International Journal of Computer Networks and Communications Security

VOL. 4, NO. 5, MAY 2016, 159–164
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Secure Transmission of Underlay Cognitive Radio with Passive Eavesdropping

Azzam Al-nahari[1], Mukarram Al-jamali[2] and Mohammed AlKhawlani[3]

[1] Department of Electrical Engineering, Ibb University, Ibb, Yemen

[2, 3] Department of Electronics Engineering, University of Science and Technology, Sana'a, Yemen

E-mail: [1]azzamyn@gmail.com, [2]mukarramja@gmail.com, [3]m.alshadadi@ust.edu

ABSTRACT

The security in cognitive radio networks (CRNs) has attracted recently a significant attention due to the open environment of the spectrum sharing networks, which make them more vulnerable to wireless attacks. In this paper, we consider the problem of physical layer security in CRNs. Our objective is to enhance the secrecy performance of the secondary user (SU) in the presence of passive eavesdropper, whose channel state information (CSI) is unknown at the transmitter side. Two beamforming techniques are proposed; transmit beamforming (BF) and beamforming with jamming (BFJ). We investigate the impact of using artificial jamming (AJ) signal in improving the secrecy performance of the SU in underlay CRNs, where the AJ noise signal is used to confuse the eavesdropper's channel. Two power constraints are considered in the system; transmit power constraint and the interference power threshold at the primary user (PU). The performance of the proposed techniques is analyzed in terms of the achievable secrecy rate and the secrecy outage probability.

Keywords: *CRNs, secrecy rate, artificial jamming, underlay cognitive radio, eavesdropping*.

1 INTRODUCTION

Cognitive radio networks (CRNs) are intelligent networks that adapt to changes in their environments to make a better use of the radio spectrum. Depending on the knowledge that is needed to coexist with the primary network, cognitive radio approaches fall into three classes: underlay, overlay and interweave [1]. In underlay paradigm, simultaneous primary and secondary transmissions are allowed as long as the interference level at the primary user (PU) side remains acceptable.

Security issues is one of the important requirements for future 5G systems, and successful deployment of CRNs and the realization of their benefits will depend on the placement of essential security mechanisms. In fact, In such complex environment, and due to the open and dynamic nature of CRNs, the conventional cryptographic authentication have become expensive and vulnerable to attacks. Therefore, physical-layer security has gained considerable attracting recently [2]. In order to improve the physical layer security of wireless transmissions, many works have been devoted to analyzing the secrecy capacity using the multiple-input multiple-output (MIMO) techniques [3]-[5] and cooperative relays [6]-[7].

Most of the previous schemes considered the case where the channel state information (CSI) of the eavesdropper is known at the transmitter. However, practically, the CSI of the eavesdropper is unknown to the transmitter. Therefore, beamforming and artificial jamming (AJ) are effective approaches to ensure secrecy when considering passive eavesdroppers [8]-[9]. Secret communication with the existence of passive eavesdroppers using AJ was first proposed in [8]. The authors showed that secrecy can be achieved by adding artificially generated noise to the information bearing signal such that it mars the eavesdropper's channel. The produced AJ lies in the null space of the legitimate receiver's channel, while the information signal is transmitted in the range space of the legitimate receiver's channel. In [9], the optimal power allocation and beamforming methods for the AN technique were presented.

Securing and protecting the broadcast channel of CRNs against eavesdropping is an important issue that should be addressed. Although physical layer security in classic wireless networks has been studied for many years, security in the physical layer of CRNs has not been investigated until recently. In [10], the two major classes of attacks, primary user emulation attack and objective function attack, were studied. The achievable secrecy rates in CRNs with external eavesdroppers have been studied in [11] and [12]. In [13], the physical layer security against eavesdropping attacks in the CRNs was investigated by introducing a multiuser scheduling scheme to achieve multiuser diversity for improving the security level of cognitive transmissions with a PU quality of service (QoS) constraint.

In this paper, we study the communication over a secure multi-input single-output (MISO) cognitive radio channels, where the multi antenna secondary user transmitter (SU-TX) sends a confidential message to the legitimate secondary user receiver (SU-RX) without affecting the QoS of the PU in the presence of passive eavesdropper, where the CSI of the eavesdropper is not known at the SU-TX. To provide secure communication in CRNs, we propose two beamforming schemes. The first is transmit beamforming (BF) toward the SU-RX, where no AJ is used at the SU-TX. Then, we consider beamforming with jamming (BFJ), where the transmitted power is divided between the information and jamming signals. The comparison between different schemes is investigated. The proposed techniques exploit the randomness of wireless channel as a means of ensuring the secrecy of wireless communication. The performance of the proposed system is analyzed in terms of the achievable secrecy rate and the secrecy outage probability.

Throughout the paper, the following notations are used. For any number x, $[x]^{+}=\max(0,x)$. Furthermore, $\hat{\mathbf{h}}$ denotes the unit norm vector of $\mathbf{h}$ i.e., $\hat{\mathbf{h}}=\mathbf{h}/\|\mathbf{h}\|$, where $\|.\|$ denotes the Euclidian norm; $\mathbf{h}^{T}$ and $\mathbf{h}^{H}$ denote transpose and conjugate transpose $\mathbf{h}$, respectively. Finally, we use $X\sim CN(0,\sigma^{2})$ to denote a circularly symmetric complex Gaussian random variable with zero-mean and variance σ^{2}.

2 SYSTEM AND CHANNEL MODELS

We consider the CRN as shown in Fig. 1, which consist of one PU transmitter (PU-TX), PU receiver (PU-RX), SU transmitter (SU-TX), SU receiver (SU-RX) and one eavesdropper receiver (ED-RX). All the nodes in the network are equipped with a single antenna except the SU-TX, which has $N\geq 2$ antennas. We assume that the CSI of the eavesdropper is unknown for all nodes in the network, and the CSI of all legitimate nodes are known at the SU-TX. A slow, flat, block Rayleigh fading is assumed, where the channel remains constant over one block and change independently in different blocks.

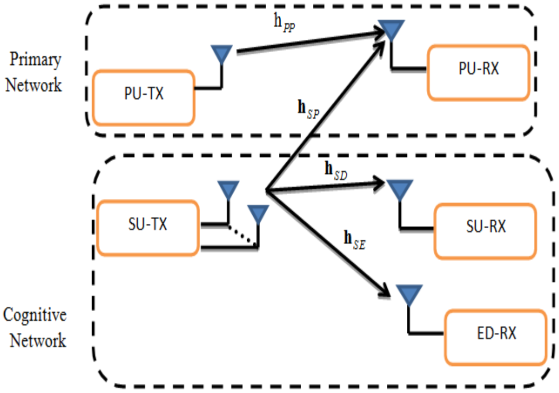

Fig. 1. System model.

Let $\mathbf{x}$ denotes the transmitted signal vector with dimensions $N\times 1$ from the SU-TX and is given by

$$\begin{aligned}\mathbf{x}&=\sqrt{p}\,\mathbf{w}_{a}\,s+\sqrt{q}\,\mathbf{V}\,\mathbf{z}\\&=\sqrt{p}\,\mathbf{w}_{a}\,s+\sqrt{q}\sum_{i=1}^{N-2}\mathbf{v}_{i}\,\mathrm{z}_{i}\end{aligned}\tag{1}$$

where p and q are the transmitted power of the information and jamming power, respectively . s is unit- power transmitted information symbol of the SU, and The beamforming vector $\mathbf{w}_{a}$, where $a\in\{BF,BFJ\}$ denotes the beamforming technique, is of dimensions $N\times 1$ and is normalized such that $\|\mathbf{w}_{a}\|=1$. The matrix $\mathbf{V}=[\mathbf{v}_{1}\,\mathbf{v}_{2}....\mathbf{v}_{N-2}]$ is the $N\times(N-2)$ precoding matrix of the jamming signal vector $\mathbf{z}=[z_{1}z_{2}.....z_{N_{t-1}}]^{T}$. The column vectors of $\mathbf{V}$ are normalized such that $\|\mathbf{v}_{i}\|=1,\forall i$. It should be noted that $\mathbf{V}$ has $(N-2)$ columns because they are designed to lie in the null space of both the two channel vectors $\mathbf{h}_{SD}$ and $\mathbf{h}_{SP}$ shown in Fig. 1. This also interprets why we use only $(N-2)$ antennas for the AJ signal at SU-TX. The received signals at the SU-RX, ED-RX and PU-RX are, respectively, given as

$$y_{d}=\sqrt{p}\mathbf{h}_{SD}\mathbf{w}_{a}s+\sqrt{q}\,\mathbf{h}_{SD}\mathbf{V}\mathbf{z}+n_{d}\tag{2}$$

$$y_{e}=\sqrt{p}\mathbf{h}_{SE}\mathbf{w}_{a}s+\sqrt{q}\,\mathbf{h}_{SE}\mathbf{V}\mathbf{z}+n_{e}\tag{3}$$

$$y_p = \sqrt{p}\mathbf{h}_{SP}\mathbf{w}_a s + \sqrt{q}\,\mathbf{h}_{SP}\mathbf{V}\mathbf{z} + n_p \quad (4)$$

where The channel vector $\mathbf{h}_{ij}$, of dimensions $1 \times N$, represents the fading coefficients of the channel from the *i*-th node to the *j*-th node, where each element is Rayleigh distributed with zero mean and variance σ_{ij}^2 . n_d, n_e and $n_p \sim CN(0,1)$ which represent the additive white Gaussian noise (AWGN) at the SU-RX, ED,RX, and PU-RX, respectively. In order to protect the PU, the interference received at the primary users must not to exceed the maximum interference threshold, denoted by I .

Let P denotes the total transmit power budget and $\phi \in [0,1]$ be the fraction of the transmitted power devoted to the information-bearing signal. Hence, p and q are bounded as

$$p \le \phi P \quad (5)$$

$$q \le \frac{(1-\phi)P}{N-2} \quad (6)$$

Note that, as will be seen later, in order to keep the interference at the PU-RX below the allowed threshold I , the transmitted power is a random variable but is limited by the maximum transmitted power.

3 PROPOSED BEAMFORMING SCHEMES

In this section, we propose two suboptimal beamforming schemes for improving the secrecy performance of CRNs; namely, transmit beamforming (BF), and beamforming with artificial jamming (BFJ). The achievable secrecy rate of the two schemes is derived. The precoding matrix of the jamming signal, $\mathbf{V}$, is designed such that the jamming signal is completely nulled out at the SU-RX and PU-RX [8]. We aim to design the precoding vector $\mathbf{w}_a$ for the information signal for each scheme. Moreover, the transmitted powers, p and q , for each scheme are allocated according to the constraints (5)-(6). Denoting the signal to noise ratios (SNRs) of the SU and eavesdropper by γ_{SD}^a and γ_{SE}^a , the achievable secrecy rate of the SU can be given as [5]

$$C_s = \left[\log_2\left(1+\gamma_{SD}^a\right) - \log_2\left(1+\gamma_{SE}^a\right)\right]^+ \quad (7)$$

where $a \in \{BF, BFJ\}$ denotes the beamforming technique.

3.1 Transmit Beamforming (BF)

In this scheme, we aim to investigate only the effect of beamforming at the SU-TX on the achievable secrecy rate. In other words, we don't consider the jamming signal in this case, and hence, the transmitted signal vector becomes $\mathbf{x} = \sqrt{p}\,\mathbf{w}_{BF}\,s$. In this case, $\phi = 1$ and $\mathbf{w}_{BF}$ should be chosen to maximize the signal at the destination while nulling out the signal at the eavesdropper, i.e. $\mathbf{w}_{BF} = \arg\ \max\left|\mathbf{h}_{SD}\mathbf{w}_{BF}\right|^2$ subjected to $\left|\mathbf{h}_{SE}\mathbf{w}_{BF}\right|^2 = 0$. However, $\mathbf{h}_{SE}$ is not available at the source. Therefore, the achievable secrecy rate is maximized by choosing

$$\mathbf{w}_{BF} = \hat{\mathbf{h}}_{SD}^H = \frac{\mathbf{h}_{SD}^H}{\left\|\mathbf{h}_{SD}^H\right\|} \quad (8)$$

which is known as maximum ratio transmission (MRT) beamforming. Clearly, with this choice for $\mathbf{w}_{BF}$, $\mathbf{w}_{BF}$ lies in the range space of $\mathbf{h}_{SD}$. Hence, the information bearing signal is transmitted in the range space of $\mathbf{h}_{SD}$, which mean that the source beamforming along the direction of the destination. Moreover, from (5), and in order to keep the interference at the PU-RX below the interference threshold I , the transmitted power p should be varied as

$$p = \min\left(P, \frac{I}{\left|\mathbf{h}_{SP}\hat{\mathbf{h}}_{SD}^H\right|^2}\right) \quad (9)$$

The received signals at all nodes are then given as

$$y_d = \sqrt{p}\mathbf{h}_{SD}\hat{\mathbf{h}}_{SD}^H s + n_d \quad (10)$$

$$y_e = \sqrt{p}\mathbf{h}_{SE}\hat{\mathbf{h}}_{SD}^H s + n_e \quad (11)$$

$$y_p = \sqrt{p}\mathbf{h}_{SP}\hat{\mathbf{h}}_{SD}^H s + n_p \quad (12)$$

The SNRs at the SU-RX and ED-RX are given as

$$\gamma_{SD}^{BF} = p\left|\mathbf{h}_{SD}\hat{\mathbf{h}}_{SD}^H\right|^2 \quad (13)$$

$$\gamma_{SE}^{BF} = p\left|\mathbf{h}_{SE}\hat{\mathbf{h}}_{SD}^H\right|^2 \quad (14)$$

Substituting (13) and (14) into (7), the achievable secrecy rate of the BF scheme can be written as

$$C_s^{BF} = \left[\log_2\left(1+p\left|\mathbf{h}_{SD}\hat{\mathbf{h}}_{SD}^H\right|^2\right) - \log_2\left(1+p\left|\mathbf{h}_{SE}\hat{\mathbf{h}}_{SD}^H\right|^2\right)\right]^+ \quad (15)$$

Finding closed form expression for the achievable ergodic secrecy rate given in (15) requires solving high dimensional integrals, which is cumbersome. However, it can be solved easily using computer simulations.

3.2 Beamforming with Artificial Jamming (BAJ)

The main idea of this approach is to use the AJ to degrade the channel of the eavesdropper while the channel of the legitimate receiver is kept unaffected. The beamforming and AJ are effective approaches to ensure secrecy in the presence of a passive eavesdropper. In this scheme, the SU-TX sends the jamming signal, independent of the information signal, to confuse the eavesdropper. So, the transmitted signal $\mathbf{x}$ is given as in (1). As the eavesdropper's CSI is not available at the SU-TX, the available option is to use beamforming toward the destination. Therefore, $\mathbf{w}_{BFJ}$ is chosen as in (8). As the jamming signal affects only the ED-RX, the information power and jamming power transmitted from each of the $N-2$ antennas are, respectively, given by

$$p = \min\left(\phi P, \frac{I}{\left|\mathbf{h}_{SP}\hat{\mathbf{h}}_{SD}^{H}\right|^{2}}\right) \tag{16}$$

$$q = \frac{(1-\phi)P}{N-2} \tag{17}$$

In this case, from (2)-(4), the received signals at all nodes, are given as

$$y_d = \sqrt{p}\,\mathbf{h}_{SD}\hat{\mathbf{h}}_{SD}^{H}s + n_d \tag{18}$$

$$y_e = \sqrt{p}\,\mathbf{h}_{SE}\hat{\mathbf{h}}_{SD}^{H}s + \sqrt{q}\,\mathbf{h}_{SE}\sum_{i=1}^{N-2}\mathbf{v}_i \mathrm{z}_i + n_e \tag{19}$$

$$y_p = \sqrt{p}\,\mathbf{h}_{SP}\hat{\mathbf{h}}_{SD}^{H}s + n_p \tag{20}$$

The SNRs at the destination and eavesdropper are, respectively, given as

$$\gamma_{SD}^{BFJ} = p\left|\mathbf{h}_{SD}\hat{\mathbf{h}}_{SD}^{H}\right|^{2} \tag{21}$$

$$\gamma_{SD}^{BFJ} = \frac{p\left|\mathbf{h}_{SE}\hat{\mathbf{h}}_{SD}^{H}\right|^{2}}{q\sum_{i=1}^{N-2}\left|\mathbf{h}_{SE}\mathbf{v}_i\right|^{2}+1} \tag{22}$$

Substituting (21) and (22) into (7), the achievable secrecy rate for this scheme can be written as

$$C_s^{BFJ} = \left[\log_2\left(1+p\left|\mathbf{h}_{SD}\hat{\mathbf{h}}_{SD}^{H}\right|^{2}\right) - \log_2\left(1+\frac{p\left|\mathbf{h}_{SE}\hat{\mathbf{h}}_{SD}^{H}\right|^{2}}{q\sum_{i=1}^{N-2}\left|\mathbf{h}_{SE}\mathbf{v}_i\right|^{2}+1}\right)\right]^{+} \tag{23}$$

4 SECRECY OUTAGE PROBABILITY

In this section, we introduce the secrecy outage probability as another performance metric for the proposed schemes. For a certain instantaneous secrecy capacity C_S, the secrecy outage probability for a target secrecy rate R_S can be expressed as $P_{out} = \Pr[C_S \le R_S]$. When R_S equals zero, the so called intercept probability is used instead of the secrecy outage probability. For the secrecy rate given in (15), the secrecy outage probability for BF scheme is given by

$$\begin{aligned} P_{out}^{BF} &= \Pr[C_s^{BF} \le R_s] \\ &= \Pr\left[\left(1+p\left|\mathbf{h}_{SD}\hat{\mathbf{h}}_{SD}^{H}\right|^{2}\right) \le 2^{R_S}\left(1+p\left|\mathbf{h}_{SE}\hat{\mathbf{h}}_{SD}^{H}\right|^{2}\right)\right] \end{aligned} \tag{24}$$

For the secrecy rate given in (23), the secrecy outage probability for BFJ scheme is given by

$$\begin{aligned} P_{out}^{BFJ} &= \Pr[C_s^{BFJ} \le R_s] \\ &= \Pr\left[\left(1+p\left|\mathbf{h}_{SD}\hat{\mathbf{h}}_{SD}^{H}\right|^{2}\right) \le 2^{R_S}\left(1+\frac{p\left|\mathbf{h}_{SE}\hat{\mathbf{h}}_{SD}^{H}\right|^{2}}{q\sum_{i=1}^{N-2}\left|\mathbf{h}_{SE}\mathbf{w}_i\right|^{2}+1}\right)\right] \end{aligned} \tag{25}$$

The secrecy outage probability is a performance measure that is more appropriate than the achievable ergodic secrecy rate in slow fading wireless channel environment.

5 NUMERICAL RESULTS

In this section, we provide numerical results to illustrate the effectiveness of the proposed BF and BFJ schemes. We follow the system model shown in Fig. 1, and perform Monte Carlo simulation consisting of 10000 independent trials to obtain the average result. The channels variances $\sigma_{ij}^2 = 1$, $\forall i, j$. In Fig. 2, the achievable ergodic secrecy rate is plotted versus the transmit power P for the two schemes when $\phi = 0.5$, and for different values of the interference limit I. As can be seen from the figure, BFJ outperforms BF when $P > 5\,\mathrm{dB}$.

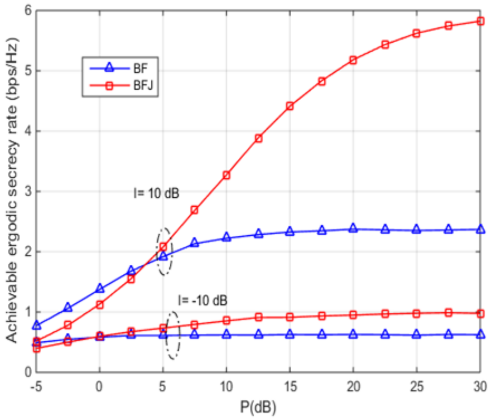

Fig. 2. Achievable ergodic secrecy rate vs. power P with $N=4$, $\phi=0.5$, and different values of I.

It can be seen that with $I=-10\,\text{dB}$, the achievable ergodic secrecy rate of both schemes saturates quickly with increasing P, with about 0.4 bps/Hz improvement using BFJ. When $I=10\,\text{dB}$, BFJ achieves large improvement compared to BF and it gradually increases with P before it saturates.

Figure 3 shows the secrecy outage probability for the different schemes versus the transmitted power. As shown, the BFJ scheme achieves better performance over the practical range of values of the transmitted power, while BF saturates quickly with increasing P. Note also that when $I=10\,\text{dB}$, BFJ achieves higher improvement compared to smaller values.

The achievable secrecy rate against ϕ, at $P=10\,\text{dB}$ and different values of I, is shown in Fig. 4. It can be noted that, at small values of ϕ, the achievable ergodic secrecy rate is low because the system uses more power to transmit the jamming signal but little for the information signal, which cause the low SNR at SU-RX. As ϕ increases, the achievable ergodic secrecy rate also increases until it reaches to a certain value then the secrecy rate starts to decrease due to the fact that a little power used to transmit AJ. As can be seen from the figure, the optimum power allocation between the information signal and artificial jamming signal is at $\phi\approx 0.5$.

In Fig. 5, the achievable ergodic secrecy rate for the two proposed schemes, at the total transmit power limit $P=10\,\text{dB}$, is plotted versus the number of transmit antennas N, with different values of the interference power threshold I. It is shown that the secrecy performance of both schemes increases logarithmically with N. The achievable ergodic secrecy rate of BFJ is better than that of BF over all values of N. As shown in the figure, the performance of BFJ is observed to fail at low values of I, but it achieves much better performance than BF at higher values of I.

6 CONCLUSIONS

This paper has dealt with the problem of physical layer security in CRN with passive eavesdropping and at the same time taking into account the QoS constraints of the PU in the network. We have proposed two beamforming schemes; namely, BF and BFJ. The performance of the two schemes is investigated and compared. Two performance metrics are considered: achievable secrecy rate and secrecy outage probability. It has been shown that the performance of the BFJ achieves better performance over the most scenarios that were considered, which reflects the fact that AJ is an effective way for combating the detrimental effects of passive eavesdropping.

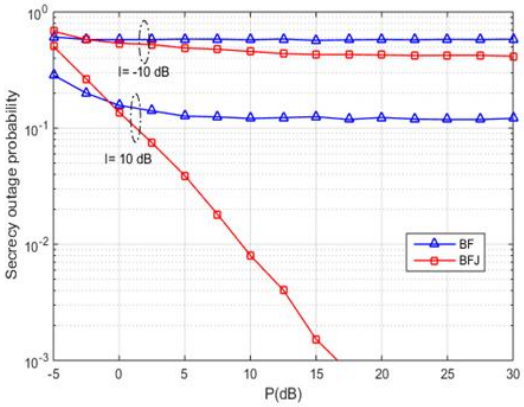

Fig. 3. The Secrecy outage probability vs. power P with $N=4$, $\phi=0.5$, and different values of I.

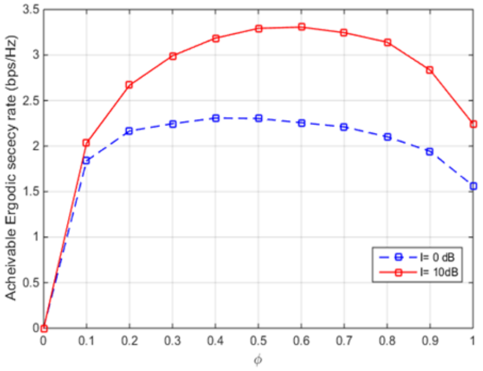

Fig. 4. Achievable ergodic secrecy rate vs. ϕ for BFJ with $N=4$, $P=10\,\text{dB}$ and different values of I

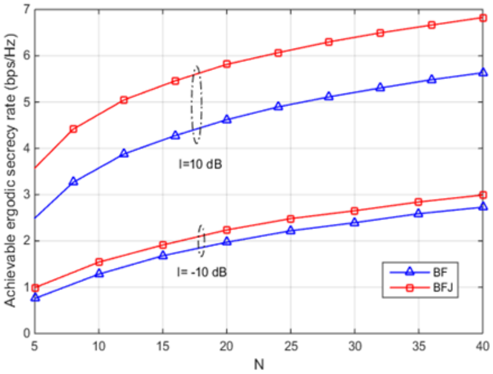

Fig. 5. Achievable ergodic secrecy rate vs. N *with* $\phi = 0.5$, $P = 10\,\mathrm{dB}$ *and different values of* I .

7 REFERENCES

[1] E. Biglieri, A. J. Goldsmith, Larry J. Greenstein, Narayan B. Mandayam and H. V. Poor, Principles of Cognitive Radio, Cambridge University Press, 2013.

[2] A. Mukherjee, A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical-layer security in multiuser wireless networks: A survey," IEEE Communications Surveys and Tutorials, vol. 16, no. 3, pp. 1550-1573, 2014.

[3] Z. Li, W. Trappe and R. Yates, "Secret communication via multi-antenna transmission," 41st Conf. Information Sciences Systems, Baltimore, MD, Mar. 2007.

[4] A. Khisti, G. Womell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in Proc. IEEE Int. Symp. Inf. Theory, Nice, France, Jun. 2007.

[5] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," IEEE Trans. Inf. Theory, vol. 57, no. 8, pp. 4961-4972, Oct. 2007.

[6] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical layer security in cooperative wireless networks," IEEE J. Sel. Areas Commun., vol. 31, no. 10, pp. 2099-2111, Oct. 2013.

[7] A. Al-nahari, I. Krikidis, A. S. Ibrahim, M. I. Dessouky, and F. A. El-Samie,"Relaying techniques for enhancing the physical layer secrecy in cooperative networks with multiple eavesdroppers", Trans. Emerging Tel. Tech (ETT), vol. 25, no. 4, pp. 445–460, April 2012.

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

[9] X. Zhou and M. R. McKay, "Physical layer security with artificial noise: Secrecy capacity and optimal power allocation", in Proc. Int. Conf. on Sig. Proc. and Commun. Syst., Omaha, NE, Sept. 2009.

[10] W. El-Hajj, H. Safa, and M. Guizani, "Survey of security issues in cognitive radio networks," J. Internet Tech., vol. 12, no. 2, pp.25–37, 2011.

[11] S. Anand and R. Chandramouli, "On the secrecy capacity of fading cognitive wireless networks," in Proc. IEEE CrownCom, May 2008.

[12] Y. Pei, Y. 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. 1494-1592 , 2010.

[13] 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, 2 013.

[14] R. Zhang and Y.-C. Liang, "Exploiting multi-antennas for opportunistic spectrum sharing in cognitive radio networks, " IEEE J. Sel. Topics Signal Process., vol. 2, no. 1, pp. 88-102, Feb. 2008.