Secure Communications in Underlay Cognitive Radio Networks: User Scheduling and Performance Analysis

Long Yang, Hai Jiang, *Senior Member, IEEE*, Sergiy A. Vorobyov, *Senior Member, IEEE*, Jian Chen, *Member, IEEE*, and Hailin Zhang, *Member, IEEE*

***Abstract*—This letter investigates secure communications against eavesdropping in an underlay cognitive radio network. The secondary users do not know the interference level that they receive from the primary transmitter, and thus, secondary transmissions may experience outages. We consider an outage probability threshold for secondary transmissions, and propose secondary user scheduling schemes for downlink and uplink, targeting at maximizing the achievable secrecy rate. We derive closed-form secrecy outage probability and show that the proposed user scheduling schemes can achieve full secrecy diversity.**

***Index Terms*—Cognitive radio, outage, physical-layer security.**

I. Introduction

NETWORK security is a major challenge in cognitive radio [1]. To protect secondary transmissions against eavesdropping attacks, physical-layer security has attracted much attention in cognitive radio research [2]–[9]. The works in [2] and [3] investigate the cognitive radio achievable secrecy rate with multiple-input single-output (MISO) channel and multiple-input multiple-output (MIMO) channel, respectively. For the case of single-input multiple-output (SIMO) channel, the work in [4] derives the secrecy outage probability (SOP) in closed form for secondary transmission. Cooperative beamforming is considered in [5] under primary users' and secondary users' secrecy constraints. When cooperative relays are used, optimal relay selection is given in [6] which maximizes the secondary secrecy rate in cognitive radio. In [7], two relays are selected, one for information forwarding, and the other for transmitting a jamming signal to the eavesdropper. SOP expressions are derived in closed form. Uplink user scheduling is considered in [8], which focuses on derivation of intercept probability and achievable secrecy rate, and in [9], which deals with derivation of SOP and secrecy diversity order.

In an underlay cognitive radio network (in which primary and secondary users can be active simultaneously), secondary users receive interference from primary users. In the above mentioned works, interference from primary users is considered only in [8] and [9], which model the interference as additive white Gaussian noise (AWGN). This modeling may not be accurate for all cases. When interference from primary users is considered, a major challenge is that the cooperation between primary and secondary users is limited, and thus, it is hard for secondary users to estimate the interference level received from primary users. Without estimate of the interference, secondary transmissions may experience outages.

To address the above challenge, we consider an underlay cognitive radio network in which it is required that the transmission outage probability (TOP) due to unknown interference level from primary users is bounded by a predetermined threshold. We then propose user scheduling schemes for the secondary network in downlink and uplink. The secrecy performance of the proposed scheduling schemes is evaluated by deriving the corresponding SOP and secrecy diversity order. It demonstrates that a full secrecy diversity order is achieved by the proposed user scheduling schemes.

II. System Model

Consider an underlay cognitive radio network that shares a licensed channel that is used by a primary transmitter denoted T and primary receiver denoted R. The cognitive radio network supports downlink and uplink transmissions between a secondary base station (SBS) denoted S and K secondary users indexed as $1, 2, \ldots, K$. For either downlink or uplink transmission, a passive eavesdropper denoted E can overhear the transmitted signal. Each node is equipped with a single antenna, and works in half-duplex mode; and each channel experiences path loss attenuation and Rayleigh fading. Thus, the channel gain (square of channel coefficient magnitude) of link $i \to j$ ($i, j \in \{T, R, S, E, 1, \ldots, K\}, i \neq j$), denoted h_{ij}, is exponentially distributed with mean $\Omega_{ij} \triangleq d_{ij}^{-\eta}$. Here d_{ij} is distance between nodes i and j, and η means path loss exponent. The AWGN at each receiver has a mean being zero and a variance being N_0.

The SBS is responsible for secondary user scheduling. For secondary downlink or uplink transmission, the interference to the primary receiver R is required to be not more than a threshold I. Since the primary system cares about interference received from secondary transmissions, the primary receiver cooperates with the secondary system to provide instantaneous channel gain information h_{SR} and h_{kR}, $k \in \mathcal{K} \triangleq \{1, \ldots, K\}$. So the SBS knows h_{SR} and h_{kR}. However, the SBS does not have instantaneous channel gain information of h_{TS} or h_{Tk}, since the primary system does not have incentive to cooperate with the secondary system to get such information. We assume that the SBS knows the mean values of h_{TS} and h_{Tk}. Further, the SBS knows channel gain information between itself and secondary users, i.e., h_{Sk} and h_{kS}, but does not know any channel gain information of links to the eavesdropper.

III. Downlink Scheduling and Analysis

Scheduling Scheme: For secondary downlink, due to the interference limit to the primary receiver, the transmit power of SBS should be set up as $P_S = \frac{I}{h_{SR}}$. If the transmission is for user

Manuscript received September 20, 2015; revised February 2, 2016; accepted March 26, 2016. Date of publication March 31, 2016; date of current version June 8, 2016. The associate editor coordinating the review of this paper and approving it for publication was Y. Zou.

L. Yang, J. Chen, and H. Zhang are with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China (e-mail: lyang@xidian.edu.cn; jianchen@mail.xidian.edu.cn; hlzhang@xidian.edu.cn).

H. Jiang is with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB T6G 1H9, Canada (e-mail: hai1@ualberta.ca).

S. A. Vorobyov is with the Department of Signal Processing and Acoustics, Aalto University, Aalto FI-00076, Finland (e-mail: svor@ieee.org).

Digital Object Identifier 10.1109/LCOMM.2016.2549011

1558-2558 © 2016 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

k ($k \in \mathcal{K}$), the signal-to-interference-plus-noise ratio (SINR) at user k is expressed as $\Gamma_{Sk} \triangleq \frac{h_{Sk} I/h_{SR}}{P_T h_{Tk}+N_0} = \frac{\gamma_{Sk}}{\gamma_{Tk}+1}$, in which P_T is the transmit power of the primary transmitter, $\gamma_{Sk} \triangleq \frac{I \cdot h_{Sk}}{N_0 h_{SR}}$, $\gamma_{Tk} \triangleq \frac{P_T h_{Tk}}{N_0}$; and the SINR at the eavesdropper E is expressed as $\Gamma_{SE} \triangleq \frac{h_{SE} I/h_{SR}}{P_T h_{TE}+N_0} = \frac{\gamma_{SE}}{\gamma_{TE}+1}$, in which $\gamma_{SE} \triangleq \frac{I \cdot h_{SE}}{N_0 h_{SR}}$, $\gamma_{TE} \triangleq \frac{P_T h_{TE}}{N_0}$.

Since the SBS does not have information of h_{Tk}, it does not know the channel capacity of its link to user k. An outage may happen if the interference from primary transmitter T is large enough such that the secondary channel capacity $\log_2(1+\Gamma_{Sk})$ is below the secondary transmission rate r_k. In specific, the downlink TOP conditioned on γ_{Sk}, given as $P_{\text{out}}^{\text{DL}}(k|\gamma_{Sk}) \triangleq \Pr(\log_2(1+\Gamma_{Sk}) < r_k|\gamma_{Sk})$ in which $\Pr(\cdot)$ means probability, can be derived as

$$P_{\text{out}}^{\text{DL}}(k|\gamma_{Sk}) = \begin{cases} 1, & \gamma_{Sk} \le 2^{r_k}-1, \\ \exp\left(-\frac{\frac{\gamma_{Sk}}{2^{r_k}-1}-1}{\bar{\gamma}_{Tk}}\right), & \gamma_{Sk} > 2^{r_k}-1, \end{cases} \tag{1}$$

where $\bar{\gamma}_{Tk} \triangleq \frac{P_T \Omega_{Tk}}{N_0}$ is the mean value of γ_{Tk}. It is required that the conditional TOP $P_{\text{out}}^{\text{DL}}(k|\gamma_{Sk})$ should be not more than a threshold value ϵ_0, which leads to $r_k \le \log_2(1+\omega_k(\epsilon_0)\,\gamma_{Sk})$, where $\omega_k(\epsilon_0) \triangleq (1-\bar{\gamma}_{Tk}\ln\epsilon_0)^{-1}$. To maximally utilize the channel, the secondary transmission rate is set to $r_k^{\text{DL}}(\epsilon_0) = \log_2(1+\omega_k(\epsilon_0)\,\gamma_{Sk})$ when secondary user k is scheduled.

If secondary user k is scheduled, the capacity of wiretap channel is given by $C_{SE} = \log_2(1+\Gamma_{SE})$. Therefore, the achievable downlink secrecy rate of link $S \to k$ with TOP constraint ϵ_0 is $R_{\text{sec}}^{\text{DL}}(k,\epsilon_0) = [r_k^{\text{DL}}(\epsilon_0) - C_{SE}]^+$, where $[x]^+ \triangleq \max\{x, 0\}$. Our target is to schedule a secondary user such that $R_{\text{sec}}^{\text{DL}}(k,\epsilon_0)$ is maximized.

In the expression of $R_{\text{sec}}^{\text{DL}}(k,\epsilon_0)$, the term C_{SE} is a common value for all secondary users. Therefore, maximization of $R_{\text{sec}}^{\text{DL}}(k,\epsilon_0)$ is equivalent to maximization of $r_k^{\text{DL}}(\epsilon_0)$, which is further equivalent to maximization of $\omega_k(\epsilon_0)\,h_{Sk}$. We propose to schedule user $k^* = \arg\max_{k\in\mathcal{K}} \omega_k(\epsilon_0)\,h_{Sk}$ for transmission. So the proposed user scheduling scheme can maximize the achievable secrecy rate in downlink.

Closed-Form SOP Expression: A *secrecy outage* is defined as an event that the achievable secrecy rate is less than a target secrecy rate τ. The SOP in downlink secure transmission can be expressed as

$$\begin{aligned} P_{\text{sec,out}}^{\text{DL}} &\triangleq \Pr(R_{\text{sec}}^{\text{DL}}(k^*,\epsilon_0) < \tau) \\ &= \Pr\left(\frac{\max_{k\in\mathcal{K}} \omega_k(\epsilon_0)\,h_{Sk}}{h_{SR}} < \frac{\mu-1}{\gamma_I} + \frac{\mu \cdot h_{SE}/h_{SR}}{\gamma_{TE}+1}\right) \\ &= \int_0^\infty \int_0^\infty \int_0^\infty \prod_{k\in\mathcal{K}} \Pr\left(\omega_k(\epsilon_0)\,h_{Sk} < \frac{\mu-1}{\gamma_I}x + \frac{\mu y}{z+1}\right) \\ &\quad \times p_{h_{SR}}(x)\,p_{h_{SE}}(y)\,p_{\gamma_{TE}}(z)\mathrm{d}x\mathrm{d}y\mathrm{d}z \\ &\overset{\text{(i)}}{=} \sum_{m=0}^{K} \sum_{\substack{\mathcal{A}_m\subseteq\mathcal{K} \\ |\mathcal{A}_m|=m}} (-1)^m \underbrace{\int_0^\infty \exp\left(-\frac{F(\mathcal{A}_m)(\mu-1)\,x}{\gamma_I}\right) p_{h_{SR}}(x)\mathrm{d}x}_{=I_1(\mathcal{A}_m)} \\ &\quad \times \underbrace{\int_0^\infty \int_0^\infty \exp\left(-\frac{F(\mathcal{A}_m)\mu y}{z+1}\right) p_{h_{SE}}(y)\,p_{\gamma_{TE}}(z)\mathrm{d}y\mathrm{d}z}_{=I_2(\mathcal{A}_m)}, \end{aligned} \tag{2}$$

where $\mu \triangleq 2^\tau$, $\gamma_I \triangleq \frac{I}{N_0}$, $\mathcal{A}_m$ is subset of $\mathcal{K}$ with cardinality $|\mathcal{A}_m| = m$, $F(\mathcal{A}_m) \triangleq \sum_{k\in\mathcal{A}_m} \frac{1}{\omega_k(\epsilon_0)\,\Omega_{Sk}}$, and $p_X(x)$ is the probability density function of random variable X. Step (i) of (2) uses the multinomial expansion, given by [10, eq. (33)] as

$$\prod_{k\in\mathcal{K}} a_k = \sum_{m=0}^{K} \sum_{\mathcal{A}_m\subseteq\mathcal{K}, |\mathcal{A}_m|=m} (-1)^m \prod_{k\in\mathcal{A}_m} (1-a_k). \tag{3}$$

Then, the terms $I_1(\mathcal{A}_m)$ and $I_2(\mathcal{A}_m)$ can be calculated as

$$\begin{aligned} I_1(\mathcal{A}_m) &= \int_0^\infty \exp\left(-\frac{F(\mathcal{A}_m)(\mu-1)\,x}{\gamma_I}\right) \frac{1}{\Omega_{SR}} \exp\left(-\frac{x}{\Omega_{SR}}\right)\mathrm{d}x \\ &= \frac{1/\Omega_{SR}}{1/\Omega_{SR} + F(\mathcal{A}_m)(\mu-1)/\gamma_I}, \end{aligned} \tag{4}$$

$$\begin{aligned} I_2(\mathcal{A}_m) &= \int_0^\infty \int_0^\infty \exp\left(-\frac{F(\mathcal{A}_m)\mu y}{z+1}\right) \frac{1}{\Omega_{SE}} \exp\left(-\frac{y}{\Omega_{SE}}\right) \\ &\quad \times \frac{1}{\bar{\gamma}_{TE}} \exp\left(-\frac{z}{\bar{\gamma}_{TE}}\right)\mathrm{d}y\mathrm{d}z \\ &= 1 - \frac{\mu\Omega_{SE}F(\mathcal{A}_m)}{\bar{\gamma}_{TE}} \int_0^\infty \frac{\exp(-z/\bar{\gamma}_{TE})}{z+1+\mu\Omega_{SE}F(\mathcal{A}_m)}\mathrm{d}z \\ &\overset{\text{(ii)}}{=} 1 + \frac{\mu\Omega_{SE}F(\mathcal{A}_m)}{\bar{\gamma}_{TE}} \exp[G(\mathcal{A}_m)]\mathrm{Ei}[-G(\mathcal{A}_m)], \end{aligned} \tag{5}$$

where $\bar{\gamma}_{TE} \triangleq \frac{P_T\Omega_{TE}}{N_0}$ is the mean value of γ_{TE}, step (ii) in (5) uses [11, eq. (3.352.4)], $\mathrm{Ei}(x) = \int_{-\infty}^{x} \frac{\exp(t)}{t}\mathrm{d}t$ is the exponential integral function [11, eq. (8.211.1)], and $G(\mathcal{A}_m) = [1 + \mu\Omega_{SE}F(\mathcal{A}_m)]/\bar{\gamma}_{TE}$. Then, substituting (4) and (5) into (2), $P_{\text{sec,out}}^{\text{DL}}$ is obtained in closed form.

Secrecy Diversity Analysis: From [9], the secrecy diversity order for secondary transmission is given as $d = -\lim_{\lambda\to\infty} \frac{\log(P_{\text{sec,out}}^{\text{floor}})}{\log(\lambda)}$, where $\lambda \triangleq \frac{\Omega_{\text{M}}}{\Omega_{\text{E}}}$ is called *main-to-eavesdropping ratio (MER)*, Ω_{M} is the average main channel gain (average of the channel gains between SBS and secondary users), Ω_{E} is the average eavesdropping channel gain (average of the channel gains from secondary transmitter(s) to the eavesdropper), and SOP floor $P_{\text{sec,out}}^{\text{floor}} \triangleq \lim_{I\to\infty} P_{\text{sec,out}}$ gives a lower bound of SOP with large interference threshold I. Using Ω_{M} and Ω_{E} as reference main channel gain and reference eavesdropping channel gain, respectively, we rewrite Ω_{Sk}, Ω_{kS}, Ω_{SE}, and Ω_{kE} as $\Omega_{Sk} = \beta_{Sk}\Omega_{\text{M}}$, $\Omega_{kS} = \beta_{kS}\Omega_{\text{M}}$, $\Omega_{SE} = \beta_{SE}\Omega_{\text{E}}$, and $\Omega_{kE} = \beta_{kE}\Omega_{\text{E}}$, where β_{Sk}, β_{kS}, β_{SE}, and β_{kE} are positive constants.

When $I \to \infty$, from (2), the floor of $P_{\text{sec,out}}^{\text{DL}}$ is given as

$$\begin{aligned} P_{\text{sec,out}}^{\text{DL,floor}} &= \Pr\left(\max_{k\in\mathcal{K}} \omega_k(\epsilon_0)\,h_{Sk} < \frac{\mu h_{SE}}{\gamma_{TE}+1}\right) = \int_0^\infty \int_0^\infty \\ &\prod_{k\in\mathcal{K}} \left[1-\exp\left(-\frac{\mu x}{\omega_k(\epsilon_0)\,\beta_{Sk}\Omega_{\text{M}}(y+1)}\right)\right] p_{h_{SE}}(x)\,p_{\gamma_{TE}}(y)\mathrm{d}x\mathrm{d}y. \end{aligned} \tag{6}$$

It is known from [12, Proposition 1] that, when MER $\lambda \to \infty$, the equation $1-\exp(-\frac{\mu x}{\omega_k(\epsilon_0)\,\beta_{Sk}\Omega_{\text{M}}(y+1)}) = \frac{\mu x}{\omega_k(\epsilon_0)\,\beta_{Sk}\Omega_{\text{M}}(y+1)}$ holds with probability 1. Thus, in high-MER regime, we have

$$\begin{aligned} P_{\text{sec,out}}^{\text{DL,floor}} &\overset{\lambda\to\infty}{\simeq} \frac{\mu^K(\Omega_{SE}\bar{\gamma}_{TE})^{-1}}{\Omega_{\text{M}}^K \prod_{k\in\mathcal{K}} \omega_k(\epsilon_0)\,\beta_{Sk}} \int_0^\infty x^K \exp(-\frac{x}{\Omega_{SE}})\mathrm{d}x \\ &\quad \times \int_0^\infty (y+1)^{-K} \exp(-\frac{y}{\bar{\gamma}_{TE}})\mathrm{d}y. \end{aligned} \tag{7}$$

Using [11, eqs. (3.351.3), (3.353.2)] in the two integrals in (7) leads to high-MER asymptotic expression of $P_{\text{sec,out}}^{\text{DL,floor}}$

$$\begin{aligned} P_{\text{sec,out}}^{\text{DL,floor}} &\overset{\lambda\to\infty}{\simeq} \frac{K(\mu\beta_{SE})^K}{\lambda^K\bar{\gamma}_{TE}\prod_{k\in\mathcal{K}}\omega_k(\epsilon_0)\,\beta_{Sk}} \left[\sum_{n=1}^{K-1}(n-1)!(\frac{-1}{\bar{\gamma}_{TE}})^{K-n-1}\right. \\ &\quad \left. -(\frac{-1}{\bar{\gamma}_{TE}})^{K-1}\exp(\frac{1}{\bar{\gamma}_{TE}})\mathrm{Ei}(\frac{-1}{\bar{\gamma}_{TE}})\right] \propto \lambda^{-K}, \end{aligned} \tag{8}$$

which means that the proposed scheduling scheme achieves a secrecy diversity order of K, i.e., full secrecy diversity.

IV. Uplink Scheduling and Analysis

Scheduling Scheme: For uplink, if user k is scheduled to transmit, its transmit power should be set as $P_k = \frac{I}{h_{kR}}$ due to the interference constraint to the primary receiver. SINR at the SBS is given as $\Gamma_{kS} \triangleq \frac{h_{kS} I/h_{kR}}{P_T h_{TS}+N_0} = \frac{\gamma_{kS}}{\gamma_{TS}+1}$, in which $\gamma_{kS} \triangleq \frac{I \cdot h_{kS}}{N_0 h_{kR}}$ and $\gamma_{TS} \triangleq \frac{P_T h_{TS}}{N_0}$. The SINR at the eavesdropper is given as $\Gamma_{kE} \triangleq \frac{h_{kE} I/h_{kR}}{P_T h_{TE}+N_0} = \frac{\gamma_{kE}}{\gamma_{TE}+1}$, in which $\gamma_{kE} \triangleq \frac{I \cdot h_{kE}}{N_0 h_{kR}}$.

Since information of h_{TS} is unknown at the SBS, a secondary transmission outage may happen if the interference from the primary transmitter is large enough. Similar to (1), if the secondary transmission rate is r_k, the uplink TOP conditioned on γ_{kS} is given as

$$P_{\text{out}}^{\text{UL}}(k|\gamma_{kS}) = \begin{cases} 1, & \gamma_{kS} \le 2^{r_k} - 1, \\ \exp(-\frac{\frac{\gamma_{kS}}{2^{r_k}-1}-1}{\bar{\gamma}_{TS}}), & \gamma_{kS} > 2^{r_k} - 1, \end{cases} \tag{9}$$

where $\bar{\gamma}_{TS} \triangleq \frac{P_T \Omega_{TS}}{N_0}$ is the mean value of γ_{TS}. Here we also require that the conditional TOP $P_{\text{out}}^{\text{UL}}(k|\gamma_{kS})$ should be not more than ϵ_0, which leads to $r_k \le \log_2(1 + \omega_0(\epsilon_0)\, \gamma_{kS})$ where $\omega_0(\epsilon_0) = (1 - \bar{\gamma}_{TS} \ln \epsilon_0)^{-1}$. To maximally utilize the channel, the secondary transmission rate is set to $r_k^{\text{UL}}(\epsilon_0) = \log_2(1 + \omega_0(\epsilon_0)\, \gamma_{kS})$ if user k is scheduled.

If user k is scheduled, the capacity of wiretap link $k \to E$ is given by $C_{kE} = \log_2(1 + \Gamma_{kE})$. So the achievable secrecy rate with TOP constraint ϵ_0 is $R_{\text{sec}}^{\text{UL}}(k, \epsilon_0) = [r_k^{\text{UL}}(\epsilon_0) - C_{kE}]^+ = [\log_2(1 + \omega_0(\epsilon_0)\, \frac{I \cdot h_{kS}}{N_0 h_{kR}}) - \log_2(1 + \frac{I \cdot h_{kE}/N_0}{(\gamma_{TE}+1)\, h_{kR}})]^+$.

Since γ_{TE} and h_{kE} are unknown in the secondary system, it is impossible to maximize $R_{\text{sec}}^{\text{UL}}(k, \epsilon_0)$ in practical user scheduling. Note that in the expression of $R_{\text{sec}}^{\text{UL}}(k, \epsilon_0)$, h_{kR} exists in term $\omega_0(\epsilon_0)\, \frac{I \cdot h_{kS}}{N_0 h_{kR}}$ and term $\frac{I \cdot h_{kE}/N_0}{(\gamma_{TE}+1)\, h_{kR}}$. Based on this, we propose that the scheduled user $k^\dagger$ is selected as $k^\dagger = \arg\max_{k \in \mathcal{K}} \omega_0(\epsilon_0)\, h_{kS}$.

Closed-Form SOP Expression: Similar to (2), for a target secrecy rate τ, the SOP if user i is scheduled is expressed as

$$\begin{aligned} P_{\text{sec,out}}^{\text{UL}}|_{k^\dagger=i} &= \Pr(R_{\text{sec}}^{\text{UL}}(i, \epsilon_0) < \tau | k^\dagger = i) \\ &= \Pr\left(\omega_0(\epsilon_0)\, \frac{\max_{k\in\mathcal{K}} h_{kS}}{h_{iR}} < \frac{\mu-1}{\gamma_I} + \frac{\mu \cdot h_{iE}/h_{iR}}{\gamma_{TE}+1}\right) \\ &= \int_0^\infty \int_0^\infty \int_0^\infty \prod_{k\in\mathcal{K}} \Pr\left(h_{kS} < \frac{\mu-1}{\omega_0(\epsilon_0)\, \gamma_I} x + \frac{\mu y}{\omega_0(\epsilon_0)\,(z+1)}\right) \\ &\quad \times p_{h_{iR}}(x) p_{h_{iE}}(y) p_{\gamma_{TE}}(z) \mathrm{d}x\mathrm{d}y\mathrm{d}z \\ &\overset{\text{(iii)}}{=} \sum_{m=0}^{K} \sum_{\substack{\mathcal{A}_m \subseteq \mathcal{K} \\ |\mathcal{A}_m|=m}} (-1)^m \underbrace{\int_0^\infty \exp\left(-\frac{F'(\mathcal{A}_m)(\mu-1)\, x}{\gamma_I}\right) p_{h_{iR}}(x) \mathrm{d}x}_{=J_{1,i}(\mathcal{A}_m)} \\ &\quad \times \underbrace{\int_0^\infty \int_0^\infty \exp\left(-\frac{F'(\mathcal{A}_m)\mu y}{z+1}\right) p_{h_{iE}}(y) p_{\gamma_{TE}}(z) \mathrm{d}y\mathrm{d}z}_{=J_{2,i}(\mathcal{A}_m)}, \end{aligned} \tag{10}$$

where $F'(\mathcal{A}_m) \triangleq \sum_{k\in\mathcal{A}_m} \frac{1}{\omega_0(\epsilon_0)\, \Omega_{kS}}$ and step (iii) uses multinomial expansion given in (3). With the similar calculation in (4) and (5), the terms $J_{1,i}(\mathcal{A}_m)$ and $J_{2,i}(\mathcal{A}_m)$ are obtained as $J_{1,i}(\mathcal{A}_m) = \frac{1/\Omega_{iR}}{1/\Omega_{iR}+F'(\mathcal{A}_m)(\mu-1)/\gamma_I}$, $J_{2,i}(\mathcal{A}_m) = 1 + \frac{\mu\Omega_{iE} F'(\mathcal{A}_m)}{\bar{\gamma}_{TE}} \exp[G_i'(\mathcal{A}_m)]\mathrm{Ei}[-G_i'(\mathcal{A}_m)]$, where $G_i'(\mathcal{A}_m) \triangleq [1 + \mu\Omega_{iE} F'(\mathcal{A}_m)]/\bar{\gamma}_{TE}$.

Based on expression (10), a closed-form SOP expression of the proposed uplink user scheduling can be expressed by using the Total Probability Theorem as $P_{\text{sec,out}}^{\text{UL}} = \sum_{i=1}^{K} \Pr(k^\dagger = i) P_{\text{sec,out}}^{\text{UL}}|_{k^\dagger=i}$ in which the term $\Pr(k^\dagger = i)$ is expressed (similar to derivations in the Appendix of [13]) as

$$\Pr(k^\dagger = i) = 1 + \sum_{n=1}^{K-1} \sum_{\substack{\mathcal{B}_n \subseteq \mathcal{K}\setminus\{i\} \\ |\mathcal{B}_n|=n}} \frac{(-1)^n 1/\beta_{iS}}{1/\beta_{iS} + \sum_{k\in\mathcal{B}_n} 1/\beta_{kS}}, \tag{11}$$

where $\mathcal{B}_n$ is subset of $\mathcal{K} \setminus \{i\}$ with cardinality $|\mathcal{B}_n| = n$.

Secrecy Diversity Analysis: As shown in (11), the probability $\Pr(k^\dagger = i)$ is only related to $\beta_{kS} (k \in \mathcal{K})$, and thus, it is independent from I and λ. With the similar procedure in (6), (7), and (8), the high-MER asymptotic expression of the floor of $P_{\text{sec,out}}^{\text{UL}}|_{k^\dagger=i}$ is obtained as

$$\begin{aligned} P_{\text{sec,out}}^{\text{UL,floor}}|_{k^\dagger=i} &\overset{\lambda\to\infty}{\simeq} \frac{K(\mu\beta_{iE})^K}{\lambda^K \bar{\gamma}_{TE} [\omega_0(\epsilon_0)]^K \prod_{k\in\mathcal{K}} \beta_{kS}} \left[\sum_{n=1}^{K-1} (n-1)! \right. \\ &\quad \left. \times (\frac{-1}{\bar{\gamma}_{TE}})^{K-n-1} - (\frac{-1}{\bar{\gamma}_{TE}})^{K-1} \exp(\frac{1}{\bar{\gamma}_{TE}}) \mathrm{Ei}(\frac{-1}{\bar{\gamma}_{TE}})\right] \propto \lambda^{-K}. \end{aligned}$$

Therefore, for the SOP floor of proposed uplink user scheduling, we have $P_{\text{sec,out}}^{\text{UL,floor}} = \sum_{i=1}^{K} \Pr(k^\dagger = i) P_{\text{sec,out}}^{\text{UL,floor}}|_{k^\dagger=i} \overset{\lambda\to\infty}{\propto} \lambda^{-K}$, which means full secrecy diversity achieved by the proposed uplink scheduling scheme.

V. Performance Evaluation

We verify our theoretical results by simulation, in which the primary transmitter, primary receiver, and SBS are located at $(-8, 1)$, $(-8, -1)$, and $(0, 0)$. Secondary users are randomly distributed in a circle centered at the SBS and with radius being $d_1 = 1$. Other system parameters are: path loss exponent $\eta = 3$, noise power $N_0 = 1$, transmit power of primary transmitter $P_T = 40$ dB, and target secrecy rate $\tau = 3$ bps/Hz.

For the proposed downlink and uplink user scheduling schemes, Fig. 1 shows the SOP obtained from both theoretical results (denoted as "Exact") and simulation, when K is 3 or 6, an eavesdropper is located at $(10, 0)$, and $\epsilon_0 = 0.01$. The theoretical results exactly match simulation results. From Fig. 1, as the interference threshold I increases, the SOP of the proposed scheduling schemes decrease, and converge when I is more than 20 dB. This is consistent with our observation in Sections III and IV that the SOP reaches its floor when the interference threshold is sufficiently large. When K increases from 3 to 6, the SOP in downlink and uplink largely decrease. This is because a secrecy diversity order of K is achieved by the proposed user scheduling schemes. For comparison, Fig. 1 also includes the simulated SOP of a genie-aided scheme that has instantaneous channel gain information of links to the eavesdropper E and selects the user such that the achievable secrecy rate is maximized, i.e., user $n^{\text{DL},*} = \arg\max_{k\in\mathcal{K}} [r_k^{\text{DL}}(\epsilon_0) - C_{SE}]^+$ and $n^{\text{UL},*} = \arg\max_{k\in\mathcal{K}} [r_k^{\text{UL}}(\epsilon_0) - C_{kE}]^+$ are selected for downlink and uplink, respectively. We also consider the following alternative uplink scheduling scheme that does not know h_{TE} and h_{kE} but knows their mean values: the scheme first substitutes h_{TE} and h_{kE} with their mean values Ω_{TE} and Ω_{kE} in expression of $R_{\text{sec}}^{\text{UL}}(k, \epsilon_0)$, and then

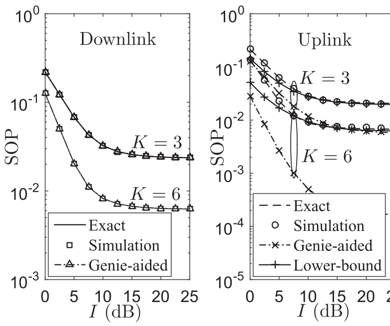

Fig. 1. SOP versus interference threshold.

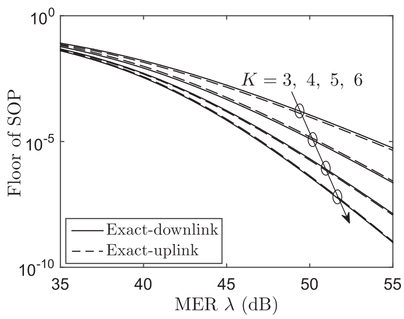

Fig. 2. SOP floor versus MER.

selects the user that maximizes the substituted $R_{\text{sec}}^{\text{UL}}(k, \epsilon_0)$. The alternative uplink scheduling scheme approximately provides an SOP lower bound for any practical scheduling scheme including our uplink scheduling scheme, and thus, is called *lower-bound-SOP scheme* here (denoted as "lower-bound" in Fig. 1). Note that neither the genie-aided scheme nor the lower-bound-SOP scheme is practical since a practical user scheduling scheme does not have information of h_{TE}, h_{kE} or their mean values. In Fig. 1, as expected, the proposed downlink user scheduling scheme has the same SOP as the downlink genie-aided scheme. The proposed uplink user scheduling scheme has a higher SOP than that of uplink genie-aided scheme, and has an SOP close to that of the lower-bound-SOP scheme, which means that the proposed uplink scheduling scheme can achieve close to the SOP lower bound of any practical scheme.

Next we evaluate secrecy diversity order of the proposed schemes with TOP constraint $\epsilon_0 = 0.01$. For this purpose, we need to plot a curve of the SOP floor versus MER. We consider that an eavesdropper is located at $(d_2, 0)$. Thus, average main channel gain is $\Omega_{\text{M}} = (\frac{d_1}{2})^{-\eta}$, average eavesdropping channel gain is $\Omega_{\text{E}} = d_2^{-\eta}$, and the MER is given as $\lambda = \frac{\Omega_{\text{M}}}{\Omega_{\text{E}}} = (\frac{2d_2}{d_1})^{\eta}$. By setting $d_1 = 1$, we vary the value of d_2 such that MER varies from 30 dB (medium MER) to 60 dB (high MER), and we obtain the SOP floor of proposed schemes (obtained by setting $I = \infty$ in (2) for downlink and in $P_{\text{sec,out}}^{\text{UL}}$ expression derived in Section IV for uplink) when $K = 3, 4, 5, 6$. The results are shown in Fig. 2 (since the accuracy of SOP expressions is validated in Fig. 1, only theoretical results are provided in Fig. 2). The SOP floor decreases fast when MER increases. This is because the eavesdropping channel becomes weaker as MER increases. When K increases from 3 to 6, the magnitude of slope of SOP floor curves in high-MER regime also increases from 3 to 6, thus verifying that our proposed schemes achieve full secrecy diversity.

Next we compare with the case when the uplink user scheduling scheme proposed in [9] is used. The scheme in [9] approximates interference from the primary transmitter as

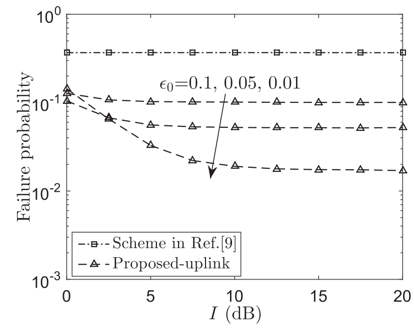

Fig. 3. Failure probability versus interference threshold.

AWGN. Thus, for our considered system, the scheme in [9] treats the interference plus noise at SBS and eavesdropper as AWGN with variances $P_T\Omega_{TS} + N_0$ and $P_T\Omega_{TE} + N_0$. Fig. 3 shows the *failure probability* (FP) (here a failure is defined as an event when a transmission outage or a secrecy outage happens) of the proposed uplink user scheduling scheme and user scheduling scheme in [9] with an eavesdropper located at (10, 0) and $K = 6$. It can be seen that the AWGN modeling of primary interference leads to a larger FP. This is because the primary interference is underestimated by the AWGN modeling. FP of proposed uplink user scheduling scheme is much lower, and largely decreases as ϵ_0 decreases from 0.1 to 0.01, because the TOP of proposed scheme is bounded by ϵ_0.

REFERENCES

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

[2] Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. 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.

[3] 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.

[4] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the security of cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3790–3795, Aug. 2015.

[5] F. Zhu and M. Yao, "Improving physical layer security for CRNs using SINR-based cooperative beamforming," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1835–1841, Mar. 2016.

[6] H. Sakran, M. Shokair, O. Nasr, S. EI-Rabaie, and A. A. EI-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Commun.*, vol. 6, no. 16, pp. 2676–2687, Nov. 2012.

[7] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 46–49, Feb. 2015.

[8] 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.

[9] Y. Zou, X. Li, and Y.-C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2222–2236, Nov. 2014.

[10] A. Bletsas, A. G. Dimitriou, and J. N. Sahalos, "Interference-limited opportunistic relaying with reactive sensing," *IEEE Trans. Wireless Commun.*, vol. 9, no. 1, pp. 14–20, Jan. 2010.

[11] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th ed. New York, NY, USA: Academic, 2007.

[12] 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.

[13] H. Ding, J. Ge, D. B. da Costa, and Z. Jiang, "A new efficient low-complexity scheme for multi-source multi-relay cooperative networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 2, pp. 716–722, Feb. 2011.