variables for different eavesdroppers with the same average channel gain denoted by $\sigma_{ie}^2 = E(|h_{ie_j}|^2)$. This assumption is widely used and valid in a statistical sense when all eavesdroppers are uniformly distributed around CUs. Moreover, proceeding as Appendix A and assuming that different eavesdroppers have the same noise variance of $N_{e_j} = N_e$, we can obtain the secrecy outage probability $P_{out,i}$ from (7), (8) and (9) as

$$P_{out,i} = 1 - \frac{\sigma_{ib}^2 I}{\sigma_{ib}^2 I + \sigma_{ip}^2(2^{R_s}-1)N_b}\left(1 + \frac{2^{R_s}\sigma_{ie}^2 N_b}{\sigma_{ib}^2 N_e}\right)^{-N}, \tag{12}$$

for the coordinated case. As aforementioned, the round-robin scheduling scheme allows M CUs to take turns in accessing the licensed spectrum and thus the secrecy outage probability of the round-robin scheduling is the mean of M CUs' secrecy outage probabilities, yielding

$$P_{out}^{round} = \frac{1}{M}\sum_{i=1}^{M} P_{out,i}, \tag{13}$$

where M is the number of CUs and $P_{out,i}$ is given by (11) and (12) for the uncoordinated and coordinated cases, respectively.

B. Optimal User Scheduling

In this subsection, we propose an optimal user scheduling scheme for the sake of improving the security of the CUs-CBS transmissions. Considering M CUs available in the cognitive radio network, a CU with the highest secrecy capacity is selected to access a given spectrum band. Therefore, using (8), we can express the optimal user scheduling criterion as

$$\text{Optimal User} = \arg\max_{i\in\mathcal{U}} C_i^s, \tag{14}$$

where $\mathcal{U}$ represents the set of CUs. Substituting (3) and (6) into (14) gives

$$\text{Optimal User} = \arg\max_{i\in\mathcal{U}} \left(\frac{|h_{ip}|^2 + I|h_{ib}|^2 N_b^{-1}}{|h_{ip}|^2 + I\max\limits_{e_j\in\mathcal{E}}|h_{ie_j}|^2 N_{e_j}^{-1}}\right), \tag{15}$$

for the uncoordinated case. Moreover, substituting (3) and (7) into (14) yields

$$\text{Optimal User} = \arg\max_{i\in\mathcal{U}} \left(\frac{|h_{ip}|^2 + I|h_{ib}|^2 N_b^{-1}}{|h_{ip}|^2 + \frac{I(\sum\limits_{e_j\in\mathcal{E}}|h_{ie_j}|^2)^2}{\sum\limits_{e_j\in\mathcal{E}}(|h_{ie_j}|^2 N_{e_j})}}\right), \tag{16}$$

for the coordinated case. One can observe from (15) and (16) that the CSIs $|h_{ib}|^2$, $|h_{ip}|^2$ and $|h_{ie_j}|^2$ of the CU$_i$-CBS, CU$_i$-PR and CU$_i$-E$_j$ links as well as the number of eavesdroppers N and the noise variance N_{e_j} are assumed in determining the optimal user among M CUs. However, the PR's and eavesdroppers' CSIs, the number of eavesdroppers, and the noise variance may be unavailable in some cases. To this end, the following subsection will consider the multi-user scheduling without the need of these information. Using (14), the secrecy outage probability of the proposed optimal user scheduling scheme can be obtained as

$$P_{out}^{optimal} = \Pr\left(\max_{i\in\mathcal{U}} C_i^s < R_s\right) = \prod_{i\in\mathcal{U}} \Pr\left(C_i^s < R_s\right), \tag{17}$$

where C_i^s is given by (8). Combining (9) and (17), we obtain the secrecy outage probability of the optimal scheduling as

$$P_{out}^{optimal} = \prod_{i\in\mathcal{U}} P_{out,i}, \tag{18}$$

where $P_{out,i}$ is given by (11) and (12) for the uncoordinated and coordinated cases, respectively.

C. Suboptimal User Scheduling

This subsection proposes a suboptimal user scheduling scheme under the condition that only the CSIs of CUs-CBS channels are available without knowing the CSI knowledge of the primary receiver and eavesdroppers. Since only the CSIs of CUs-CBS channels are known in this case, a CU with the highest instantaneous fading gain to CBS is typically regarded as the optimal user, yielding

$$\text{Optimal User} = \arg\max_{i\in\mathcal{U}} |h_{ib}|^2, \tag{19}$$

where $\mathcal{U}$ represents the set of M CUs. It is observed from (19) that only $|h_{ib}|^2$ is needed in the suboptimal user scheduling scheme without the PR's and eavesdroppers' CSIs $|h_{ip}|^2$ and $|h_{ie_j}|^2$. This is different from the aforementioned optimal user scheduling scheme which requires the CSIs of all CU$_i$-CBS, CU$_i$-PR and CU$_i$-E$_j$ channels (i.e., $|h_{ib}|^2$, $|h_{ip}|^2$, and $|h_{ie_j}|^2$). For notational convenience, let 'o' denote the optimal user determined by (19). Thus, the secrecy capacity of the transmission from the optimal user (o) to CBS in the presence of N uncoordinated eavesdroppers is obtained as

$$C_o^s = C_{ob} - \max_{e_j\in\mathcal{E}} C_{oe_j}, \tag{20}$$

where C_{ob} and C_{oe_j}, respectively, represent the channel capacities from the optimal user to CBS and to eavesdropper E$_j$, which are given by

$$C_{ob} = \log_2(1 + \frac{|h_{ob}|^2 I}{|h_{op}|^2 N_b}), \tag{21}$$

and

$$C_{oe_j} = \log_2(1 + \frac{|h_{oe_j}|^2 I}{|h_{op}|^2 N_{e_j}}), \tag{22}$$

where $|h_{ob}|^2$, $|h_{op}|^2$, and $|h_{oe_j}|^2$ represent fading coefficients of the channels from the optimal user to CBS, to PR, and to eavesdropper E$_j$, respectively. Combining (20)-(22), we obtain the secrecy outage probability of the proposed suboptimal user scheduling scheme as

$$\begin{aligned} P_{out}^{sub} &= \Pr\left(C_o^s < R_s\right) \\ &= \Pr\left(2^{R_s} I \max_{e_j\in\mathcal{E}} \frac{|h_{oe_j}|^2}{N_{e_j}} > \frac{I}{N_b}|h_{ob}|^2 - (2^{R_s}-1)|h_{op}|^2\right), \end{aligned} \tag{23}$$

for the uncoordinated case. By using the law of total probability and denoting $t = \frac{I}{N_b}|h_{ib}|^2 - (2^{R_s}-1)|h_{ip}|^2$, (23) is rewritten as

$$P_{out}^{sub} = \sum_{i=1}^{M} \Pr\left(2^{R_s} I \max_{e_j\in\mathcal{E}} \frac{|h_{ie_j}|^2}{N_{e_j}} > t,\ o = i\right). \tag{24}$$

Combining (19) and (24), we have

$$P_{out}^{sub} = \sum_{i=1}^{M} \Pr\left(\begin{array}{c} 2^{R_s} I \max\limits_{e_j\in\mathcal{E}} \frac{|h_{ie_j}|^2}{N_{e_j}} > t, \\ \max\limits_{\substack{k\in\mathcal{U}\\ k\neq i}} |h_{kb}|^2 < |h_{ib}|^2 \end{array}\right). \tag{25}$$

By using the result of Appendix B, the secrecy outage probability P_{out}^{sub} is obtained from (25) as

$$\begin{aligned} P_{out}^{sub} =& \sum_{i=1}^{M}\sum_{n=1}^{2^N-1} (-1)^{|\mathcal{E}_n|+1}\left(P_{out,I}^{sub} - P_{out,II}^{sub}\right) \\ &+ \sum_{i=1}^{M} P_{out,III}^{sub}, \end{aligned} \tag{26}$$

for the uncoordinated case, where $\mathcal{E}_n$ represents the n-th non-empty subset of the elements of $\mathcal{E}$, $P_{out,I}^{sub}$, $P_{out,II}^{sub}$ and $P_{out,III}^{sub}$ are given by (B.11)-(B.12), (B.13)-(B.14) and (B.15) respectively. The following presents the secrecy outage probability analysis of the suboptimal user scheduling for the coordinated eavesdroppers. As mentioned earlier in Section III-A, it is challenging to obtain a general closed-form expression of the secrecy outage probability for the coordinated case. We here consider that the fading coefficients $|h_{ie_j}|^2$ for $e_j \in \mathcal{E}$ are i.i.d. with the same mean of σ_{ie}^2 and different eavesdroppers have the same noise variance of N_e. Hence, substituting $N_{e_j} = N_e$ into (7) and using the law of total probability, we obtain the secrecy outage probability P_{out}^{sub} of the suboptimal user scheduling as (27) for the coordinated case, which is further given by (see Appendix C)

$$P_{out}^{sub} = \sum_{i=1}^{M} (P_{out,I} + P_{out,II} + P_{out,III}), \tag{28}$$

where $P_{out,I}$, $P_{out,II}$ and $P_{out,III}$ are given by (C.13), (C.14) and (C.15), respectively. So far, we have derived closed-form secrecy outage expressions for the round-robin scheduling as well as the optimal and suboptimal scheduling schemes in the presence of the uncoordinated and coordinated eavesdroppers, which will be used in Section V for conducting numerical evaluation of the secrecy outage performance.

IV. Secrecy Diversity Analysis

In this section, we analyze the secrecy diversity performance of multi-user cognitive transmissions in the presence of multiple uncoordinated and coordinated eavesdroppers. Although the closed-form secrecy outage expressions shown in (13), (18), (26) and (28) can be used to show the transmission security performance of various user scheduling schemes, they fail to provide an intuitive insight into the impact of the number of CUs and eavesdroppers on the cognitive transmission security. As a consequence, this section presents the secrecy diversity analysis of the round-robin scheduling as well as the optimal and suboptimal scheduling schemes.

A. Round-Robin Scheduling

Let us consider the round-robin scheduling as a baseline for comparison. First, the cognitive radio transmission is subject

$$P_{out}^{sub}=\sum_{i=1}^{M}\Pr\left(\sum_{e_j\in\mathcal{E}}|h_{ie_j}|^2>\frac{N_e}{2^{R_s}N_b}|h_{ib}|^2-\frac{(2^{R_s}-1)N_e}{2^{R_s}I}|h_{ip}|^2,\max_{\substack{k\in\mathcal{U}\\k\neq i}}|h_{kb}|^2<|h_{ib}|^2\right) \tag{27}$$

to the primary QoS constraint i.e. the maximum tolerable interference level at PR I. Generally speaking, with an increasing I, the secrecy outage probability of cognitive transmissions decreases accordingly. From (11) and (13), we obtain

$$\lim_{I\to\infty}P_{out}^{round}=\frac{1}{M}\sum_{i=1}^{M}\sum_{n=1}^{2^N-1}\frac{(-1)^{|\mathcal{E}_n|+1}2^{R_s}N_b}{2^{R_s}N_b+\sum\limits_{e_j\in\mathcal{E}_n}\sigma_{ib}^2\sigma_{ie_j}^{-2}N_{e_j}}, \tag{29}$$

for the uncoordinated case. One can observe from (29) that as the maximum tolerable interference level I tends to infinity, the secrecy outage probability of the round-robin scheduling scheme converges to a non-zero constant. From (1), an infinite I means that the transmit power of CUs approaches infinity. Hence, as the CUs' transmit power increases to infinity, a secrecy outage probability floor occurs. Notice that the secrecy outage floor provides a lower bound on the secrecy outage probability that a cognitive radio system can achieve with high interference temperature. It is also meaningful and effective to employ the secrecy outage floor as a metric to evaluate the security performance of different signal processing techniques in a cognitive radio system. For notational convenience, the secrecy outage floor of the round-robin scheduling scheme is denoted by $P_{out,floor}^{round}$, i.e., $P_{out,floor}^{round}=\lim\limits_{I\to\infty}P_{out}^{round}$. Denoting $\sigma_{ib}^2=\theta_{ib}\sigma_m^2$ and $\sigma_{ie_j}^2=\theta_{ie_j}\sigma_e^2$, where σ_m^2 and σ_e^2, respectively, represent the reference channel gain of the main links from CUs to CBS and that of the wiretap links from CUs to eavesdroppers, we may obtain the secrecy outage floor of the round-robin scheduling scheme from (29) as

$$P_{out,floor}^{round}=\frac{1}{M}\sum_{i=1}^{M}\sum_{n=1}^{2^N-1}\frac{(-1)^{|\mathcal{E}_n|+1}2^{R_s}N_b}{2^{R_s}N_b+\lambda_{me}\sum\limits_{e_j\in\mathcal{E}_n}\theta_{ib}\theta_{ie_j}^{-1}N_{e_j}}, \tag{30}$$

for the uncoordinated case, where $\lambda_{me}=\sigma_m^2/\sigma_e^2$ is called the main-to-eavesdropper ratio (MER). The traditional diversity gain is defined in [27] as

$$d=-\lim_{\mathrm{SNR}\to\infty}\frac{\log P_e(\mathrm{SNR})}{\log \mathrm{SNR}},$$

where SNR stands for the signal-to-noise ratio and $P_e(\mathrm{SNR})$ represents the bit error rate as a function of SNR. However, as the CUs' transmit power increases to infinity, the secrecy outage probability of (30) tends to a non-zero constant, which makes the traditional diversity definition become inappropriate for the secrecy outage analysis. It is also observed from (30) that with an infinite transmit power, the secrecy outage probability becomes nothing to do with the CUs-PR channel h_{ip} and is mainly determined by the main channel h_{ib} and eavesdropping channel h_{ie_j}. Motivated by this observation, we here define a secrecy diversity gain as an asymptotic ratio of the logarithmic secrecy outage floor to the logarithmic MER λ_{me} (i.e., the ratio between the reference gains of the main channel and eavesdropping channel) as $\lambda_{me}\to\infty$ [28], yielding

$$d_{round}=-\lim_{\lambda_{me}\to\infty}\frac{\log(P_{out,floor}^{round})}{\log(\lambda_{me})}, \tag{31}$$

which, in turn, results in the secrecy outage floor $P_{out,floor}^{round}$ behaving as $\lambda_{me}^{-d_{round}}$ in high MER region. This also shows that as MER increases, the secrecy outage floor $P_{out,floor}^{round}$ decreases faster with a higher diversity order d_{round}. Therefore, the secrecy diversity order can be used as a simple but effective metric to evaluate the secrecy outage floor performance, especially in high MER region. Substituting (30) into (31), we obtain the secrecy diversity of the round-robin scheduling scheme as

$$d_{round}=1, \tag{32}$$

for the uncoordinated case, which shows that the secrecy diversity order of only one is achieved by the round-robin scheduling scheme, when the eavesdroppers are independent of each other in intercepting the cognitive transmissions. In what follows, we analyze the secrecy diversity of the round-robin scheduling for the coordinated case. Noting $N_{e_j}>0$ and using the inequality $\min\limits_{e_j\in\mathcal{E}}N_{e_j}\sum\limits_{e_j\in\mathcal{E}}|h_{ie_j}|^2\le\sum\limits_{e_j\in\mathcal{E}}|h_{ie_j}|^2N_{e_j}\le\max\limits_{e_j\in\mathcal{E}}N_{e_j}\sum\limits_{e_j\in\mathcal{E}}|h_{ie_j}|^2$ into (7), we have

$$\log_2(1+\frac{I\sum\limits_{e_j\in\mathcal{E}}|h_{ie_j}|^2}{|h_{ip}|^2\max\limits_{e_j\in\mathcal{E}}N_{e_j}})\le C_{ie}\le\log_2(1+\frac{I\sum\limits_{e_j\in\mathcal{E}}|h_{ie_j}|^2}{|h_{ip}|^2\min\limits_{e_j\in\mathcal{E}}N_{e_j}}), \tag{33}$$

which may be further given by

$$\log_2(1+\frac{I\max\limits_{e_j\in\mathcal{E}}|h_{ie_j}|^2}{|h_{ip}|^2\max\limits_{e_j\in\mathcal{E}}N_{e_j}})\le C_{ie}\le\log_2(1+\frac{NI\max\limits_{e_j\in\mathcal{E}}|h_{ie_j}|^2}{|h_{ip}|^2\min\limits_{e_j\in\mathcal{E}}N_{e_j}}), \tag{34}$$

which is obtained by using the inequality $\max\limits_{e_j\in\mathcal{E}}|h_{ie_j}|^2\le\sum\limits_{e_j\in\mathcal{E}}|h_{ie_j}|^2\le N\max\limits_{e_j\in\mathcal{E}}|h_{ie_j}|^2$, where N is the number of eavesdroppers. Combining (33) and (34) with (9), we have

$$P_{out,i}^{lower}\le P_{out,i}\le P_{out,i}^{upper}, \tag{35}$$

where the lower and upper bounds $P_{out,i}^{lower}$ and $P_{out,i}^{upper}$ are given by

$$P_{out,i}^{lower}=\Pr\left(\begin{array}{r}\max\limits_{e_j\in\mathcal{E}}\dfrac{|h_{ie_j}|^2}{\max\limits_{e_j\in\mathcal{E}}N_{e_j}}>\dfrac{1}{2^{R_s}N_b}|h_{ib}|^2\\-\dfrac{2^{R_s}-1}{2^{R_s}I}|h_{ip}|^2\end{array}\right), \tag{36}$$

and

$$P_{out,i}^{upper}=\Pr\left(\begin{array}{r}N\max\limits_{e_j\in\mathcal{E}}\dfrac{|h_{ie_j}|^2}{\min\limits_{e_j\in\mathcal{E}}N_{e_j}}>\dfrac{1}{2^{R_s}N_b}|h_{ib}|^2\\-\dfrac{2^{R_s}-1}{2^{R_s}I}|h_{ip}|^2\end{array}\right), \tag{37}$$

for the coordinated case. Comparing (36) and (37) with (10) and using (30), we readily obtain

$$\lim_{I\to\infty} P_{out,i}^{lower} = \sum_{n=1}^{2^N-1} \frac{(-1)^{|\mathcal{E}_n|+1} 2^{R_s} N_b}{2^{R_s} N_b + \lambda_{me} \sum\limits_{e_j\in\mathcal{E}_n} \theta_{ib}\theta_{ie_j}^{-1} \max\limits_{e_j\in\mathcal{E}} N_{e_j}}, \tag{38}$$

and

$$\lim_{I\to\infty} P_{out,i}^{upper} = \sum_{n=1}^{2^N-1} \frac{(-1)^{|\mathcal{E}_n|+1} 2^{R_s} N_b}{2^{R_s} N_b + \lambda_{me} \sum\limits_{e_j\in\mathcal{E}_n} \theta_{ib}\theta_{ie_j}^{-1} N^{-1} \min\limits_{e_j\in\mathcal{E}} N_{e_j}}. \tag{39}$$

Combining (38) and (39) with (13) yields

$$\frac{1}{M}\sum_{i=1}^{M} \lim_{I\to\infty} P_{out,i}^{lower} \le P_{out,floor}^{round} \le \frac{1}{M}\sum_{i=1}^{M} \lim_{I\to\infty} P_{out,i}^{upper}, \tag{40}$$

for the coordinated case. Substituting (40) into (31) and using (38) and (39) give

$$1 \le d_{round} \le 1, \tag{41}$$

which can be further obtained from the squeeze theorem as

$$d_{round} = 1, \tag{42}$$

for the coordinated case. As shown in (32) and (42), no matter whether the eavesdroppers collaborate or not, the round-robin scheduling scheme always achieves the diversity order of only one. This also means that the round-robin scheme fails to achieve any secrecy diversity benefits with multiple CUs.

B. Optimal User Scheduling

This subsection analyzes the secrecy diversity order of the proposed optimal user scheduling scheme. Using (18) and letting $I \to \infty$, we obtain the secrecy outage floor of the optimal user scheduling scheme as

$$P_{out,floor}^{optimal} = \prod_{i\in\mathcal{U}} \lim_{I\to\infty} P_{out,i}, \tag{43}$$

where $\lim\limits_{I\to\infty} P_{out,i}$ is further computed from (11) as

$$\lim_{I\to\infty} P_{out,i} = \sum_{n=1}^{2^N-1} \frac{(-1)^{|\mathcal{E}_n|+1} 2^{R_s} N_b}{2^{R_s} N_b + \lambda_{me} \sum\limits_{e_j\in\mathcal{E}_n} \theta_{ib}\theta_{ie_j}^{-1} N_{e_j}}, \tag{44}$$

for the uncoordinated case, where N is the number of eavesdroppers, $\theta_{ib} = \sigma_{ib}^2/\sigma_m^2$, $\theta_{ie_j} = \sigma_{ie_j}^2/\sigma_e^2$, and $\lambda_{me} = \sigma_m^2/\sigma_e^2$. Substituting (44) into (43) gives

$$P_{out,floor}^{optimal} = \prod_{i\in\mathcal{U}} \left[\sum_{n=1}^{2^N-1} \frac{(-1)^{|\mathcal{E}_n|+1} 2^{R_s} N_b}{2^{R_s} N_b \lambda_{me}^{-1} + \sum\limits_{e_j\in\mathcal{E}_n} \theta_{ib}\theta_{ie_j}^{-1} N_{e_j}} \right] \cdot \left(\frac{1}{\lambda_{me}}\right)^M, \tag{45}$$

where M is the number of CUs. Similarly to (31), the secrecy diversity order of the optimal user scheduling scheme is defined as

$$d_{optimal} = -\lim_{\lambda_{me}\to\infty} \frac{\log(P_{out,floor}^{optimal})}{\log(\lambda_{me})}. \tag{46}$$

Substituting (45) into (46) yields

$$d_{optimal} = M, \tag{47}$$

for the uncoordinated case, which demonstrates that the secrecy diversity order of M is achieved by the optimal scheduling scheme when the eavesdroppers are independent of each other in tapping the cognitive transmissions. Similarly to (40), we may obtain the secrecy outage floor of the optimal user scheduling as

$$\prod_{i\in\mathcal{U}} \lim_{I\to\infty} P_{out,i}^{lower} \le P_{out,floor}^{optimal} \le \prod_{i\in\mathcal{U}} \lim_{I\to\infty} P_{out,i}^{upper}, \tag{48}$$

for the coordinated case, where $\lim\limits_{I\to\infty} P_{out,i}^{lower}$ and $\lim\limits_{I\to\infty} P_{out,i}^{upper}$ are given by (38) and (39), respectively. Substituting (48) into (46), we have

$$M \le d_{optimal} \le M, \tag{49}$$

from which the secrecy diversity of the optimal user scheduling scheme is readily obtained as

$$d_{optimal} = M, \tag{50}$$

for the coordinated case. It is seen from (47) and (50) that for both the uncoordinated and coordinated eavesdroppers, the optimal user scheduling achieves the diversity order of M. This can also be interpreted as that the secrecy outage probability floor of the optimal user scheduling behaves as $(\frac{1}{\lambda_{me}})^M$ in high MER region. Therefore, with an increasing number of CUs, the secrecy outage floor of the optimal user scheduling decreases significantly, showing its advantage over the round-robin scheduling scheme.

C. Suboptimal User Scheduling

This subsection is focused on the secrecy diversity analysis of the suboptimal user scheduling scheme. Let us first analyze the secrecy outage floor of the suboptimal user scheduling with an infinite I. From (25), we obtain (51) at the top of the following page for the uncoordinated case. Considering that $|h_{ie_j}|^2$ and $|h_{kb}|^2$ are independent exponentially distributed random variables with respective means $\sigma_{ie_j}^2$ and σ_{kb}^2 and denoting $|h_{ib}|^2 = x$, we can equivalently rewrite (51) as

$$P_{out,floor}^{sub} = \sum_{i=1}^{M} \int_0^\infty \left[1 - \prod_{e_j\in\mathcal{E}} \left(1 - \exp(-\frac{N_{e_j} x}{\sigma_{ie_j}^2 2^{R_s} N_b})\right)\right] \times \prod_{\substack{k\in\mathcal{U}\\ k\neq i}} \left(1 - \exp(-\frac{x}{\sigma_{kb}^2})\right) \frac{1}{\sigma_{ib}^2} \exp(-\frac{x}{\sigma_{ib}^2}) dx. \tag{52}$$

Using the binomial theorem, $\prod\limits_{e_j\in\mathcal{E}} \left(1 - \exp(-\frac{N_{e_j} x}{\sigma_{ie_j}^2 2^{R_s} N_b})\right)$ can be expanded as

$$\prod_{e_j\in\mathcal{E}} \left(1 - \exp(-\frac{N_{e_j} x}{\sigma_{ie_j}^2 2^{R_s} N_b})\right) = 1 - \sum_{n=1}^{2^N-1} (-1)^{|\mathcal{E}_n|+1} \exp(-\sum_{e_j\in\mathcal{E}_n} \frac{N_{e_j} x}{\sigma_{ie_j}^2 2^{R_s} N_b}), \tag{53}$$

$$P_{out,floor}^{sub} = \lim_{I\to\infty} P_{out}^{sub} = \sum_{i=1}^{M} \Pr\left(2^{R_s} \max_{e_j\in\mathcal{E}} \frac{|h_{ie_j}|^2}{N_{e_j}} > \frac{1}{N_b}|h_{ib}|^2, \ \max_{\substack{k\in\mathcal{U}\\ k\neq i}} |h_{kb}|^2 < |h_{ib}|^2 \right) \tag{51}$$

where $\mathcal{E}_n$ represents the n-th non-empty subset of the elements of $\mathcal{E}$. Substituting (53) into (52) yields

$$\begin{aligned} P_{out,floor}^{sub} = & \sum_{i=1}^{M} \sum_{n=1}^{2^N-1} \frac{(-1)^{|\mathcal{E}_n|+1}}{\sigma_{ib}^2} \int_0^\infty \exp(-\frac{x}{\sigma_{ib}^2}) \\ & \times \exp(-\sum_{e_j\in\mathcal{E}_n} \frac{N_{e_j}x}{\sigma_{ie_j}^2 2^{R_s} N_b}) \\ & \times \prod_{\substack{k\in\mathcal{U}\\ k\neq i}} \left(1-\exp(-\frac{x}{\sigma_{kb}^2})\right) dx. \end{aligned} \tag{54}$$

Using the result of Appendix D, we have

$$1-\exp(-\frac{x}{\sigma_{kb}^2}) \stackrel{1}{=} \frac{x}{\sigma_{kb}^2}, \tag{55}$$

for $\lambda_{me}\to\infty$, where $\stackrel{1}{=}$ represents an equality with probability 1, and x is a random variable with the following PDF

$$g(x) = \frac{1}{\sigma_{ib}^2}\exp(-\frac{x}{\sigma_{ib}^2} - \sum_{e_j\in\mathcal{E}_n} \frac{N_{e_j}x}{\sigma_{ie_j}^2 2^{R_s} N_b}), \tag{56}$$

wherein $0 < x < \infty$. Hence, letting $\lambda_{me}\to\infty$ and substituting (55) into (54) yield (57) for the uncoordinated case. Similarly to (31), the secrecy diversity order of the suboptimal user scheduling scheme is defined as

$$d_{sub} = -\lim_{\lambda_{me}\to\infty} \frac{\log(P_{out,floor}^{sub})}{\log(\lambda_{me})}. \tag{58}$$

Combining (57) and (58), we obtain the diversity order of the suboptimal user scheduling as

$$d_{sub} = M, \tag{59}$$

for the uncoordinated case. Additionally, combining (3) and (34), we may obtain the lower and upper bounds on the secrecy outage probability floor of the suboptimal user scheduling scheme as

$$P_{out,floor}^{lower} \le P_{out,floor}^{sub} = \lim_{I\to\infty} P_{out}^{sub} \le P_{out,floor}^{upper}, \tag{60}$$

where P_{out}^{lower} and P_{out}^{upper} are given by

$$P_{out,floor}^{lower} = \sum_{i=1}^{M} \Pr\left(\begin{array}{l} 2^{R_s} \max\limits_{e_j\in\mathcal{E}} \dfrac{|h_{ie_j}|^2}{\max\limits_{e_j\in\mathcal{E}} N_{e_j}} > \dfrac{1}{N_b}|h_{ib}|^2, \\ \max\limits_{\substack{k\in\mathcal{U}\\ k\neq i}} |h_{kb}|^2 < |h_{ib}|^2 \end{array} \right), \tag{61}$$

and

$$P_{out,floor}^{upper} = \sum_{i=1}^{M} \Pr\left(\begin{array}{l} 2^{R_s} N \max\limits_{e_j\in\mathcal{E}} \dfrac{|h_{ie_j}|^2}{\min\limits_{e_j\in\mathcal{E}} N_{e_j}} > \dfrac{1}{N_b}|h_{ib}|^2, \\ \max\limits_{\substack{k\in\mathcal{U}\\ k\neq i}} |h_{kb}|^2 < |h_{ib}|^2 \end{array} \right), \tag{62}$$

for the coordinated case. Comparing (61) and (62) with (51) and using (57), we similarly obtain (63) and (64) at the top of the following page.

Substituting (60) into (58) and using (63) and (64), we obtain the secrecy diversity of the suboptimal user scheduling as

$$M \le d_{sub} \le M,$$

which results in

$$d_{sub} = M, \tag{65}$$

for the coordinated case. It can be observed from (59) and (65) that no matter whether the eavesdroppers are coordinated or not, the suboptimal user scheduling scheme achieves the diversity order of M, which is the same as the optimal user scheduling approach. It is worth mentioning that the suboptimal user scheduling only needs the CSIs of CUs-CBS links. However, the optimal user scheduling assumes that the CSIs of all links from CUs to CBS, to PR and to E_j are known, which makes it challenging to be applied in practical cognitive radio systems. Therefore, from a practical perspective, the suboptimal scheduling scheme is more attractive than the optimal scheduling.

V. Numerical Results and Discussions

In this section, we present numerical comparison among the round-robin scheduling, the optimal user scheduling and the suboptimal user scheduling in terms of secrecy outage probability. Throughout the numerical secrecy outage evaluation, we assume that the background noise and interference received at any node in the cognitive radio network shown in Fig. 1 (including CBS and N eavesdroppers) have the same variance, i.e., $N_b = N_{e_j}$ for $e_j\in\mathcal{E}$. For notational convenience, let λ_I denote the ratio of the maximum allowable interference power I to the noise variance N_b, i.e., $\gamma_I = I/N_b$.

Fig. 2 shows the secrecy outage probability versus the maximum allowable interference level γ_I of the round-robin scheduling as well as the optimal and suboptimal scheduling schemes for the uncoordinated and coordinated cases by using (13), (18), (26) and (28). Simulation results of the secrecy outage probability for these three schemes are also provided in this figure. It is observed from Fig. 2 that as the maximum allowable interference level γ_I increases, the secrecy outage probabilities of the round-robin scheduling, the suboptimal user scheduling and the optimal user scheduling schemes all decrease. This can be explained that with an increasing γ_I, CUs are allowed to transmit with higher power, leading to a decrease of the secrecy outage probability. One can see from Fig. 2 that as γ_I increases beyond a certain value, these three schemes converge to their respective secrecy outage probability floors, where the optimal and suboptimal scheduling schemes both have a lower secrecy outage floor than the round-robin scheduling. Moreover, for both the uncoordinated and coordinated cases, the optimal user scheduling strictly

$$P_{out,floor}^{sub} = \sum_{i=1}^{M}\sum_{n=1}^{2^N-1} \frac{(-1)^{|\mathcal{E}_n|+1}}{\theta_{ib}} \prod_{\substack{k\in\mathcal{U}\\k\neq i}} \frac{1}{\theta_{kb}} \left(\frac{1}{\theta_{ib}\lambda_{me}} + \sum_{e_j\in\mathcal{E}_n} \frac{N_{e_j}}{\theta_{ie_j} 2^{R_s} N_b}\right)^{-M} \cdot \left(\frac{1}{\lambda_{me}}\right)^{M} \tag{57}$$

$$P_{out,floor}^{lower} = \sum_{i=1}^{M}\sum_{n=1}^{2^N-1} \frac{(-1)^{|\mathcal{E}_n|+1}}{\theta_{ib}} \prod_{\substack{k\in\mathcal{U}\\k\neq i}} \frac{1}{\theta_{kb}} \left(\frac{1}{\theta_{ib}\lambda_{me}} + \sum_{e_j\in\mathcal{E}_n} \frac{\max\limits_{e_j\in\mathcal{E}} N_{e_j}}{\theta_{ie_j} 2^{R_s} N_b}\right)^{-M} \cdot \left(\frac{1}{\lambda_{me}}\right)^{M} \tag{63}$$

$$P_{out,floor}^{upper} = \sum_{i=1}^{M}\sum_{n=1}^{2^N-1} \frac{(-1)^{|\mathcal{E}_n|+1}}{\theta_{ib}} \prod_{\substack{k\in\mathcal{U}\\k\neq i}} \frac{1}{\theta_{kb}} \left(\frac{1}{\theta_{ib}\lambda_{me}} + \sum_{e_j\in\mathcal{E}_n} \frac{\min\limits_{e_j\in\mathcal{E}} N_{e_j}}{N\theta_{ie_j} 2^{R_s} N_b}\right)^{-M} \cdot \left(\frac{1}{\lambda_{me}}\right)^{M} \tag{64}$$

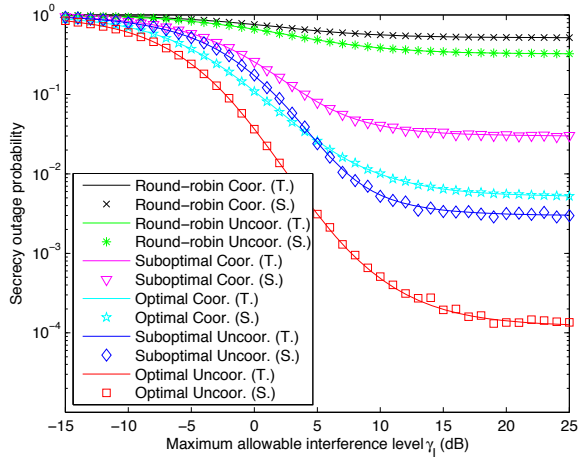

Fig. 2. Secrecy outage probability versus maximum allowable interference level γ_I of the round-robin scheduling, the suboptimal user scheduling and the optimal user scheduling schemes for both the uncoordinated and coordinated cases with $M = 8$, $N = 4$, $R_s = 1$ bit/s/Hz, $\lambda_{me} = 10$ dB, and $\sigma_{ib}^2 = \sigma_{ip}^2 = \theta_{ib} = \theta_{ie_j} = 1$.

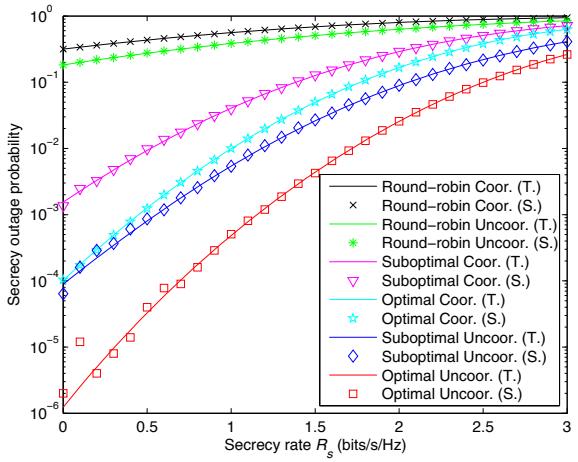

Fig. 3. Secrecy outage probability versus secrecy rate R_s of the round-robin scheduling, the suboptimal user scheduling and the optimal user scheduling schemes for both the uncoordinated and coordinated cases with $M = 8$, $N = 4$, $\lambda_{me} = 10$ dB, $\gamma_I = 10$ dB, and $\sigma_{ib}^2 = \sigma_{ip}^2 = \theta_{ib} = \theta_{ie_j} = 1$.

outperforms the suboptimal user scheduling in terms of the secrecy outage probability. Fig. 2 also illustrates that the secrecy outage performance of the round-robin scheduling as well as the optimal and suboptimal scheduling corresponding to the uncoordinated eavesdroppers is expectedly better than that of these three schemes corresponding to the coordinated eavesdroppers. This means that the eavesdroppers may collaborate with each other for the sake of degrading the secrecy outage performance of cognitive transmissions. In addition, the simulation results match well the theoretical secrecy outage probabilities, confirming the correctness of the secrecy outage analysis.

Fig. 3 depicts the secrecy outage probability versus secrecy rate R_s of the round-robin scheduling, the suboptimal user scheduling and the optimal user scheduling schemes for both the uncoordinated and coordinated cases. As shown in Fig. 3, with an increasing secrecy rate R_s, the secrecy outage probabilities of these three schemes in the presence of coordinated or uncoordinated eavesdroppers all increase accordingly. In other words, when a higher secrecy rate R_s is adopted by CUs for better throughput performance, it is less likely to achieve the perfect secure transmission against eavesdropping attacks. It is also seen from Fig. 3 that for both the coordinated and uncoordinated cases, the optimal user scheduling scheme achieves the best secrecy outage performance and the round-robin scheduling performs the worst across the whole secrecy rate region.

In Fig. 4, we show the secrecy outage probability versus the number of eavesdroppers N of the round-robin scheduling, the suboptimal user scheduling and the optimal user scheduling schemes for both the uncoordinated and coordinated eavesdroppers. One can observe from Fig. 4 that as the number of eavesdroppers N increases, the secrecy outage probabilities of these three schemes all increase for both the uncoordinated and coordinated cases. Nevertheless, given a certain number of uncoordinated (or coordinated) eavesdroppers, the optimal and suboptimal user scheduling schemes both perform better than the round-robin scheduling in terms of the secrecy outage probability.

Fig. 5 illustrates the secrecy outage probability versus the number of CUs M of the round-robin scheduling as well

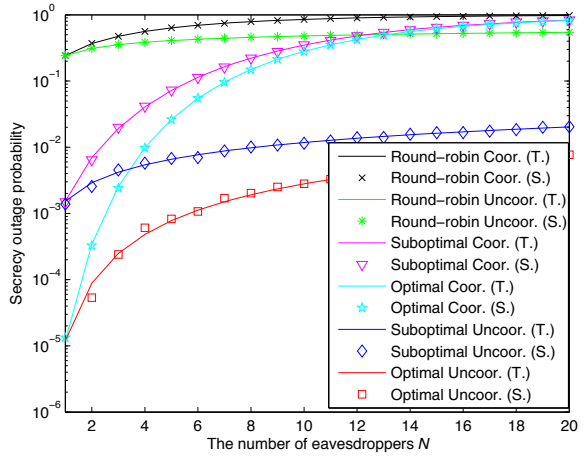

Fig. 4. Secrecy outage probability versus the number of eavesdroppers N of the round-robin scheduling, the suboptimal user scheduling and the optimal user scheduling schemes for both the uncoordinated and coordinated cases with $M = 8$, $R_s = 1$ bit/s/Hz, $\lambda_{me} = 10$ dB, $\gamma_I = 10$ dB, and $\sigma_{ib}^2 = \sigma_{ip}^2 = \theta_{ib} = \theta_{ie_j} = 1$.

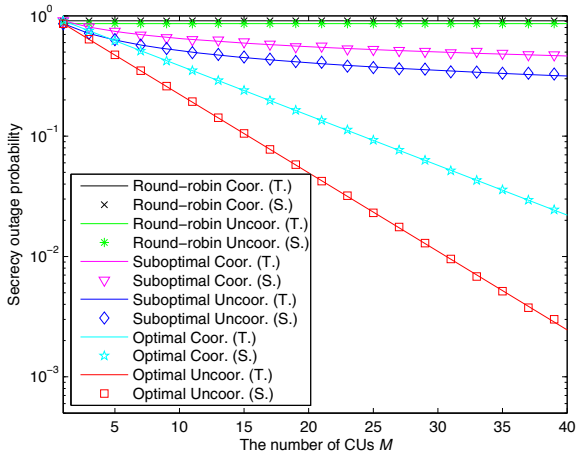

Fig. 5. Secrecy outage probability versus the number of CUs M of the round-robin scheduling, the suboptimal user scheduling and the optimal user scheduling schemes for both the uncoordinated and coordinated cases with $N = 2$, $R_s = 0.2$ bit/s/Hz, $\lambda_{me} = -3$ dB, $\gamma_I = 10$ dB, and $\sigma_{ib}^2 = \sigma_{ip}^2 = \theta_{ib} = \theta_{ie_j} = 1$.

as the optimal and suboptimal scheduling schemes for both the uncoordinated and coordinated cases with a low MER of $\lambda_{me} = -3$ dB, which means that the average channel gain of the eavesdroppers is two times better than that of the legitimate CUs. It is shown from Fig. 5 that upon increasing the number of CUs, the secrecy outage probability of the round-robin scheduling scheme keeps unchanged for both the uncoordinated and coordinated cases, showing no security benefits achieved with an increasing number of CUs. By contrast, the secrecy outage probabilities of the optimal and suboptimal user scheduling schemes both significantly decrease, as the number of CUs increases. Therefore, when either the optimal or suboptimal user scheduling is adopted, the security of cognitive transmissions may be improved by increasing the number of CUs. In other words, upon increasing the number of CUs, any target secrecy outage probability can be guaranteed by relying on the optimal or suboptimal user scheduling scheme even with a very low MER.

VI. Conclusion

In this paper, we have studied the secrecy outage and diversity performance of a multi-user multi-eavesdropper cognitive radio system, where CUs transmit to a common CBS with a primary QoS constraint in the presence of multiple coordinated or uncoordinated eavesdroppers. We have presented the round-robin scheduling, optimal user scheduling and suboptimal user scheduling schemes to protect the CUs-CBS transmissions against the eavesdropping attacks. Closed-form expressions of the secrecy outage probability of these three schemes have been derived for both the coordinated and uncoordinated cases. We have also conducted the secrecy diversity analysis of the round-robin scheduling as well as the optimal and suboptimal user scheduling in the presence of the coordinated and uncoordinated eavesdroppers. It has been proven that no matter whether the eavesdroppers collaborate or not, the round-robin scheduling achieves the secrecy diversity order of only one, whereas the optimal and suboptimal scheduling schemes both obtain the diversity order of M, where M is the number of CUs. Numerical results have demonstrated that as the maximum allowable interference level increases, the secrecy outage performance of the round-robin scheduling as well as the optimal and suboptimal user scheduling improves accordingly. Additionally, for both the coordinated and uncoordinated cases, the optimal and suboptimal user scheduling schemes significantly outperform the round-robin scheduling approach in terms of the secrecy outage probability.

In the present paper, we only studied the physical-layer security of CUs-CBS transmissions without considering the PUs' security for the primary network. In cognitive radio networks, CUs and PUs typically share the same spectrum band, thus the eavesdroppers may tap both the CUs' and PUs' transmissions. It is thus of high interest to investigate the impact of the uncoordinated and coordinated eavesdroppers on the security of both CUs and PUs. Considering the fact that PUs have a higher priority than CUs in accessing the licensed spectrum, we may impose a security constraint on the PUs' transmissions (e.g., the secrecy capacity, secrecy outage probability, etc.) with an objective of maximizing the CUs' security performance with the aid of some signal processing techniques, e.g. multi-user scheduling and beamforming. Besides, due to estimation errors in practical channel estimators, the perfect CSI is impossible to be obtained. It is interesting to further examine the impact of CSI estimation errors on the secrecy outage performance of various scheduling schemes. We leave these interesting problems for our future work.

Appendix A
Proof of (11) and (12)

For notational convenience, let X denote term $\frac{1}{2^{R_s}N_b}|h_{ib}|^2 - \frac{2^{R_s}-1}{2^{R_s}I}|h_{ip}|^2$, i.e., $X = \frac{1}{2^{R_s}N_b}|h_{ib}|^2 - \frac{2^{R_s}-1}{2^{R_s}I}|h_{ip}|^2$. Note that random variables $|h_{ib}|^2$ and $|h_{ip}|^2$ are exponentially distributed and independent of each other.

Denoting $X_1 = |h_{ib}|^2$ and $X_2 = |h_{ip}|^2$, we obtain the cumulative distribution function (CDF) of X as

$$\Pr(X < x) = \Pr\left(\frac{1}{2^{R_s}N_b}X_1 - \frac{2^{R_s}-1}{2^{R_s}I}X_2 < x\right), \quad \text{(A.1)}$$

where $-\infty < x < \infty$. For $x < 0$, (A.1) can be given by

$$\Pr(X < x) = \frac{\sigma_{ip}^2(2^{R_s}-1)N_b}{\sigma_{ip}^2(2^{R_s}-1)N_b + \sigma_{ib}^2 I} \times \exp\left(\frac{2^{R_s}I}{(2^{R_s}-1)\sigma_{ip}^2}x\right), \quad \text{(A.2)}$$

where $\sigma_{ib}^2 = E(|h_{ib}|^2)$ and $\sigma_{ip}^2 = E(|h_{ip}|^2)$. Besides, for $x > 0$, (A.1) is obtained as

$$\Pr(X < x) = 1 - \frac{\sigma_{ib}^2 I}{\sigma_{ib}^2 I + \sigma_{ip}^2(2^{R_s}-1)N_b} \times \exp\left(-\frac{2^{R_s}N_b}{\sigma_{ib}^2}x\right). \quad \text{(A.3)}$$

Combining (A.2) and (A.3), we can prove that the CDF of X is first-order differentiable for $-\infty < x < \infty$ and obtain the probability density function (PDF) of X as

$$f_X(x) = \begin{cases} \dfrac{2^{R_s}N_bI}{A}\exp\left(\dfrac{2^{R_s}Ix}{\sigma_{ip}^2(2^{R_s}-1)}\right), & x < 0 \\ \dfrac{2^{R_s}N_bI}{A}\exp\left(-\dfrac{2^{R_s}N_b}{\sigma_{ib}^2}x\right), & x > 0, \end{cases} \quad \text{(A.4)}$$

where $A = \sigma_{ip}^2(2^{R_s}-1)N_b + \sigma_{ib}^2 I$. Noting that $|h_{ie_j}|^2$ for $e_j \in \mathcal{E}$ are independent exponentially distributed random variables with respective means of $\sigma_{ie_j}^2$ for different eavesdroppers, we can rewrite (10) as

$$P_{out,i} = 1 - \Pr\left(\max_{e_j\in\mathcal{E}}\frac{|h_{ie_j}|^2}{N_{e_j}} < X\right) = 1 - \int_0^\infty \prod_{e_j\in\mathcal{E}}\left(1-\exp(-\frac{N_{e_j}x}{\sigma_{ie_j}^2})\right) f_X(x)dx. \quad \text{(A.5)}$$

Substituting (A.4) into (A.5) yields

$$P_{out,i} = 1 - \frac{2^{R_s}N_bI}{\sigma_{ib}^2 I + \sigma_{ip}^2(2^{R_s}-1)N_b} \times \int_0^\infty \prod_{e_j\in\mathcal{E}}\left(1-\exp(-\frac{N_{e_j}x}{\sigma_{ie_j}^2})\right) \times \exp(-\frac{2^{R_s}N_b}{\sigma_{ib}^2}x)dx, \quad \text{(A.6)}$$

where term $\prod_{e_j\in\mathcal{E}}\left(1-\exp(-\frac{N_{e_j}x}{\sigma_{ie_j}^2})\right)$ can be expanded with the binomial theorem as

$$\prod_{e_j\in\mathcal{E}}\left(1-\exp(-\frac{N_{e_j}x}{\sigma_{ie_j}^2})\right) = 1 - \sum_{n=1}^{2^N-1}(-1)^{|\mathcal{E}_n|+1}\exp(-\sum_{e_j\in\mathcal{E}_n}\frac{N_{e_j}x}{\sigma_{ie_j}^2}), \quad \text{(A.7)}$$

where N is the number of eavesdroppers, $\mathcal{E}_n$ represents the n-th non-empty subset of the elements of $\mathcal{E}$, and $|\mathcal{E}_n|$ is the cardinality of set $\mathcal{E}_n$. Substituting (A.7) into (A.6) and performing the integration yield

$$P_{out,i} = \frac{\sigma_{ip}^2(2^{R_s}-1)N_b + \sum_{n=1}^{2^N-1}\frac{(-1)^{|\mathcal{E}_n|+1}2^{R_s}N_bI}{\sigma_{ib}^{-2}2^{R_s}N_b + \sum_{e_j\in\mathcal{E}_n}(\sigma_{ie_j}^{-2}N_{e_j})}}{\sigma_{ib}^2 I + \sigma_{ip}^2(2^{R_s}-1)N_b}, \quad \text{(A.8)}$$

which is (11). Additionally, substituting (3), (7) and (8) into (9) and assuming different eavesdroppers with the same noise variance of $N_{e_j} = N_e$, we have

$$P_{out,i} = \Pr\left(\sum_{e_j\in\mathcal{E}}\frac{|h_{ie_j}|^2}{N_e} > \frac{1}{2^{R_s}N_b}|h_{ib}|^2 - \frac{2^{R_s}-1}{2^{R_s}I}|h_{ip}|^2\right), \quad \text{(A.9)}$$

for the coordinated case. For notational convenience, we denote $X = \frac{1}{2^{R_s}N_b}|h_{ib}|^2 - \frac{2^{R_s}-1}{2^{R_s}I}|h_{ip}|^2$ and $Y = \sum_{e_j\in\mathcal{E}}\frac{|h_{ie_j}|^2}{N_e}$, where the PDF of X is given by (A.4). Moreover, considering that random variables $|h_{ie_j}|^2$ for $e_j \in \mathcal{E}$ are i.i.d. with the same mean of σ_{ie}^2, we obtain that Y is Gamma distributed with the mean of $\frac{N\sigma_{ie}^2}{N_e}$, whose PDF is given by

$$f_Y(y) = \frac{(N_e)^N}{\Gamma(N)\sigma_{ie}^{2N}}y^{N-1}\exp(-\frac{N_e y}{\sigma_{ie}^2}), \quad \text{(A.10)}$$

for $y > 0$, where N is the number of eavesdroppers. Noting that random variables X and Y are independent and combining (A.4), (A.9) and (A.10), we obtain

$$P_{out,i} = 1 - \Pr(Y < X) = 1 - \frac{\sigma_{ib}^2 I}{\sigma_{ib}^2 I + \sigma_{ip}^2(2^{R_s}-1)N_b}(1 + \frac{2^{R_s}\sigma_{ie}^2 N_b}{\sigma_{ib}^2 N_e})^{-N}, \quad \text{(A.11)}$$

which is (12).

Appendix B
Derivation of (26)

Considering that $|h_{ib}|^2$ and $|h_{ip}|^2$ are independent exponentially distributed and denoting $X = |h_{ib}|^2$ and $Y = |h_{ip}|^2$, we can easily obtain the joint PDF of random variables $(X,\ Y)$ as

$$f(x,y) = \frac{1}{\sigma_{ib}^2\sigma_{ip}^2}\exp(-\frac{x}{\sigma_{ib}^2} - \frac{y}{\sigma_{ip}^2}), \quad \text{(B.1)}$$

for $(x > 0,\ y > 0)$. Thus, we can rewrite (25) as

$$P_{out}^{sub} = \sum_{i=1}^{M}\Pr\left(\begin{matrix} 2^{R_s}I\max\limits_{e_j\in\mathcal{E}}\dfrac{|h_{ie_j}|^2}{N_{e_j}} > \dfrac{I}{N_b}X - (2^{R_s}-1)Y, \\ \max\limits_{\substack{k\in\mathcal{U}\\k\neq i}}|h_{kb}|^2 < X \end{matrix}\right)$$
$$= \sum_{i=1}^{M}\iint\Pr\left(2^{R_s}I\max_{e_j\in\mathcal{E}}\frac{|h_{ie_j}|^2}{N_{e_j}} > \frac{I}{N_b}x - (2^{R_s}-1)y\right) \times \Pr\left(\max_{\substack{k\in\mathcal{U}\\k\neq i}}|h_{kb}|^2 < x\right) f(x,y)dxdy, \quad \text{(B.2)}$$

where the second equation arises from the fact that random variables $|h_{ie_j}|^2$ and $|h_{kb}|^2$ (for $e_j \in \mathcal{E}$ and $k \in \mathcal{U}$) are

$$P_{out}^{sub} = \sum_{i=1}^{M} \iint\limits_{\Omega} \left[1 - \prod_{e_j \in \mathcal{E}} \left(1 - \exp(-\frac{N_{e_j} N_b^{-1} Ix - N_{e_j}(2^{R_s}-1)y}{\sigma_{ie_j}^2 2^{R_s} I})\right)\right] \prod_{\substack{k \in \mathcal{U} \\ k \neq i}} \left(1 - \exp(-\frac{x}{\sigma_{kb}^2})\right) f(x,y)dxdy + \sum_{i=1}^{M} \iint\limits_{\Phi} \prod_{\substack{k \in \mathcal{U} \\ k \neq i}} \left(1 - \exp(-\frac{x}{\sigma_{kb}^2})\right) f(x,y)dxdy \tag{B.3}$$

independent of each other. Noting that $|h_{ie_j}|^2$ and $|h_{kb}|^2$ are exponential random variables with respective means $\sigma_{ie_j}^2$ and σ_{kb}^2, (B.2) can be further obtained as (B.3) above, where $\Omega = \left\{(x,y)|N_b^{-1}Ix - (2^{R_s}-1)y > 0\right\}$ and $\Phi = \left\{(x,y)|N_b^{-1}Ix - (2^{R_s}-1)y < 0\right\}$. By using the binomial theorem, term $\prod\limits_{e_j \in \mathcal{E}} \left(1 - \exp(-\frac{N_{e_j} N_b^{-1} Ix - N_{e_j}(2^{R_s}-1)y}{\sigma_{ie_j}^2 2^{R_s} I})\right)$ is expanded by

$$\prod_{e_j \in \mathcal{E}} \left(1 - \exp(-\frac{N_{e_j} N_b^{-1} Ix - N_{e_j}(2^{R_s}-1)y}{\sigma_{ie_j}^2 2^{R_s} I})\right) = 1 - \sum_{n=1}^{2^N-1} (-1)^{|\mathcal{E}_n|+1} \exp(-\sum_{e_j \in \mathcal{E}_n} \frac{N_{e_j} N_b^{-1} Ix - N_{e_j}(2^{R_s}-1)y}{\sigma_{ie_j}^2 2^{R_s} I}), \tag{B.4}$$

where $\mathcal{E}_n$ represents the n-th non-empty subset of the elements of $\mathcal{E}$ and $|\mathcal{E}_n|$ is the cardinality of set $\mathcal{E}_n$. Similarly, we can obtain term $\prod\limits_{\substack{k \in \mathcal{U} \\ k \neq i}} \left(1 - \exp(-\frac{x}{\sigma_{kb}^2})\right)$ as

$$\prod_{\substack{k \in \mathcal{U} \\ k \neq i}} \left(1 - \exp(-\frac{x}{\sigma_{kb}^2})\right) = 1 - \sum_{m=1}^{2^{M-1}-1} (-1)^{|\mathcal{U}_m|+1} \exp(-\sum_{k \in \mathcal{U}_m} \frac{x}{\sigma_{kb}^2}), \tag{B.5}$$

where $\mathcal{U}_m$ represents the m-th non-empty subset of the elements of $\mathcal{U} - \{\mathrm{CU}_i\}$, '$-$' represents the set difference, and $|\mathcal{U}_m|$ is the cardinality of set $\mathcal{U}_m$. Substituting (B.4) and (B.5) into (B.3) yields

$$P_{out}^{sub} = \sum_{i=1}^{M} \sum_{n=1}^{2^N-1} (-1)^{|\mathcal{E}_n|+1} \left(P_{out,I}^{sub} - P_{out,II}^{sub}\right) + \sum_{i=1}^{M} P_{out,III}^{sub}, \tag{B.6}$$

where $P_{out,I}^{sub}$, $P_{out,II}^{sub}$ and $P_{out,III}^{sub}$ are given by

$$P_{out,I}^{sub} = \iint\limits_{\Omega} \exp(-\sum_{e_j \in \mathcal{E}_n} \frac{N_{e_j} N_b^{-1} Ix - N_{e_j}(2^{R_s}-1)y}{\sigma_{ie_j}^2 2^{R_s} I}) \times f(x,y)dxdy, \tag{B.7}$$

and

$$P_{out,II}^{sub} = \sum_{m=1}^{2^{M-1}-1} (-1)^{|\mathcal{U}_m|+1} \iint\limits_{\Omega} \exp(-\sum_{k \in \mathcal{U}_m} \frac{x}{\sigma_{kb}^2}) \times \exp(-\sum_{e_j \in \mathcal{E}_n} \frac{N_{e_j} N_b^{-1} Ix - N_{e_j}(2^{R_s}-1)y}{\sigma_{ie_j}^2 2^{R_s} I}) \times f(x,y)dxdy, \tag{B.8}$$

and

$$P_{out,III}^{sub} = \iint\limits_{\Phi} \left[1 - \sum_{m=1}^{2^{M-1}-1} (-1)^{|\mathcal{U}_m|+1} \exp(-\sum_{k \in \mathcal{U}_m} \frac{x}{\sigma_{kb}^2})\right] \times f(x,y)dxdy. \tag{B.9}$$

Combining (B.1) and (B.7), we obtain

$$P_{out,I}^{sub} = \int_0^{\infty} \frac{1}{\sigma_{ib}^2} \exp(-\frac{x}{\sigma_{ib}^2} - \sum_{e_j \in \mathcal{E}_n} \frac{N_{e_j} x}{\sigma_{ie_j}^2 2^{R_s} N_b})dx \times \int_0^{\frac{Ix}{(2^{R_s}-1)N_b}} \frac{1}{\sigma_{ip}^2} \exp(-\frac{y}{\sigma_{ip}^2}) \times \exp(\sum_{e_j \in \mathcal{E}_n} \frac{N_{e_j}(2^{R_s}-1)y}{\sigma_{ie_j}^2 2^{R_s} I})dy, \tag{B.10}$$

which is further computed as

$$P_{out,I}^{sub} = \frac{I(\frac{1}{\sigma_{ib}^2} + \sum\limits_{e_j \in E_n} \frac{N_{e_j}}{\sigma_{ie_j}^2 2^{R_s} N_b})^{-2}}{\sigma_{ib}^2 \sigma_{ip}^2 (2^{R_s}-1) N_b}, \tag{B.11}$$

for $\sum\limits_{e_j \in \mathcal{E}_n} \frac{(2^{R_s}-1)N_{e_j}}{\sigma_{ie_j}^2 2^{R_s} I} = \frac{1}{\sigma_{ip}^2}$. Moreover, if $\sum\limits_{e_j \in \mathcal{E}_n} \frac{(2^{R_s}-1)N_{e_j}}{\sigma_{ie_j}^2 2^{R_s} I} \neq \frac{1}{\sigma_{ip}^2}$, we can obtain $P_{out,I}^{sub}$ from (B.10) as

$$P_{out,I}^{sub} = \frac{(1 + \sum\limits_{e_j \in \mathcal{E}_n} \frac{\sigma_{ib}^2 N_{e_j}}{\sigma_{ie_j}^2 2^{R_s} N_b})^{-1} - (1 + \frac{\sigma_{ib}^2 I}{\sigma_{ip}^2 (2^{R_s}-1) N_b})^{-1}}{1 - \sum\limits_{e_j \in \mathcal{E}_n} \frac{\sigma_{ip}^2 N_{e_j}(2^{R_s}-1)}{\sigma_{ie_j}^2 2^{R_s} I}}. \tag{B.12}$$

Similarly, substituting (B.1) into (B.8) yields

$$P_{out,II}^{sub} = \sum_{m=1}^{2^{M-1}-1} \frac{(-1)^{|\mathcal{U}_m|+1} I(B + \sum\limits_{e_j \in \mathcal{E}_n} \frac{N_{e_j}}{\sigma_{ie_j}^2 2^{R_s} N_b})^{-2}}{\sigma_{ib}^2 \sigma_{ip}^2 (2^{R_s}-1) N_b}, \tag{B.13}$$

for $\sum_{e_j\in\mathcal{E}_n}\frac{(2^{R_s}-1)N_{e_j}}{\sigma_{ie_j}^2 2^{R_s}I}=\frac{1}{\sigma_{ip}^2}$, wherein $B=\frac{1}{\sigma_{ib}^2}+\sum_{k\in\mathcal{U}_m}\frac{1}{\sigma_{kb}^2}$. In case of $\sum_{e_j\in\mathcal{E}_n}\frac{(2^{R_s}-1)N_{e_j}}{\sigma_{ie_j}^2 2^{R_s}I}\neq\frac{1}{\sigma_{ip}^2}$, we obtain $P_{out,II}^{sub}$ as

$$P_{out,II}^{sub}=\sum_{m=1}^{2^{M-1}-1}(-1)^{|\mathcal{U}_m|+1}\frac{(\sigma_{ib}^2B+\sum_{e_j\in\mathcal{E}_n}\frac{\sigma_{ib}^2N_{e_j}}{\sigma_{ie_j}^2 2^{R_s}N_b})^{-1}}{1-\sum_{e_j\in\mathcal{E}_n}\frac{\sigma_{ip}^2N_{e_j}(2^{R_s}-1)}{\sigma_{ie_j}^2 2^{R_s}I}}-\sum_{m=1}^{2^{M-1}-1}(-1)^{|\mathcal{U}_m|+1}\frac{(\sigma_{ib}^2B+\frac{\sigma_{ib}^2I}{\sigma_{ip}^2(2^{R_s}-1)N_b})^{-1}}{1-\sum_{e_j\in\mathcal{E}_n}\frac{\sigma_{ip}^2N_{e_j}(2^{R_s}-1)}{\sigma_{ie_j}^2 2^{R_s}I}}. \tag{B.14}$$

In addition, combining (B.1) and (B.9), we obtain $P_{out,III}^{sub}$ as

$$P_{out,III}^{sub}=\left(1+\frac{\sigma_{ib}^2I}{\sigma_{ip}^2(2^{R_s}-1)N_b}\right)^{-1}-\sum_{m=1}^{2^{M-1}-1}(-1)^{|\mathcal{U}_m|+1}\left(\sigma_{ib}^2B+\frac{\sigma_{ib}^2I}{\sigma_{ip}^2(2^{R_s}-1)N_b}\right)^{-1}, \tag{B.15}$$

where $B=\frac{1}{\sigma_{ib}^2}+\sum_{k\in\mathcal{U}_m}\frac{1}{\sigma_{kb}^2}$. Finally, substituting (B.11)-(B.15) into (B.6) yields (26).

Appendix C
Derivation of (28)

Denoting $|h_{ib}|^2=X$, $|h_{ip}|^2=Y$ and $\sum_{e_j\in\mathcal{E}}|h_{ie_j}|^2=Z$, we can rewrite (27) as

$$P_{out}^{sub}=\sum_{i=1}^{M}\Pr\left(\begin{array}{l}Z>\frac{N_e}{2^{R_s}N_b}X-\frac{(2^{R_s}-1)N_e}{2^{R_s}I}Y,\\ \max\limits_{\substack{k\in\mathcal{U}\\k\neq i}}|h_{kb}|^2<X\end{array}\right). \tag{C.1}$$

Considering that the fading coefficients $|h_{ie_j}|^2$ for $e_j\in\mathcal{E}$ are i.i.d. with the same mean of σ_{ie}^2, we readily obtain that the random variable z is Gamma distributed with the mean of $N\sigma_{ie}^2$. Since $|h_{ib}|^2$ and $|h_{ip}|^2$ are independent and exponentially distributed with respective means of σ_{ib}^2 and σ_{ip}^2, we obtain the joint PDF of (X,Y,Z) as

$$f(x,y,z)=\frac{z^{N-1}}{\Gamma(N)\sigma_{ib}^2\sigma_{ip}^2\sigma_{ie}^{2N}}\exp(-\frac{x}{\sigma_{ib}^2}-\frac{y}{\sigma_{ip}^2}-\frac{z}{\sigma_{ie}^2}), \tag{C.2}$$

for $(x,y,z)>0$. Noting that $|h_{kb}|^2$ and $|h_{ib}|^2$ are independent exponential random variables and combining (C.1) and (C.2), we have

$$P_{out}^{sub}=\sum_{i=1}^{M}\iiint_{\Theta}\prod_{\substack{k\in\mathcal{U}\\k\neq i}}\left(1-\exp(-\frac{x}{\sigma_{kb}^2})\right)f(x,y,z)dxdydz, \tag{C.3}$$

where $\Theta=\left\{(x,y,z)|z>\frac{N_e}{2^{R_s}N_b}x-\frac{(2^{R_s}-1)N_e}{2^{R_s}I}y\right\}$. Noting $(x,y,z)>0$, we may divide Θ into two mutually exclusively sets i.e. Θ_1 and Θ_2, where Θ_1 and Θ_2 are given by

$$\Theta_1=\left\{(x,y,z)\left|\begin{array}{l}N_b^{-1}Ix-(2^{R_s}-1)y>0,\\ z>\frac{N_e}{2^{R_s}N_b}x-\frac{(2^{R_s}-1)N_e}{2^{R_s}I}y\end{array}\right.\right\}, \tag{C.4}$$

and

$$\Theta_2=\left\{(x,y,z)|N_b^{-1}Ix-(2^{R_s}-1)y<0,z>0\right\}. \tag{C.5}$$

By using $(x,y,z)>0$, Θ_1 can be further divided into two mutually exclusively sets Θ_{11} and Θ_{12}, which are described as

$$\Theta_{11}=\left\{(x,y,z)\left|\begin{array}{l}\frac{Ix}{(2^{R_s}-1)N_b}>y,\\ y>\frac{Ix}{(2^{R_s}-1)N_b}-\frac{2^{R_s}Iz}{(2^{R_s}-1)N_e},\\ \frac{N_e}{2^{R_s}N_b}x-z>0\end{array}\right.\right\}, \tag{C.6}$$

and

$$\Theta_{12}=\left\{(x,y,z)\left|\begin{array}{l}\frac{Ix}{(2^{R_s}-1)N_b}>y>0,\\ \frac{N_e}{2^{R_s}N_b}x-z<0\end{array}\right.\right\}. \tag{C.7}$$

Substituting $\Theta=\Theta_{11}\cup\Theta_{12}\cup\Theta_2$ into (C.3) yields

$$P_{out}^{sub}=\sum_{i=1}^{M}(P_{out,I}+P_{out,II}+P_{out,III}), \tag{C.8}$$

where $P_{out,I}$, $P_{out,II}$ and $P_{out,III}$ are given by

$$P_{out,I}=\sum_{i=1}^{M}\iiint_{\Theta_{11}}\prod_{\substack{k\in\mathcal{U}\\k\neq i}}\left(1-\exp(-\frac{x}{\sigma_{kb}^2})\right)f(x,y,z)dxdydz, \tag{C.9}$$

and

$$P_{out,II}=\sum_{i=1}^{M}\iiint_{\Theta_{12}}\prod_{\substack{k\in\mathcal{U}\\k\neq i}}\left(1-\exp(-\frac{x}{\sigma_{kb}^2})\right)f(x,y,z)dxdydz, \tag{C.10}$$

and

$$P_{out,III}=\sum_{i=1}^{M}\iiint_{\Theta_2}\prod_{\substack{k\in\mathcal{U}\\k\neq i}}\left(1-\exp(-\frac{x}{\sigma_{kb}^2})\right)f(x,y,z)dxdydz. \tag{C.11}$$

Substituting (C.2) and (C.6) into (C.9) yields

$$P_{out,I}=\int_0^{\infty}\frac{z^{N-1}}{\Gamma(N)\sigma_{ie}^{2N}}\exp(-\frac{z}{\sigma_{ie}^2})dz\times\int_{\frac{2^{R_s}N_bz}{N_e}}^{\infty}\frac{1}{\sigma_{ib}^2}\exp(-\frac{x}{\sigma_{ib}^2})\prod_{\substack{k\in\mathcal{U}\\k\neq i}}\left(1-\exp(-\frac{x}{\sigma_{kb}^2})\right)dx\times\int_{\frac{Ix}{(2^{R_s}-1)N_b}-\frac{2^{R_s}Iz}{(2^{R_s}-1)N_e}}^{\frac{Ix}{(2^{R_s}-1)N_b}}\frac{1}{\sigma_{ip}^2}\exp(-\frac{y}{\sigma_{ip}^2})dy, \tag{C.12}$$

where the term $\prod_{\substack{k\in\mathcal{U}\\k\neq i}}\left(1-\exp(-\frac{x}{\sigma_{kb}^2})\right)$ may be expanded to $\sum_{m=0}^{2^{M-1}-1}(-1)^{|\mathcal{U}_m|}\exp(-\sum_{k\in\mathcal{U}_m}\frac{x}{\sigma_{kb}^2})$ by using the Binomial theorem, wherein $\sum_{k\in\mathcal{U}_m}\frac{x}{\sigma_{kb}^2}=0$ for $\mathcal{U}_m=\mathcal{U}_0$ and $\mathcal{U}_0$ represents an empty set. Substituting this result into (C.12),

$$P_{out,I}=\frac{(-1)^{|\mathcal{U}_m|}(\frac{1}{\sigma_{ie}^2}+\frac{2^{R_s}N_b}{\sigma_{ib}^2N_e}+\sum\limits_{k\in\mathcal{U}_m}\frac{2^{R_s}N_b}{\sigma_{kb}^2N_e})^{-N}}{\sigma_{ib}^2\sigma_{ie}^{2N}[\sigma_{ib}^{-2}+\sum\limits_{k\in\mathcal{U}_m}\sigma_{kb}^{-2}+\frac{I(2^{R_s}-1)^{-1}}{\sigma_{ip}^2N_b}]}-\frac{(-1)^{|\mathcal{U}_m|}[\sigma_{ie}^{-2}+\frac{2^{R_s}N_b}{\sigma_{ib}^2N_e}+\sum\limits_{k\in\mathcal{U}_m}\frac{2^{R_s}N_b}{\sigma_{kb}^2N_e}+\frac{I2^{R_s}}{(2^{R_s}-1)N_e\sigma_{ip}^2}]^{-N}}{\sigma_{ib}^2\sigma_{ie}^{2N}[\sigma_{ib}^{-2}+\sum\limits_{k\in\mathcal{U}_m}\sigma_{kb}^{-2}+I(2^{R_s}-1)^{-1}\sigma_{ip}^{-2}N_b^{-1}]} \quad \text{(C.13)}$$

we obtain (C.13) above. Similarly, substituting (C.2) and (C.7) into (C.10) yields (C.14).

$$P_{out,II}=\frac{(-1)^{|\mathcal{U}_m|}(\sigma_{ie}^{2N}-C^{-N})}{\sigma_{ib}^2\sigma_{ie}^{2N}(\sigma_{ib}^{-2}+\sum\limits_{k\in\mathcal{U}_m}\sigma_{kb}^{-2})}-\frac{(-1)^{|\mathcal{U}_m|}[\sigma_{ie}^{2N}-(C+\frac{2^{R_s}I}{(2^{R_s}-1)\sigma_{ip}^2N_e})^{-N}]}{\sigma_{ib}^2\sigma_{ie}^{2N}[B+I(2^{R_s}-1)^{-1}\sigma_{ip}^{-2}N_b^{-1}]}, \quad \text{(C.14)}$$

where $B=\frac{1}{\sigma_{ib}^2}+\sum\limits_{k\in\mathcal{U}_m}\frac{1}{\sigma_{kb}^2}$ and $C=\frac{1}{\sigma_{ie}^2}+\frac{2^{R_s}N_b}{\sigma_{ib}^2N_e}+\sum\limits_{k\in\mathcal{U}_m}\frac{2^{R_s}N_b}{\sigma_{kb}^2N_e}$. Additionally, substituting (C.2) and (C.5) into (C.11), we have

$$P_{out,III}=\sum_{m=0}^{2^{M-1}-1}(-1)^{|U_m|}\left(\sigma_{ib}^2B+\frac{I\sigma_{ib}^2}{(2^{R_s}-1)\sigma_{ip}^2N_b}\right)^{-1}, \quad \text{(C.15)}$$

where $B=\frac{1}{\sigma_{ib}^2}+\sum\limits_{k\in\mathcal{U}_m}\frac{1}{\sigma_{kb}^2}$. This completes the derivation of (28).

APPENDIX D
PROOF OF (55)

Without loss of generality, let z denote $\frac{x}{\sigma_{kb}^2}$, i.e., $z=\frac{x}{\sigma_{kb}^2}$. Thus, the mean of random variable z is obtained as

$$E(z)=\frac{1}{\sigma_{kb}^2}E(x), \quad \text{(D.1)}$$

which can be further computed from (56) as

$$E(z)=\frac{1}{\sigma_{kb}^2}\int_0^\infty\frac{x}{\sigma_{ib}^2}\exp(-\frac{x}{\sigma_{ib}^2}-\sum_{e_j\in\mathcal{E}_n}\frac{N_{e_j}x}{\sigma_{ie_j}^2 2^{R_s}N_b})dx$$
$$=\frac{1}{\sigma_{kb}^2\sigma_{ib}^2}\left(\frac{1}{\sigma_{ib}^2}+\sum_{e_j\in\mathcal{E}_n}\frac{N_{e_j}}{\sigma_{ie_j}^2 2^{R_s}N_b}\right)^{-2}. \quad \text{(D.2)}$$

Denoting $\sigma_{kb}^2=\theta_{kb}\sigma_m^2$, $\sigma_{ib}^2=\theta_{ib}\sigma_m^2$ and $\sigma_{ie_j}^2=\theta_{ie_j}\sigma_e^2$, we can rewrite (D.2) as

$$E(z)=\frac{1}{\theta_{kb}\theta_{ib}}\left(\frac{1}{\theta_{ib}\lambda_{me}}+\sum_{e_j\in\mathcal{E}_n}\frac{N_{e_j}}{\theta_{ie_j}2^{R_s}N_b}\right)^{-2}\cdot(\frac{1}{\lambda_{me}})^2, \quad \text{(D.3)}$$

where $\lambda_{me}=\frac{\sigma_m^2}{\sigma_e^2}$. Meanwhile, we can also obtain the mean of z^2 as

$$E(z^2)=\frac{1}{\theta_{kb}^2\theta_{ib}}\left(\frac{1}{\theta_{ib}\lambda_{me}}+\sum_{e_j\in\mathcal{E}_n}\frac{N_{e_j}}{\theta_{ie_j}2^{R_s}N_b}\right)^{-3}\cdot(\frac{1}{\lambda_{me}})^3. \quad \text{(D.4)}$$

One can observe from (D.3) and (D.4) that for $\lambda_{me}\to\infty$, both $E(z)$ and $E(z^2)$ tend to zero. This implies that as $\lambda_{me}\to\infty$, random variable z approaches zero with probability 1, yielding $z\overset{1}{=}0$ for $\lambda_{me}\to\infty$, where $\overset{1}{=}$ denotes an equality with probability 1. Also, from the Maclaurin series expansion and the Cauchy's Mean-Value theorem, we obtain

$$1-\exp(-z)=z+\frac{z^2}{2}\exp(-\theta z), \quad \text{(D.5)}$$

where $0<\theta<1$. From (D.5), we have

$$\lim_{\lambda_{me}\to\infty}1-\exp(-z)=z+\lim_{\lambda_{me}\to\infty}\frac{z^2}{2}\exp(-\theta z). \quad \text{(D.6)}$$

Similarly to (D.3) and (D.4), we can easily prove that for $\lambda_{me}\to\infty$, the mean and variance of z^2 are high-order infinitesimals as compared with the mean and variance of z. Meanwhile, due to $0<\theta<1$ and $z>0$, we have $0<\exp(-\theta z)<1$. Thus, term $\frac{z^2}{2}\exp(-\theta z)$ is high-order infinitesimal compared to z, as $\lambda_{me}\to\infty$. Ignoring the high-order infinitesimal in (D.6) yields

$$\lim_{\lambda_{me}\to\infty}1-\exp(-z)\overset{1}{=}z. \quad \text{(D.7)}$$

Substituting $z=\frac{x}{\sigma_{kb}^2}$ into (D.7) yields

$$1-\exp(-\frac{x}{\sigma_{kb}^2})\overset{1}{=}\frac{x}{\sigma_{kb}^2}, \quad \text{(D.8)}$$

for $\lambda_{me}\to\infty$, which is (55).

REFERENCES

[1] J. Mitola and G. Q. Maguire, "Cognitive radio: Making software radios more personal," *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13-18, Aug. 1999.

[2] IEEE 802.22 Working Group, "IEEE P802.22/D1.0 draft standard for wireless regional area networks part 22: Cognitive wireless RAN medium access control (MAC) and physical layer (PHY) specifications: Policies and procedures for operation in the TV bands," Apr. 2008.

[3] Y. Zou, Y.-D. Yao, and B. Zheng, "Cooperative relay techniques for cognitive radio systems: Spectrum sensing and secondary user transmissions," *IEEE Commun. Mag.*, vol. 50, no. 4, pp. 98-103. Apr. 2012.

[4] Y.-C. Liang, Y. Zeng, E. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1326-1337, Apr. 2008.

[5] Y. Zou, Y.-D. Yao, and B. Zheng, "Cognitive transmissions with multiple relays in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 648-659, Feb. 2011.

[6] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surv. & Tut.*, vol. 15, no. 1 , pp. 428-445, Feb. 2013.

[7] A. D.Wyner, "The wire-tap channel," *Bell Syst. Tech. Journ.*, vol. 54, no. 8, pp. 1355-1387, 1975.

[8] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, pp. 451-456, Jul. 1978.

[9] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534, Jun. 2008.

[10] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretic security", MA: Now Publishers, vol. 5, no. 4-5, pp. 355-580, 2008.

[11] 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, Oct. 2008.
[12] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961-4972, Oct. 2007.
[13] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, July 2008.
[14] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71-74, Feb. 2012.
[15] W. Liao, T. Chang, W. Ma, and C. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Veh. Tech.*, vol. 59, no. 3, pp. 1202-1216, Mar. 2011.
[16] A. Mukherjee amd A. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351-361, Jan. 2011.
[17] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532-3545, Jul. 2012.
[18] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71-74, Feb. 2012.
[19] Y. Pei, Y.-C. Liang, K.C. Teh, and K. Li, "Secure communication in multiantenna cognitive radio networks with imperfect channel state information," *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1683-1693, Apr. 2011.
[20] 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 Trans. Commun.*, vol. 58, no. 6, pp. 1877-1886, Jun. 2010.
[21] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Commun.*, vol. 6, no. 16, pp. 2676-2687, Nov. 2011.
[22] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5103-5113, Dec. 2013.
[23] J. Lee, H. Wang, J. G. Andrews, and D. Hong, "Outage probability of cognitive relay networks with interference constraints," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 390-395, Feb. 2011.
[24] T. Q. Duong, D. Benevides, M. Elkashlan, and V. Bao, "Cognitive amplify-and-forward relay networks over Nakagami-m fading," *IEEE Trans. Veh. Tech.*, vol. 61, no. 5, pp. 2368-2374, Jun. 2012.
[25] K. Tourki, K. A. Qaraqe, M.-S. Alouini, "Outage analysis for underlay cognitive networks using incremental regenerative relaying," *IEEE Trans. Veh. Tech.*, vol. 62, no. 2, pp. 721-734, Feb. 2013.
[26] R. Etkin, A. Parekh, and D. Tse, "Spectrum sharing for unlicensed bands," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 2, pp. 517-528, Apr. 2007.
[27] L. Zheng and D. Tse, "Diversity and multiplexing: A fundamental tradeoff in multiple antenna channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1073C1096, May 2003.
[28] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099-2111, Oct. 2013.

Yulong Zou (S'07-M'12-SM'13) is a Full Professor at the Nanjing University of Posts and Telecommunications (NUPT), Nanjing, China. He received the B.Eng. degree in Information Engineering from NUPT, Nanjing, China, in July 2006, the first Ph.D. degree in Electrical Engineering from the Stevens Institute of Technology, New Jersey, United States, in May 2012, and the second Ph.D. degree in Signal and Information Processing from NUPT, Nanjing, China, in July 2012. His research interests span a wide range of topics in wireless communications and signal processing, including the cooperative communications, cognitive radio, wireless security, and energy-efficient communications.

Dr. Zou is currently serving as an editor for the IEEE Communications Surveys & Tutorials, IEEE Communications Letters, EURASIP Journal on Advances in Signal Processing, and KSII Transactions on Internet and Information Systems. He has also served as the lead guest editor for a special issue on "Security Challenges and Issues in Cognitive Radio Networks" in the EURASIP Journal on Advances in Signal Processing. In addition, he has acted as symposium chairs, session chairs, and TPC members for a number of IEEE sponsored conferences, including the IEEE Wireless Communications and Networking Conference (WCNC), IEEE Global Communications Conference (GLOBECOM), IEEE International Conference on Communications (ICC), IEEE Vehicular Technology Conference (VTC), International Conference on Communications in China (ICCC), and so on.

Xuelong Li (M'02-SM'07-F'12) is a Full Professor with the Center for OPTical IMagery Analysis and Learning (OPTIMAL), State Key Laboratory of Transient Optics and Photonics, Xi'an Institute of Optics and Precision Mechanics, Chinese Academy of Sciences, Xi'an 710119, Shaanxi, P. R. China.

Ying-Chang Liang (F'11) is a Principal Scientist in the Institute for Infocomm Research (I2R), Agency for Science, Technology & Research (A*STAR), Singapore. He was a visiting scholar in the Department of Electrical Engineering, Stanford University, CA, USA, from Dec 2002 to Dec 2003, and was an adjunct staff in National University of Singapore and Nanyang Technological University from 2004 - 2009. His research interest spans the area of communications and signal processing, with emphasis on dynamic spectrum access, cognitive radio, space-time wireless communications, cooperative communications, broadband wireless networks, and statistical signal processing.

Dr Liang was elected as a Fellow of the IEEE in December 2010 for contributions to cognitive radio communications, and was recognized by Thomson Reuters as a Highly Cited Researcher and listed in The World's Most Influential Scientific Minds 2014. He received the Institute of Engineers Singapore (IES)'s Prestigious Engineering Achievement Award in 2007, and the IEEE Standards Association's Outstanding Contribution Appreciation Award in 2011, for his contributions to the development of IEEE 802.22 standard. He has also received five Best Paper Awards, including the first IEEE Communications Society APB Outstanding Paper Award in 2012, and EURASIP Journal of Wireless Communications and Networking Best Paper Award in 2010.

Dr Liang serves as Editor-in-Chief of IEEE Journal on Selected Areas in Communications - Cognitive Radio Series, and is the key founder of new journal IEEE Transactions on Cognitive Communications and Networking. He was an Editor of IEEE Transactions on Wireless Communications from 2002 to 2005, and an Associate Editor of IEEE Transactions on Vehicular Technology from 2008 to 2012, and served as a Guest Editor of five special issues on emerging topics published in IEEE, EURASIP and Elsevier journals in the past years. Dr Liang is currently a Distinguished Lecturer of the IEEE Communications Society and the IEEE Vehicular Technology Society, and has been a member of the Board of Governors of the IEEE Asia-Pacific Wireless Communications Symposium since 2009.