Secrecy Capacity of the Primary System in a Cognitive Radio Network

Van-Dinh Nguyen, Tiep M. Hoang, and Oh-Soon Shin, *Member, IEEE*

***Abstract*—With fast growth of wireless services, secrecy has become an increasingly important issue for wireless networks. In this paper, we investigate the secrecy capacity of the primary system in a cognitive radio system based on artificial noise, which has been proposed to deal with the eavesdropper. We first consider a special case of one eavesdropper and two regimes of the eavesdropping channel condition. Specifically, we analyze the impact of interference generated by a secondary system towards the primary system in a cognitive radio system. The channel state information of the primary channel is assumed to be perfectly known at both the primary transmitter and receiver, whereas that for the eavesdropper is partially known. Under these assumptions, we derive analytical expressions for the ergodic secrecy capacity in the cases of strong eavesdropping channel and weak eavesdropping channel, and analyze the impact of the secondary system on the primary ergodic secrecy capacity. Moreover, we extend the analysis to the general case of arbitrary eavesdropping channel condition and arbitrary number of eavesdroppers. Some numerical results will also be presented to verify the analysis.**

***Index Terms*—Artificial noise, channel state information, cognitive radio, interference, secrecy capacity.**

I. Introduction

Cognitive radio is considered as a promising solution to improve spectrum utilization in wireless networks, as the radio spectrum becomes crowded and scarce. In a cognitive radio network, secondary users are allowed to use the frequency bands of the primary user only when these bands are not occupied [1], [2]. Therefore, the secondary user needs to figure out whether a certain frequency band is in use or not using spectrum sensing and/or geo-location database. In practice, however, either spectrum sensing or geo-location database may not always provide correct information on the spectrum occupancy. Once the secondary user comes to use a certain band that the primary user is using, they will cause co-channel interference to each other. Hence, it is of significant importance to deal with the potential interference between the primary and secondary users in cognitive radio networks.

On the other hand, maintaining secrecy of information is critical for wireless networks, as wireless devices become pervasive and personalized. The general purpose of secure communication is to guarantee that the legitimate receivers can obtain the right message, while the others cannot. Traditionally, the secrecy mechanism has been established at the upper layers using a secret key exchange between the source and destination, such as Diffie-Hellman key exchange [3], independently of the physical medium. However, the key exchange algorithm may be vulnerable to eavesdropping attacks in wireless networks, due to the broadcast nature of wireless channel. To solve this problem, information-theoretic security as a physical-layer approach has been widely studied as a means for providing secure wireless communication [4]–[7]. A pioneering work by Wyner has shown that perfect secrecy can be attained when an eavesdropper channel is a degraded version of the main source-to-destination channel [4]. One approach realizing the physical layer security relies on the use of cooperative relays [5], [6], [8]. Another approach that eliminates the reliance on relays is based on the use of beamforming technique combined with the injection of artificial noise [7], [9].

The security issues on the physical layer was introduced in [10] for a cognitive radio network. The secrecy capacity of the secondary system was investigated in [11]–[13], where multiple antennas was exploited to protect the transmit signal from the eavesdropper in cognitive radio networks. In [14], a multiuser scheduling scheme was developed to enhance cognitive transmission security against eavesdropping attacks. A maximum achievable rate at which information can be transmitted secretly from the source to its intended destination is referred to as secrecy capacity [15]. In the context of the secrecy capacity, it plays a crucial role whether the channel state information (CSI) of the eavesdropper is available at the source or not. The CSI of the eavesdropper may be accurately known at the source in the case that the eavesdropper is active [15]. In [16], the secrecy capacity of a cognitive radio network was analyzed under the assumption of perfect CSI for the eavesdropper. In realistic environments, however, it is hard to obtain the CSI of the eavesdropper, since the eavesdropper is generally passive and its location is unknown to the transmitter. For these reasons, some previous studies assumed that only partial knowledge on the eavesdropper channel is available at the transmitter [17]. However, the authors in [17] did not consider a cognitive radio network where interference between the primary and secondary systems is present. They also ignored the noise at the eavesdropper, leading to the conclusion that the capacity at eavesdroppers depends only on the number of eavesdroppers, but it is independent of the signal-to-noise ratio (SNR) at the eavesdropper.

In this paper, we first consider a cognitive radio network when there exists an eavesdropper that can overhear the trans-

The authors are with the School of Electronic Engineering, Soongsil University, Seoul 156-743, Korea (e-mail: nguyenvandinh@ssu.ac.kr; hmt1803@gmail.com; osshin@ssu.ac.kr).

This work was supported by Basic Research Laboratories (BRL) through National Research Foundation (NRF) grant funded by the Korea government (MSIP) (No. 2013056381).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2014.2359246, IEEE Transactions on Vehicular Technology

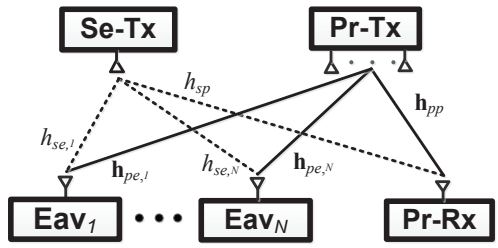

Fig. 1. A cognitive radio network model with N eavesdroppers.

missions from the primary user and from the secondary user. The primary system is assumed to adopt artificial noise and transmit beamforming as a security provisioning mechanism. We derive the secrecy capacity of the primary system in the presence of a secondary system. In particular, we derive exact closed-form expressions for the ergodic secrecy capacity as well as the probability density function (PDF) of the signal-to-interference-plus-noise ratio (SINR), in two extreme cases where the eavesdropping channel is very strong and very weak. Based on the derived capacity formula, the impact of the secondary system on the secrecy capacity of the primary system is analyzed. In particular, we point out that when the eavesdropper is very far from the primary system, the use of artificial noise is not effective to protect the primary system from eavesdropping. Furthermore, we extend the analysis to the general case of arbitrary eavesdropping channel condition and arbitrary number of eavesdroppers. It is found that the use of artificial noise is effective, unless all the eavesdroppers are far from the primary system. We also discuss how the optimal power allocation for the artificial noise is affected by the SNR at the eavesdroppers and interference from the secondary system as well as by the number of eavesdroppers. Some numerical results will be presented to verify the analysis.

The rest of this paper is organized as follows. Section II describes a cognitive radio network model with an eavesdropper. In Section III, the ergodic secrecy capacity of the primary system is derived for the cognitive radio network in two extreme cases where the eavesdropping channel is very strong and very weak, and the impact of the secondary system is analyzed. In Section IV, the analysis is extended to the general case of arbitrary eavesdropping channel condition and arbitrary number of eavesdroppers. In Section V, some numerical results are provided and discussed. Finally, conclusions are drawn in Section VI.

II. System Model

A. Cognitive Radio Network

We consider a cognitive radio network model with a primary system, a secondary system, and N eavesdroppers (Eav's), as illustrated in Fig. 1. In this model, we assume that the primary transmitter (Pr-Tx) is equipped with M antennas, while the secondary transmitter (Se-Tx), primary receiver (Pr-Rx), and each eavesdropper are, respectively, equipped with a single antenna. It should be noted that the case of a single eavesdropper will be considered up to Section III, and the result will be extended to an arbitrary number of eavesdroppers in Section IV. The Se-Tx is assumed to employ an energy detector to sense the spectrum and decide on the status of the spectrum. Let $\mathcal{E}$ denote the test statistic for the energy detector. Then, the probability of false alarm for the energy detector is given as [18]

$$\mathcal{P}_F = \Pr\{\mathcal{E} > \zeta | \mathcal{H}_0\} = \int_{\zeta}^{\infty} p_{\mathcal{E}}(\epsilon|\mathcal{H}_0) d\epsilon, \tag{1}$$

where ζ denotes the decision threshold, $\mathcal{H}_0$ indicates the hypothesis that the primary system is inactive, and $p_{\mathcal{E}}(\epsilon|\mathcal{H}_0)$ denotes the conditional PDF of $\mathcal{E}$ under the hypothesis $\mathcal{H}_0$. Similarly, the probability of detection can be computed as

$$\mathcal{P}_D = \Pr\{\mathcal{E} > \zeta | \mathcal{H}_1\} = \int_{\zeta}^{\infty} p_{\mathcal{E}}(\epsilon|\mathcal{H}_1) d\epsilon, \tag{2}$$

where $\mathcal{H}_1$ indicates the hypothesis that the primary system is active, and $p_{\mathcal{E}}(\epsilon|\mathcal{H}_1)$ denotes the conditional PDF of $\mathcal{E}$ under the hypothesis $\mathcal{H}_1$. Let Θ denote the event that the secondary system is present ($\Theta = 1$) or absent ($\Theta = 0$) in the band, under the condition that the primary system is active (hypothesis $\mathcal{H}_1$). Then, Θ follows the Bernoulli distribution as

$$\Theta = \begin{cases} 0 \text{ with probability } \mathcal{P}_0 = \mathcal{P}_D, \\ 1 \text{ with probability } \mathcal{P}_1 = 1 - \mathcal{P}_0. \end{cases} \tag{3}$$

The received signals at the Pr-Rx and at the Eav can be expressed as

$$y_p = \sqrt{\frac{\gamma_{pp}}{M}} \mathbf{h}_{pp} \mathbf{x}_p + \Theta \sqrt{\gamma_{sp}} h_{sp} x_s + n_p, \tag{4}$$

$$y_e = \sqrt{\frac{\gamma_{pe}}{M}} \mathbf{h}_{pe} \mathbf{x}_p + \Theta \sqrt{\gamma_{se}} h_{se} x_s + n_e, \tag{5}$$

where $\mathbf{x}_p \in \mathbb{C}^{M \times 1}$ and $x_s \in \mathbb{C}$ are the signal transmitted from the Pr-Tx and Se-Tx, respectively, and they satisfy the power constraints $\frac{1}{M}\mathbb{E}\{\mathbf{x}_p^\dagger \mathbf{x}_p\} = 1$ and $\mathbb{E}\{x_s^\dagger x_s\} = 1$. $\mathbf{h}_{pp} \in \mathbb{C}^{1 \times M}$ and $\mathbf{h}_{pe} \in \mathbb{C}^{1 \times M}$ are fading channel gains from the Pr-Tx to the Pr-Rx and from the Pr-Tx to the Eav, respectively, such that $\mathbf{h}_{pp} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_M)$ and $\mathbf{h}_{pe} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_M)$[1]. Similarly, $h_{sp} \in \mathbb{C}$ and $h_{se} \in \mathbb{C}$ are fading channel gains from the Se-Tx to the Pr-Rx and from the Se-Tx to the Eav, respectively, such that $h_{sp} \sim \mathcal{CN}(0,1)$ and $h_{se} \sim \mathcal{CN}(0,1)$. $n_p \sim \mathcal{CN}(0,1)$ and $n_e \sim \mathcal{CN}(0,1)$ are additive white Gaussian noise (AWGN) at the Pr-Rx and at the Eav, respectively. γ_{pp} and γ_{pe} are the average SNR at the Pr-Rx and at the Eav, respectively, for the signal transmitted by the Pr-Tx. Similarly, γ_{sp} and γ_{se} are the average SNR at the Pr-Rx and at the Eav, respectively, for the signal transmitted by the Se-Tx.

B. Artificial Noise

The use of artificial noise for secure communication has been proposed by Goel [7]. We assume that the Pr-Tx exploits artificial noise in combination with beamforming. The transmitter composes $\mathbf{x}_p$ as a weighted sum of information bearing

[1] $\mathcal{CN}(\mathbf{0}, \mathbf{\Sigma})$ denotes complex Gaussian distribution with zero mean and covariance matrix $\mathbf{\Sigma}$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2014.2359246, IEEE Transactions on Vehicular Technology

signal $s_p \in \mathbb{C}$ and an artificial noise signal $\mathbf{w}_p \in \mathbb{C}^{(M-1)\times 1}$. Note that the power of s_p and $\mathbf{w}_p$ are normalized such that $\mathbb{E}\{|s_p|^2\} = 1$ and $\mathbf{w}_p \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{M-1})$. Accordingly, $\mathbf{x}_p$ can be expressed as

$$\mathbf{x}_p = \sqrt{\phi}\mathbf{u}_p s_p + \sqrt{\frac{1-\phi}{M-1}}\mathbf{W}_p\mathbf{w}_p, \tag{6}$$

where ϕ denotes the ratio of the power of information bearing signal to the total power P : $P = \sigma_s^2 + (M-1)\sigma_w^2$, where $\sigma_s^2 = \phi P$ and $\sigma_w^2 = (1-\phi)P/(M-1)$ with σ_s^2 and σ_w^2 denoting the signal power and the variance of each component of the artificial noise, respectively. The beamforming vector $\mathbf{u}_p$ in (6) is designed to maximize the power of the information bearing signal at the intended destination, such that $\mathbf{u}_p = \mathbf{h}_{pp}^\dagger / \|\mathbf{h}_{pp}\|$, while the nulling matrix $\mathbf{W}_p \in \mathbb{C}^{M\times(M-1)}$ is chosen such that $\mathbf{h}_{pp}$ lies in the left-hand null space of $\mathbf{W}_p$, i.e., $\mathbf{h}_{pp}\mathbf{W}_p = \mathbf{0}$.

With $\mathbf{x}_p$ defined in (6), the received signals in (4) and (5) can be rewritten as

$$y_p = \sqrt{\frac{\phi\gamma_{pp}}{M}}\|\mathbf{h}_{pp}\| s_p + \Theta\sqrt{\gamma_{sp}}h_{sp}x_s + n_p \tag{7}$$

$$y_e = \sqrt{\frac{\phi\gamma_{pe}}{M}}\psi_I s_p + \sqrt{\frac{1-\phi}{M-1}\frac{\gamma_{pe}}{M}}\boldsymbol{\psi}_A\mathbf{w}_p + \Theta\sqrt{\gamma_{se}}h_{se}x_s + n_e \tag{8}$$

where $\psi_I \triangleq \mathbf{h}_{pe}\mathbf{u}_p \in \mathbb{C}$ is associated with the information bearing signal, and $\boldsymbol{\psi}_A \triangleq \mathbf{h}_{pe}\mathbf{W}_p \in \mathbb{C}^{1\times(M-1)}$ is associated with the artificial noise. From (7), we can see that x_s, which is transmitted when spectrum sensing fails at the Se-Tx, causes interference to the primary system. From (8), we can also observe that Eav can attempt to decode s_p, subject to the artificial noise and interference from the secondary system. Thus, the primary, secondary, and eavesdropper systems are all coupled to one another. Correspondingly, it is not apparent whether the use of artificial noise always benefits the primary system in the presence of secondary system and eavesdropper.

III. Ergodic Secrecy Capacity of the Primary System

In this section, we derive the secrecy capacity of the primary system described in Section II. In the derivation, we assume that the Pr-Rx has perfect knowledge on the CSI for $\mathbf{h}_{pp}$ and h_{sp}, while the Eav knows only the statistics of the channels $\mathbf{h}_{pe}$ and h_{se}. We will consider two extreme cases, weak eavesdropping channel and strong eavesdropping channel, according to the channel condition between the Pr-Tx and Eav, represented by γ_{pe}. The secrecy capacity will be provided in Theorems 1 and 2 for the two cases.

The secrecy capacity of primary system, denoted as C_s, is defined as [19]

$$C_s = \max\{C_p - C_e, 0\} = (C_p - C_e)^+, \tag{9}$$

where C_p is the ergodic capacity of the primary system, and C_e is the ergodic capacity of the eavesdropping channel, i.e., the channel between Pr-Tx and Eav. From (7), the ergodic capacity of primary system with perfect CSI is given as

$$C_p = \mathbb{E}_\Theta\{\log_2[1 + \mathrm{SINR}_p]\}, \tag{10}$$

where SINR_p is the SINR at the Pr-Rx for decoding s_p, given as

$$\mathrm{SINR}_p = \frac{\left(\phi\frac{\gamma_{pp}}{M}\right)\|\mathbf{h}_{pp}\|^2}{1 + \gamma_{sp}\Theta\,|h_{sp}|^2}. \tag{11}$$

By substituting (11) into (10) and using (3), we obtain the ergodic capacity as

$$\begin{aligned} C_p = {} & \mathcal{P}_0 \log_2\left(1 + \phi\frac{\gamma_{pp}}{M}\|\mathbf{h}_{pp}\|^2\right) \\ & + \mathcal{P}_1 \log_2\left(1 + \frac{\left(\phi\frac{\gamma_{pp}}{M}\right)\|\mathbf{h}_{pp}\|^2}{1 + \gamma_{sp}\,|h_{sp}|^2}\right). \end{aligned} \tag{12}$$

Remark 1: From (12), we can see that γ_{sp} represents the effect of the interference from the Se-Tx to the Pr-Rx, and C_s decreases as γ_{sp} increases. Specifically, we have

$$\begin{aligned} \lim_{\gamma_{sp}\to 0} C_p &= \mathcal{P}_0 C_{p|\Theta=0} + \mathcal{P}_1 C_{p|\Theta=0} = C_{p|\Theta=0}, \\ \lim_{\gamma_{sp}\to \infty} C_p &= \mathcal{P}_0 C_{p|\Theta=0} + \mathcal{P}_0 \cdot 0 = \mathcal{P}_0 C_{p|\Theta=0}. \end{aligned} \tag{13}$$

□

Remark 1 shows that if γ_{sp} increases from 0 to ∞, C_s decreases by at most the quantity $\max\Delta C_s = \max\Delta C_p = \mathcal{P}_1 C_{p|\Theta=0}$. Moreover, it is known that $C_{p|\Theta=0} = \frac{1}{\ln 2}\exp\left(\frac{M}{\phi\gamma_{pp}}\right)\sum_{m=1}^{M} E_m\left(\frac{M}{\phi\gamma_{pp}}\right)$ [17], where $E_m(\cdot)$ denotes the generalized exponential integral. This indicates that $\max\Delta C_s$ increases with M, ϕ, and γ_{pp}. The influence of ϕ on ΔC_s will be discussed in Section V.

On the other hand, from (8), the ergodic capacity of the primary-Eav channel with knowledge on the statistics of the eavesdropping channel is given by

$$\begin{aligned} C_e &= \mathbb{E}_{\Theta,h_{se},\psi_I,\boldsymbol{\psi}_A}\{\log_2[1 + \mathrm{SINR}_e]\} \\ &= \mathcal{P}_0\mathbb{E}_{h_{se},\psi_I,\boldsymbol{\psi}_A}\{\log_2[1 + \mathrm{SINR}_{e|\Theta=0}]\} \\ &\quad + \mathcal{P}_1\mathbb{E}_{h_{se},\psi_I,\boldsymbol{\psi}_A}\{\log_2[1 + \mathrm{SINR}_{e|\Theta=1}]\}, \end{aligned} \tag{14}$$

where SINR_e is the SINR at the Eav for decoding s_p, given as

$$\mathrm{SINR}_e = \frac{\left(\phi\frac{\gamma_{pe}}{M}\right)|\psi_I|^2}{1 + \gamma_{se}\Theta\,|h_{se}|^2 + \frac{1-\phi}{M-1}\frac{\gamma_{pe}}{M}\|\boldsymbol{\psi}_A\|^2}. \tag{15}$$

A. Case of Weak Eavesdropping Channel ($\gamma_{pe} \ll 1$)

Theorem 1: In the case that the Pr-Tx is very far from the Eav ($\gamma_{pe} \ll 1$), the ergodic secrecy capacity of the primary system with perfect instantaneous CSI of the legitimate channel is given as

$$\begin{aligned} C_s = {} & \left(\mathcal{P}_0 \log_2\left(1 + \phi\frac{\gamma_{pp}}{M}\|\mathbf{h}_{pp}\|^2\right)\right. \\ & + \mathcal{P}_1 \log_2\left(1 + \frac{\left(\phi\frac{\gamma_{pp}}{M}\right)\|\mathbf{h}_{pp}\|^2}{1 + \gamma_{sp}\,|h_{sp}|^2}\right) - \frac{\mathcal{P}_0}{\ln 2}e^{\frac{M}{\phi\gamma_{pe}}}E_1\left(\frac{M}{\phi\gamma_{pe}}\right) \\ & \left. - \frac{\mathcal{P}_1}{\ln 2}\frac{1}{1-\alpha}\left\{e^{\frac{M}{\phi\gamma_{pe}}}E_1\left(\frac{M}{\phi\gamma_{pe}}\right) - e^{\frac{1}{\gamma_{se}}}E_1\left(\frac{1}{\gamma_{se}}\right)\right\}\right)^+, \end{aligned} \tag{16}$$

where $\alpha \triangleq \frac{M\gamma_{se}}{\phi\gamma_{pe}}$ and $E_1(u) \triangleq \int_1^\infty e^{-ut}t^{-1}dt$. □

Proof: After dividing both the numerator and denominator of (15) by γ_{pe}, let γ_{pe} go to 0. Then, we can easily

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2014.2359246, IEEE Transactions on Vehicular Technology

see that the third term in the denominator can be neglected, since $\|\boldsymbol{\psi}_A\|^2$ associated with the artificial noise will be finite. Therefore, when $\gamma_{pe} \ll 1$, SINR_e in (15) is approximated as

$$\mathrm{SINR}_e \approx \mathcal{X} = \frac{\left(\phi\frac{\gamma_{pe}}{M}\right)|\psi_I|^2}{1+\gamma_{se}\Theta\,|h_{se}|^2}. \tag{17}$$

The PDF of $\mathcal{X}$ can be found as $f_{\mathcal{X}}(x) = \mathcal{P}_0 f_{\mathcal{X}}(x|\Theta=0) + \mathcal{P}_1 f_{\mathcal{X}}(x|\Theta=1)$, where

$$\begin{aligned} f_{\mathcal{X}}(x|\Theta=0) &= \frac{M}{\phi\gamma_{pe}} e^{-\frac{M}{\phi\gamma_{pe}}x}, \\ f_{\mathcal{X}}(x|\Theta=1) &= \frac{M}{\phi\gamma_{pe}} e^{-\frac{M}{\phi\gamma_{pe}}x}\left\{\left(1+\frac{M\gamma_{se}}{\phi\gamma_{pe}}x\right)^{-1}\right. \\ &\quad \left. + \gamma_{se}\left(1+\frac{M\gamma_{se}}{\phi\gamma_{pe}}x\right)^{-2}\right\}. \end{aligned} \tag{18}$$

See Appendix A for more details. Using (18), C_e in (14) can be approximated as

$$\begin{aligned} C_e &= \mathcal{P}_0 C_{e|\Theta=0} + \mathcal{P}_1 C_{e|\Theta=1} \\ &= \frac{\mathcal{P}_0}{\ln 2} e^{\frac{M}{\phi\gamma_{pe}}} E_1\left(\frac{M}{\phi\gamma_{pe}}\right) \\ &\quad + \frac{\mathcal{P}_1}{\ln 2}\frac{1}{1-\alpha}\left\{e^{\frac{M}{\phi\gamma_{pe}}} E_1\left(\frac{M}{\phi\gamma_{pe}}\right) - e^{\frac{1}{\gamma_{se}}} E_1\left(\frac{1}{\gamma_{se}}\right)\right\}, \end{aligned} \tag{19}$$

where

$$\begin{aligned} C_{e|\Theta=0} &= \int_0^\infty \log_2(1+x) f_{\mathcal{X}}(x|\Theta=0)dx \\ &= \frac{1}{\ln 2} e^{\frac{M}{\phi\gamma_{pe}}} E_1\left(\frac{M}{\phi\gamma_{pe}}\right), \\ C_{e|\Theta=1} &= \int_0^\infty \log_2(1+x) f_{\mathcal{X}}(x|\Theta=1)dx \\ &= \frac{1}{\ln 2}\frac{1}{1-\alpha}\left\{e^{\frac{M}{\phi\gamma_{pe}}} E_1\left(\frac{M}{\phi\gamma_{pe}}\right) - e^{\frac{1}{\gamma_{se}}} E_1\left(\frac{1}{\gamma_{se}}\right)\right\}. \end{aligned} \tag{20}$$

See Appendix B for more details. From (12) and (19), the ergodic secrecy capacity in (9) is computed as (16). ■

Corollary 1: From (19) and (20), we get

$$\begin{aligned} \lim_{\gamma_{se}\to 0} C_e &= \mathcal{P}_0 C_{e|\Theta=0} + \mathcal{P}_1 C_{e|\Theta=0} = C_{e|\Theta=0}, \\ \lim_{\gamma_{se}\to \infty} C_e &= \mathcal{P}_0 C_{e|\Theta=0} + \mathcal{P}_0 \cdot 0 = \mathcal{P}_0 C_{e|\Theta=0}. \end{aligned} \tag{21}$$

□

According to Corollary 1, if γ_{se} changes from 0 to ∞, the C_s can improve by at most the quantity $\max\Delta C_s = \max\Delta C_e = \mathcal{P}_1 C_{e|\Theta=0}$. Moreover, from (20) we can see that $C_{e|\Theta=0} \ll \frac{1}{\ln 2} e^2 E_1(2) \approx 0.521$, since $e^z E_1(z)$ decreases with $z \triangleq M/(\phi\gamma_{pe}) \gg M/\phi \geq 2$. Therefore, the quantity $\max\Delta C_s \ll 0.521\mathcal{P}_1$ is not significant.

Corollary 2: Observing (19) and (20), we see that $C_{e|\Theta=0}$ and $C_{e|\Theta=1}$ increase with ϕ, as $e^{\frac{M}{\phi\gamma_{pe}}} E_1\left(\frac{M}{\phi\gamma_{pe}}\right)$ increases with ϕ. □

The Corollary 2 implies that in low γ_{pe} regime, employing artificial noise is not effective to protect the primary user from eavesdropping. However, this will not be the case when there are many eavesdroppers, as discussed in [16], or when there are amplifying relays between the primary user and eavesdropper, as discussed in [7].

B. Case of Strong Eavesdropping Channel ($\gamma_{pe} \gg 1$)

Theorem 2: Assuming that the Pr-Tx is very close to the Eav ($\gamma_{pe} \gg 1$), the ergodic secrecy capacity of the primary system with perfect instantaneous CSI of the legitimate channel is given as

$$\begin{aligned} C_s = \left(\mathcal{P}_0 \log_2\left(1+\phi\frac{\gamma_{pp}}{M}\|\mathbf{h}_{pp}\|^2\right) + \mathcal{P}_1 \log_2\left(1+\frac{\phi\frac{\gamma_{pp}}{M}\|\mathbf{h}_{pp}\|^2}{1+\gamma_{sp}|h_{sp}|^2}\right)\right. \\ \left. - \frac{\mathcal{P}_0}{\ln 2}\frac{1-\phi}{\phi}\mathcal{I}_M(\eta) - \frac{\mathcal{P}_1}{\ln 2}\left\{\frac{A\ln\alpha}{\alpha(\alpha-1)} + \sum_{k=2}^{M} B_k \mathcal{I}_k(\eta)\right\}\right)^+, \end{aligned} \tag{22}$$

where

$$\begin{aligned} \eta &\triangleq \frac{1}{M-1}\frac{1-\phi}{\phi}, \\ A &\triangleq (\alpha-\eta)\left(1-\frac{\eta}{\alpha}\right)^{-M}, \\ B_k &\triangleq (1-k)(\alpha-\eta)\left(1-\frac{\alpha}{\eta}\right)^{-2}\left(1-\frac{\eta}{\alpha}\right)^{k-M}, \\ \mathcal{I}_k(\eta) &\triangleq \begin{cases} \frac{1}{(k-1)^2}, & \text{if } \eta = 1, \\ \frac{(1-\eta)^{1-k}}{(k-1)\eta}\left[-\ln\eta + \sum_{i=1}^{k-2}\frac{(k-2)!(-\eta)^i}{(k-i-2)!i!i}(\eta^{-i}-1)\right], & \\ \quad \text{otherwise.} \end{cases} \end{aligned} \tag{23}$$

□

Proof: After dividing both the numerator and denominator of (15) by γ_{pe}, let γ_{pe} go to ∞. Then, we can easily see that the first term in the denominator can be neglected. Therefore, when $\gamma_{pe} \gg 1$, the SINR_e in (15) can be approximated as

$$\mathrm{SINR}_e \approx \mathcal{Y} = \frac{\phi\frac{\gamma_{pe}}{M}|\psi_I|^2}{\gamma_{se}\Theta\,|h_{se}|^2 + \frac{1-\phi}{M-1}\frac{\gamma_{pe}}{M}\|\boldsymbol{\psi}_A\|^2}. \tag{24}$$

The PDF of $\mathcal{Y}$ can be expressed as $f_{\mathcal{Y}}(y) = \mathcal{P}_0 f_{\mathcal{Y}}(y|\Theta=0) + \mathcal{P}_1 f_{\mathcal{Y}}(y|\Theta=1)$, where

$$\begin{aligned} f_{\mathcal{Y}}(y|\Theta=0) &= \frac{1-\phi}{\phi\left(1+\frac{1-\phi}{\phi(M-1)}y\right)^M}, \\ f_{\mathcal{Y}}(y|\Theta=1) &= \frac{\alpha+(M-1)\eta+M\alpha\eta y}{(1+\alpha y)^2(1+\eta y)^M}. \end{aligned} \tag{25}$$

See Appendix A for more details. Using (25), C_e in (14) can be expressed as

$$\begin{aligned} C_e &= \mathcal{P}_0 C_{e|\Theta=0} + \mathcal{P}_1 C_{e|\Theta=1} \\ &= \frac{\mathcal{P}_0}{\ln 2}\frac{1-\phi}{\phi}\mathcal{I}_M(\eta) + \frac{\mathcal{P}_1}{\ln 2}\left(\frac{A\ln\alpha}{\alpha(\alpha-1)} + \sum_{k=2}^{M} B_k\mathcal{I}_k(\eta)\right), \end{aligned} \tag{26}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2014.2359246, IEEE Transactions on Vehicular Technology

where

$$\begin{aligned} C_{e|\Theta=0} &= \int_0^\infty \log_2(1+y) f_{\mathcal{Y}}(y|\Theta=0)dy \\ &= \frac{1}{\ln 2}\frac{1-\phi}{\phi}\mathcal{I}_M(\eta), \\ C_{e|\Theta=1} &= \int_0^\infty \log_2(1+y) f_{\mathcal{Y}}(y|\Theta=1)dy \\ &= \frac{1}{\ln 2}\left(\frac{A\ln\alpha}{\alpha(\alpha-1)} + \sum_{k=2}^{M} B_k \mathcal{I}_k(\eta)\right). \end{aligned} \tag{27}$$

See Appendix B for more details. By substituting (12) and (26) into (9), we arrive at the desired result (22). ■

Corollary 3: For $\gamma_{se} \ll \gamma_{pe}$, the term associated to γ_{se} in the denominator of (15) can be eliminated, which is equivalent to setting $\Theta = 0$. □

It should be noted that the disappearance of Θ in (15) does not mean that the secondary system disappears. The setting $\Theta = 0$ results in $\mathrm{SINR}_{e|\Theta=0} = \mathrm{SINR}_{e|\Theta=1}$ if $\gamma_{se} \ll \gamma_{pe}$. Consequently, C_e in (14) also becomes equal to $C_{e|\Theta=0}$: $\lim_{\frac{\gamma_{se}}{\gamma_{pe}}\to 0}\mathrm{SINR}_e = \mathrm{SINR}_{e|\Theta=0} \Rightarrow \lim_{\frac{\gamma_{se}}{\gamma_{pe}}\to 0} C_e = C_{e|\Theta=0}$ and $C_s \to \left(C_p - C_{e|\Theta=0}\right)^+$.

IV. Multiple Eavesdroppers

In Section III, the ergodic secrecy capacity of the primary system has been derived for two extreme cases of the SNR for the eavesdropping channel condition: $\gamma_{pe} \ll 1$ and $\gamma_{pe} \gg 1$, and only one eavesdropper is assumed to exist. In this section, we extend the result to the general case of arbitrary eavesdropping channel condition and arbitrary number of eavesdroppers. Let N ($N \geq 1$) denote the number of eavesdroppers, and $\gamma_{pe,n}$ and $\mathrm{SINR}_{e,n} \triangleq \mathcal{Z}_n$, respectively, denote the average SNR and instantaneous SINR at the n-th Eav for the signal transmitted by the Pr-Tx. For simplicity but without loss of generality, we assume that all the Eav's have the same SNR for the signal transmitted by the Se-Tx: $\gamma_{se,1} = \gamma_{se,2} = \cdots = \gamma_{se,N} = \gamma_{se}$.

The ergodic capacity of the compound wiretap channel, C_e, is defined as [8], [20]

$$C_e \triangleq \max_n C_{e,n} = \mathbb{E}_{\Theta,h_{se},\psi_I,\boldsymbol{\psi}_A}\{\log_2[1+\max_n \mathcal{Z}_n]\}. \tag{28}$$

Let $\mathcal{Z} \triangleq \max_n \mathcal{Z}_n$. Assuming that N eavesdropping channels are independent, the cumulative distribution function (CDF) of $\mathcal{Z}$ can be written as

$$F_{\mathcal{Z}}(z) = \Pr(\mathcal{Z} < z) = \prod_{n=1}^{N} F_{\mathcal{Z}_n}(z), \tag{29}$$

where $F_{\mathcal{Z}_n}(z)$ denotes the CDF of $\mathcal{Z}_n$.

Theorem 3: When there exist N eavesdroppers, the ergodic secrecy capacity of the primary system with perfect instantaneous CSI of the legitimate channel is given as

$$\begin{aligned} C_s = \Bigg(&\mathcal{P}_0 \log_2\left(1+\phi\frac{\gamma_{pp}}{M}\left\|\mathbf{h}_{pp}\right\|^2\right) \\ &+ \mathcal{P}_1 \log_2\left(1+\frac{\phi\frac{\gamma_{pp}}{M}\left\|\mathbf{h}_{pp}\right\|^2}{1+\gamma_{sp}\left|h_{sp}\right|^2}\right) \\ &- \frac{\mathcal{P}_0}{\ln 2}\mathcal{K}\mathcal{J}_0 - \frac{\mathcal{P}_1}{\ln 2}\mathcal{K}\{\mathcal{J}_1+\mathcal{J}_2\}\Bigg)^+, \end{aligned} \tag{30}$$

where

$$\begin{aligned} \mathcal{K} &= \sum_{j=1}^{N}(-1)^{j-1}\sum_{\substack{n_1=\cdots=n_j=1 \\ n_1<\cdots<n_j}}^{N}, \\ \mathcal{J}_0 &= \sum_{k=0}^{\infty}(-1)^k\frac{\mu_j^k}{k!}\frac{1}{\eta^k\Gamma\left((M-1)j\right)} \\ &\quad\times\left(\mu_j G_{3,3}^{2,3}\left(\frac{1}{\eta}\middle|{}^{-k,1,1}_{(M-1)j-k-1,1,0}\right)\right. \\ &\quad\left.+\eta G_{3,3}^{2,3}\left(\frac{1}{\eta}\middle|{}^{-k,1,1}_{(M-1)j-k,1,0}\right)\right), \\ \mathcal{J}_1 &= \sum_{k=0}^{\infty}\sum_{p_1=1}^{L_1}\sum_{q_1=1}^{r_{p_1}}(-1)^k\mathcal{A}_{1,p_1,q_1}\frac{\mu_j^k}{k!}\frac{\theta_{p_1}^{k-q_1}}{\Gamma(q_1)} \\ &\quad\times\left(\mu_j\theta_{p_1}G_{3,3}^{2,3}\left(\theta_{p_1}\middle|{}^{-k,1,1}_{q_1-k-1,1,0}\right)+G_{3,3}^{2,3}\left(\theta_{p_1}\middle|{}^{-k,1,1}_{q_1-k,1,0}\right)\right), \\ \mathcal{J}_2 &= \sum_{k=0}^{\infty}\widetilde{\sum}\sum_{p_2=1}^{L_2}\sum_{q_2=1}^{r_{p_2}}(-1)^k\mathcal{A}_{2,p_2,q_2}\frac{\mu_j^k}{k!}\frac{\theta_{p_2}^{k-q_2}}{\Gamma(q_2)} \\ &\quad\times\left(\mu_j\theta_{p_2}G_{3,3}^{2,3}\left(\theta_{p_2}\middle|{}^{-k,1,1}_{q_2-k-1,1,0}\right)+G_{3,3}^{2,3}\left(\theta_{p_2}\middle|{}^{-k,1,1}_{q_2-k,1,0}\right)\right), \\ \mu_j &\triangleq \frac{M}{\phi\bar{\gamma}_{pe,j}}, \quad \bar{\gamma}_{pe,j} \triangleq \left(\sum_{t=1}^{j}\frac{1}{\gamma_{pe,n_t}}\right)^{-1}, \\ \widetilde{\sum} &= \sum_{t=1}^{j}\sum_{k_1=2}^{M}\sum_{k_2=2}^{M}\cdots\sum_{k_j=2}^{M}. \end{aligned} \tag{31}$$

Note that $\mathcal{A}_{1,p_1,q_1}$ and $\mathcal{A}_{2,p_2,q_2}$ in (31) are defined in Appendix A, and that $G_{p,q}^{m,n}\left(x\middle|{}^{a_1,\cdots,a_p}_{b_1,\cdots,b_q}\right)$ and $\Gamma(x)$ denote the Meijer G-function [21, Eq. (9.301)] and gamma function [21, Eq. (8.310)], respectively. □

Proof: In the general case, the SINR of the n-th Eav in (15) is given as

$$\mathcal{Z}_n = \frac{\left(\phi\frac{\gamma_{pe,n}}{M}\right)\left|\psi_I\right|^2}{1+\gamma_{se}\Theta\left|h_{se}\right|^2+\frac{1-\phi}{M-1}\frac{\gamma_{pe,n}}{M}\left\|\boldsymbol{\psi}_A\right\|^2}. \tag{32}$$

The conditional CDF of $\mathcal{Z}_n$ can be found as

$$\begin{aligned} F_{\mathcal{Z}_n}(z|\Theta=0) &= 1-e^{-\frac{M}{\phi\gamma_{pe,n}}z}(\eta z+1)^{-M+1}, \\ F_{\mathcal{Z}_n}(z|\Theta=1) &= 1-e^{-\frac{M}{\phi\gamma_{pe,n}}z}\left[\frac{A_n}{\alpha_n(\alpha_n z+1)}\right. \\ &\quad\left.+\sum_{k=2}^{M}\frac{B_{k,n}}{\eta(\eta z+1)^{k-1}}\right]. \end{aligned} \tag{33}$$

Note that if we approximate (33) under the assumption of $\gamma_{pe} \ll 1$ and $\gamma_{pe} \gg 1$ and differentiate the equations with respect to z, we can get (18) and (25). Using (29), the PDF of $\mathcal{Z}$ can be computed from $f_{\mathcal{Z}}(z) = \mathcal{P}_0 f_{\mathcal{Z}}(z|\Theta=0) + \mathcal{P}_1 f_{\mathcal{Z}}(z|\Theta=1)$, where

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2014.2359246, IEEE Transactions on Vehicular Technology

$$
\begin{aligned}
&f_{\mathcal{Z}}(z|\Theta=0)\\
&=\mathcal{K}e^{-\mu_j z}\left(\eta z+1\right)^{-(M-1)j-1}\left[\mu_j(\eta z+1)+(M-1)j\eta\right],\\
&f_{\mathcal{Z}}(z|\Theta=1)\\
&=\mathcal{K}e^{-\mu_j z}\left(\sum_{p_1=1}^{L_1}\sum_{q_1=1}^{r_{p_1}}\frac{\mathcal{A}_{1,p_1,q_1}}{(z+\theta_{p_1})^{q_1}}\left(\mu_j+\frac{q_1}{(z+\theta_{p_1})}\right)\right.\\
&\quad\left.+\widetilde{\sum}\sum_{p_2=1}^{L_2}\sum_{q_2=1}^{r_{p_2}}\frac{\mathcal{A}_{2,p_2,q_2}}{(z+\theta_{p_2})^{q_2}}\left(\mu_j+\frac{q_2}{(z+\theta_{p_2})}\right)\right).
\end{aligned}
\tag{34}
$$

See Appendix A for more details on the derivation of the conditional PDF's in (34). Using (34), C_e in (14) can be expressed as

$$
\begin{aligned}
C_e&=\mathcal{P}_0C_{e|\Theta=0}+\mathcal{P}_1C_{e|\Theta=1}\\
&=\frac{\mathcal{P}_0}{\ln 2}\mathcal{K}\mathcal{J}_0+\frac{\mathcal{P}_1}{\ln 2}\mathcal{K}\left(\mathcal{J}_1+\mathcal{J}_2\right),
\end{aligned}
\tag{35}
$$

where

$$
\begin{aligned}
C_{e|\Theta=0}&=\int_0^\infty\log_2(1+z)f_{\mathcal{Z}}(z|\Theta=0)dz=\frac{1}{\ln 2}\mathcal{K}\mathcal{J}_0,\\
C_{e|\Theta=1}&=\int_0^\infty\log_2(1+z)f_{\mathcal{Z}}(z|\Theta=1)dz\\
&=\frac{1}{\ln 2}\mathcal{K}\left(\mathcal{J}_1+\mathcal{J}_2\right).
\end{aligned}
\tag{36}
$$

See Appendix B for more details. By substituting (12) and (35) into (9), we obtain (30). ■

The resulting equation (30) looks very complicated. However, it should be pointed out that the gamma function and Meijer G-function in Theorem 3 are built-in functions that can easily be computed by standard software packages, such as Matlab and Mathematica. From (28), it is apparent that the secrecy capacity will be most influenced by the eavesdropper who can overhear the primary transmission in the best condition. This implies that the use of artificial noise can increase the secrecy capacity, once at least one eavesdropper is close to the primary transmitter, and the optimal power allocation ratio will be determined by the channel condition of the eavesdropper. On the contrary, in the case that all the eavesdroppers are far from the primary system, the use of artificial noise is not effective any more, as discussed in Corollary 2. These can easily be verified using the generalized formula (30).

V. Numerical Results

In this section, we present numerical results to verify the analysis given in Sections III and IV, and discuss the results in some specific scenarios of cognitive radio networks. In all the following figures, we set the number of antennas at the Pr-Tx to M = 3, unless otherwise specified. The average SNR γ_{pp} is set to 20dB, and the average SNR γ_{sp} is set to 15dB except for Fig. 5.

Fig. 2 shows the ergodic secrecy capacity in (16) versus the ratio of the power ϕ for several values of $\mathcal{P}_1$, in the case that the Pr-Tx is very far from the Eav. We see that the ergodic secrecy capacity does not change as γ_{se} changes from -40dB to 40dB, which supports the claim made in Corollary 1. It is also seen that the secrecy capacity is the largest when $\phi=1$, which corresponds to the case where artificial noise is not injected. This implies that the use of artificial noise is not effective when the Pr-Tx is very far from the Eav.

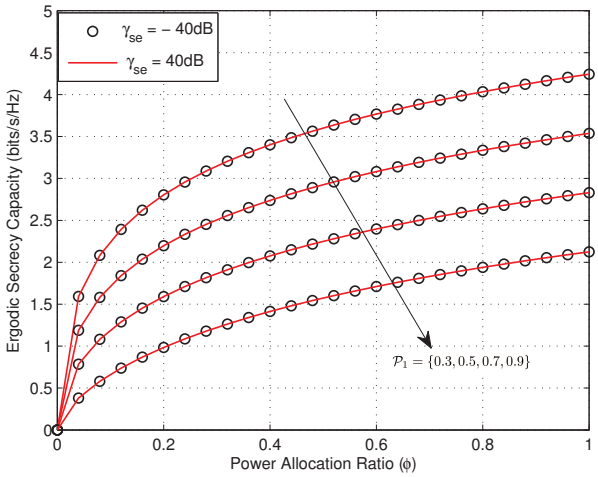

Fig. 2. Ergodic secrecy capacity vs ϕ, when $\gamma_{pe}=-30$dB and $\mathcal{P}_1\in\{0.3,0.5,0.7,0.9\}$.

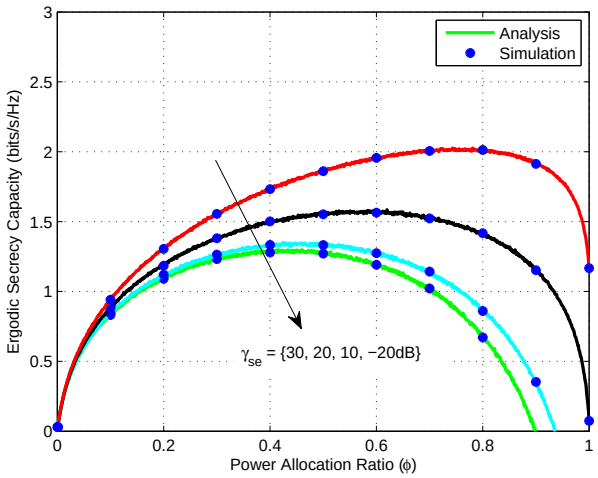

Fig. 3. Ergodic secrecy capacity vs. ϕ, when $\gamma_{pe}=30$dB and $\mathcal{P}_1=0.8$.

Fig. 3 shows the ergodic secrecy capacity in (22) versus the ratio of the power ϕ, in the case that the Pr-Tx is very close to the Eav. The value of γ_{pe} is set to 30dB as in [8]. The results show that in high γ_{pe} regime, the secrecy capacity changes significantly with γ_{se}. We can also find the optimal value of the power allocation ratio ϕ that maximizes the secrecy capacity. For instance, the optimal value of the power allocation ratio ϕ are 0.42, 0.45, 0.6, and 0.8 for $\gamma_{se}=-20$dB, 10dB, 20dB, and 30dB, respectively. Fig. 4 shows the ergodic secrecy capacity in (22) versus γ_{pp} for several values of M, when the optimal value of ϕ is adopted. The optimal value of ϕ has been found through numerical search. We observe that the ergodic secrecy

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2014.2359246, IEEE Transactions on Vehicular Technology

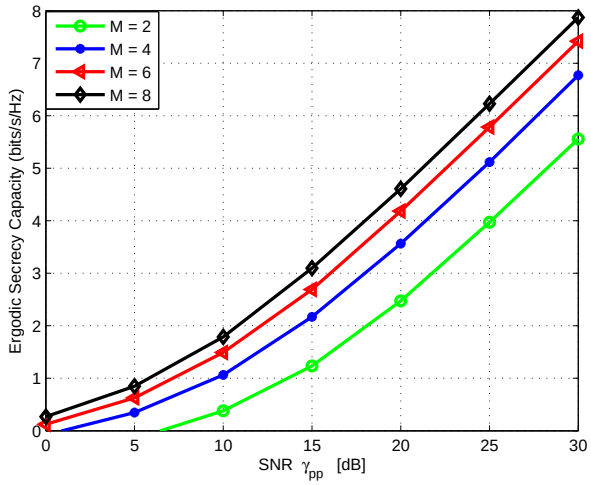

Fig. 4. Ergodic secrecy capacity vs. γ_{pp} for optimal ϕ, when $\gamma_{pe} = 30$dB and $\mathcal{P}_1 = 0.8$.

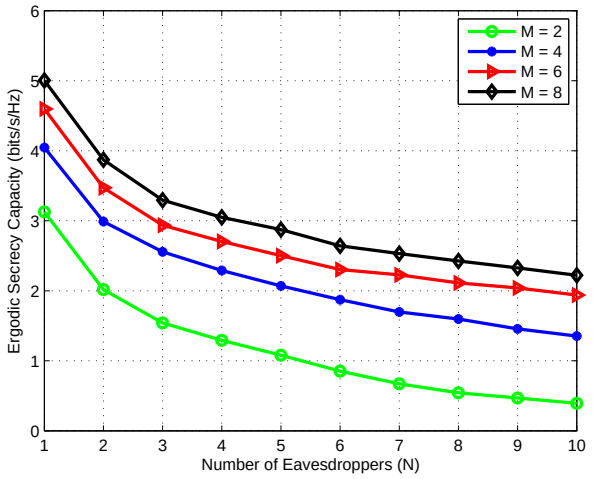

Fig. 6. Ergodic secrecy capacity vs. the number of eavesdroppers, when $\gamma_{pe,n} = 20$dB for all n, $\gamma_{sp} = 15$dB, $\phi = 0.5$, and $\mathcal{P}_1 = 0.8$.

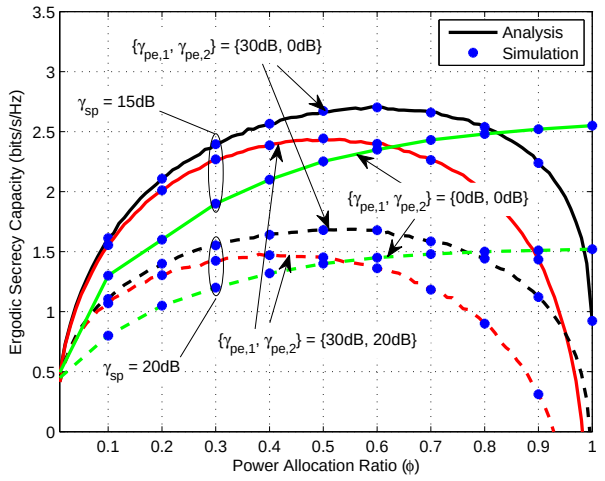

Fig. 5. Ergodic secrecy capacity vs. ϕ, when $\mathcal{P}_1 = 0.8$ and $\{\gamma_{pe,1}, \gamma_{pe,2}\} = \{30\text{dB}, 20\text{dB}\}$, $\{30\text{dB},\ 0\text{dB}\}, \{0\text{dB}, 0\text{dB}\}$.

capacity decreases as M increases.

We next illustrate how different channel conditions of multiple eavesdroppers affect the ergodic secrecy capacity of the primary system. In Fig. 5, two eavesdroppers are assumed to be in three different channel conditions for the primary signal. The channel conditions are represented by a pair of the average SNR values $\{\gamma_{pe,1}, \gamma_{pe,2}\}$, which is set to $\{30\text{dB}, 30\text{dB}\}$, $\{30\text{dB}, 20\text{dB}\}$, and $\{0\text{dB}, 0\text{dB}\}$. First of all, the simulation results and analytical results show exact agreement, which verifies the accuracy of our analysis. From the figure, we can observe that the use of artificial noise is effective for the first and second cases. Comparing the first and second cases, the first case attains lower secrecy capacity and lower value of optimal ϕ than the second case, since the first case will have higher chance of overhearing information. Note that lower ϕ corresponds to allocating more power to the artificial noise. In the third case, the secrecy capacity is largest when $\phi = 1$, which implies that the artificial noise is useless in this case. In addition, we also illustrate the effect of the secondary system on the primary system in Fig. 5. As discussed in Remark 1, the results show that the secrecy capacity is reduced by approximately 1 bps/Hz, when γ_{sp} increases from 15dB to 20dB, and the gap increases as ϕ grows up.

Fig. 6 shows the ergodic secrecy capacity of the primary system versus the number of eavesdroppers, N, for several different values of M. We assume that all the eavesdroppers have the same SNR: $\gamma_{pe,n} = 20\text{dB}, n = 1, 2, \cdots, N$. The secrecy capacity is found to decrease with N, since the chance of wiretapping will increase for larger number of eavesdroppers. Similarly to the result in Fig. 4, the secrecy capacity is shown to increase as the number of antennas, M, increases.

VI. Conclusion

In this paper, we have analyzed the ergodic secrecy capacity of the primary system in a cognitive radio network. As a security provisioning method, we have considered the combined use of beamforming technique and artificial noise at the primary transmitter. First, the effect of the secondary system on the secrecy capacity of the primary system has been analyzed in two regimes of eavesdropping channel, when only one eavesdropper is present. We have found that employing the artificial noise is not effective for a weak eavesdropping channel. On the other hand, for a strong eavesdropping channel, it has been found that the power allocation ratio between the desired signal and artificial noise needs to be optimized in order to improve the secrecy capacity of the primary system. Furthermore, we have extended the analysis to arbitrary eavesdropping channel condition and arbitrary number of eavesdroppers. It has been found that the use of artificial noise is effective unless all the eavesdroppers are far from the primary transmitter. We have also discussed how the optimal power allocation for the artificial noise is influenced by the eavesdropping channel condition, interference from the secondary system, and the number of eavesdroppers.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2014.2359246, IEEE Transactions on Vehicular Technology

Simulations have been used to demonstrate the validity of the analysis. It is left for future work to find the optimal power allocation ratio analytically.

APPENDIX

A. PDF of $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$

1) PDF of $\mathcal{X}$: The PDF of $\mathcal{X}$ can be expressed as

$$f_{\mathcal{X}}(x) = \mathcal{P}_0 f_{\mathcal{X}}(x|\Theta=0) + \mathcal{P}_1 f_{\mathcal{X}}(x|\Theta=1). \tag{37}$$

The conditional PDF $f_{\mathcal{X}}(x|\Theta=0)$ can be obtained from $\mathcal{X} = \left(\phi\frac{\gamma_{pe}}{M}\right)|\psi_I|^2$ when $\Theta=0$, in which $|\psi_I|^2$ follows an exponential distribution, since it is a square of the Gaussian random variable. Therefore, the conditional PDF is found as [22, Theorem 3.19]

$$f_{\mathcal{X}}(x|\Theta=0) = \frac{M}{\phi\gamma_{pe}} e^{-\frac{M}{\phi\gamma_{pe}}x}. \tag{38}$$

Similarly, the conditional PDF $f_{\mathcal{X}}(x|\Theta=1)$ can be derived from $\mathcal{X} = \frac{\phi\frac{\gamma_{pe}}{M}|\psi_I|^2}{1+\gamma_{se}|h_{se}|^2}$ when $\Theta=1$. Let $U \triangleq \phi\frac{\gamma_{pe}}{M}|\psi_I|^2$ and $V \triangleq 1+\gamma_{se}|h_{se}|^2$. Since $|\psi_I|^2$ and $|h_{se}|^2$ follow the exponential distribution, $f_U(u) = \frac{M}{\phi\gamma_{pe}} e^{-\frac{M}{\phi\gamma_{pe}}u}$ and $f_V(v) = \frac{1}{\gamma_{se}} e^{-\frac{v-1}{\gamma_{se}}}$ [22, Theorem 3.21]. We first compute the conditional CDF $F_{\mathcal{X}}(x|\Theta_0) = \Pr\left(\mathcal{X} = \frac{U}{V} < x\right)$, and then we have the conditional PDF $f_{\mathcal{X}}(x|\Theta=1) = \frac{d(F_{\mathcal{X}}(x|\Theta=1)}{dx}$ given as

$$\begin{aligned} f_{\mathcal{X}}(x|\Theta=1) &= \frac{M}{\phi\gamma_{pe}} e^{-\frac{M}{\phi\gamma_{pe}}x} \\ &\times \left\{ \left(1+\frac{M\gamma_{se}}{\phi\gamma_{pe}}x\right)^{-1} + \gamma_{se}\left(1+\frac{M\gamma_{se}}{\phi\gamma_{pe}}x\right)^{-2} \right\}. \end{aligned} \tag{39}$$

2) PDF of $\mathcal{Y}$: The PDF of $\mathcal{Y}$ can be expressed as

$$f_{\mathcal{Y}}(y) = \mathcal{P}_0 f_{\mathcal{Y}}(y|\Theta=0) + \mathcal{P}_1 f_{\mathcal{Y}}(y|\Theta=1). \tag{40}$$

The conditional PDF $f_{\mathcal{Y}}(y|\Theta=0)$ can be obtained from $\mathcal{Y} = \frac{\phi\frac{\gamma_{pe}}{M}|\psi_I|^2}{\frac{1-\phi}{M-1}\frac{\gamma_{pe}}{M}\|\boldsymbol{\psi}_A\|^2}$ when $\Theta=0$. Note that $|\psi_I|^2$ follows the exponential distribution, and $\|\boldsymbol{\psi}_A\|^2$ is the sum of squared exponential random variables and thus it follows the Erlang distribution. Therefore, the conditional PDF $f_{\mathcal{Y}}(y|\Theta=0)$ is derived as

$$f_{\mathcal{Y}}(y|\Theta=0) = \frac{1-\phi}{\phi\left(1+\frac{1-\phi}{\phi(M-1)}y\right)^M}. \tag{41}$$

Similarly, the conditional PDF $f_{\mathcal{Y}}(y|\Theta=1)$ is found as

$$f_{\mathcal{Y}}(y|\Theta=1) = \frac{\alpha+(M-1)\eta+M\alpha\eta y}{(1+\alpha y)^2(1+\eta y)^M}, \tag{42}$$

where $\alpha \triangleq \frac{M}{\phi}\frac{\gamma_{se}}{\gamma_{pe}}$ and $\eta \triangleq \frac{1}{M-1}\frac{1-\phi}{\phi}$. We can rewrite (42) in the form of partial fraction expansion as

$$f_{\mathcal{Y}}(y|\Theta=1) = \frac{A}{(1+\alpha y)^2} + \sum_{k=1}^{M}\frac{B_k}{(1+\eta y)^k}, \tag{43}$$

where

$$\begin{aligned} A &= (\alpha-\eta)\left(1-\frac{\eta}{\alpha}\right)^{-M}, \\ B_k &= (1-k)(\alpha-\eta)\left(1-\frac{\alpha}{\eta}\right)^{-2}\left(1-\frac{\eta}{\alpha}\right)^{k-M}. \end{aligned} \tag{44}$$

Note that $B_1 = 0$, and thus we get

$$f_{\mathcal{Y}}(y|\Theta=1) = \frac{A}{(1+\alpha y)^2} + \sum_{k=2}^{M}\frac{B_k}{(1+\eta y)^k}. \tag{45}$$

3) PDF of $\mathcal{Z}$: From (29), the conditional CDF's of $\mathcal{Z}$ can be computed as follows.

$$\begin{aligned} &F_{\mathcal{Z}}(z|\Theta=0) = \prod_{n=1}^{N} F_{\mathcal{Z}_n}(z|\Theta=0) \\ &= \prod_{n=1}^{N}\left(1-e^{-\frac{M}{\phi\gamma_{pe,n}}z}(\eta z+1)^{-M+1}\right) \\ &= \sum_{j=0}^{N}\frac{(-1)^j}{j!}\underbrace{\sum_{n_1=1}^{N}\cdots\sum_{n_j=1}^{N}}_{n_1\neq n_2\neq\cdots\neq n_j}\prod_{t=1}^{j} e^{-\frac{M}{\phi\gamma_{pe,n_t}}z}(\eta z+1)^{-M+1} \\ &= \sum_{j=1}^{N}(-1)^{j-1}\sum_{\substack{n_1=\cdots=n_j=1 \\ n_1<\cdots<n_j}}^{N}\left(1-e^{-\frac{M}{\phi\bar{\gamma}_{pe,j}}z}(\eta z+1)^{-(M-1)j}\right) \\ &= 1-\sum_{j=1}^{N}(-1)^{j-1}\sum_{\substack{n_1=\cdots=n_j=1 \\ n_1<\cdots<n_j}}^{N} e^{-\mu_j z}(\eta z+1)^{-(M-1)j}, \end{aligned} \tag{46}$$

where μ_j and $\bar{\gamma}_{pe,j}$ are defined in (31).

$$\begin{aligned} &F_{\mathcal{Z}}(z|\Theta=1) \\ &= \prod_{n=1}^{N}\left(1-e^{-\frac{M}{\phi\gamma_{pe,n}}z}\left[\frac{A_n}{\alpha_n(\alpha_n z+1)}+\sum_{k=2}^{M}\frac{B_{k,n}}{\eta(\eta z+1)^{k-1}}\right]\right) \\ &= \sum_{j=0}^{N}\frac{(-1)^j}{j!}\underbrace{\sum_{n_1=1}^{N}\cdots\sum_{n_j=1}^{N}}_{n_1\neq n_2\neq\cdots\neq n_j}\prod_{t=1}^{j} e^{-\frac{M}{\phi\gamma_{pe,n_t}}z} \\ &\quad\times\left[\frac{A_{n_t}}{\alpha_{n_t}(\alpha_{n_t}z+1)}+\sum_{k=2}^{M}\frac{B_{k,n_t}}{\eta(\eta z+1)^{k-1}}\right] \\ &= \sum_{j=1}^{N}(-1)^{j-1}\sum_{\substack{n_1=\cdots=n_j=1 \\ n_1<\cdots<n_j}}^{N}\left(1-e^{-\frac{M}{\phi\bar{\gamma}_{pe,j}}z}\prod_{t=1}^{j}\right. \\ &\quad\left.\times\left[\frac{A_{n_t}}{\alpha_{n_t}(\alpha_{n_t}z+1)}+\sum_{k=2}^{M}\frac{B_{k,n_t}}{\eta(\eta z+1)^{k-1}}\right]\right) \\ &= 1-\sum_{j=1}^{N}(-1)^{j-1}\sum_{\substack{n_1=\cdots=n_j=1 \\ n_1<\cdots<n_j}}^{N} e^{-\mu_j z}\left(\mathcal{L}_1(z)+\widetilde{\sum}\mathcal{L}_2(z)\right), \end{aligned} \tag{47}$$

where $\mathcal{L}_1(z) = \prod_{t=1}^{j}\frac{A_{n_t}}{\alpha_{n_t}(\alpha_{n_t}z+1)}$, $\mathcal{L}_2(z) = \prod_{n_u\neq\left\{\{n_t\}_{t=1}^{j}\cap\{n_i\}_{i=1}^{t}\right\}}\frac{A_{n_u}}{\alpha_{n_u}(\alpha_{n_u}z+1)}\frac{B_{k_1,n_1}\cdots B_{k_j,n_j}}{\eta^j(\eta z+1)^{k_1+\cdots k_j-j}}$, and $\widetilde{\sum}$ is defined in (31).

By exploiting Heaviside's expansion [23], we can express $\mathcal{L}_1(z)$ as

$$\prod_{t=1}^{j}\frac{A_{n_t}}{\alpha_{n_t}(\alpha_{n_t}z+1)} = \sum_{p_1=1}^{L_1}\sum_{q_1=1}^{r_{p_1}}\frac{\mathcal{A}_{1,p_1,q_1}}{(z+\theta_{p_1})^{q_1}}, \tag{48}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2014.2359246, IEEE Transactions on Vehicular Technology

where θ_{p_1} are L_1 distinct elements of the set $\{\alpha_{n_t}\}_{t=1}^{j}$ in the decreasing order, and $\mathcal{A}_{1,p_1,q_1}$ are the coefficients of the partial fraction expansion given as [8]

$$\mathcal{A}_{1,p_1,q_1} = \frac{1}{(r_{p_1}-q_1)!}\left\{\frac{\partial^{(r_{p_1}-q_1)}}{\partial z^{(r_{p_1}-q_1)}}\left[(z+\theta_{p_1})^{r_{p_1}}\,\mathcal{L}_1(z)\right]\right\}\Big|_{z=-\theta_{p_1}}. \tag{49}$$

Similarly, we can express $\mathcal{L}_2(z)$ as

$$\mathcal{L}_2(z) = \sum_{p_2=1}^{L_2}\sum_{q_2=1}^{r_{p_2}}\frac{\mathcal{A}_{2,p_2,q_2}}{(z+\theta_{p_2})^{q_2}}, \tag{50}$$

where

$$\mathcal{A}_{2,p_2,q_2} = \frac{1}{(r_{p_2}-q_2)!}\left\{\frac{\partial^{(r_{p_2}-q_2)}}{\partial z^{(r_{p_2}-q_2)}}\left[(z+\theta_{p_2})^{r_{p_2}}\,\mathcal{L}_2(z)\right]\right\}\Big|_{z=-\theta_{p_2}}. \tag{51}$$

If $n_u=\{0\}$, then $\mathcal{L}_2(z)=\frac{B_{k_1,n_1}\cdots B_{k_j,n_j}}{\eta^j(\eta z+1)^{k_1+\cdots k_j-j}}$. By differentiating $F_{\mathcal{Z}}(z|\Theta=0)$ and $F_{\mathcal{Z}}(z|\Theta=1)$ with respect to z, we arrive at (34).

B. Integrals

1) Derivation of Eq. (20):

$$\begin{aligned}
C_{e|\Theta=0} &= \int_0^\infty \log_2(1+x) f_{\mathcal{X}}(x|\Theta=0)dx \\
&= \frac{1}{\ln 2}\int_0^\infty e^{ux}\frac{1}{1+x}dx \\
&= \frac{1}{\ln 2}e^u\int_1^\infty e^{-ux}x^{-1}dx = \frac{1}{\ln 2}e^u E_1(u), \\
C_{e|\Theta=1} &= \int_0^\infty \log_2(1+x) f_{\mathcal{X}}(x|\Theta=1)dx \\
&= \frac{1}{\ln 2}\frac{1}{1-\alpha}\left(\int_0^\infty e^{ux}\frac{1}{1+x}dx\right. \\
&\quad \left.+\int_0^\infty e^{vx}\frac{1}{1+x}dx\right) \\
&= \frac{1}{\ln 2}\frac{1}{1-\alpha}\left(e^u E_1(u)+e^v E_1(v)\right),
\end{aligned} \tag{52}$$

where $u \triangleq \frac{M}{\phi\gamma_{pe}}$ and $v \triangleq \frac{1}{\gamma_{se}}$.

2) Derivation of Eq. (27):

$$\begin{aligned}
C_{e|\Theta=0} &= \int_0^\infty \log_2(1+y) f_{\mathcal{Y}}(y|\Theta=0)dy \\
&= \frac{1-\phi}{\phi\ln 2}\int_0^\infty \ln(1+y)\left(1+\eta y\right)^{-M}dy \\
&= \frac{1-\phi}{\phi\ln 2}\int_0^\infty \frac{1}{\eta(M-1)(1+y)}\left(1+\eta y\right)^{-M+1}dy \\
&= \frac{1-\phi}{\phi\ln 2}\int_1^\infty \frac{1}{\eta(M-1)y}\left(1-\eta+\eta y\right)^{-M+1}dy \\
&= \frac{1-\phi}{\phi\ln 2}\mathcal{I}_M(\eta), \\
C_{e|\Theta=1} &= \int_0^\infty \log_2(1+y) f_{\mathcal{Y}}(y|\Theta=1)dy \\
&= \int_0^\infty \log_2(1+y)\frac{A}{(1+\alpha y)^2}dy \\
&\quad +\sum_{k=2}^{M}\int_0^\infty \log_2(1+y)\frac{B_k}{(1+\eta y)^k}dy \\
&= \frac{1}{\ln 2}\int_0^\infty \ln(1+y)\frac{A}{(1+\alpha y)^2}dy \\
&\quad +\frac{1}{\ln 2}\sum_{k=2}^{M}\int_0^\infty \ln(1+y)\frac{B_k}{(1+\eta y)^k}dy \\
&= \frac{1}{\ln 2}\left(\frac{A\ln\alpha}{\alpha(\alpha-1)}+\sum_{k=2}^{M}B_k\mathcal{I}_k(\eta)\right),
\end{aligned} \tag{53}$$

where $M>1$, $k>1$ and $\eta\neq 0$. If $\eta=1$, $\mathcal{I}_k(\eta)$ in (53) becomes $\mathcal{I}_k(1)=\frac{1}{(k-1)^2}$. Otherwise, if $\eta\neq 1$, $\mathcal{I}_k(\eta)$ becomes $\mathcal{I}_k(\eta) = \frac{(1-\eta)^{1-k}}{(k-1)\eta}\left[-\ln\eta+\sum_{i=1}^{k-2}\frac{(k-2)!(-\eta)^i}{(k-i-2)!i!i}(\eta^{-i}-1)\right]$ based on [24, Eq. (100)].

3) Derivation of Eq. (36):

$$\begin{aligned}
C_{e|\Theta=0} &= \int_0^\infty \log_2(1+z) f_{\mathcal{Z}}(z|\Theta=0)dz \\
&= \frac{\mathcal{K}}{\ln 2}\int_0^\infty \ln(1+z)e^{-\mu_j z}\left(\eta z+1\right)^{-(M-1)j-1} \\
&\quad \times\left[\mu_j(\eta z+1)+(M-1)j\eta\right]dz \\
&= \frac{\mathcal{K}}{\ln 2}\sum_{k=0}^{\infty}(-1)^k\frac{(\mu_j)^k}{k!}\int_0^\infty z^k\left(\eta z+1\right)^{-(M-1)j-1} \\
&\quad \times\left[\mu_j(\eta z+1)+(M-1)j\eta\right]G_{2,2}^{1,2}\left(z\Big|_{1,0}^{1,1}\right)dz \\
&= \frac{\mathcal{K}}{\ln 2}\sum_{k=0}^{\infty}(-1)^k\frac{\mu_j^k}{k!}\left(\frac{\mu_j}{\Gamma\left((M-1)j\right)}G_{3,3}^{2,3}\left(\frac{1}{\eta}\Big|_{(M-1)j-k-1,1,0}^{-k,1,1}\right)\right. \\
&\quad \left.+\frac{(M-1)j\eta}{\Gamma\left((M-1)j+1\right)}G_{3,3}^{2,3}\left(\frac{1}{\eta}\Big|_{(M-1)j-k,1,0}^{-k,1,1}\right)\right) \\
&= \frac{\mathcal{K}}{\ln 2}\sum_{k=0}^{\infty}(-1)^k\frac{\mu_j^k}{k!}\frac{1}{\eta^k\Gamma\left((M-1)j\right)} \\
&\quad \times\left(\mu_j G_{3,3}^{2,3}\left(\frac{1}{\eta}\Big|_{(M-1)j-k-1,1,0}^{-k,1,1}\right)+\eta G_{3,3}^{2,3}\left(\frac{1}{\eta}\Big|_{(M-1)j-k,1,0}^{-k,1,1}\right)\right) \\
&= \frac{\mathcal{K}}{\ln 2}\mathcal{J}_0,
\end{aligned} \tag{54}$$

Note that the third equality in (54) follows by expressing the integrand $\ln(1+z)$ in terms of Meijer G-function [25, Eq. (8.4.6.5)] as $\ln(1+z)=G_{2,2}^{1,2}\left(z\Big|_{1,0}^{1,1}\right)$, and expressing $e^{-\mu_j z}$ using the Maclaurin series expansion: $e^{-\mu_j z}=$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2014.2359246, IEEE Transactions on Vehicular Technology

$\sum_{k=0}^{\infty}(-1)^k \frac{(\mu_j z)^k}{k!}$. We use [21, Eq. (7.811.5)] to obtain the fourth equality, and $\Gamma(x+1) = x\Gamma(x)$ [21, Eq. (8.311.1)] to get the fifth equality.

Similarly to (54), $C_{e|\Theta=1}$ can be expressed as

$$\begin{aligned} C_{e|\Theta=1} &= \int_0^{\infty} \log_2(1+z) f_{\mathcal{Z}}(z|\Theta=1) dz \\ &= \frac{\mathcal{K}}{\ln 2} \left\{ \mathcal{J}_1 + \mathcal{J}_2 \right\}, \end{aligned} \tag{55}$$

where $\mathcal{J}_1$ and $\mathcal{J}_2$ are defined in (31).

REFERENCES

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

[2] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Select. Areas Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[3] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

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

[5] M. Bloch and J. Barros, *Physical-Layer Security.* Cambridge Univ. Press, 2011.

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

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

[8] V. N. Q. Bao, N. L. Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6076–6085, Dec. 2013.

[9] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Select. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sept. 2013.

[10] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 28–33, May/June 2013.

[11] 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.

[12] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, "On the relationship between the multi-antenna secrecy communications and cognitive radio communications," *IEEE Trans. Commun.*, vol. 58, no. 6, pp. 1877–1886, June 2010.

[13] Y. Pei, Y. C. Liang, L. Zhang, 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.

[14] 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.

[15] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inform. Theory*, vol. 57, no. 8, pp. 4691–4972, Aug. 2011.

[16] Z. Shu, Y. Yang, Y. Qian, and R. Q. Hu, "Impact of interference on secrecy capacity in a cognitive radio network," in *Proc. IEEE Global Commun. Conf. 2011 (GLOBECOM 2011)*, Houston, TX, Dec. 2011, pp. 1–6.

[17] 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.

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

[19] P. Gopala, L. Lai, and H. Gamal,"On the secrecy capacity of fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[20] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wiretap channels," *EURASIP J. Wireless Commun. & Net.*, vol. 2009, pp. 1-12, Oct. 2009.

[21] I. S. Gradshteyn and I. M. Ryzhik *Tables of Integrals, Series, and Products*, 7th Ed., San Diego: Academic Press, 2007.

[22] R. D. Yates and D. J. Goodman, *Probability and Stochastic Processes: A Friendly Introduction for Electrical and Computer Engineers*, 2nd Ed., John Wiley & Sons, 2005.

[23] E. Kreyszig, *Advanced Engineering Mathematics*, 8th Ed., New York: John Wiley & Sons, 1999.

[24] H. Dwight, *Tables of Integrals and Other Mathematical Data*, 3rd Ed., New York: MacMillan, 1957.

[25] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integrals and Series, Volume 3: More Special Functions*, New York: Gordon & Breach Science, 1990.