**Proceedings Paper:**
Deng, Y, Wang, L, Zaidi, SAR et al. (2 more authors) (2015) On the Security of Large Scale Spectrum Sharing Networks. In: 2015 IEEE International Conference on Communications. 2015 IEEE International Conference on Communications, 08-12 Jun 2015, ExCel London, IK. IEEE , pp. 4877-4882.

https://doi.org/10.1109/icc.2015.7249095

# On the Security of Large Scale Spectrum Sharing Networks

Yansha Deng*, Lifeng Wang*, Syed Ali Raza Zaidi†, Jinhong Yuan‡, and Maged Elkashlan*
*School of Electronic Engineering and Computer Science, Queen Mary University of London, London, UK
† School of Electronics and Electrical Engineering, University of Leeds, Leeds, United Kingdom
‡School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, Australia

***Abstract*—We investigate beamforming and artificial noise generation at the secondary transmitters to establish secure transmission in large scale spectrum sharing networks, where multiple non-colluding eavesdroppers attempt to intercept the secondary transmission. We develop a comprehensive analytical framework to accurately assess the secrecy performance under the primary user's quality of service constraint. Our aim is to characterize the impact of beamforming and artificial noise generation on this complex large scale network. We first derive the exact expressions for the average secrecy rate and the secrecy outage probability. Our results show that there exists an average secrecy rate wall beyond which the primary user's quality of service is violated. Interestingly, we find that different from the conventional network with fixed nodes where equal power allocation achieves near optimal average secrecy rate, the equal power allocation may not be a good option for large scale spectrum sharing networks.**

## I. Introduction

The sky-rocketing growth of multimedia infotainment applications and broadband-hungry mobile devices (smart-phone, tablets, machine-to-machine (M2M) communication devices) exacerbate the stringent demand for high data rate and data service. To cope with this, the Federal Communication Commission (FCC) approved to allow the unlicensed users to transmit on the spectrum reserved for the wireless broadband devices as long as the quality of service (QoS) of the primary network is satisfied [1–3]. This is the so-called cognitive radio networks (CRNs).

Due to the open and dynamic characteristics of cognitive wireless channels, new classes of security threats and challenges are introduced into CRNs (opportunistic utilization of licensed channels). In this paper, we focus on the eavesdropping attacks targeted at the secondary users (SUs), where the eavesdroppers attempt to intercept the transmission between the secondary transceivers [4]. In this case, the eavesdroppers always keep silent without transmitting any signals, and can hardly be detected by the SUs.

Recently, beamforming and artificial noise generation (BF&AN) at the legitimate transmitter has been proposed as a promising technique to confuse the eavesdroppers and enhance the security [5, 6]. In this paper, we study the secrecy performance of large scale underlay spectrum sharing networks with BF&AN at the SU transmitter. Stochastic geometry and random geometric graphs are used to model the proposed network [7, 8]. Equipping the SU transmitter with multiple antennas capable of transmitting information signal and artificial noise (AN) simultaneously brings array gains at the legitimate receiver and disrupts the reception at the eavesdropper. This will boost the signal-to-interference ratio (SIR) at the SU receiver while impair the received signals at the eavesdroppers. We concentrate on characterizing the impact of several key system parameters such as the power allocation factor, the number of antennas at the SU transmitter, the densities of PUs, SUs, and eavesdroppers on the secrecy performance. Our contributions are summarized as follows:

1) We quantify the permissive transmit power region where the primary network's QoS can be guaranteed, as presented in **Theorem 1**. It is shown that from the PU receiver's perspective, the permissive transmit power region fluctuates significantly for different densities of SUs and PUs.
2) We derive the exact expressions for the average secrecy rate and the secrecy outage probability of the secondary network with BF&AN at the SU transmitters, as presented in **Theorems 2** and **3**. It is shown that there exists an average secrecy rate wall beyond which the PU receiver's QoS is violated. It is revealed that the optimal power allocation factor which achieves the maximum average secrecy rate varies for different system parameters, and the equal power allocation may not achieve near optimal average secrecy rate.

## II. System and Channel Model

We consider the secure communication in an underlay spectrum sharing network where the SU transmitters communicate with the corresponding SU receivers under the potential malicious attempt of multiple eavesdroppers, as shown in Fig. 1. Each SU transmitter has $N_s$ antennas, and others in this model are all single-antenna nodes. We have a set of PU transmitters, SU transmitters, and eavesdroppers locations, denoted by $\Phi_p$, $\Phi_s$ and $\Phi_e$, in which $\Phi_p$, $\Phi_s$ and $\Phi_e$ follow independent homogeneous Poisson point processes (HPPPs) with densities $\lambda_p$, $\lambda_s$ and $\lambda_e$, respectively. This model is practical and representative for the decentralized networks where each node has substantial mobility or networks deployed randomly [9]. Following the bipolar network model [10, 11], we assume that each PU/SU transmitter communicates with its unique associated intended PU/SU receiver at distances $r_p$ and $r_s$, respectively.

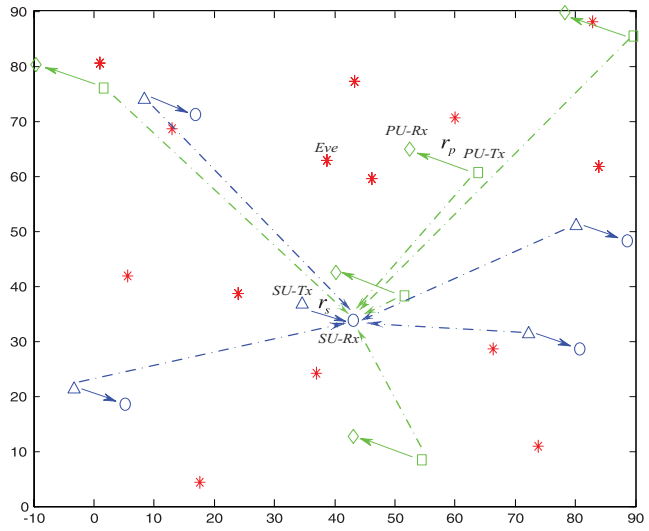


Fig. 1. A realization of a large scale spectrum sharing network model describing the received signal at a SU receiver. In this network, the green square represents the PU transmitter, the diamond represents the PU receiver, the triangle represents the SU transmitter, the circle represents the SU receiver, and the red star represents the eavesdropper. The blue solid line represents the secondary transmission, the green solid line represents the primary transmission, the blue dashed line represents the interference from the SU transmitter, and the green dashed line presents the interference from the PU transmitter.

The wireless channels are modeled as independent quasi-static Rayleigh fading. The eavesdroppers interpret the secondary transmitter's signal without trying to modify it. In this complex CRNs, we consider the interference-limited case where the thermal noise is negligible compared with the aggregate interference from other transmitters. Similar as [12, 13], we utilize the SIR to characterize the performance.

We mask the beamformed broadcast information with the AN at the SU transmitters to confuse the eavesdroppers. Each SU transmitter broadcasts the information-bearing signals and artificial noise simultaneously. The AN is transmitted in the null space of the intended SU receiver's channel, thus imposing no effect on the secondary channel, whereas degrading the eavesdropper's channel. We denote the intended channel vector between the $i$th SU transmitter ($i \in \Phi_s$) and the corresponding SU receiver as $\mathbf{h}_{i,s_i} \in \mathcal{C}^{1\times N_s}$, the channel state information (CSI) of which is known at the $i$th SU transmitter. An orthonormal basis of $\mathcal{C}^{N_s\times N_s}$ is generated at the $i$th SU transmitter as $\left[\mathbf{h}_{i,s_i}^{\dagger}\Big/\|\mathbf{h}_{i,s_i}\|,\ \mathbf{G}_{i,s_i}\right]_{N_s\times N_s}$ [1], where $\mathbf{G}_{i,s_i}$ is a $N_s \times (N_s-1)$ matrix. Note that each column of $\mathbf{G}_{i,s_i}$ and $\mathbf{h}_{i,s_i}^{\dagger}\Big/\|\mathbf{h}_{i,s_i}\|$ are mutually orthogonal. We define $b_i$ as the information-bearing signal, and $\mathbf{n}_A$ as the artificial noise. The transmitted beamforming and AN symbol vector is modelled as

$$\mathbf{x}_{s_i} = \frac{\mathbf{h}_{i,s_i}^{\dagger}}{\|\mathbf{h}_{i,s_i}\|} b_i + \mathbf{G}_{i,s_i}\mathbf{n}_A, \tag{1}$$

[1] $\dagger$ is the conjugate transpose operator.

where $E\left\{b_i b_i^{\dagger}\right\} = \delta_s^2$, and $N_s - 1$ elements of $\mathbf{n}_A$ are independent and identically distributed (i.i.d) complex Gaussian random variables with zero mean and variance $\sigma_n^2$. Thus, the total transmit power per transmission $P_s$ is given by $P_s = P_I + P_A$, where the power allocated to the information signal is $P_I = \sigma_s^2$ and the power allocated to the AN is $P_A = (N_s - 1)\,\sigma_n^2$. We also define $\mu$ as the fraction of power assigned to the information signal, thus, $P_I = \mu P_s$ .

In the primary network, we consider an arbitrary pair of PU transceiver, referred to as the typical PU transmitter and receiver. We assume the typical PU receiver is located at the origin of the coordinate system, and the distance between the PU transmitter and its associated PU receiver is $r_p$. According to the Slivnyak's theorem [14], adding a probe point to the HPPP at an arbitrary location does not affect the law of the point process. For each PU receiver, the information-bearing signal and AN generated by the secondary transmitter are regarded as interference, thus the received SIR at the typical PU receiver is given by

$$\gamma_{\mathtt{SIR}}^{p,AN} = \frac{|h_{p_0}|^2 {r_p}^{-\alpha}}{I_{p,p_0} + P_p^{-1} I_{s,p_0}}, \tag{2}$$

where $I_{p,p_0} = \sum_{j\in\Phi_p\setminus\{0\}} |h_{j,p_0}|^2 |X_{j,p_0}|^{-\alpha}$, $I_{s,p_0} = \sum_{i\in\Phi_s}\left[\sigma_s^2 \left|\mathbf{h}_{i,p_0}\frac{\mathbf{h}_{i,s_i}^{\dagger}}{\|\mathbf{h}_{i,s_i}^{\dagger}\|}\right|^2 + \sigma_n^2\left\|\mathbf{h}_{i,p_0}\mathbf{G}_{i,s_i}\right\|^2\right]|X_{i,p_0}|^{-\alpha}$. In (2), $\alpha$ is the path-loss exponent, $h_{p_0}$ is the channel fading gain between the typical PU transmitter and the typical PU receiver, $h_{j,p_0}$ and $|X_{j,p_0}|$ are the interfering channel fading gain and distance between the $j$th PU transmitter and the typical PU receiver, respectively, $\mathbf{h}_{i,p_0} \in \mathcal{C}^{1\times N_s}$ and $|X_{i,p_0}|$ are the interfering channel vector and distance between the $i$th SU transmitter and the typical PU receiver, respectively, and $P_p$ is the transmit power at the PU transmitter.

In the secondary network, we shift the coordinate system to put the typical SU receiver at the origin, and assume $\mathbf{h}_{0,s_0} \in \mathcal{C}^{1\times N_s}$ and $r_s$ to be the channel vector and distance between the typical SU transmitter and corresponding typical SU receiver. Note that each SU transmitter transmits the signal vector expressed as (1), we obtain the effective signal at the typical SU receiver as $\mathbf{h}_{0,s_0}\mathbf{x}_{s_0} = \mathbf{h}_{0,s_0}\frac{\mathbf{h}_{0,s_0}^{\dagger}}{\|\mathbf{h}_{0,s_0}\|}b_0 + \mathbf{h}_{0,s_0}\mathbf{G}_{0,s_0}\mathbf{n}_A = \|\mathbf{h}_{0,s_0}\|b_0$. Due to the concurrent transmission in the underlay spectrum sharing network, the typical SU receiver is subject to the aggregate interference from the PU transmitters and other SU transmitters, thus, the received SIR at the typical SU receiver is given by

$$\gamma_{\mathtt{SIR}}^{s,AN} = \frac{\sigma_s^2\|\mathbf{h}_{0,s_0}\|^2 {r_s}^{-\alpha}}{I_{s,s_0} + P_p I_{p,s_0}}, \tag{3}$$

where $I_{p,s_0} = \sum_{j\in\Phi_p}|h_{j,s_0}|^2|X_{j,s_0}|^{-\alpha}$, $I_{s,s_0} = \sum_{i\in\Phi_s\setminus\{0\}}\left[\sigma_s^2\left|\mathbf{h}_{i,s_0}\frac{\mathbf{h}_{i,s_i}^{\dagger}}{\|\mathbf{h}_{i,s_i}^{\dagger}\|}\right|^2 + \sigma_n^2\left\|\mathbf{h}_{i,s_0}\mathbf{G}_{i,s_i}\right\|^2\right]|X_{i,s_0}|^{-\alpha}$. In (3), $h_{j,s_0}$ and $|X_{j,s_0}|$ are the channel fading gain and distance between the $j$th PU transmitter and the typical SU receiver, respectively, $\mathbf{h}_{i,s_0} \in \mathcal{C}^{1\times N_s}$ and $|X_{i,s_0}|$ are the

interfering channel vector and distance between the $i$th SU transmitter and the typical SU receiver, respectively.

In the eavesdropping channel, we consider the most detrimental eavesdropper that has the highest SIR for a typical SU transmitter [15]. Note that eavesdroppers are only interested in the secondary transmissions, and interpret the primary transmissions as interference. This assumption is practical since the primary networks operate in the Digital Video Broadcasting (DVB) spectrum and broadcast the public service to households, which do not have any confidential messages. We assume $\mathbf{h}_{0,e_k} \in \mathcal{C}^{1\times N_s}$ to be the channel vector between the typical SU transmitter and an arbitrary eavesdropper $e_k \in \Phi_e$. As such, the SIR at the most detrimental eavesdropper is expressed as

$$\gamma_{\mathtt{SIR}}^{e,AN} = \max_{e_k\in\Phi_e}\left\{\gamma_{\mathtt{SIR}}^{e_k,AN}\right\}, \tag{4}$$

where

$$\gamma_{\mathtt{SIR}}^{e_k,AN} = \frac{\sigma_s^2\left|\mathbf{h}_{0,e_k}\frac{\mathbf{h}_{0,s_0}^\dagger}{\left\|\mathbf{h}_{0,s_0}^\dagger\right\|}\right|^2|X_{e_k}|^{-\alpha}}{I_{s,e_k}+P_pI_{p,e_k}+\sigma_n^2I_{s_0,e_k,an}}. \tag{5}$$

In (5), $I_{p,e_k} = \sum_{j\in\Phi_p}|h_{j,e_k}|^2|X_{j,e_k}|^{-\alpha}$, $I_{s,e_k} = \sum_{i\in\Phi_s\setminus\{0\}}\left[\sigma_s^2\left|\mathbf{h}_{i,e_k}\frac{\mathbf{h}_{i,s_i}^\dagger}{\left\|\mathbf{h}_{i,s_i}^\dagger\right\|}\right|^2+\sigma_n^2\left\|\mathbf{h}_{i,e_k}\mathbf{G}_{i,s_i}\right\|^2\right]|X_{i,e_k}|^{-\alpha}$, $I_{s_0,e_k,an} = \|\mathbf{h}_{0,e_k}\mathbf{G}_{0,s_0}\|^2|X_{e_k}|^{-\alpha}$. Note that $h_{j,e_k}$ and $|X_{j,e_k}|$ are the channel fading gain and distance between the $j$th PU transmitter and the $k$th eavesdropper, respectively, $\mathbf{h}_{i,e_k}\in\mathcal{C}^{1\times N_s}$ and $|X_{i,e_k}|$ are the channel vector and distance between the $i$th SU transmitter and the $k$th eavesdropper, respectively, $|X_{e_k}|$ is the distance between the typical SU transmitter and the $k$th eavesdropper.

To facilitate the performance analysis, we first present the Laplace transform of the aggregate interference from SU transmitters $I_{s,z}=\sum_{i\in\Phi_s}W_{s_i,z}|X_{i,z}|^{-\alpha}$ in (2), (3), and (4) as the following lemma, where $z\in\{p_0,d_0,e_k\}$. Here, we define $W_{s_i,z} = \sigma_s^2\left|\mathbf{h}_{i,z}\frac{\mathbf{h}_{i,s_i}^\dagger}{\left\|\mathbf{h}_{i,s_i}^\dagger\right\|}\right|^2+\sigma_n^2\left\|\mathbf{h}_{i,z}\mathbf{G}_{i,s_i}\right\|^2$, where $\mathbf{h}_{i,s_i}$ is the intended channel, and the BF&AN signal $\mathbf{x}_{s_i}$ in (1) transmitted by the $i$th SU transmitter is received by the non-intended receiver $z$, rather than the $i$th SU receiver.

**Lemma 1.** *The Laplace transform of the interference from the SU transmitters with BF&AN to the non-intended receiver $I_{s,z}$ is derived as*

$$\mathcal{L}_{I_{s,z}}(s) = \begin{cases} \exp\left(-\lambda_s\pi P_s^{\frac{2}{\alpha}}\Upsilon_1\Gamma\left(1-\frac{2}{\alpha}\right)s^{\frac{2}{\alpha}}\right) & \mu\neq\frac{1}{N_s} \\ \exp\left(-\lambda_s\pi(\mu P_s)^{\frac{2}{\alpha}}\Gamma\left(N_s+\frac{2}{\alpha}\right)\frac{\Gamma\left(1-\frac{2}{\alpha}\right)}{\Gamma(N_s)}s^{\frac{2}{\alpha}}\right) & \mu=\frac{1}{N_s}, \end{cases} \tag{6}$$

*where*

$$\Upsilon_1 = \left(1-\frac{(1-\mu)}{(N_s-1)\,\mu}\right)^{1-N_s}\Big[\mu^{\frac{2}{\alpha}}\Gamma\big(1+\frac{2}{\alpha}\big)-\frac{1}{\mu} \left(\frac{(1-\mu)}{N_s-1}\right)^{1+\frac{2}{\alpha}}\sum_{k=0}^{N_s-2}\left(1-\frac{(1-\mu)}{(N_s-1)\,\mu}\right)^k\frac{\Gamma\left(k+1+\frac{2}{\alpha}\right)}{\Gamma(k+1)}\Big]. \tag{7}$$

Due to the limited space, detailed derivation is not included.

## III. Exact Secrecy Perfromance

In this section, we first present the SU's permissive transmit power region, and then examine key secrecy performance, namely the average secrecy rate and the secrecy outage probability, in large scale spectrum sharing network with BF&AN at the SU transmitters.

### A. Beamforming and Artificial Noise Generation

*1) PUs' Quality of Service Requirement:* According to the rule of underlay spectrum sharing networks, the concurrent transmission of PUs and SUs occurs under the prerequisite that the QoS requirement of the primary transmission is satisfied. The QoS of primary network is characterized that the outage probability should be no larger than the peak allowable value $\rho_{\mathtt{out}}^p$, which is expressed as

$$P_{out}^{\{p\}} = Pr\left\{\gamma_{\mathtt{SIR}}^{p,AN}<\gamma_{th}^{\{p\}}\right\}<\rho_{out}^{\{p\}}, \tag{8}$$

where $\gamma_{th}^{\{p\}}$ is the desired SIR threshold at the PU receiver.

In the following theorem, we present the SU's permissive transmit power region.

**Theorem 1.** *With BF&AN at the SU transmitter, the permissive transmit power region at the SU transmitter is given as $P_s\in(0,\,P_s^{\max}]$, where*

$$P_s^{\max} = \begin{cases} \left(-\frac{\Theta}{\Upsilon_1\lambda_s}\right)^{\frac{\alpha}{2}}P_p & \mu\neq\frac{1}{N_s} \\ \left(-\frac{\Theta\Gamma(N_s)}{\lambda_s\Gamma\left(N_s+\frac{2}{\alpha}\right)}\right)^{\frac{\alpha}{2}}\frac{P_p}{\mu} & \mu=\frac{1}{N_s}, \end{cases} \tag{9}$$

*$\Upsilon_1$ is given by* (7)*, and*

$$\Theta = \frac{\ln\left(1-\rho_{out}^{\{p\}}\right)}{\pi\Gamma\left(1-\frac{2}{\alpha}\right)\left(\gamma_{th}^{\{p\}}\right)^{\frac{2}{\alpha}}{r_p}^2}+\lambda_p\Gamma\big(1+\frac{2}{\alpha}\big). \tag{10}$$

*2) New Statistics:* In order to examine the secrecy performance, we derive the CDFs of SIRs at the typical SU receiver and the most detrimental eavesdropper in the following **Lemma 2** and **Lemma 3**, respectively.

**Lemma 2.** *With BF&AN at the SU transmitters, the CDF of SIR at the typical SU receiver is derived as*

$$F_{\gamma_{\mathtt{SIR}}^{s,AN}}^{\{s\}}\left(\gamma_{th}^{\{s\}}\right) = 1-\exp\left(-\Lambda_l\big(\gamma_{th}^{\{s\}}\big)^{\frac{2}{\alpha}}r_s^2\right)-\sum_{m=1}^{N_s-1}\frac{(r_s^\alpha)^m}{m!(-1)^m} \sum\prod_{i=1}^{m}\frac{m!}{m_i!i!^{m_i}}\exp\left(-\Lambda_l\big(\gamma_{th}^{\{s\}}\big)^{\frac{2}{\alpha}}r_s^2\right) \tag{11}$$

$$\prod_{j=1}^{m}\Big(\big(-\Lambda_l\big(\gamma_{th}^{\{s\}}\big)^{\frac{2}{\alpha}}\big)(r_s)^{2-j\alpha}\prod_{k=0}^{j-1}\big(\frac{2}{\alpha}-k\big)\Big)^{m_j},$$

*where*

$$\Lambda_l=\begin{cases}\Lambda_2 & \mu=\frac{1}{N_s}\\ \Lambda_3 & \mu\neq\frac{1}{N_s}.\end{cases}\tag{12}$$

*In* (12), $\Lambda_2$ *and* $\Lambda_3$ *are given by*

$$\Lambda_2=\pi\Big(\lambda_s\frac{\Gamma\big(N_s+\frac{2}{\alpha}\big)}{\Gamma\big(N_s\big)}+\lambda_p\Gamma\big(1+\frac{2}{\alpha}\big)\big(\mu\frac{P_s}{P_p}\big)^{-\frac{2}{\alpha}}\Big)\Gamma\big(1-\frac{2}{\alpha}\big),\tag{13}$$

$$\Lambda_3=\pi\Big(\lambda_p\Gamma\big(1+\frac{2}{\alpha}\big)\big(\frac{P_s}{P_p}\big)^{-\frac{2}{\alpha}}+\lambda_s\Upsilon_1\Big)\Gamma\big(1-\frac{2}{\alpha}\big)(\mu)^{-\frac{2}{\alpha}},\tag{14}$$

*respectively. Here,* $\sum_{i=1}^{m} i\cdot m_i=m$, *and* $\Upsilon_1$ *is given by* (7), *and* $P_s$ *is the maximum permissive transmit power, which is given in* (9).

Based on the SIR at the most detrimental eavesdropper in (4), we derive the CDF for $\gamma_{\mathtt{SIR}}^{e,AN}$ in the following lemma.

**Lemma 3.** *With BF&AN at the SU transmitters, the CDF of SIR at the most detrimental eavesdropper is derived as*

$$F_{\gamma_{\mathtt{SIR}}^{e,AN}}\big(\gamma_{th}^{\{e\}}\big)=\exp\Big(-\frac{\pi\lambda_e}{\Lambda_l}\big(\gamma_{th}^{\{e\}}\big)^{-\frac{2}{\alpha}}\big(\frac{1-\mu}{(N_s-1)\mu}\gamma_{th}^{\{e\}}+1\big)^{1-N_s}\Big),\tag{15}$$

*where* $\Lambda_l$ *is given in* (12). *Note that* $P_s$ *is the maximum permissive transmit power, which is given in* (9).

We observe from (15) that the CDF of $\gamma_{\mathtt{SIR}}^{e,AN}$ is an increasing function of $\lambda_s$ and $\lambda_p$, and a decreasing function of $\lambda_e$.

*3) Average Secrecy Rate:* The instantaneous secrecy rate is defined as [15]

$$C_{\mathtt{se}}=[C_{\mathtt{su}}-C_{\mathtt{E}}]^{+}.\tag{16}$$

where $[x]^{+}=\max\{x,0\}$, $C_{\mathtt{su}}=\log_2\big(1+\gamma_{\mathtt{SIR}}^{s,AN}\big)$ is the capacity of a typical secondary link, and $C_{\mathtt{E}}=\log_2\big(1+\gamma_{\mathtt{SIR}}^{e,AN}\big)$ is the capacity of the eavesdropping channel between the typical SU transmitter and the most detrimental eavesdropper. Here, $\gamma_{\mathtt{SIR}}^{e,AN}=\max\limits_{e_k\in\Phi_e}\{\gamma_{\mathtt{SIR}}^{e_k,AN}\}$ corresponds to the non-colluding eavesdropping case [16].

The average secrecy rate is the average of the instantaneous secrecy rate $C_{\mathtt{se}}$ over $\gamma_{\mathtt{SIR}}^{s,AN}$ and $\gamma_{\mathtt{SIR}}^{e,AN}$. As such, the average secrecy rate is given by [17]

$$\begin{aligned}\bar{C}_{\mathtt{se}}&=\int_0^\infty\int_0^\infty C_{\mathtt{se}}f_{\gamma_{\mathtt{SIR}}^{s,AN}}(x_1)\,f_{\gamma_{\mathtt{SIR}}^{e,AN}}(x_2)dx_1dx_2\\&=\frac{1}{\ln 2}\int_0^\infty\frac{F_{\gamma_{\mathtt{SIR}}^{e,AN}}(x_2)}{1+x_2}\big(1-F_{\gamma_{\mathtt{SIR}}^{s,AN}}(x_2)\big)dx_2.\end{aligned}\tag{17}$$

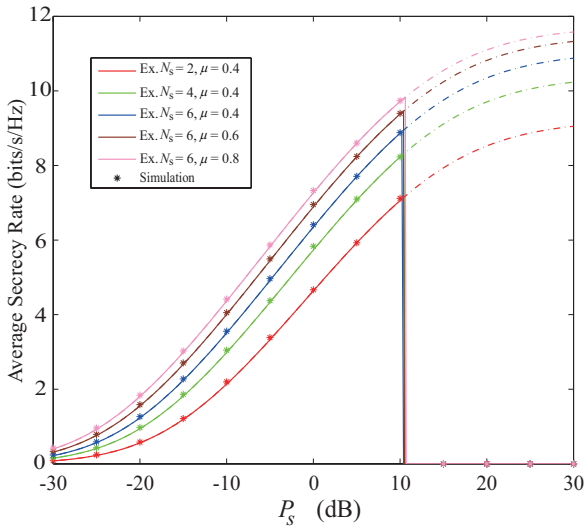


Fig. 2. Average secrecy rate of a large scale spectrum sharing network with the transmit power adaptation scheme. Parameters: $\lambda_e=\lambda_p=\lambda_s=10^{-4}$, $\alpha=3$, $r_p=6$, $r_s=3$, $P_p=15$ dB, and $\gamma_{th}^{\{p\}}=6$ dB.

By substituting the CDF of $\gamma_{\mathtt{SIR}}^{s,AN}$ in (11) and the CDF of $\gamma_{\mathtt{SIR}}^{e,AN}$ in (15) into (17), we derive the average secrecy rate in the following theorem.

**Theorem 2.** *With BF&AN at the SU transmitters, the average secrecy rate is derived as*

$$\begin{aligned}\bar{C}_{se,AN}=&\frac{1}{\ln 2}\int_0^\infty\frac{\exp\big(-\frac{\pi\lambda_e}{\Lambda_l}x_2{}^{\frac{2}{\alpha}}\big(\frac{1-\mu}{(N_s-1)\mu}x_2+1\big)^{1-N_s}\big)}{1+x_2}\\&\exp\big(-\Lambda_l x_2{}^{\frac{2}{\alpha}}r_s^2\big)\Big[1+\sum_{m=1}^{N_s-1}\frac{(r_s^\alpha)^m}{m!(-1)^m}\sum m!\\&\prod_{j=1}^{m}\frac{\big((-\Lambda_l x_2{}^{\frac{2}{\alpha}})(r_s)^{2-j\alpha}\prod_{k=0}^{j-1}\big(\frac{2}{\alpha}-k\big)\big)^{m_j}}{m_j!j!^{m_j}}\Big]dx_2,\end{aligned}\tag{18}$$

*where* $\Lambda_l$ *is given in* (12). *Here,* $P_s$ *is the maximum permissive transmit power, which is given in* (9).

*4) Secrecy Outage Probability:* The secrecy outage is declared when the secrecy capacity $C_{se}$ is less than the expected secrecy rate $R_s$. As such, the secrecy outage probability is defined as [17]

$$\begin{aligned}P_{out}(R_s)&=\Pr(C_{\mathtt{se}}<R_s)\\&=\int_0^\infty f_{\gamma_{\mathtt{SIR}}^{e,AN}}(x_2)\,F_{\gamma_{\mathtt{SIR}}^{s,AN}}\big(2^{R_s}(1+x_2)-1\big)dx_2.\end{aligned}\tag{19}$$

By substituting the probability density function (PDF) of $\gamma_{\mathtt{SIR}}^{e,AN}$ and CDF of $\gamma_{\mathtt{SIR}}^{s,AN}$ into (19), we derive the secrecy outage probability in the following theorem.

**Theorem 3.** *With BF&AN at the SU transmitters, the secrecy*

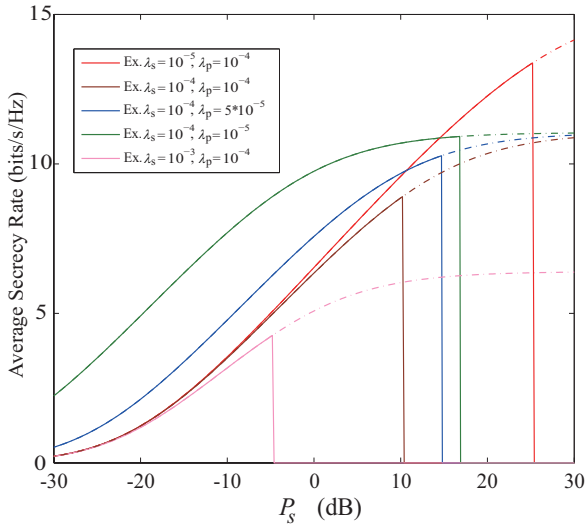


Fig. 3. Average secrecy rate of a large scale spectrum sharing network with the transmit power adaptation scheme. Parameters: $\lambda_e = 10^{-4}$, $N_s = 6$, $\alpha = 3$, $r_p = 6$, $r_s = 3$, $\mu = 0.4$, $P_p = 15$ dB, and $\gamma_{th}^{\{p\}} = 6$ dB.

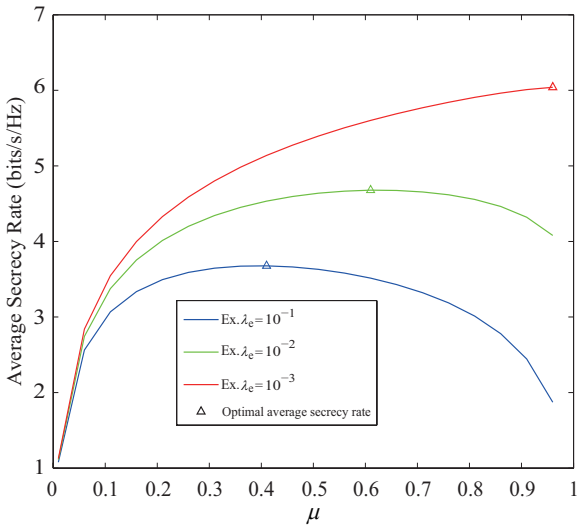


Fig. 4. Average secrecy rate of a large scale spectrum sharing network. Parameters: $\lambda_p = 10^{-4}$, $\lambda_s = 10^{-3}$, $\alpha = 3$, $r_p = 6$, $r_s = 3$, $N_s = 6$, $P_p = 15$ dB, and $\gamma_{th}^{\{p\}} = 0$ dB.

*outage probability is derived as*

$$P_{out,AN}(R_s) = \int_0^{\infty} \frac{\pi\lambda_e x_2^{-\frac{2}{\alpha}}\left(\frac{2}{\alpha}x_2^{-1}\left(\frac{1-\mu}{(N_s-1)\mu}x_2+1\right)+1\right)}{\Lambda_l\left(\frac{1-\mu}{(N_s-1)\mu}x_2+1\right)^{N_s}}$$
$$\exp\left(-\frac{\pi\lambda_e}{\Lambda_l}x_2^{-\frac{2}{\alpha}}\left(\frac{1-\mu}{(N_s-1)\mu}x_2+1\right)^{1-N_s}\right)\Big[1-$$
$$\exp\left(-\Lambda_3\left(2^{R_s}\left(1+x_2\right)-1\right)^{\frac{2}{\alpha}}r_s^2\right)\Big(1+\sum_{m=1}^{N_s-1}\frac{\left(r_s^{\alpha}\right)^m}{m!\left(-1\right)^m}\sum m!$$
$$\prod_{j=1}^{m}\frac{\left(\left(-\Lambda_l(2^{R_s}(1+x_2)-1)^{\frac{2}{\alpha}}\right)(r_s)^{2-j\alpha}\prod_{k=0}^{j-1}\left(\frac{2}{\alpha}-k\right)\right)^{m_j}}{m_j!j!^{m_j}}\Big)\Big]dx_2, \quad (20)$$

*where $\Lambda_l$ is given in* (12)*. Here, $P_s$ is the maximum permissive transmit power, which is given in* (9)*.*

## IV. Numerical Results

Fig. 2 and Fig. 3 plot the average secrecy rate of large scale underlay spectrum sharing network under the primary network's QoS constraint $\rho_{out}^{\{p\}} = 0.1$ with the transmit power adaptation scheme. From the figures, we see that the exact analytical curves are well validated by Monte Carlo simulations. The solid lines represent the operational achievable average secrecy rate where the primary's QoS constraint is always satisfied, i.e. $P_{out}^{pri,AN}\left(\gamma_{th}^{\{p\}}\right) \leq 0.1$. The dashed lines represent the unachievable average secrecy rate where the primary network's QoS constraint is violated, i.e. $P_{out}^{pri,AN}\left(\gamma_{th}^{\{p\}}\right) > 0.1$. We named the solid line as the "average secrecy rate wall". The vertical line of this "average secrecy rate wall" is determined by the maximum permissive transmit power at the SU $P_s^{max}$, which is quantified and evaluated by using (9).

Fig. 2 plots the average secrecy rate versus the SU's transmit power with various numbers of transmit antennas $N_s$ at the SU and power allocation factor $\mu$, and we consider the same density for PUs, SUs, and eavesdroppers. The exact analytical curves are obtained from (18). Several observations can be concluded as follows: 1) The width of the "average secrecy rate wall" is weakly dependent on the number of transmit antennas at the SU and the power allocation factor, which can be explained by (9); 2) For the fixed power allocation factor $\mu = 0.4$, the average secrecy rate increases with increasing $N_s$; 3) For the same $N_s$, the average secrecy rate improves with increasing $\mu$, which shows more power should be allocated to the information signal in this scenario.

Fig. 3 plots the average secrecy rate versus $P_s$ for various densities of PUs and SUs. We observe that 1) the "average secrecy rate wall" will be pushed to the left as the PUs and SUs become more dense. This can be predicted from (9) that $P_s^{\max}$ is a decreasing function of $\lambda_p$ and $\lambda_s$; 2) With the identical density of PUs, we see that the average secrecy rate decreases with increasing the density of SUs. This is because the aggregate interference from other SUs increases with increasing $\lambda_s$, which restricts the secrecy performance of the typical SU; 3) Given the fixed density of SUs, the average secrecy rate decreases with increasing $\lambda_p$ due to the increased aggregate interference from PUs.

Fig. 4 plots the average secrecy rate versus the power allocation factor $\mu$ for various densities of eavesdropper $\lambda_e$. Here, we use the maximum permissive transmit power to transmit the signal at SU, which is given by (18), and we

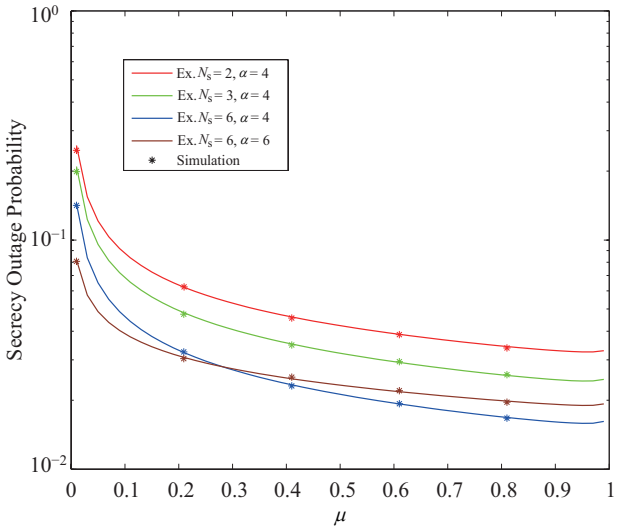


Fig. 5. Secrecy outage probability versus $\mu$ for various $N_s$ and $\alpha$. Parameters: $\rho_{out}^{\{p\}} = 0.1$, $\lambda_e = 10^{-4}$, $\lambda_p = 10^{-4}$, $\lambda_s = 10^{-3}$, $\alpha = 3$, $r_p = 6$, $r_s = 3$, $N_S = 6$, $Rs = 1$, $P_p = 15$ dB, and $\gamma_{th}^{\{p\}} = 0$ dB.

set $P_s = P_s^{max}$ and $\rho_{out}^{\{p\}} = 0.1$. The triangles represent the maximum achievable average secrecy rate. Interestingly, we find that in Fig. 4 the optimal power allocation factor $\mu^*$ varies for different $\lambda_e$. It is revealed that less power should be allocated to the AN for the network with less dense eavesdroppers. More importantly, when $\lambda_e = 10^{-3}$, the optimal $\mu$ for achieving the maximum average secrecy rate is close to 1. It is shown that the equal power allocation strategy $\mu = 0.5$ may not achieve near optimal average secrecy rate.

Fig. 5 plots the secrecy outage probability versus the power allocation factor $\mu$ for various numbers of antennas at SU transmitter $N_s$. The exact analytical curves are obtained from (20), which are well validated by Monte Carlo simulations. We assume $P_s = P_s^{max}$. We see that the secrecy outage probability decreases with increasing $\mu$. When $\mu$ approaches 1, the lowest secrecy outage probability can be achieved. This is because when we set the density of eavesdroppers to be small compared with the density of SU, the effect of delivering information overtakes the effect of combating the eavesdropping on the secrecy outage probability. As expected, the secrecy outage probability decreases with increasing $N_s$, which is due to the array gains brought by additional antennas.

## V. Conclusion

In this paper, we studied the secure communication in large scale spectrum sharing network in the presence of multiple non-colluding eavesdroppers. We employed the beamforming and artificial noise generation at the SU transmitters to achieve the secure transmission against those malicious eavesdroppers. We obtained the exact expression for the average secrecy rate, through which we observed the average secrecy rate wall. We also derived the exact expression for the secrecy outage probability. The impact of different system parameters on the average secrecy rate and the secrecy outage probability was demonstrated. It is shown that the optimal power allocation factor that maximizes the average secrecy rate needs not to be the equal power allocation. The results in this paper provide valuable insights for the design of large scale spectrum sharing networks.

## References


[1] W. El-Hajj, H. Safa, and M. Guizani, "Survey of security issues in cognitive radio networks," *J. Internet Tech.*, vol. 12, no. 2, pp. 181–198, 2011.

[2] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proc. IEEE*, vol. 97, no. 5, pp. 894–914, May. 2009.

[3] D. Liu, Y. Chen, K. K. Chai, T. Zhang, and M. Elkashlan, "Opportunistic user association for multi-service hetnets using nash bargaining solution," *IEEE Commun. Lett.*, vol. 18, no. 3, pp. 463–466, Mar. 2014.

[4] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Netw.*, vol. 27, no. 3, pp. 28–33, Jun. 2013.

[5] S. Shafiee and S. Ulukus, "Achievable rates in gaussian MISO channels with secrecy constraints," in *Proc. IEEE ISIT*, Nice, France, Jun. 2007, pp. 2466–2470.

[6] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[7] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—part I: Connectivity," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.

[8] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006–2021, Jun. 2014.

[9] S. Weber, J. G. Andrews, and N. Jindal, "An overview of the transmission capacity of wireless networks," *IEEE Trans. Commun.*, vol. 58, no. 12, pp. 3593–3604, Dec. 2010.

[10] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, Sep. 2009.

[11] S. A. R. Zaidi, D. C. McLernon, and M. Ghogho, "Breaking the area spectral efficiency wall in cognitive underlay networks," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 1–17, Feb. 2014.

[12] C. han Lee and M. Haenggi, "Interference and outage in poisson cognitive networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 4, pp. 1392–1401, Apr. 2012.

[13] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1802–1814, Nov. 2013.

[14] D. Stoyan, W. Kendall, and J. Mecke, "Stochastic geometry and its applications," *Wiley New York*, vol. 2, 1987.

[15] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[16] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[17] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 247–258, Feb. 2014.