Article:
Deng, Y, Wang, L, Zaidi, SAR et al. (2016) Artificial-Noise Aided Secure Transmission in Large Scale Spectrum Sharing Networks. IEEE Transactions on Communications, 64 (5). pp. 2116-2129. ISSN: 0090-6778

https://doi.org/10.1109/TCOMM.2016.2544300

Artificial-Noise Aided Secure Transmission in Large Scale Spectrum Sharing Networks

Yansha Deng, *Member, IEEE*, Lifeng Wang, *Member, IEEE*, Syed Ali Raza Zaidi, *Member, IEEE*, Jinhong Yuan, *Fellow, IEEE*, and Maged Elkashlan, *Member, IEEE*

***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 users' quality of service constraint. Our aim is to characterize the impact of beamforming and artificial noise generation (BF&AN) on this complex large scale network. We first derive exact expressions for the average secrecy rate and the secrecy outage probability. We then derive an easy-to-evaluate asymptotic average secrecy rate and asymptotic secrecy outage probability when the number of antennas at the secondary transmitter goes to infinity. Our results show that the equal power allocation between the useful signal and artificial noise is not always the best strategy to achieve maximum average secrecy rate in large scale spectrum sharing networks. Another interesting observation is that the advantage of BF&AN over BF on the average secrecy rate is lost when the aggregate interference from the primary and secondary transmitters is strong, such that it overtakes the effect of the generated AN.**

***Index Terms*—Artificial noise, physical layer security, power allocation, spectrum sharing networks, stochastic geometry.**

I. Introduction

The sky-rocketing growth of multimedia infotainment applications and broadband-hungry mobile devices exacerbate the stringent demand for ultra high data rate and services. Such urgent demand is further driven by the exponential growth of smartphones, tablets, machine-to-machine (M2M) communication devices. To cope with this, unlicensed users are allowed 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 [2, 3]. These networks are often referred to as cognitive radio networks (CRNs).

The open and dynamic characteristics of CRNs have lead to several new classes of security threats and challenges due to opportunistic utilization of licensed channels [4]. There exists six major types of attacks at the physical layer of CRNs, which are commonly known as primary user emulation, objective function attack, learning attack, spectrum sensing data falsification, jamming attack, and eavesdropping [5]. Among them, we focus on the eavesdropping attacks targeted at the secondary users (SUs). In this case, the eavesdroppers attempt to intercept and overhear the secondary transmission without transmitting any signals.

Traditional security, which is achieved through the higher layer cryptographic authentication and identification, becomes expensive and vulnerable to attacks. Particularly, in the emerging large scale networks with high mobility terminals, the implementation and management of higher-layer key distribution face increasing challenges [6, 7]. In other words, the establishment of the secret keys to achieve encrypted transmission in large scale decentralized networks are even more complicated and expensive than the point-to-point communications [7]. To cope with these issues, physical layer security has been proposed as a complementary security method to protect the confidential information from eavesdropping [8]. A comprehensive overview of physical layer security in multiuser wireless networks has been presented in [5].

Recently, physical layer security has been introduced into large scale wireless networks with randomly located eavesdroppers [9–11], single antenna legitimate nodes and eavesdroppers [7], multiple jammers [12], and cellular users [13, 14]. In these works, the stochastic geometry and random graphs were applied for modeling these networks [15]. This mathematical tool is attractive since it captures the topological randomness of these networks, and provides a simple and tractable model for characterizing the performance [16].

Various advanced techniques have been developed to enhance the secrecy performance [17]. Beamforming (BF) is proved to be the optimal transmission scheme to achieve the maximum achievable secrecy rate in multiple input single output (MISO) systems [18]. Generating artificial noise (AN) at the legitimate transmitter is proposed to be an effective technique to confound the eavesdroppers [19]. In the AN-based method, the power allocation between the information-bearing signal and the AN at the transmitter is critically important, which reveals the tradeoff between enhancing the main channel by increasing the power allocated to information-bearing signal and degrading the eavesdropper's channel by allocating more power to the AN. In [20] and [21], the optimal power allocation strategies were studied in the conventional wireless network with fixed nodes, and wireless ad hoc networks with mobile nodes, respectively. However, all these

Manuscript received May. 27, 2015; revised Nov. 21, 2015; accepted Mar. 10, 2016. This paper was presented in part at the Proc. IEEE Int. Conf. Commun. (ICC), London, UK, Jun. 2015 [1]. The editor coordinating the review of this manuscript and approving it for publication was Prof. Ali Tajer.

Y. Deng and L. Wang were with Queen Mary University of London, London, UK (e-mail:{ y.deng, lifeng.wang}@qmul.ac.uk).

M. Elkashlan is with Queen Mary University of London, London, UK (e-mail: maged.elkashlan@qmul.ac.uk).

Syed Ali Raza Zaidi is with the School of Electronics and Electrical Engineering, University of Leeds, Leeds, United Kingdom (e-mail: elsarz@leeds.ac.uk).

Jinhong Yuan is with the School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney 2052, Australia (e-mail: j.yuan@unsw.edu.au).

works [18–22] have considered the physical layer security in legacy networks.

Compared with the physical layer security in conventional networks, there exist several major differences in the security of CRNs: 1) the QoS requirement of the primary network needs to be satisfied; 2) the SU receiver is subject to the aggregate interference from the PU transmitters; and 3) the secondary network is more susceptible to security threats. In light of the aforementioned circumstances, the research on enhancing the security at the physical layer of CRNs has received increasing attentions. In [23–25], the secondary user acts as a jammer to enhance the secrecy transmission of a primary network. In [26], multiuser scheduling was proposed to improve the security level of secondary transmission with primary QoS constraint. In [27], it was demonstrated that the best secrecy performance of secondary network can be achieved when the perfect channel state information (CSI) of all links are available. In [28], it was proved that beamforming is the optimal transmission strategy to secure MISO CRN with the perfect knowledge of all channels. The authors of [28] then extended their work to the networks with imperfect knowledge in [29]. In [30], the beamforming and artificial noise generation (BF&AN) was adopted at the SU transmitter to enhance the secrecy throughput of a multiple-input, single-output, multieavesdropper (MISOME) primary network. Note that [26–30] only considered fixed location nodes. In [31], the secrecy capacity of cognitive radio networks with uniformly distributed secondary transmitters and primary transmitters was examined. In [32], the secrecy capacity of the primary network was analyzed in CRNs, where PUs, SUs, and Eves followed the mutually independent homogeneous Poisson process.

Different from the aforementioned works, we treat the secrecy performance of large scale spectrum sharing networks with BF&AN at the SU transmitters. Compared against the security of non-cognitive radio networks in [21], the prerequisite of underlay spectrum sharing networks is to guarantee the QoS of the primary network. This can be fulfilled by constraining the outage probability at the PU receiver below a predetermined threshold (i.e., the peak allowable outage probability). The use of BF&AN at the SU transmitter brings array gains at the legitimate receiver and disrupts the reception at the eavesdropper. Although BF&AN has been well treated in the conventional physical layer security network in [20], no work has considered BF&AN in large scale spectrum sharing networks. Therefore, the question of *how BF&AN impacts the security design of such a complex network* remains unknown. Our contributions are summarized as follows:

1) We derive a new exact closed-form expression for the maximum permissive transmit power at the SU transmitter with BF&AN. We accurately quantify the permissive transmit power region where the primary network's QoS can be guaranteed, as presented in **Theorem 1**. 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**.
2) We show that there exists an average secrecy rate boundary beyond which the PU receiver's QoS is violated. We reveal that the optimal power allocation factor for maximizing the average secrecy rate varies for different system parameters. Equal power allocation may not achieve the near optimal average secrecy rate in large scale spectrum sharing networks.
3) To provide insights into system design from an implementation viewpoint, we compare the average secrecy rate of BF&AN with that of BF. We observe the same average secrecy rate boundary for BF&AN and BF. The advantage of BF&AN over BF on the average secrecy rate is lost, when the aggregate interference from the PU and SU transmitters is strong, such that it overtakes the effect of the generated AN.
4) We derive the asymptotic average secrecy rate and the asymptotic secrecy outage probability of the secondary network with BF&AN at the SU transmitters when the number of SU transmit antennas N_s goes to infinity, as presented in **Propositions 1, 2**, and **3**. Our asymptotic results well predict the exact performance in the medium and large N_s regime. We determine the antenna gap, which showcases the number of additional antennas required to achieve the same asymptotic average secrecy rate in more dense networks.

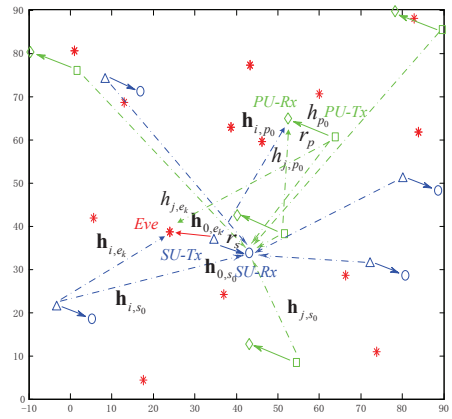


Fig. 1. A realization of a large scale spectrum sharing network model describing the received signal at a SU receiver. In this network, the green square represents the PU transmitter, the diamond represents the PU receiver, the triangle represents the SU transmitter, the circle represents the SU receiver, 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.

II. System and Channel Model

We consider 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. Each SU transmitter has N_s antennas, and the remaining nodes in this model are all single-antenna nodes. As shown in Fig. 1, we have a set of PU transmitters, SU transmitters, and eavesdroppers locations,

denoted by Φ_p, Φ_s and Φ_e, in which Φ_p, Φ_s and Φ_e follow independent homogeneous Poisson point processes (HPPPs) with densities λ_p, λ_s and λ_e, respectively. This model is practical and representative of the decentralized networks, where the nodes are randomly deployed or have substantial mobility [33]. We assume that each PU/SU transmitter communicates with its unique associated intended PU/SU receiver at a fixed distance, respectively, in order to simplify the analysis and provide some design insights [21, 34, 35]. Note that this fixed distance assumption can be relaxed by taking into account the probability density distribution of the distance.

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 the other transmitters. Similar as [20, 21], 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 AN simultaneously. We assume that the perfect CSI between each SU transmitter and each SU receiver are available[1]. 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 ith 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 ith SU transmitter. An orthonormal basis of $\mathcal{C}^{N_s\times N_s}$ is generated at the ith SU transmitter as $\left[\mathbf{h}_{i,s_i}^{\dagger}\Big/\|\mathbf{h}_{i,s_i}\|,\ \mathbf{G}_{i,s_i}\right]_{N_s\times N_s}$ [2], 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 AN. The transmitted BF&AN symbol vector is modeled as

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

where $\mathbb{E}\left\{b_i b_i^{\dagger}\right\} = \delta_s^2$, 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 σ_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 μ as the fraction of power assigned to the information signal, thus $P_I = \mu P_s$.

In the primary network, we assume the typical PU receiver is located at the origin of the coordinate system, and the distance between the typical PU transmitter and its associated PU receiver is r_p. According to the Slivnyak's theorem [36], adding a probe point to the HPPP at an arbitrary location does not affect the law of the point process. 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

$$I_{p,p_0} = \sum_{j\in\Phi_p\setminus\{0\}} |h_{j,p_0}|^2 |X_{j,p_0}|^{-\alpha}, \tag{3}$$

and

$$I_{s,p_0} = \sum_{i\in\Phi_s} \left[\sigma_s^2 \left|\mathbf{h}_{i,p_0} \frac{\mathbf{h}_{i,s_i}^{\dagger}}{\left\|\mathbf{h}_{i,s_i}^{\dagger}\right\|}\right|^2 + \sigma_n^2 \left\|\mathbf{h}_{i,p_0}\mathbf{G}_{i,s_i}\right\|^2\right] \left|X_{i,p_0}\right|^{-\alpha}. \tag{4}$$

In (2), α 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 jth 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 ith SU transmitter and the typical PU receiver, respectively. P_p is the transmit power at the PU transmitter. Note that $P_p I_{p,p_0}$ is the interference from other PU transmitters to the typical PU receiver, I_{s,p_0} is the co-channel interference from the SU transmitters to the typical PU receiver.

In the secondary network, we 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

$$\mathbf{h}_{0,s_0}\mathbf{x}_{s_0} = \mathbf{h}_{0,s_0}\frac{\mathbf{h}_{0,s_0}^{\dagger}}{\|\mathbf{h}_{0,s_0}\|} b_0 + \mathbf{h}_{0,s_0}\mathbf{G}_{0,s_0}\mathbf{n}_A = \|\mathbf{h}_{0,s_0}\| b_0. \tag{5}$$

The received SIR at the typical SU receiver is given by

$$\gamma_{\mathtt{SIR}}^{s,AN} = \frac{\sigma_s^2 \|\mathbf{h}_{0,s_0}\|^2 r_s{}^{-\alpha}}{I_{s,s_0} + P_p I_{p,s_0}}, \tag{6}$$

where

$$I_{p,s_0} = \sum_{j\in\Phi_p} |h_{j,s_0}|^2 |X_{j,s_0}|^{-\alpha}, \tag{7}$$

and

$$I_{s,s_0} = \sum_{i\in\Phi_s\setminus\{0\}} \left[\sigma_s^2 \left|\mathbf{h}_{i,s_0} \frac{\mathbf{h}_{i,s_i}^{\dagger}}{\left\|\mathbf{h}_{i,s_i}^{\dagger}\right\|}\right|^2 + \sigma_n^2 \left\|\mathbf{h}_{i,s_0}\mathbf{G}_{i,s_i}\right\|^2\right] \left|X_{i,s_0}\right|^{-\alpha}. \tag{8}$$

In (6), h_{j,s_0} and $|X_{j,s_0}|$ are the channel fading gain and distance between the jth 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 ith SU transmitter and the typical SU receiver, respectively. Note that $P_p I_{p,s_0}$ is the co-channel interference from the PU transmitters to the typical SU receiver, and I_{s,s_0} is the aggregate interference from other SU transmitters to the typical SU receiver.

[1] In practice, perfect CSI may not be easy to obtained, as such, our analysis provides the upper bound on the actual achievable secrecy performance.

[2] † is the conjugate transpose operator.

In the eavesdropping channel, we consider the most detrimental eavesdropper that has the highest SIR for a typical SU transmitter [37]. Note that eavesdroppers are only interested in the secondary transmissions, and interpret the primary transmissions as interference[3]. 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 $e_k \in \Phi_e$. With BF&AN at the SU transmitter, the received signal from the typical SU transmitter at the kth eavesdropper is given by

$$\mathbf{h}_{0,e_k}\mathbf{x}_{s_0} = \mathbf{h}_{0,e_k}\frac{\mathbf{h}_{0,s_0}^{\dagger}}{\|\mathbf{h}_{0,s_0}\|}b_0 + \mathbf{h}_{0,e_k}\mathbf{G}_{0,s_0}\mathbf{n}_A, \tag{9}$$

where the first part is the useful received information signal, and the second part is the received AN. As such, the SIR at the most detrimental eavesdropper is expressed as

$$\gamma_{\mathtt{SIR}}^{e,AN} = \max_{e_k\in\Phi_e}\left\{\frac{\sigma_s^2\big|\mathbf{h}_{0,e_k}\frac{\mathbf{h}_{0,s_0}^{\dagger}}{\|\mathbf{h}_{0,s_0}^{\dagger}\|}\big|^2|X_{e_k}|^{-\alpha}}{I_{s,e_k}+P_pI_{p,e_k}+\sigma_n^2I_{s_0,e_k,an}}\right\}, \tag{10}$$

where

$$I_{p,e_k} = \sum_{j\in\Phi_p}|h_{j,e_k}|^2|X_{j,e_k}|^{-\alpha}, \tag{11}$$

$$I_{s,e_k} = \sum_{i\in\Phi_s\setminus\{0\}}\left[\sigma_s^2\big|\mathbf{h}_{i,e_k}\frac{\mathbf{h}_{i,s_i}^{\dagger}}{\left\|\mathbf{h}_{i,s_i}^{\dagger}\right\|}\big|^2+\sigma_n^2\big\|\mathbf{h}_{i,e_k}\mathbf{G}_{i,s_i}\big\|^2\right] |X_{i,e_k}|^{-\alpha}, \tag{12}$$

and

$$I_{s_0,e_k,an} = \|\mathbf{h}_{0,e_k}\mathbf{G}_{0,s_0}\|^2|X_{e_k}|^{-\alpha}. \tag{13}$$

Note that h_{j,e_k} and $|X_{j,e_k}|$ are the channel fading gain and distance between the jth PU transmitter and the kth 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 ith SU transmitter and the kth eavesdropper, respectively. $|X_{e_k}|$ is the distance between the typical SU transmitter and the kth eavesdropper. It is known that P_pI_{p,e_k} is the aggregate interference from PU transmitters, $\sigma_n^2I_{s_0,e_k,an}$ is the AN from the typical SU transmitter, and I_{s,e_k} is the aggregate interference from other SU transmitters.

We now define

$$W_{s_i,z} = \sigma_s^2\big|\mathbf{h}_{i,z}\frac{\mathbf{h}_{i,s_i}^{\dagger}}{\left\|\mathbf{h}_{i,s_i}^{\dagger}\right\|}\big|^2+\sigma_n^2\big\|\mathbf{h}_{i,z}\mathbf{G}_{i,s_i}\big\|^2, \tag{14}$$

where $\mathbf{h}_{i,s_i}$ is the intended channel, $\mathbf{h}_{i,z}$ is the channel between the ith SU transmitter and the non-intended receiver z (except for the ith SU receiver), and $z \in \{p_0, d_{0,}e_k\}$. To facilitate the performance analysis, we derive the Laplace transform of the aggregate interference from the SU transmitters $I_{s,z} = \sum_{i\in\Phi_s}W_{s_i,z}|X_{i,z}|^{-\alpha}$ in (2), (6), and (10) as the following lemma.

[3]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.

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*

$$\mathcal{L}_{I_{s,z}}(s) = \begin{cases} \exp\left(-\lambda_s\pi P_s^{\frac{2}{\alpha}}\Upsilon_1\Gamma\left(1-\frac{2}{\alpha}\right)s^{\frac{2}{\alpha}}\right) & \mu\neq\frac{1}{N_s}, \\ \exp\left(-\lambda_s\pi(\mu P_s)^{\frac{2}{\alpha}}\Gamma\left(N_s+\frac{2}{\alpha}\right)\frac{\Gamma\left(1-\frac{2}{\alpha}\right)}{\Gamma(N_s)}s^{\frac{2}{\alpha}}\right) & \mu=\frac{1}{N_s}, \end{cases} \tag{15}$$

where

$$\Upsilon_1 = \left(1-\frac{(1-\mu)}{(N_s-1)\,\mu}\right)^{1-N_s}\Big[\mu^{\frac{2}{\alpha}}\Gamma\big(1+\frac{2}{\alpha}\big)-\frac{1}{\mu} \left(\frac{(1-\mu)}{N_s-1}\right)^{1+\frac{2}{\alpha}}\sum_{k=0}^{N_s-2}\left(1-\frac{(1-\mu)}{(N_s-1)\,\mu}\right)^k\frac{\Gamma\left(k+1+\frac{2}{\alpha}\right)}{\Gamma\left(k+1\right)}\Big]. \tag{16}$$

Proof. See Appendix A. □

III. Exact Secrecy Perfromance

In this section, we first present the SU's permissive transmit power region. We then present the exact expressions for the average secrecy rate and the secrecy outage probability in large scale spectrum sharing networks with BF&AN at the SU transmitters. To obtain key insights through a comparison of BF&AN with BF, we derive exact expressions for the average secrecy rate and the secrecy outage probability in large scale spectrum sharing networks with BF 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 [38]. As such, we first examine the transmit power operating region at the SU transmitters under the primary network's QoS constraint. 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 [39]

$$P_{out}^{\{p\}} = Pr\big\{\gamma_{\mathtt{SIR}}^{p,AN} < \gamma_{th}^{\{p\}}\big\} < \rho_{out}^{\{p\}}, \tag{17}$$

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*

$$P_s^{\max} = \begin{cases} \left(-\frac{\Theta}{\Upsilon_1\lambda_s}\right)^{\frac{\alpha}{2}}P_p & \mu\neq\frac{1}{N_s} \\ \left(-\frac{\Theta\Gamma(N_s)}{\lambda_s\Gamma\left(N_s+\frac{2}{\alpha}\right)}\right)^{\frac{\alpha}{2}}\frac{P_p}{\mu} & \mu=\frac{1}{N_s}, \end{cases} \tag{18}$$

where Υ_1 is given by (16)*, and*

$$\Theta = \frac{\ln\left(1-\rho_{out}^{\{p\}}\right)}{\pi\Gamma\left(1-\frac{2}{\alpha}\right)\left(\gamma_{th}^{\{p\}}\right)^{\frac{2}{\alpha}}{r_p}^2} + \lambda_p\Gamma\big(1+\frac{2}{\alpha}\big). \tag{19}$$

Proof. See Appendix B. □

The following are some observations from (18).

- For the fixed primary network's QoS constraint, the maximum permissive transmit power at the SU transmitter can be relaxed by reducing the distance of the typical PU transceivers r_p, due to the fact that the PU can tolerate more interference from the SU transmitters.
- With increasing number of SU nodes and PU nodes per unit area, the transmit power constraint imposed on the SU transmitter is more severe. This is due to the increasing aggregate interference from the SU transmitters and the other interfering PU transmitters.

To study the impact of BF&AN on the secrecy performance within the permissive transmit power region, we consider two important metrics: the average secrecy rate and the secrecy outage probability.

2) Average Secrecy Rate: The instantaneous secrecy rate is defined as [37]

$$R_{\mathtt{se}} = [\log_2\left(1+\gamma_{\mathtt{SIR}}^{s,AN}\right) - \log_2\left(1+\gamma_{\mathtt{SIR}}^{e,AN}\right)]^+. \quad (20)$$

where $[x]^+ = \max\{x, 0\}$. 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 [40].

The average secrecy rate is the average of the instantaneous secrecy rate $R_{\mathtt{se}}$ over $\gamma_{\mathtt{SIR}}^{s,AN}$ and $\gamma_{\mathtt{SIR}}^{e,AN}$. As such, the average secrecy rate is given by [41]

$$\begin{aligned}\bar{R}_{\mathtt{se}} &= \int_0^\infty\int_0^\infty R_{\mathtt{se}} f_{\gamma_{\mathtt{SIR}}^{s,AN}}(x_1)\, f_{\gamma_{\mathtt{SIR}}^{e,AN}}(x_2)dx_1dx_2 \\ &= \frac{1}{\ln 2}\int_0^\infty \frac{F_{\gamma_{\mathtt{SIR}}^{e,AN}}(x_2)}{1+x_2}\big(1-F_{\gamma_{\mathtt{SIR}}^{s,AN}}(x_2)\big)dx_2. \quad (21)\end{aligned}$$

In order to examine the average secrecy rate, 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*

$$\begin{aligned}F_{\gamma_{\mathtt{SIR}}^{s,AN}}^{\{s\}}\big(\gamma_{th}^{\{s\}}\big) &= 1-\exp\left(-\Lambda_l\big(\gamma_{th}^{\{s\}}\big)^{\frac{2}{\alpha}} r_s^2\right) - \sum_{m=1}^{N_s-1}\frac{(r_s^\alpha)^m}{m!(-1)^m} \\ &\sum \frac{m!}{\prod_{i=1}^{m} m_i! i!^{m_i}} \exp\left(-\Lambda_l\big(\gamma_{th}^{\{s\}}\big)^{\frac{2}{\alpha}} r_s^2\right) \\ &\prod_{j=1}^{m}\left(\big(-\Lambda_l\big(\gamma_{th}^{\{s\}}\big)^{\frac{2}{\alpha}}\big)(r_s)^{2-j\alpha}\prod_{k=0}^{j-1}\big(\frac{2}{\alpha}-k\big)\right)^{m_j}, \quad (22)\end{aligned}$$

where

$$\Lambda_l = \begin{cases}\Lambda_2 & \mu = \frac{1}{N_s} \\ \Lambda_3 & \mu \neq \frac{1}{N_s}.\end{cases} \quad (23)$$

In (23)*, Λ_2 and Λ_3 are given by*

$$\Lambda_2 = \pi\Big(\lambda_s\frac{\Gamma\big(N_s+\frac{2}{\alpha}\big)}{\Gamma(N_s)} + \lambda_p\Gamma\big(1+\frac{2}{\alpha}\big)\big(\mu\frac{P_s}{P_p}\big)^{-\frac{2}{\alpha}}\Big)\Gamma\big(1-\frac{2}{\alpha}\big), \quad (24)$$

$$\Lambda_3 = \pi\Big(\lambda_p\Gamma\big(1+\frac{2}{\alpha}\big)\big(\frac{P_s}{P_p}\big)^{-\frac{2}{\alpha}} + \lambda_s\Upsilon_1\Big)\Gamma\big(1-\frac{2}{\alpha}\big)(\mu)^{-\frac{2}{\alpha}}, \quad (25)$$

respectively. Here, $\sum\limits_{i=1}^{m} i\cdot m_i = m$, and Υ_1 is given by (16)*, and P_s is the maximum permissive transmit power, which is given in* (18)*.*

Proof. See Appendix C. □

Based on the SIR at the most detrimental eavesdropper in (10), 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*

$$\begin{aligned}&F_{\gamma_{\mathtt{SIR}}^{e,AN}}^{\{e\}}\big(\gamma_{th}^{\{e\}}\big) = \\ &\exp\left(-\frac{\pi\lambda_e}{\Lambda_l}\big(\gamma_{th}^{\{e\}}\big)^{-\frac{2}{\alpha}}\big(\frac{1-\mu}{(N_s-1)\mu}\gamma_{th}^{\{e\}}+1\big)^{1-N_s}\right), \quad (26)\end{aligned}$$

where Λ_l is given in (23)*. Note that P_s is the maximum permissive transmit power, which is given in* (18)*.*

Proof. See Appendix D. □

Different from [7] and [21] where only the approximation or bound on CDF of SIR at the eavesdropper was derived, our result is derived in a simple exact closed-form expression. It is observed from (26) that the CDF of $\gamma_{\mathtt{SIR}}^{e,AN}$ is an increasing function of λ_s and λ_p, and a decreasing function of λ_e.

By substituting the CDF of $\gamma_{\mathtt{SIR}}^{s,AN}$ in (22) and the CDF of $\gamma_{\mathtt{SIR}}^{e,AN}$ in (26) into (21), 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*

$$\begin{aligned}\bar{R}_{se,AN} =& \frac{1}{\ln 2}\int_0^\infty \frac{\exp\left(-\frac{\pi\lambda_e}{\Lambda_l}x_2{}^{-\frac{2}{\alpha}}\big(\frac{1-\mu}{(N_s-1)\mu}x_2+1\big)^{1-N_s}\right)}{1+x_2} \\ &\exp\left(-\Lambda_l x_2{}^{\frac{2}{\alpha}} r_s^2\right)\Big[1+\sum_{m=1}^{N_s-1}\frac{(r_s^\alpha)^m}{m!(-1)^m}\sum m! \\ &\prod_{j=1}^{m}\frac{\big((-\Lambda_l x_2{}^{\frac{2}{\alpha}})(r_s)^{2-j\alpha}\prod_{k=0}^{j-1}(\frac{2}{\alpha}-k)\big)^{m_j}}{m_j! j!^{m_j}}\Big]dx_2, \quad (27)\end{aligned}$$

where Λ_l is given in (23)*. Here, P_s is the maximum permissive transmit power, which is given in* (18)*.*

Note that the average secrecy rate given in (27) is applicable to arbitrary N_s, μ and α.

3) Secrecy Outage Probability: The secrecy outage is declared when the instantaneous secrecy rate R_{se} is less than the expected secrecy rate R_s. As such, the secrecy outage probability is defined as [41]

$$\begin{aligned}P_{out}(R_s) &= \Pr(R_{\mathtt{se}} < R_s) \\ &= \int_0^\infty f_{\gamma_{\mathtt{SIR}}^{e,AN}}(x_2)\, F_{\gamma_{\mathtt{SIR}}^{s,AN}}\left(2^{R_s}(1+x_2)-1\right)dx_2. \quad (28)\end{aligned}$$

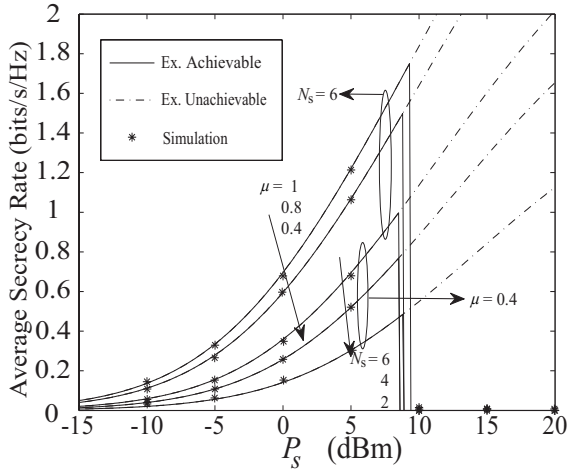


Fig. 2. Average secrecy rate of a large scale spectrum sharing network with the transmit power adaptation scheme. Parameters: $\lambda_e = \lambda_p = 10^{-4}\ m^{-2}$, $\lambda_s = 10^{-3}\ m^{-2}$, $\alpha = 4$, $r_p = 15\ m$, $r_s = 10\ m$, $P_p = 36$ dBm, and $\gamma_{th}^{\{p\}} = 0$ dBm.

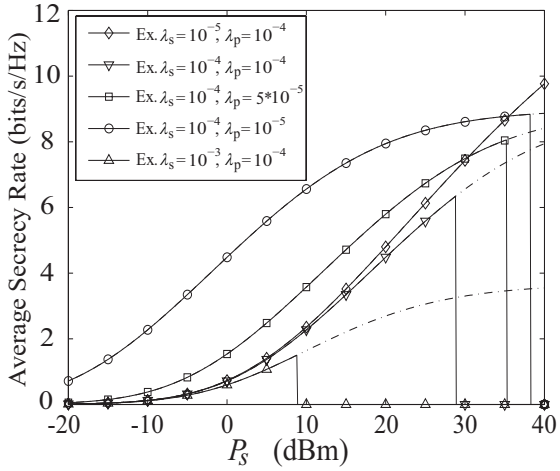


Fig. 3. Average secrecy rate of a large scale spectrum sharing network with the transmit power adaptation scheme. Parameters: $\lambda_e = 10^{-4}\ m^{-2}$, $N_s = 6$, $\alpha = 4$, $r_p = 15\ m$, $r_s = 10\ m$, $\mu = 0.8$, $P_p = 36$ dBm, and $\gamma_{th}^{\{p\}} = 0$ dBm.

By substituting the probability density function (PDF) of $\gamma_{\mathtt{SIR}}^{e,AN}$ and CDF of $\gamma_{\mathtt{SIR}}^{s,AN}$ into (28), we derive the secrecy outage probability in the following theorem.

Theorem 3. *With BF&AN at the SU transmitters, the secrecy outage probability is derived as*

$$P_{out,AN}\left(R_s\right) = \int_0^{\infty} \frac{\pi\lambda_e x_2^{-\frac{2}{\alpha}}\left(\frac{2}{\alpha}x_2^{-1}\left(\frac{1-\mu}{(N_s-1)\mu}x_2+1\right)+1\right)}{\Lambda_l\left(\frac{1-\mu}{(N_s-1)\mu}x_2+1\right)^{N_s}}$$
$$\exp\left(-\frac{\pi\lambda_e}{\Lambda_l}x_2^{-\frac{2}{\alpha}}\left(\frac{1-\mu}{(N_s-1)\,\mu}x_2+1\right)^{1-N_s}\right)\Big[1-$$
$$\exp\left(-\Lambda_3\left(2^{R_s}\left(1+x_2\right)-1\right)^{\frac{2}{\alpha}}r_s^2\right)\Big(1+\sum_{m=1}^{N_s-1}\frac{\left(r_s^{\alpha}\right)^m}{m!\left(-1\right)^m}\sum m!$$
$$\prod_{j=1}^{m}\frac{\left(\left(-\Lambda_l(2^{R_s}(1+x_2)-1)^{\frac{2}{\alpha}}\right)(r_s)^{2-j\alpha}\prod_{k=0}^{j-1}\left(\frac{2}{\alpha}-k\right)\right)^{m_j}}{m_j!j!^{m_j}}\Big)\Big]dx_2, \tag{29}$$

where Λ_l is given in (23)*. Here, P_s is the maximum permissive transmit power, which is given in* (18)*.*

B. Numerical Examples for BF & AN

1) *Average Secrecy Rate Boundary*

Fig. 2 and Fig. 3 plot the average secrecy rate of large scale underlay spectrum sharing networks under the primary network's QoS constraint $\rho_{out}^{\{p\}} = 0.15$ with the transmit power adaptation scheme. From these 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 network's QoS constraint is always satisfied, i.e., $P_{out}^{pri,AN}\left(\gamma_{th}^{\{p\}}\right) \leq 0.15$. The dashed lines represent the unachievable average secrecy rate where the primary network's QoS constraint is violated, i.e., $P_{out}^{pri,AN}\left(\gamma_{th}^{\{p\}}\right) > 0.15$. We named the solid line as "average secrecy rate boundary".

2) *Impact of N_s and μ on the average secrecy rate*

Fig. 2 plots the average secrecy rate versus the SU's transmit power with various number of transmit antennas N_s at the SU and power allocation factor μ, and we consider the same density for PUs, SUs, and eavesdroppers. The exact analytical curves are obtained from (27). We find that for fixed $\mu = 0.4$, the average secrecy rate increases with increasing N_s.

3) *Impact of λ_s and λ_p on the average secrecy rate*

Fig. 3 plots the average secrecy rate versus P_s for various densities of PUs and SUs. We observe that there is a shift of the "average secrecy rate wall" to the left with increasing the density of PUs and SUs. This can be predicted from (18) that $P_s^{\max}$ is a decreasing function of λ_p and λ_s. As expected, the average secrecy rate decreases with increasing the density of SUs and PUs, due to the increased aggregate interference from the SUs and the PUs.

4) *Optimal μ for the average secrecy rate*

Fig. 4 plots the average secrecy rate versus μ for various densities of eavesdroppers λ_e. Here, we use the maximum permissive transmit power to transmit the signal from SU, which is given by (27), and we set $P_s = P_s^{max}$ and $\rho_{out}^{\{p\}} = 0.1$. The triangles represent the maximum achievable average secrecy rate. For the scenarios where the density of eavesdroppers is higher than the density of SUs, the average secrecy rate first increases and then decreases with increasing μ. An optimal power allocation factor μ^* exists at which the maximum average secrecy rate is achieved. For the region $\mu < \mu^*$, we see that increasing the power allocated to the useful signal ensures more message delivery (increasing $C_{\mathtt{su}}$)

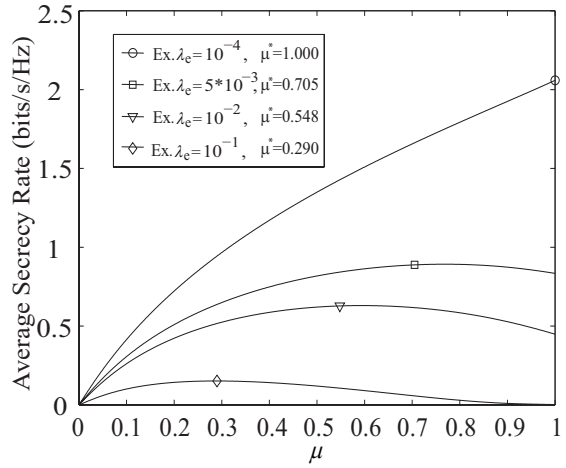


Fig. 4. Average secrecy rate of a large scale spectrum sharing network. Parameters: $\lambda_p = 10^{-4}\ m^{-2}$, $\lambda_s = 10^{-3}\ m^{-2}$, $\alpha = 3$, $r_p = 15\ m$, $r_s = 10\ m$, $N_s = 6$, $P_p = 15$ dBm, and $\gamma_{th}^{\{p\}} = 0$ dBm.

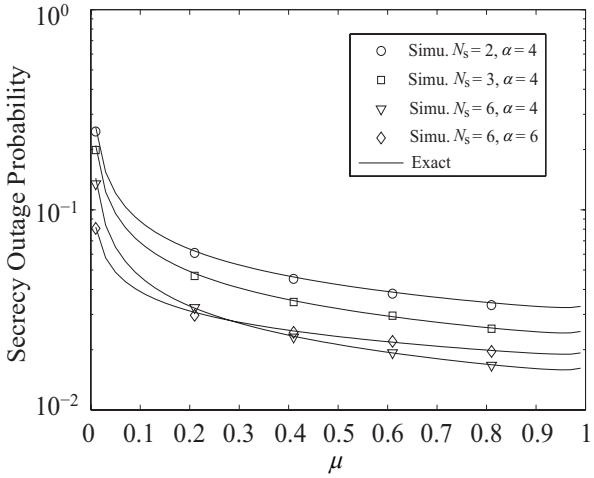


Fig. 6. Secrecy outage probability versus μ for various N_s and α. Parameters: $\rho_{out}^{\{p\}} = 0.1$, $\lambda_e = 10^{-4}\ m^{-2}$, $\lambda_p = 10^{-4}\ m^{-2}$, $\lambda_s = 10^{-3}\ m^{-2}$, $r_p = 6\ m$, $r_s = 3\ m$, $N_S = 6$, $Rs = 1$, $P_p = 15$ dBm, and $\gamma_{th}^{\{p\}} = 0$ dBm.

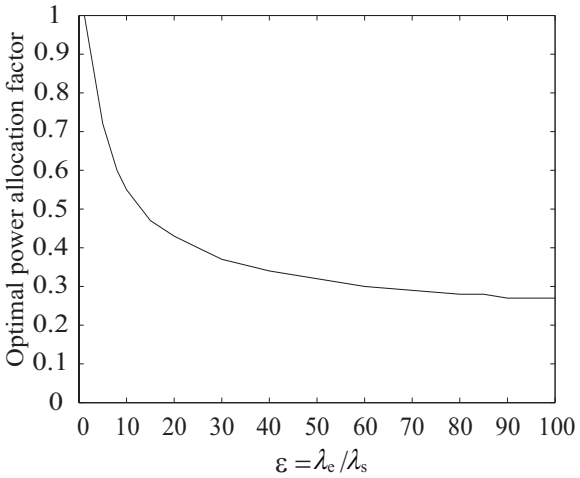


Fig. 5. Optimum μ for maximum average secrecy rate versus ε. Parameters: $\lambda_s = 10^{-3}\ m^{-2}$, $\lambda_p = \lambda_s/10$, $N_s = 4$, $\rho_{out}^{\{p\}} = 0.1$, $\alpha = 3$, $r_p = 15\ m$, $r_s = 10\ m$, $P_p = 15$ dBm, and $\gamma_{th}^{\{p\}} = 0$ dBm.

and plays a dominant role in improving the average secrecy rate; for the region $\mu > \mu^*$, reducing the power allocated to the AN increases C_{E}, and thus degrades the average secrecy rate. We conclude that a tradeoff exists between increasing the capacity of secondary channel and decreasing the capacity of eavesdropping channel. Interestingly, we see from Fig. 4 that μ^* varies for different λ_e. We find that less power should be allocated to the AN for a network with less dense eavesdroppers. Out of expectation, the equal power allocation may not be a good strategy to achieve the maximum average secrecy rate.

5) *Impact of density ratio on the optimal μ*

To better illustrate the relationship between the optimal power allocation factor and the density of SUs and eavesdroppers. We first define the ratio between λ_e and λ_s as $\varepsilon = \lambda_e/\lambda_s$. In Fig. 5, we plot μ^* versus the density ratio ε. We set $P_s = P_s^{max}$, $\lambda_s = 10^{-3}\ m^{-2}$, and $\lambda_p = 10^{-4}\ m^{-2}$. We find that 1) The power allocated to AN should be increased with increasing the density ratio between the eavesdroppers and the SUs ε to achieve the optimal average secrecy rate; 2) For extremely low density ratio ε, all of the power should be allocated to information signal without injecting AN to achieve the maximum average secrecy rate. This reveals that improving the information delivery is more important than combating the eavesdropping in this scenario.

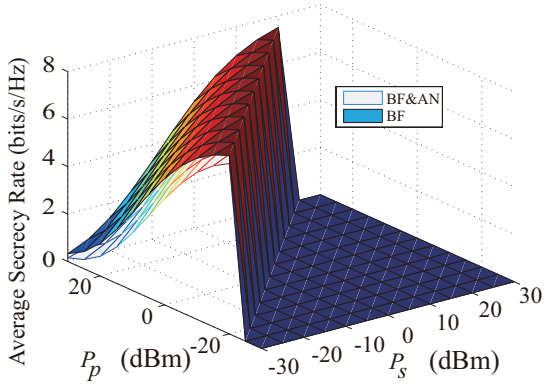
6) *Impact of N_s and α on the secrecy outage probability*

Fig. 6 plots the secrecy outage probability versus μ for various number of antennas at SU transmitter N_s. The exact analytical curves are obtained from (29), which are well validated by Monte Carlo simulations. We assume $P_s = P_s^{max}$. In this setting, we see that the secrecy outage probability decreases with increasing μ, and when μ approaches 1, the lowest secrecy outage probability is achieved. This is because when the density of eavesdroppers is small compared to that of SU, the effect of delivering information overtakes the effect of combating the eavesdropping. As expected, the secrecy outage probability decreases with increasing N_s, which is due to the array gains brought by additional antennas.

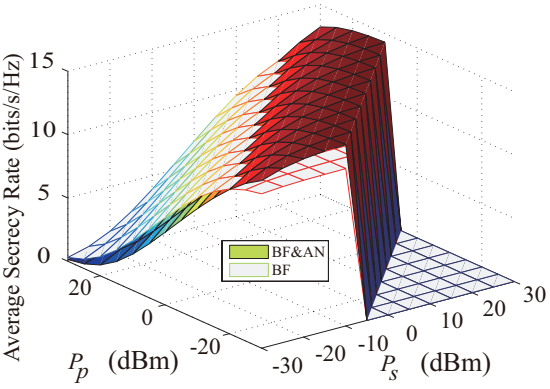
C. Numerical examples for the comparison between BF&AN and BF

In this subsection, we compare the secrecy performance of our proposed network with BF&AN to that with BF, and examine the potential benefits of AN on the secrecy performance. Note that BF can be viewed as a special case of BF&AN with $\mu = 1$.

In Fig. 7(a) and Fig. 7(b), we plot the operational achievable average secrecy rate region for the large scale spectrum sharing



(a) Parameters: $\lambda_s = \lambda_e = 10^{-4}\ m^{-2}$, $\lambda_p = 10^{-5}\ m^{-2}$, $\rho_{out}^{\{p\}} = 0.1$, $\mu = 0.4$, $r_p = 15\ m$, $r_s = 10\ m$, and $\alpha = 4$



(b) Parameters: $\lambda_p = \lambda_s = 10^{-6}\ m^{-2}$, $\lambda_e = 10^{-5}\ m^{-2}$, $\rho_{out}^{\{p\}} = 0.1$, $\mu = 0.4$, $r_p = 15\ m$, $r_s = 10\ m$, and $\alpha = 3$

Fig. 7. Comparison of average secrecy rate versus P_s and P_p between BF&AN and BF.

network with BF&AN and BF. We see the same permissive transmit power region for BF&AN and BF in each figure. This is because, from the typical PU receiver's perspective, both AN and the information signal transmitted from SU are viewed as interference, which is equivalent to the case of BF. In both figures, we notice that the same unachievable average secrecy rate region located in $P_s \in (0, 30)$ dBm with $P_p \in (0, -30)$ dBm. This can be explained by the fact that the QoS constraint is severely violated in this setting when the aggregate interference is much higher compared to the useful signal received at PU.

In contrast to the fact that it is often beneficial to emit AN on top of the information-bearing signal in the physical layer security model with fixed nodes [42], we see from Fig. 7(a) that BF outperforms BF&AN or has the same performance as BF&AN in all operational region. This is because the strong aggregate interference from the PUs overtakes the effect of the AN generated by SU. In this case, more power needs to be allocated to transmit information signal at SUs to contend with the interference from PUs. Interestingly, Fig. 7(b) shows that BF&AN outperforms BF in some regions, owing to the fact that the effect of AN generated by SU overtakes the relatively low aggregate interference from PUs. In this case, more power should be allocated to transmit AN to disrupt the eavesdropping.

IV. Large Antenna arrays analysis

In this section, we study the asymptotic secrecy performance of the large scale spectrum sharing networks where the SU transmitters are equipped with large antenna arrays. We examine the asymptotic behavior of the average secrecy rate and the secrecy outage probability, when the number of antennas at the SU transmitters goes to infinity.

We first present the Lemma 4 based on the law of large numbers as follows:

Lemma 4. $\lim_{N_s\to\infty} \|\mathbf{h}_z\|^2 = N_s$, *and* $\lim_{N_s\to\infty} \|\mathbf{h}_{i,z}\mathbf{G}_{i,s_i}\|^2 = N_s - 1$.

Proof. This is due to the fact that $\|\mathbf{h}_z\|^2 \sim Gamma\,(N_s, 1)$ and $\|\mathbf{h}_{i,z}\mathbf{G}_{i,s_i}\|^2 \sim Gamma\,(N_s - 1, 1)$. □

By using Lemma 4, we rewrite the SIR at the typical PU in (2) as

$$\gamma_{\mathtt{SIR}}^{p,\infty} \overset{d}{\sim} \frac{|h_{p_0}|^2 r_p{}^{-\alpha}}{I_{p,p_0} + \eta I_{s,p_0,\infty}}, \tag{30}$$

where

$$I_{p,p_0} = \sum_{j\in\Phi_p\setminus\{0\}} |h_{j,p_0}|^2 |X_{j,p_0}|^{-\alpha} \tag{31}$$

and

$$I_{s,p_0,\infty} = \sum_{i\in\Phi_s} \left[\mu \left|\mathbf{h}_{i,p_0} \frac{\mathbf{h}_{i,s_i}^\dagger}{\left\|\mathbf{h}_{i,s_i}^\dagger\right\|}\right|^2 + (1-\mu)\right] |X_{i,p_0}|^{-\alpha}. \tag{32}$$

For large N_s, the SIR at typical SU is given as

$$\gamma_{\mathtt{SIR}}^{s,\infty} \overset{d}{\sim} \frac{\mu N_s r_s{}^{-\alpha}}{I_{s,s_0,\infty} + \eta^{-1} I_{p,s_0}}, \tag{33}$$

where

$$I_{p,s_0} = \sum_{j\in\Phi_p} |h_{j,s_0}|^2 |X_{j,s_0}|^{-\alpha} \tag{34}$$

and

$$I_{s,s_0,\infty} = \sum_{i\in\Phi_s\setminus\{0\}} \left[\mu \left|\mathbf{h}_{i,s_0} \frac{\mathbf{h}_{i,s_i}^\dagger}{\left\|\mathbf{h}_{i,s_i}^\dagger\right\|}\right|^2 + (1-\mu)\right] |X_{i,s_i}|^{-\alpha}. \tag{35}$$

From (33), we find that the received SIR at typical SU scale by N_s.

For large N_s, the SIR at the most detrimental eavesdropper is given as

$$\gamma_{\mathtt{SIR}}^{e,\infty} = \max_{e_k\in\Phi_e} \left\{\gamma_{\mathtt{SIR}}^{e_k,\infty}\right\}, \tag{36}$$

where

$$\gamma_{\mathtt{SIR}}^{e_k,\infty} \overset{d}{\sim} \frac{\mu \left|\mathbf{h}_{0,e_k} \frac{\mathbf{h}_{i,s_i}^\dagger}{\left\|\mathbf{h}_{i,s_i}^\dagger\right\|}\right|^2 |X_{e_k}|^{-\alpha}}{I_{s_0,e_k,\infty} + \eta^{-1} I_{p,e_k} + (1-\mu)\,|X_{e_k}|^{-\alpha}}, \tag{37}$$

where

$$I_{p,e_k} = \sum_{j\in\Phi_p} |h_{j,e_k}|^2 |X_{j,e_k}|^{-\alpha} \tag{38}$$

and

$$I_{s_0,e_k,\infty} = \sum_{i\in\Phi_s\setminus\{0\}} \Big[\mu \Big| \mathbf{h}_{i,e_k} \frac{\mathbf{h}_{i,s_i}^{\dagger}}{\big\|\mathbf{h}_{i,s_i}^{\dagger}\big\|}\Big|^2 + (1-\mu)\Big] |X_{i,e_k}|^{-\alpha}. \tag{39}$$

Based on the SIR at the typical PU in (30), with the help of the Laplace transform in [43, eq. (8)], and similar method provided in the proof for the **Theorem 1**, we present the permissive transmit power region at the SU transmitter at large N_s in the following proposition.

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

$$P_s^{max} = \Big[-\Theta\big(\int_0^{\infty} \big(\mu t + (1-\mu)\big)^{\frac{2}{\alpha}} e^{-t} dt\big)^{-1} {\lambda_s}^{-1}\Big]^{\frac{\alpha}{2}} P_p, \tag{40}$$

and Θ is given by (19)*.*

To facilitate the analysis of the average secrecy rate and the secrecy outage probability, we need to first derive the asymptotic CDFs of $\gamma_{\mathtt{SIR}}^{e,\infty}$ and $\gamma_{\mathtt{SIR}}^{s,\infty}$. Using the method presented in Appendix B, we derive the asymptotic CDF of $\gamma_{\mathtt{SIR}}^{e,\infty}$ given in (36) as

$$F_{\gamma_{\mathtt{SIR}}^{e,\infty}}\big(\gamma_{th}^{\{e\}}\big) = \exp\Big(-\frac{\pi\lambda_e e^{\left(1-\mu^{-1}\right)\gamma_{th}^{\{e\}}}}{\Xi\Gamma\big(1-\frac{2}{\alpha}\big)} \big(\frac{\mu P_s}{\gamma_{th}^{\{e\}} P_p}\big)^{\frac{2}{\alpha}}\Big), \tag{41}$$

where

$$\Xi = \lambda_p \Gamma\big(1+\frac{2}{\alpha}\big) + \lambda_s \big(\frac{P_s}{P_p}\big)^{\frac{2}{\alpha}} \int_0^{\infty} \big(\mu t + (1-\mu)\big)^{\frac{2}{\alpha}} e^{-t} dt. \tag{42}$$

To derive the asymptotic CDF of $\gamma_{\mathtt{SIR}}^{s,\infty}$, we first present

$$F_{\gamma_{\mathtt{SIR}}^{s,\infty}}\left(\gamma_{th}^{s}\right) = \int_{\frac{\mu N_s}{\gamma_{th}^{s} {r_{s_0}}^{\alpha}}}^{\infty} f_{I_{\mathrm{sec},\infty}}(x)\, dx, \tag{43}$$

where

$$I_{\mathrm{sec},\infty} = \mu \sum_{i\in\Phi_s\setminus\{0\}} \big|\mathbf{h}_{i,s_0} \frac{\mathbf{h}_{i,s_i}^{\dagger}}{\big\|\mathbf{h}_{i,s_i}^{\dagger}\big\|}\big|^2 |X_{i,s_i}|^{-\alpha} + (1-\mu) \sum_{i\in\Phi_s\setminus\{0\}} |X_{i,s_i}|^{-\alpha} + \big(\frac{P_s}{P_p}\big)^{-1} \sum_{j\in\Phi_p} |h_{j,s_0}|^2 |X_{j,s_0}|^{-\alpha}. \tag{44}$$

In (43), $f_{I_{\mathrm{sec},\infty}}(x)$ is the inverse Laplace transform of $\mathcal{L}_{I_{\mathrm{sec},\infty}}(s)$, which can be expressed as $f_{I_{\mathrm{sec},\infty}}(x) = \mathcal{L}^{-1}_{I_{\mathrm{sec},\infty}}(s)$. Due to the intractability of this inverse Laplace transform, some alternative ways have been proposed, such as using numerical inversion to evaluate $\mathcal{L}^{-1}_{I_{\mathrm{sec},\infty}}(s)$ [44], or the log-normal approximations to approximate $f_{I_{\mathrm{sec},\infty}}(x)$. However, in our case, there exists singularity at $|X_{i,s_i}| = |X_{j,s_0}| = 0$, thus the mean and variance of $I_{\mathrm{sec},\infty}$ derived from the moment generating function diverge [14, 45], which renders the derivation of the PDF of $I_{\mathrm{sec},\infty}$. Alternatively, we utilize the Gil-Pelaez theorem [46] to facilitate the derivation of the asymptotic CDF of SIR at the typical SU in the following lemma.

Lemma 5. *With BF&AN at the SU transmitters, the asymptotic CDF of SIR at the typical SU at large N_s is given as*

$$F_{\gamma_{\mathtt{SIR}}^{s,\infty}}\big(\gamma_{th}^{s}\big) = 1 - F_{I_{\mathrm{sec},\infty}}\big(\frac{\mu N_s}{\gamma_{th}^{s} {r_{s_0}}^{\alpha}}\big) = \frac{1}{2} + \frac{1}{\pi}\int_0^{\infty} \frac{\mathrm{Im}\big[e^{-\frac{jw\mu N_s}{\gamma_{th}^{s} {r_{s_0}}^{\alpha}}} \varphi^*(w)\big]}{w} dw, \tag{45}$$

where $F_{I_{\mathrm{sec},\infty}}(x)$ is the CDF of $I_{\mathrm{sec},\infty}$, $j = \sqrt{(-1)}$, and $\varphi(w)$ is the conjugate of the characteristic function, which is given by

$$\varphi(w) = \exp\big(-\pi\Xi\Gamma\big(1-\frac{2}{\alpha}\big)\eta^{-\frac{2}{\alpha}}(jw)^{\frac{2}{\alpha}}\big). \tag{46}$$

Since we can not derive the closed form expression for the general form for the PDF of $I_{\mathrm{sec},\infty}$, we present the special case for the path loss component $\alpha = 4$. In the following corollary, we derive the asymptotic CDF of SIR for the typical secondary user with $\alpha = 4$.

Corollary 1. *With BF&AN at the SU transmitters and $\alpha = 4$, the asymptotic CDF of SIR at the typical SU is derived as*

$$F^{\infty}_{\gamma_{\mathtt{SIR}}^{s,AN}}\big(\gamma_{th}^{s}\big) = \Phi\big(\frac{\pi\Xi}{2}\sqrt{\frac{\pi\gamma_{th}^{s} {r_{s_0}}^{\alpha}}{\mu N_s}}\big), \tag{47}$$

where

$$\Phi(x) = \frac{1}{\sqrt{\pi}}\int_0^{x^2} \frac{e^{-t}}{\sqrt{t}} dt. \tag{48}$$

Note that our derived asymptotic CDF of SIR at the typical SU for $\alpha = 4$ is in exact closed-form.

A. Average Secrecy Rate

Based on the CDF of SIR at the most detrimental eavesdroppers in (41) and the CDF of SIR at the typical SU in (45), we derive the general case of the asymptotic average secrecy rate using (21) in the following proposition.

Proposition 2. *With BF&AN at the SU transmitters, the asymptotic average secrecy rate at large N_s is derived as*

$$\bar{C}_{se}^{\infty} = \frac{1}{\ln 2}\int_0^{\infty} \frac{1}{1+x_2} \exp\big(-\frac{\pi\lambda_e e^{\left(1-\mu^{-1}\right)x_2}}{\Xi\Gamma\big(1-\frac{2}{\alpha}\big)}\big(\frac{\mu P_s}{x_2 P_p}\big)^{\frac{2}{\alpha}}\big)\Big[\frac{1}{2} - \frac{1}{\pi}\int_0^{\infty} \mathrm{Im}\big[\frac{\big(\exp(-\pi\Xi\Gamma(1-\frac{2}{\alpha})(\frac{P_s}{P_p})^{-\frac{2}{\alpha}}(jw)^{\frac{2}{\alpha}})\big)^*}{e^{\frac{jw\mu N_s}{x_2 {r_{s_0}}^{\alpha}}}}\big]\frac{1}{w} dw\Big] dx_2. \tag{49}$$

Having (41) and (47), we derive the asymptotic average secrecy rate for the special case of $\alpha = 4$ in the following corollary.

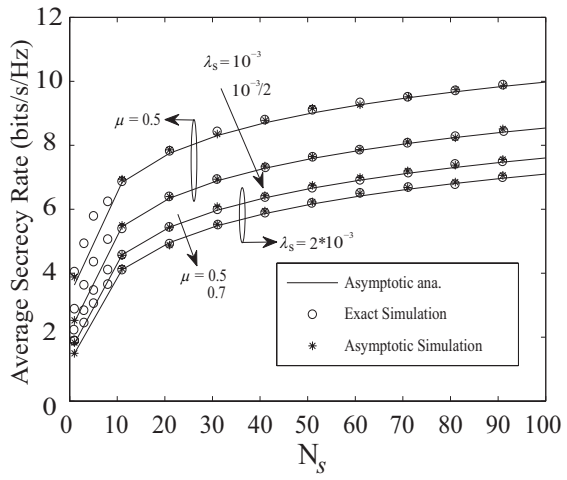


Fig. 8. Asymptotic average secrecy rate versus N_s. Parameters: $\rho_{out}^{\{p\}} = 0.1$, $\lambda_p = 10^{-4}\ m^{-2}$, $\lambda_e = 10^{-4}\ m^{-2}$, $r_p = 6\ m$, $\mu = 0.7$, $\alpha = 3$, $r_s = 3\ m$, $P_p = 15$ dBm, and $\gamma_{th}^{\{p\}} = 6$ dBm.

Corollary 2. *With BF&AN at the SU transmitters and $\alpha = 4$, the asymptotic average secrecy rate at large N_s is derived as*

$$\bar{C}_{se}^{\infty} = \frac{1}{\ln 2}\int_0^{\infty} \frac{1}{1+x_2}\exp\big(-\frac{\pi\lambda_e e^{\left(1-\mu^{-1}\right)x_2}}{\Xi\Gamma\left(1-\frac{2}{\alpha}\right)}\big(\frac{\mu}{x_2}\big)^{\frac{2}{\alpha}}\big) \big(1-\Phi\big(\frac{\pi\Xi}{2}\sqrt{\frac{\pi x_2}{\mu N_s {r_{s_0}}^{-\alpha}}}\big)\big)dx_2. \quad (50)$$

B. Secrecy Outage Probability

We then turn our attention to the asymptotic secrecy outage probability. We take the derivative of the asymptotic CDF of SIR at the most detrimental eavesdroppers in (41), and substitute it with the asymptotic CDF of SIR at the typical SU in (47) into (28), to yield the general case of the asymptotic secrecy outage probability in the following proposition.

Proposition 3. *With BF&AN at the SU transmitters, the asymptotic secrecy outage probability at large N_s is derived as*

$$P_{out,AN}^{\infty}\left(R_s\right) = \int_0^{\infty} \frac{\pi\lambda_e(\mu P_s/P_p)^{\frac{2}{\alpha}}}{\Xi\Gamma(1-\frac{2}{\alpha}){x_2}^{\frac{2}{\alpha}}}\exp\big(-\frac{\pi\lambda_e e^{(1-\mu^{-1})x_2}}{\Xi\Gamma(1-\frac{2}{\alpha})}\big(\frac{\mu P_s}{x_2 P_p}\big)^{\frac{2}{\alpha}}\big) e^{\left(1-\mu^{-1}\right)x_2}\Big(\big(1-\mu^{-1}\big)-\big(-\frac{2}{\alpha}\big){x_2}^{-1}\Big)\Big[\frac{1}{2}+\frac{1}{\pi} \int_0^{\infty}\mathrm{Im}\big[\frac{(\exp(-\pi\Xi\Gamma(1-\frac{2}{\alpha})(P_s/P_p)^{-\frac{2}{\alpha}}(jw)^{\frac{2}{\alpha}}))^*}{e^{\frac{jw\mu N_s}{(2^{R_s}(1+x_2)-1){r_{s_0}}^{\alpha}}}}\big] \frac{1}{w}dw\Big]\,dx_2. \quad (51)$$

Based on (47), we derive the secrecy outage probability for $\alpha = 4$ as a special case in the following corollary.

Corollary 3. *With BF&AN at the SU transmitters and $\alpha = 4$, the asymptotic secrecy outage probability at large N_s is derived as*

$$P_{out,AN}^{\infty}\left(R_s\right) = \int_0^{\infty} \frac{\pi\lambda_e\mu^{\frac{2}{\alpha}}}{\Xi\Gamma\left(1-\frac{2}{\alpha}\right)}\exp\big(-\frac{\pi\lambda_e e^{\left(1-\mu^{-1}\right)x_2}}{\Xi\Gamma\left(1-\frac{2}{\alpha}\right)}\big(\frac{\mu}{x_2}\big)^{\frac{2}{\alpha}}\big) {x_2}^{-\frac{2}{\alpha}} e^{\left(1-\mu^{-1}\right)x_2}\Big(\big(1-\mu^{-1}\big)-\big(-\frac{2}{\alpha}\big){x_2}^{-1}\Big) \Phi\big(\frac{\pi\Xi}{2}\sqrt{\frac{\pi\left(2^{R_s}\left(1+x_2\right)-1\right)}{\mu N_s {r_{s_0}}^{-\alpha}}}\big)dx_2. \quad (52)$$

C. Numerical examples for the asymptotic secrecy performance of BF&AN

Fig. 8 plots the asymptotic average secrecy rate of large scale spectrum sharing networks with BF&AN for various power allocation factor μ and λ_s. We assume $P_s = P_s^{max}$. The analytical results of asymptotic secrecy rate plotted using (49) are in precise agreement with the simulation points of asymptotic secrecy rate. It is also shown that the asymptotic average secrecy rate converges to the exact average secrecy rate at large N_s.

We observe that the average secrecy rate increases with increasing N_s. This can be indicated by (33) that the received SIR at the typical SU proportionally increases with μN_s. For the same μ, to achieve the same average secrecy rate, there exists antenna gaps between the curves with different density of SU. This antenna gap quantifies how many additional antennas needed to be employed at the SU transmitter to achieve the same average secrecy rate when the network double its density of SU.

Fig. 9 plots the asymptotic secrecy outage probability versus N_s. The analytical results of asymptotic outage probability plotted using (51) are in precise agreement with the simulation points of asymptotic outage probability. Furthermore, the asymptotic secrecy outage probability converges to the exact secrecy outage probability at large N_s. We see that the secrecy outage probability decreases with increasing N_s, due to the increase of the array gains at the SU receiver. We also see that the secrecy outage probability decreases with increasing μ, which reflects that for the scenario with relatively less dense eavesdroppers, more power should be allocated to transmit useful information to the SU receiver for the information delivery enhancement.

V. Conclusion

In this paper, we considered secure communication in large scale spectrum sharing networks in the presence of multiple non-colluding eavesdroppers. We employed beamforming and artificial noise generation (BF&AN) at the SU transmitters to achieve secure transmission against malicious eavesdroppers. We obtained an exact expression for the average secrecy rate, through which we observed the average secrecy rate boundary. We also derived an exact expression for the secrecy outage

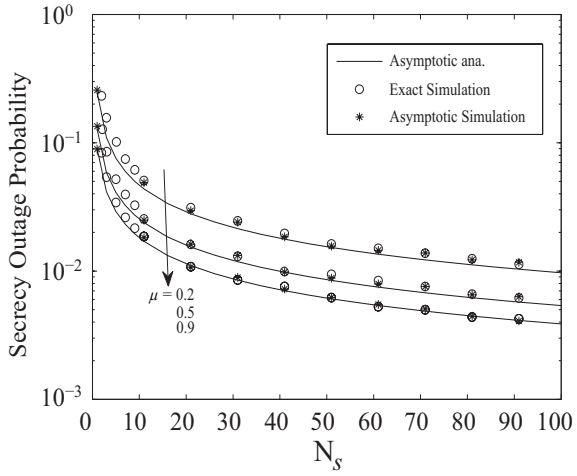


Fig. 9. Secrecy outage probability for large N_s. Parameters: $\rho_{out}^{\{p\}} = 0.1$, $\lambda_p = 10^{-4}\ m^{-2}$, $\lambda_s = 10^{-3}\ m^{-2}$, $\lambda_e = 10^{-4}\ m^{-2}$, $r_p = 6\ m$, $\alpha = 3$, $r_s = 3\ m$, $R_s = 1$, $P_p = 15$ dBm, and $\gamma_{th}^{\{p\}} = 6$ dBm.

probability. Interestingly, our results show that to achieve the optimal average secrecy rate, more power should be allocated to AN with increasing the density ratio between the eavesdroppers and the SUs; whereas for extremely low density ratio, all of the power should be allocated to information signal without injecting AN. Moreover, we derived the asymptotic average secrecy rate and the asymptotic secrecy outage probability as the number of antennas at the SU transmitters grows large to showcase the large gain brought to the secrecy performance.

Appendix A
A Proof of Lemma 1

Consider a HPPP Φ_s with density λ_s, the aggregate interference from the SU transmitters is given by

$$I_{s,z} = \sum\nolimits_{i\in\Phi_s} W_{s_i,z}|X_{i,z}|^{-\alpha}. \tag{A.1}$$

The Laplace transform of $I_{s,z}$ is

$$\mathcal{L}_{I_{s,z}}(s) = \mathbb{E}\Big(\prod_{i\in\Phi_s} \mathbb{E}_{W_{s_i,z}}\left(\exp\left(-sW_{s_i,z}|X_{i,z}|^{-\alpha}\right)\right)\Big). \tag{A.2}$$

Applying the Generating functional of HPPP in [36] and the polar-coordinate system, we have

$$\mathcal{L}_{I_{s,z}}(s) = \exp\left(-\lambda_s\pi\mathbb{E}\big[W_{s_i,z}^{\frac{2}{\alpha}}\big]\Gamma\big(1-\frac{2}{\alpha}\big)s^{\frac{2}{\alpha}}\right). \tag{A.3}$$

Then we turn our attention to derive the expectation of $W_{s_i,z}$. According to [47] and [21], $\left|\mathbf{h}_{0,z}\frac{\mathbf{h}_{i,s_i}^{\dagger}}{\left\|\mathbf{h}_{i,s_i}^{\dagger}\right\|}\right|^2 \sim Exp(1)$, and $\|\mathbf{h}_{i,z}\mathbf{G}_{i,s_i}\|^2 \sim Gamma(N_s-1,1)$. Thus, we have the PDF distribution of $W_{s_i,z} = \sigma_s^2\left|\mathbf{h}_{i,z}\frac{\mathbf{h}_{i,s_i}^{\dagger}}{\left\|\mathbf{h}_{i,s_i}^{\dagger}\right\|}\right|^2 + \sigma_n^2\|\mathbf{h}_{i,z}\mathbf{G}_{i,s_i}\|^2$ as

$$f_{W_{s_i,z}}(x) = \begin{cases} \big(1-\frac{P_A}{(N_s-1)P_I}\big)^{1-N_s}\big(P_I e^{\frac{x}{P_I}}\big)^{-1}\Big[1- \\ \quad\sum\limits_{k=0}^{N_s-2}\big(\frac{N_s-1}{P_A}-\frac{1}{P_I}\big)^k\frac{x^k}{k!}e^{-\left(\frac{N_s-1}{P_A}-\frac{1}{P_I}\right)x}\Big] & \mu\neq\frac{1}{N_s}, \\ \frac{x^{N_s-1}e^{-\frac{x}{P_I}}}{P_I{}^{N_s-1}(N_s-1)!} & \mu=\frac{1}{N_s}. \end{cases} \tag{A.4}$$

Taking the expectation of $W_{s_i,z}$ by using

$$\mathbb{E}\big[W_{s_i,z}^{\frac{2}{\alpha}}\big] = \int_0^{\infty} x^{\frac{2}{\alpha}} f_{W_{s_i,z}}(x)\,dx, \tag{A.5}$$

and substituting the derived expression of $\mathbb{E}\big[W_{s_i,z}^{\frac{2}{\alpha}}\big]$ into (A.3), we obtain (15).

Appendix B
A Proof of Theorem 1

According to the SIR of the typical PU receiver in (2), we define the sum interference at the typical PU receiver as

$$I_{Pri,AN} = I_{p,p_0} + P_p^{-1}I_{s,p_0}, \tag{B.1}$$

thus the CDF of $\gamma_{\mathtt{SIR}}^{p}$ is expressed as

$$F_{\gamma_{\mathtt{SIR}}^{p}}^{\{p\}}\big(\gamma_{th}^{\{p\}}\big) = \mathbb{E}_{\Phi_p}\left\{\mathbb{E}_{\Phi_s}\left\{\Pr\left\{|h_{p_0}|^2 \le \gamma_{th}^{\{p\}} I_{Pri,AN} {r_p}^{\alpha}\middle|\, \Phi_s,\Phi_p\right\}\right\}\right\} = 1-\mathcal{L}_{I_{Pri,AN}}\big(\gamma_{th}^{\{p\}}{r_p}^{\alpha}\big) \tag{B.2}$$

By utilizing similar approach in Appendix A of [34] and based on **Lemma 1**, we derive the outage probability at the typical PU receiver as

$$P_{out}^{pri,AN}\big(\gamma_{th}^{\{p\}}\big) = \begin{cases} 1-\exp\Big(-\pi\big(\lambda_p\Gamma\left(1+\frac{2}{\alpha}\right)+\lambda_s\big(\frac{P_s}{P_p}\big)^{\frac{2}{\alpha}}\Upsilon_1\big)\delta\Big) & \mu\neq\frac{1}{N_s}, \\ 1-\exp\Big(-\pi\big(\lambda_p\Gamma\left(1+\frac{2}{\alpha}\right)+\lambda_s\big(\mu\frac{P_s}{P_p}\big)^{\frac{2}{\alpha}}\frac{\Gamma\left(N_s+\frac{2}{\alpha}\right)}{\Gamma(N_s)}\big)\delta\Big) & \mu=\frac{1}{N_s}. \end{cases} \tag{B.3}$$

where $\delta = \Gamma\left(1-\frac{2}{\alpha}\right)\big(\gamma_{th}^{\{p\}}\big)^{\frac{2}{\alpha}}{r_p}^2$. By inversing (B.3), we can derive the maximum permissive transmit power at the SU transmitters as (18).

Appendix C
A Proof of Lemma 2

The PDF and CDF of $\|\mathbf{h}_{0,s_0}\|^2$ are given by

$$f_{\|\mathbf{h}_{0,s_0}\|^2}(x) = \frac{x^{N_s-1}e^{-x}}{(\mathrm{N_s}-1)!}, \tag{C.1}$$

and

$$F_{\|\mathbf{h}_{0,s_0}\|^2}(x) = 1-e^{-x}\Big(\sum_{m=0}^{N_s-1}\frac{x^m}{m!}\Big), \tag{C.2}$$

respectively.

Let us define $I_{Sec,AN} = P_p I_{p,s_0} + I_{s,s_0}$.

Based on the SIR in (6), the CDF of $\gamma_{\mathtt{SIR}}^{s,AN}$ can be represented as

$$\begin{aligned}
&F_{\gamma_{\mathtt{SIR}}^{s,AN}}^{\{s\}}\left(\gamma_{th}^{\{s\}}\right) \\
&= 1 - \sum_{m=0}^{N_s-1} \mathbb{E}_{\Phi_p}\Big\{\mathbb{E}_{\Phi_s}\Big\{\int_0^\infty e^{-\tau\gamma_{th}^{\{s\}} r_s^\alpha \sigma_s^{-2}} \left(\tau\gamma_{th}^{\{s\}} r_s^\alpha \sigma_s^{-2}\right)^m \\
&\quad d\Pr\left(I_{Sec,AN} \le \tau\right)\Big\}\Big\}\frac{1}{m!} \\
&\overset{(a)}{=} 1 - \mathbb{E}_{\Phi_p}\Big\{\mathbb{E}_{\Phi_s}\Big\{\int_0^\infty e^{-\tau\gamma_{th}^{\{s\}} r_s^\alpha \sigma_s^{-2}} d\Pr\left(I_{Sec,AN} \le \tau\right)\Big\}\Big\} \\
&\quad - \sum_{m=1}^{N_s-1} \frac{(r_s^\alpha)^m}{m!(-1)^m} \mathbb{E}_{\Phi_p}\Big\{\mathbb{E}_{\Phi_s}\Big\{\int_0^\infty \frac{d^m\left(e^{-\tau\gamma_{th}^{\{s\}} x\sigma_s^{-2}}\right)}{dx^m}\Big|_{x=r_s^\alpha} \\
&\quad d\Pr\left(I_{Sec,AN} \le \tau\right)\Big\}\Big\},
\end{aligned} \tag{C.3}$$

where (a) follows from the fact that

$$\frac{d^m(e^{-\tau\gamma_{th}^{\{s\}} x\sigma_s^{-2}})}{dx^m}\Big|_{x=r_s^\alpha} = (-\tau\gamma_{th}^{\{s\}}\sigma_s^{-2})^m e^{-\tau\gamma_{th}^{\{s\}} r_s^\alpha \sigma_s^{-2}}. \tag{C.4}$$

After some manipulations, we have

$$\begin{aligned}
F_{\gamma_{\mathtt{SIR}}^{s,AN}}^{\{s\}}\left(\gamma_{th}^{\{s\}}\right) &= 1 - \mathcal{L}_{I_{Sec,AN}}\left(\gamma_{th}^{\{s\}} r_s^\alpha \sigma_s^{-2}\right) \\
&\quad - \sum_{m=1}^{N_s-1} \frac{\left(r_s^\alpha\right)^m}{m!\left(-1\right)^m} \frac{d^m\left\{\mathcal{L}_{I_{Sec,AN}}\left(\gamma_{th}^{\{s\}} x\sigma_s^{-2}\right)\right\}}{dx^m}\Big|_{x=r_s^\alpha}.
\end{aligned} \tag{C.5}$$

We then need to derive the Laplace transform of $I_{Sec,AN}$. Utilizing [34, eq. (4)] and **Lemma 2**, we obtain

$$\mathcal{L}_{I_{Sec,AN}}\left(\gamma_{th}^{\{s\}} r_s^\alpha \sigma_s^{-2}\right) = \exp\left(-\Lambda_l\left(\gamma_{th}^{\{s\}}\right)^{\frac{2}{\alpha}} r_s^2\right), \tag{C.6}$$

where Λ_l is given in (23).

Now, we apply the Faà di Bruno's formula to solve the derivative of mth order as follows:

$$\begin{aligned}
&\frac{d^m\left[\exp\left(-\Lambda_l\left(\gamma_{th}^{\{s\}}\right)^{\frac{2}{\alpha}} x^{\frac{2}{\alpha}}\right)\right]}{dx^m}\Big|_{x=r_s^\alpha} = \exp\left(-\Lambda_l\left(\gamma_{th}^{\{s\}}\right)^{\frac{2}{\alpha}} r_s^2\right) \\
&\quad \sum m! \prod_{j=1}^{m} \frac{\left(\left(-\Lambda_l(\gamma_{th}^{\{s\}})^{\frac{2}{\alpha}}\right) \prod_{k=0}^{j-1}\left(\frac{2}{\alpha}-k\right)(r_s)^{2-j\alpha}\right)^{m_j}}{m_j! j!^{m_j}}.
\end{aligned} \tag{C.7}$$

By substituting (C.7) into (C.5), we get the closed-form expression for the CDF of SIR at the typical secondary user as (22).

Appendix D
A Proof of Lemma 3

Let us define $I_{Eve,AN} = P_p I_{p,e_k} + I_{s,e_k} + \sigma_n^2 I_{s_0,e_k,an}$.

The CDF of $\gamma_{\mathtt{SIR}}^{e}$ can be written as

$$\begin{aligned}
F_{\gamma_{\mathtt{SIR}}^{e,AN}}^{\{e\}}\left(\gamma_{th}^{\{e\}}\right) = \mathbb{E}_{\Phi_e}\Big\{\mathbb{E}_{\Phi_p}\Big\{\mathbb{E}_{\Phi_s}\Big\{\prod_{e_k\in\Phi_e} \Pr\Big\{\Big|\mathbf{h}_{0,e}\frac{\mathbf{h}_{0,s_i}^\dagger}{\left\|\mathbf{h}_{0,s_i}^\dagger\right\|}\Big|^2 \le \\
\sigma_s^{-2} I_{Eve,AN}\gamma_{th}^{\{e\}}\left|X_{e_k}\right|^\alpha \Big|\Phi_s,\Phi_p,\Phi_e\Big\}\Big\}\Big\}\Big\}.
\end{aligned} \tag{D.1}$$

According to [47], $\mathbf{h}_{0,e_k}\frac{\mathbf{h}_{0,s_i}^\dagger}{\left\|\mathbf{h}_{0,s_i}^\dagger\right\|}$ is a zero-mean complex Gaussian variable, which is independent of $\mathbf{h}_{0,s_i}^\dagger$, and $\left|\mathbf{h}_{0,e_k}\frac{\mathbf{h}_{0,s_i}^\dagger}{\left\|\mathbf{h}_{0,s_i}^\dagger\right\|}\right|^2$ follows the exponential distribution with unit mean. Thus, the CDF of $\gamma_{\mathtt{SIR}}^{e}$ can be represented as

$$\begin{aligned}
F_{\gamma_{\mathtt{SIR}}^{e,AN}}^{\{e\}}\left(\gamma_{th}^{\{e\}}\right) = \mathbb{E}_{\Phi_e}\Big\{\prod_{e_k\in\Phi_e}\Big(1 - \mathbb{E}_{\Phi_p}\Big\{\mathbb{E}_{\Phi_s}\Big\{\int_0^\infty e^{-\tau\sigma_s^{-2}\gamma_{th}^{\{e\}}} \\
\left|X_{e_k}\right|^\alpha d\Pr\left(I_{Eve,AN} \le \tau\right)\Big\}\Big\}\Big)\Big\}.
\end{aligned} \tag{D.2}$$

According to the proof of Lemma 3.1 in [35], we express (D.2) as

$$F_{\gamma_{\mathtt{SIR}}^{e,AN}}^{\{e\}}\left(\gamma_{th}\right) = \mathbb{E}_{\Phi_e}\Big\{\prod_{e_k\in\Phi_e}\Big(1 - \mathcal{L}_{I_{Eve,AN}}\left(\sigma_s^{-2}\gamma_{th}^{\{e\}}|X_{e_k}|^\alpha\right)\Big)\Big\}. \tag{D.3}$$

By using the Generating functional of HPPP Φ_e [36], we solve (D.3) as

$$\begin{aligned}
F_{\gamma_{\mathtt{SIR}}^{e,AN}}^{\{e\}}\left(\gamma_{th}\right) &= \exp\Big[-\lambda_e \int_{R^2} \mathcal{L}_{I_{Eve,AN}}\left(\sigma_s^{-2}\gamma_{th}^{\{e\}}|X_{e_k}|^\alpha\right) de\Big] \\
&= \exp\Big[-2\pi\lambda_e \int_0^\infty \mathcal{L}_{I_{Eve,AN}}\left(\sigma_s^{-2}\gamma_{th}^{\{e\}}|X_{e_k}|^\alpha\right)|X_{e_k}|\, d\,|X_{e_k}|\Big].
\end{aligned} \tag{D.4}$$

Now we utilize [34, eq. (4)] and **Lemma 2**, we derive the Laplace transform of $I_{Eve,AN}$ as

$$\begin{aligned}
&\mathcal{L}_{I_{Eve,AN}}(s) = \\
&\begin{cases}
\exp\Big(-\pi\big(\lambda_p\Gamma\big(1+\frac{2}{\alpha}\big)\eta^{-\frac{2}{\alpha}}\mu^{-\frac{2}{\alpha}} + \lambda_s\frac{\Gamma\left(N_s+\frac{2}{\alpha}\right)}{\Gamma\left(N_s\right)}\big) \\
\quad \Gamma\big(1-\frac{2}{\alpha}\big)\big(\gamma_{th}^{\{e\}}\big)^{\frac{2}{\alpha}}\left|X_{e_k}\right|^2\Big)\big(\frac{1-\mu}{\left(N_s-1\right)\mu}\gamma_{th}^{\{e\}}+1\big)^{-(N_s-1)} \\
\qquad\qquad \mu = \frac{1}{N_s}, \\
\exp\Big(-\pi\big(\lambda_p\Gamma\left(1+\frac{2}{\alpha}\right)\eta^{-\frac{2}{\alpha}} + \lambda_s\Upsilon_1\big)\Gamma\left(1-\frac{2}{\alpha}\right) \\
\quad \big(\gamma_{th}^{\{e\}}\big)^{\frac{2}{\alpha}}\mu^{-\frac{2}{\alpha}}|X_{e_k}|^2\Big)\big(\frac{1-\mu}{(N_s-1)\mu}\gamma_{th}^{\{e\}}+1\big)^{-(N_s-1)} \\
\qquad\qquad \mu \ne \frac{1}{N_s}.
\end{cases}
\end{aligned} \tag{D.5}$$

By substituting (D.5) into (D.4), we obtain

$$\begin{aligned}
F_{\gamma_{\mathtt{SIR}}^{e}}^{\{e\}}\left(\gamma_{th}^{\{e\}}\right) = \exp\Big[-2\pi\lambda_e\Big(\frac{1-\mu}{\left(N_s-1\right)\mu}\gamma_{th}^{\{e\}}+1\Big)^{-(N_s-1)} \\
\int_0^\infty \exp\left(-\Lambda_l\left(\gamma_{th}^{\{e\}}\right)^{\frac{2}{\alpha}}|X_{e_k}|^2\right)|X_{e_k}|\, d\,|X_{e_k}|\Big],
\end{aligned} \tag{D.6}$$

where Λ_l is given in (23).

By applying [48, Eq. 3.326.2.10], we derive the CDF of $\gamma_{\mathtt{SIR}}^{e,AN}$ as (26).

References

[1] Y. Deng, L. Wang, S. A. R. Zaidi, J. Yuan, and M. Elkashlan, "On the security of large scale spectrum sharing networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 4877–4882.

[2] A. Goldsmith, S. 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] Y. Deng, L. Wang, M. Elkashlan, K. J. Kim, and T. Q. Duong, "Generalized selection combining for cognitive relay networks over nakagami- m fading," *IEEE Trans. Signal Process.*, vol. 63, no. 8, pp. 1993–2006, Apr. 2015.

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

[5] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Mar. 2014.

[6] B. Wang, Y. Wu, K. J. R. Liu, and T. C. Clancy, "An anti-jamming stochastic game for cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 877–889, Apr. 2011.

[7] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

[8] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[9] Y. Deng, L. Wang, M. Elkashlan, A. Nallanathan, and R. K. Mallik, "Physical layer security in three-tier wireless sensor networks: A stochastic geometry approach," *IEEE Trans. Inf. Forensics Security*, to appear 2016.

[10] T.-X. Zheng, H.-M. Wang, and Q. Yin, "On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers," *IEEE Commun. Lett.*, vol. 18, no. 8, pp. 1299–1302, Aug. 2014.

[11] T. Zheng, H. Wang, J. Yuan, D. Towsley, and M. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, to appear 2015.

[12] C. Wang, H.-M. Wang, X. gen Xia, and C. Liu, "Uncoordinated jammer selection for securing SIMOME wiretap channels: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2596–2612, May. 2015.

[13] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2776–2787, Jun. 2013.

[14] 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.

[15] 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.

[16] H. ElSawy, E. Hossain, and M. Haenggi, "Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: A survey," *IEEE Commun. Surveys and Tutorials*, vol. 15, no. 3, pp. 996–1019, Jul. 2013.

[17] H.-M. Wang and X.-G. Xia, "Enhancing wireless secrecy via cooperation: signal design and optimization," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 47–53, Dec. 2015.

[18] 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.

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

[20] 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.

[21] 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.

[22] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, Taipei, China, Apr. 2009, pp. 2437–2440.

[23] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 134–145, Jan. 2013.

[24] N. Zhang, N. Lu, N. Cheng, J. W. Mark, and X. S. Shen, "Cooperative spectrum access towards secure information transfer for CRNs," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 11, pp. 2453–2464, Nov. 2013.

[25] Y. He, J. Evans, and S. Dey, "Secrecy rate maximization for cooperative overlay cognitive radio networks with artificial noise," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 1663–1668.

[26] 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.

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

[28] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.

[29] 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.

[30] C. Wang and H.-M. Wang, "On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1814–1827, Nov. 2014.

[31] S. Anand and R. Chandramouli, "On the secrecy capacity of fading cognitive wireless networks," in *Proc. IEEE Int. Conf. Cogn. Radio Oriented Wireless Netw. Commun.*, May 2008, pp. 1–5.

[32] 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.

[33] 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.

[34] S. Zaidi, D. 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.

[35] F. Baccelli, B. Blaszczyszyn, and P. Muhlethaler, "An aloha protocol for multihop mobile wireless networks," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 421–436, Feb. 2006.

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

[37] 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.

[38] Y. Deng, M. Elkashlan, P. L. Yeoh, N. Yang, and R. K. Mallik, "Cognitive MIMO relay networks with generalized selection combining," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4911–4922, Sep. 2014.

[39] Y. Deng, M. Elkashlan, N. Yang, P. L. Yeoh, and R. K. Mallik, "Impact of primary network on secondary network with generalized selection combining," *IEEE Trans. Veh. Technol.*, vol. 64, no. 7, pp. 3280–3285, Jul. 2015.

[40] 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.

[41] 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.

[42] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Processing Mag.*, vol. 30, no. 5, pp. 29–40, Sep. 2013.

[43] 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.

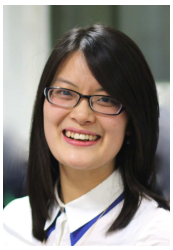
[44] K. J. Hollenbeck, Invlap.m: A Matlab Function for Numerical Inversion of Laplace Transforms by the de Hoog Algorithm 1998. [Online]. Available:http://www.mathworks.com/matlabcentral/fileexchange/32824-numerical-inversion-of-Laplace-transforms-in-matlab/content/INVLAP.m.

[45] J. Venkataraman, M. Haenggi, and O. Collins, "Shot noise models for outage and throughput analyses in wireless ad hoc networks," in *Proc. 44th Annu. Allerton Conf. Communication, Control, and Computing, Monticello, IL*, Sep. 2006, pp. 1–7.

[46] J. G. Wendel, "The non-absolute convergence of Gil-Pelaez' inversion integral," *The Annals of Mathematical Statistics*, vol. 32, no. 1, pp. 338–339, Mar. 1961.

[47] H. Q. Ngo, M. Matthaiou, T. Q. Duong, and E. G. Larsson, "Uplink performance analysis of multicell MU-MIMO systems with ZF receivers," *IEEE Trans. Veh. Technol.*, vol. 62, no. 9, pp. 4471–4482, Nov. 2013.

[48] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 6th ed. New York, NY, USA: Academic Press, 2000.

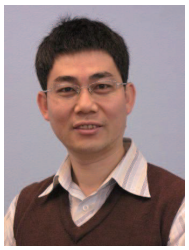


Yansha Deng (M'16) received the Ph.D. degree in Electrical Engineering from Queen Mary University of London, UK, 2015. She is currently the postdoctoral research fellow in the Department of Informatics, at King's College London, UK.

Her research interests include massive MIMO, HetNets, molecular communication, cognitive radio, cooperative networks, and physical layer security. She has served as TPC member for many IEEE conferences such as IEEE GLOBECOM and ICC.

Lifeng Wang (M'16) is the postdoctoral research fellow in the Department of Electronic and Electrical Engineering, University College London (UCL). He received the M.S. degree in Electronic Engineering at University of Electronic Science and Technology of China in 2012, and Ph.D. degree in Electronic Engineering at Queen Mary University of London in April 2015. His research interests include millimeter-wave communications, Massive MIMO, HetNets, Cloud-RAN, cognitive radio, physical layer security and wireless energy harvesting. He received the Exemplary Reviewer Certificate of the IEEE Communications Letters in 2013. He has served as TPC member for many IEEE conferences such as IEEE GLOBECOM and ICC.

Syed Ali Raza Zaidi is currently University Academic Fellow (Lecturer) at the University of Leeds, UK. Prior to this, he was a Research Fellow in SPCOM Research Group at Leeds. He received his B. Eng. degree in information and communication system engineering from the School of Electronics and Electrical Engineering, NUST, Pakistan in 2008. He was awarded the NUST's most prestigious Rector's gold medal for his final year project. From September 2007 till August 2008, he served as a Research Assistant in Wireless Sensor Network Lab on a collaborative research project between NUST, Pakistan and Ajou University, South Korea. In 2008, he was awarded overseas research student scholarship along with Tetley Lupton and Excellence Scholarships to pursue his PhD at the School of Electronics and Electrical Engineering, the University of Leeds, U.K. He was also awarded with COST IC0902, DAAD and Royal Academy of Engineering grants to promote his research. In 2013, he was conferred with prestigious F. W. Carter Prize for outstanding Doctoral thesis by the University of Leeds. Dr. Ali was a visiting research scientist at Qatar Innovations and Mobility Centre from October to December 2013. He has served as an invited reviewer IEEE flagship journals and conferences. Dr. Ali is also UK Liaison for the European Association for Signal Processing (EURASIP). He is currently serving as an editor for IEEE Communication Letters and Lead Guest Editor for IET Signal Processing SI on 5G Wireless Networks. He is also the general secretary for IEEE Technical Committee on 5G Networks. He has published more than 60 papers in leading IEEE Journals and conferences and has chaired several IEEE workshops/conferences. His current research interests are in the area of design and implementation of large scale networks for machine-to-machine communication (including robotics and autonomous systems).



Jinhong Yuan (M'02–SM'11–F'16) received the B.E. and Ph.D. degrees in electronics engineering from the Beijing Institute of Technology, Beijing, China, in 1991 and 1997, respectively. From 1997 to 1999, he was a Research Fellow with the School of Electrical Engineering, University of Sydney, Sydney, Australia. In 2000, he joined the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia, where he is currently a Telecommunications Professor with the School. He has published two books, three book chapters, over 200 papers in telecommunications journals and conference proceedings, and 40 industrial reports. He is a co-inventor of one patent on MIMO systems and two patents on low-density-parity-check codes. He has co-authored three Best Paper Awards and one Best Poster Award, including the Best Paper Award from the IEEE Wireless Communications and Networking Conference, Cancun, Mexico, in 2011, and the Best Paper Award from the IEEE International Symposium on Wireless Communications Systems, Trondheim, Norway, in 2007. He is currently serving as an Associate Editor for the IEEE Transactions on Communications. He served as the IEEE NSW Chair of Joint Communications/Signal Processions/Ocean Engineering Chapter during 2011-2014. His current research interests include error control coding and information theory, communication theory, and wireless communications.

Maged Elkashlan (M'06) received the Ph.D. degree in Electrical Engineering from the University of British Columbia, Canada, 2006. From 2007 to 2011, he was with the Wireless and Networking Technologies Laboratory at Commonwealth Scientific and Industrial Research Organization (CSIRO), Australia. During this time, he held an adjunct appointment at University of Technology Sydney, Australia. In 2011, he joined the School of Electronic Engineering and Computer Science at Queen Mary University of London, UK. He also holds visiting faculty appointments at the University of New South Wales, Australia, and Beijing University of Posts and Telecommunications, China. His research interests fall into the broad areas of communication theory, wireless communications, and statistical signal processing for distributed data processing, heterogeneous networks, and Massive MIMO.

Dr. Elkashlan currently serves as Editor of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and IEEE COMMUNICATIONS LETTERS. He also serves as Lead Guest Editor for the special issue on "Green Media: The Future of Wireless Multimedia Networks" of the IEEE WIRELESS COMMUNICATIONS MAGAZINE, Lead Guest Editor for the special issue on "Millimeter Wave Communications for 5G" of the IEEE COMMUNICATIONS MAGAZINE, Guest Editor for the special issue on "Energy Harvesting Communications" of the IEEE COMMUNICATIONS MAGAZINE, and Guest Editor for the special issue on "Location Awareness for Radios and Networks" of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He received the Best Paper Award at the IEEE International Conference on Communications (ICC) in 2014, the International Conference on Communications and Networking in China (CHINACOM) in 2014, and the IEEE Vehicular Technology Conference (VTC-Spring) in 2013. He received the Exemplary Reviewer Certificate of the IEEE Communications Letters in 2012.