Proposed Relay Selection Scheme for Physical Layer Security in Cognitive Radio Networks

Hefdhallah Sakran[1], Omar Nasr[2], Mona Shokair[3], El Sayed El-Rabaie[3] and Atef Abou El-Azm[3]
[1]Faculty of Engineering, Ibb University, Ibb, Yemen
[2]Faculty of Engineering, Cairo University, Giza, Egypt
[3]Faculty of Engineering, El-Menoufia University, El-Menoufia, Egypt
Email: hefdh_sakran@yahoo.com

***Abstract*—Cognitive Radio (CR) technology is one of the strong candidate technologies to solve the spectrum scarcity problems. In this paper, we tackle the problem of secure data transmission between a secondary user transmitter and receiver through a relay in the presence of an eavesdropper in a cognitive radio network. The proposed scheme selects the best Decode-and-Forward relay among different relays to assist the transmitter, and to maximize the achievable secrecy rate without harming the primary user. Simulation results show that the secrecy capacity of the network using this scheme will almost be double the capacity when selecting the conventional scheme of relay selection.**

***Index Terms*—cognitive radio; secrecy rate; relay selection; outage probability.**

I. Introduction

There is an unparalleled increase in the usage of wireless devices in the last decade. However, most of the frequency spectrum has already been licensed exclusively to operators by government agencies, such as Federal Communications Commission (FCC). Therefore, there exists an apparent spectrum scarcity for new wireless applications and services. In a series of studies done by different organizations, especially by the FCC, it is reported that there are vast temporal and spatial variations in the allocated spectrum utilization. The spectrum utilization efficiency can be as low as 15% [1]. Cognitive radio technology[2], [3] has been proposed as a strong candidate to solve the spectrum scarcity problem . It allows cognitive users (unlicensed users) to transmit concurrently on the same frequency bands with the licensed primary users (PUs) as long as the resulting interference power at the PU receivers kept below the interference temperature limit [4]. In this setting, security is one of the most important aspects. Traditionally, security is achieved through cryptographic approaches, which can be broadly classified into public-key and private key protocols. These protocols are described in detail in [5]. With the advance of the infrastructure networks such as mobile ad hoc networks, further challenges have appeared which made the nodes more vulnerable to attack. Some of these challenges are memory and power-limited terminal, especially in sensor and ad-hoc networks, and the absence of centralized hardware for security problems.

To cope with these limitations, physical layer security was introduced to offer low complexity security techniques. The theoretical foundation to study physical layer security in the wiretap channel and the information-theoretic notion of secrecy were introduced by Wyner [6]. Wyner considered the wiretap channel model, in which the eavesdropper has degraded observations from the channel compared to the legitimate receiver, i.e., the eavesdropper is said to be degraded. Under this assumption, Wyner showed that the advantage of the main channel over that of the eavesdropper, in terms of the low noise level, can be exploited to transmit secrecy bits. In other words, it is possible to achieve a non-zero secret rate without sharing a key, where the eavesdropper is limited to learn almost nothing from the transmissions. An extension of this work to the case of broadcast channel with confidential messages was proposed in [7].

The first attempt to deal with the secure transmission in a Cognitive Radio Network (CRN) in the context of information-theoretic point of view was considered in [8]. A secure multiple-input single-output (MISO) CR channel, in which a multiantenna SU-Tx sends confidential information to a single-antenna SU-Rx in the presence of a single-antenna PU-Rx and a single-antenna eavesdropper receiver (ED-Rx), was considered. In [9], the issue of optimal transmitter design to achieve physical layer security for a cognitive radio network was addressed. The authors in [9] assumed that all the channel state information of the secondary, primary and eavesdropper channels are not perfectly known at the SU-Tx. In all previous papers that studied physical layer security techniques in CRN, the authors assumed the existence of multiple antenna systems to improve the secrecy rate. However, due to cost and size limitations, multiple antennas may not be available at network nodes. In this paper, we tackle the problem of optimal relay selection in a CRN from secrecy point of view. The network consists of a PU, SU-Tx and SU-Rx that can communicate through one relay from a set of relays. Our goals is to select the optimal relay that maximizes the secrecy rate, without exceeding the allowed interference temperature of the PU.

The rest of this paper is organized as follows. In section II, the system model is introduced. The proposed relay selection scheme will be explained in section III. In section IV, we study the direct transmission secrecy rate and secrecy outage probability. In section V, we introduce the benchmark selection scheme. Simulation results that shows the potential gains of our schemes are shown in section VI, followed by the conclusion of this work.

Notation: Matrices and vectors are denoted using boldface

upper and lower-case letters, respectively. $\mathbf{I}_m$ denotes an $m \times m$ identity matrix. The symbol $\triangleq$denotes "defined as". $\mathcal{CN}(\mu, N_0)$ denotes circularly symmetric complex Gaussian random variable with mean μ and variance N_0. $[x]^+ \triangleq \max\{0, x\}$.

II. System Model

We consider a CR network model as shown in figure 1. It consists of one secondary user transmitter (SU-Tx), N relay nodes (R), one destination node (SU-Rx), one primary user PU, and one eavesdropper (E). The SU-Tx communicates with the SU-Rx with the help of relay nodes. The eavesdropper tries to overhear the transmitted information. In the following, benchmark scheme without cooperation (direct transmission) and decode and forward scheme will be described.

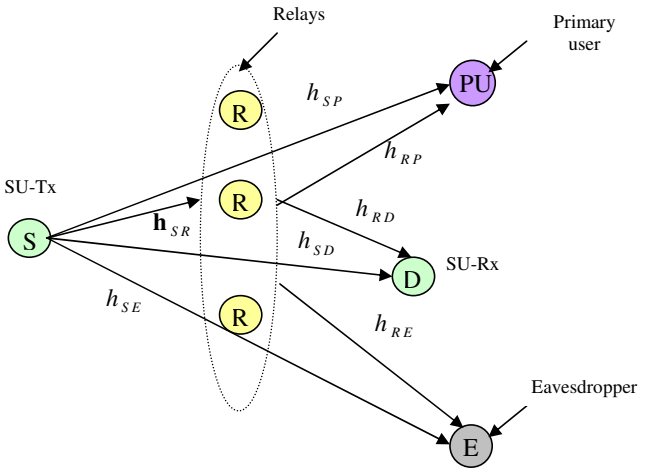

Figure 1: Illustration of system model.

A. Direct Transmission (DT)

For DT, the SU-Tx transmits its symbols directly to the SU-Rx. The received signal at the SU-Rx is given by

$$y_d = \sqrt{P_s} h_{SD} x + z_d \tag{1}$$

Where x is the transmitted symbol from the SU-Tx, P_s denotes the average transmitted power per symbol at the SU-Tx, $z_d \sim \mathcal{CN}(0, N_0)$ is the complex Gaussian noise at the SU-Rx, and h_{SD} is the channel gains between SU-Tx and SU-Rx. All channels are assumed to undergo flat fading and quasistatic.

The received message at the eavesdropper is given by

$$y_e = \sqrt{P_s} h_{SE} x + z_e \tag{2}$$

Where h_{SE} denotes the channel gain between SU-Tx and eavesdropper and z_e represent complex Gaussian noise at the eavesdropper.

The received message at the PU is given by

$$y_p = \sqrt{P_s} h_{SP} x + z_p \tag{3}$$

Where h_{SP} denotes the channel gains between SU-Tx and PU, z_p represents complex Gaussian noise at the PU.

B. Decode and Forward (DF)

In our system , decode and forward (DF) will have two stages. In the first stage, a SU-Tx broadcasts its encoded signal to trusted relay nodes. The relay nodes try to decode the transmitted message, and re-encode it. Then from the set of relays that correctly decoded the message, the relay which gives maximum secrecy rate subject to the interference power constraints at the primary user is chosen to transmit a version of the re-encoded signal.

The received messages at the *N* relays in the *first stage* are given by

$$\mathbf{y}_r = \sqrt{P_s} \mathbf{h}_{SR} x + \mathbf{z}_r \tag{4}$$

Where $\mathbf{y}_r$ is an $N \times 1$ vector which represents the received signal at relays , $\mathbf{h}_{SR}$ is an $N \times 1$ vector which denotes the channel gains between SU-Tx and relays. $\mathbf{z_r} \sim \mathcal{CN}(0, N_0 \mathbf{I}_N)$ is $N \times 1$ vector which represents complex Gaussian noise at the relays.

In the *second stage*, one of the relays that successfully decoded the message from SU-Tx is selected to transmit the re-encoded message to the SU-Rx.

The received messages at the SU-Rx, the primary user and the eavesdropper are given as

$$y_d = \sqrt{P_R} h_{RD} x + z_d \tag{5}$$

$$y_p = \sqrt{P_R} h_{RP} x + z_p \tag{6}$$

$$y_e = \sqrt{P_R} h_{RE} x + z_e \tag{7}$$

Where h_{RD} is the channel gains between the selected relay and SU-Rx, h_{RP} and h_{RE} are the channel for selected relay-primary user and selected relay-eavesdropper, respectively. P_R denotes the transmitted power at the relay. Maximum ratio combining (MRC) is used to combine the two received signals that is represented in (1) and (5) at the destination.

III. Proposed Relay Selection Scheme

The objective of this scheme is to select the relay node R that maximizes the achieved secrecy rate. The instantaneous achievable secrecy rate for the network shown in figure 1 with decoding set C_d, is given by [10]

$$C_s^{|C_d|}(R) = \begin{cases} \left[\frac{1}{2}\log_2(1+\gamma_{SD}) - \frac{1}{2}\log_2(1+\gamma_{SE})\right]^+ \\ \qquad if\ |C_d| = 0 \\ \left[\frac{1}{2}\log_2(1+\gamma_{SD}+\gamma_{RD}) - \right. \\ \left. \frac{1}{2}\log_2(1+\gamma_{SE}+\gamma_{RE})\right]^+ \quad if\ |C_d| > 0 \end{cases} \tag{8}$$

Where $R \in C_d$, C_d is the decoding set which contains the relays that have correctly decoded the received messages in the first time slot. γ_{SD}, γ_{SE} are the instantaneous signal-to-noise ratios (SNRs) for the SU-Tx – SU-Rx link and SU-Tx –

eavesdropper link respectively. γ_{RD}, γ_{RE} are the instantaneous SNRs for the selected relay – SU-Rx link and the selected relay – eavesdropper link respectively. $|C_d|$ denotes the cardinality of set C_d.

In our model, we assume that the distribution of the channel coefficient between the nodes i and j (h_{ij}) is modeled as a zero-mean, independent Gaussian random variable with variance σ_{ij}^2 , $h_{i,j} \sim \mathcal{CN}(0, \sigma_{i,j}^2)$, where $\sigma_{ij}^2 \triangleq \mathbf{E}\left\{|h_{ij}|^2\right\} = d_{ij}^{-\alpha}$. d_{ij} is the Euclidean distance between node i and j, and α is the path-loss exponent.

The secrecy outage probability in traditional wireless networks is defined as the probability that the secrecy rate is less than a given target secrecy rate R_s, $R_s > 0$[11]. Outage in cognitive radio networks occurs in two cases: the secrecy rate is less than a given target with the interference power at the PU below the interference temperature, or the interference power at the primary user is larger than the interference temperature limit.

Similar to [12], we assume $|C_d| > 0$. Based on (8), the secrecy outage probability in a cognitive radio network with the existence of relays CRN is

$$P_{sop} = \sum_{n=1}^{N} \Pr\{|C_d| = n\} \left[\Pr\{C_s^n(R) < R_s\} \times \Pr(I_p^R \leq \Gamma) + \Pr(I_p^R > \Gamma)\right] \quad (9)$$

Where I_p^R : is the interference power at the primary user from the SU-Tx, noise and relay R. Γ is the interference temperature limit.

With changing channel conditions, the best relay is selected that satisfies the following

$$R^* = \arg\max_{R \in C_d} \left\{C_s^{|C_d|}(R)\right\} \quad s.t. \qquad I_p^{R^*} \leq \Gamma \quad (10)$$

Note that the decoding set C_d changes depending on the channel conditions between the SU-Tx and the different relays. Another selection criteria is the selection scheme that minimizes the long term secrecy outage probability

$$R^* = \arg\min_{R \in C_d} \left\{\Pr(C_s^{|C_d|}(R) < R_s) \Pr(I_p^R \leq \Gamma) + \Pr(I_p^R > \Gamma)\right\} \quad (11)$$

Note that, in this paper, the selection criteria is based on the instantaneous SNR values, not the long outage probability.

For certain SNRs values, the instantaneous secrecy rate is given by

$$C_s(R) = \left[\frac{1}{2}\log_2\left(\frac{1+\gamma_{SD}+\gamma_{RD}}{1+\gamma_{SE}+\gamma_{RE}}\right)\right]^+ \quad (12)$$

Hence, the the optimal instantaneous relay that will maximize the secrecy capacity given in (12) is chosen based on the following:

$$R^* = \arg\max_{R \in C_d} \left\{\frac{1+\gamma_{SD}+\gamma_{RD}}{1+\gamma_{SE}+\gamma_{RE}}\right\} \quad s.t. \qquad I_p^{R^*} \leq \Gamma \quad (13)$$

IV. DT Secrecy Rate and Outage Probability

In the direct transmission case, the instantaneous achievable secrecy rate for the network is given as

$$C_s = \left[\log_2(1+\gamma_{SD}) - \log_2(1+\gamma_{SE})\right]^+ \quad (14)$$

Based on (14), the secrecy outage probability for CRN is given as

$$P_{sop} = \Pr\{C_s < R_s\} \Pr(I_p \leq \Gamma) + \Pr(I_p > \Gamma) \quad (15)$$

Where I_p : is the interference power at the primary user from the SU-Tx and noise.

V. Conventional Relay Selection Scheme

Conventionally, the selection of the best relay is based on the instantaneous channel condition between the relay and the SU-Tx (γ_{RD}), such that the relay transmission does not exceed the interference temperature level of the PU. The conventional scheme does not take the link between the relay and eavesdropper into account while choosing the best relay.

$$R^* = \arg\max_{R \in C_d} \{\gamma_{RD}\} \quad s.t. \qquad I_p^{R^*} \leq \Gamma \quad (16)$$

The secrecy outage probability is given by (9) .

VI. Simulation Results

We perform Monte Carlo simulation consisting of 10000 independent trials to obtain the average results. All distances are in meters. The system parameters are:

- $N = 4$ relays which are located at (15,0), (10,0), (17,0) and (30,0) (unit: meters).
- one eavesdropper, located at (60,0).
- one SU-Rx, located at (50, 0).
- a primary user, located at (100,0).
- relay transmit power, P_R = 10 W (10dB).
- interference temperature limit Γ= - 4 dB.
- path loss exponent α =3.
- The SU-Tx transmission rate is 2 bits/s/Hz. The target secrecy rate used to calculate outage is 0.1 bits/s/Hz.

Figure 2 shows the average secrecy rate of the direct transmission (DT), optimal selection (OS) and conventional selection (CS) versus the power at SU-Tx. For the OS, R is selected using (10). For the CS, R is selected using (16). It can be seen from figure 2 that the OS scheme significantly improves the secrecy rate. Moreover, the secrecy rate reaches a peak at 12 dB, and then monotonically decreases. Increasing the transmit power beyond this value increases the interference on

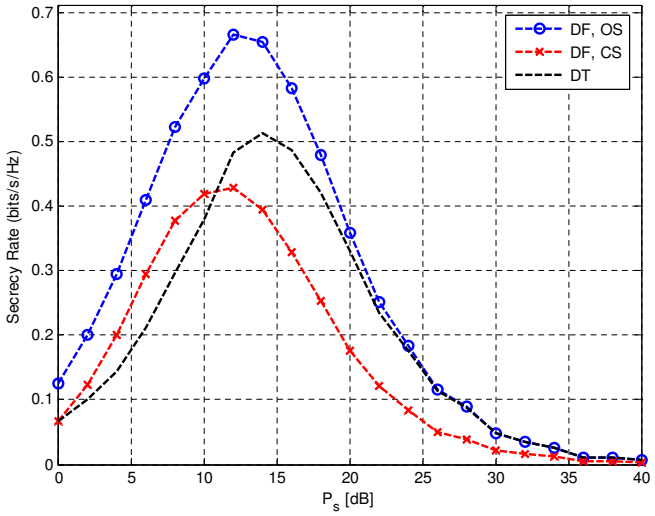

Figure 2: Secrecy rate versus power at SU-Tx.

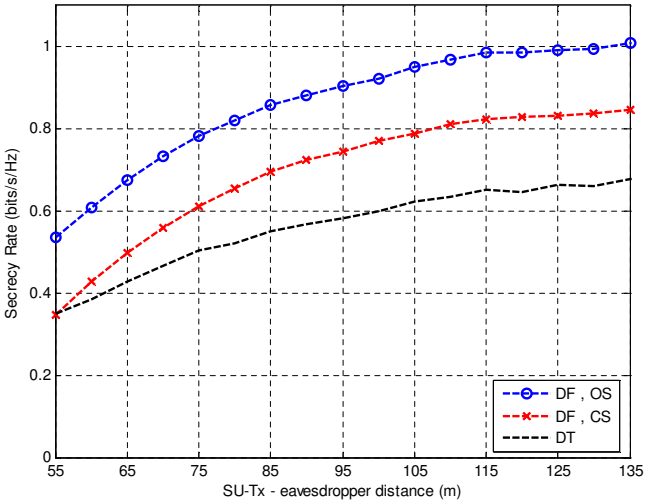

Figure 4: Secrecy rate versus SU-Tx to eavesdropper distance.

the PU, which increases the outage probability and decreases the secrecy rate.

Figure 3 shows the relation between the primary user location and the achievable secrecy rate. In this figure, the location of the primary user varies from (55, 0) to (135, 0), the power of SU-Tx is fixed at 10 dB. From this figure, It can be seen that as the PU moves away from the relays (and the SU-Tx), the secrecy rate increases first and then becomes stable at primary user locations larger than 115 m.

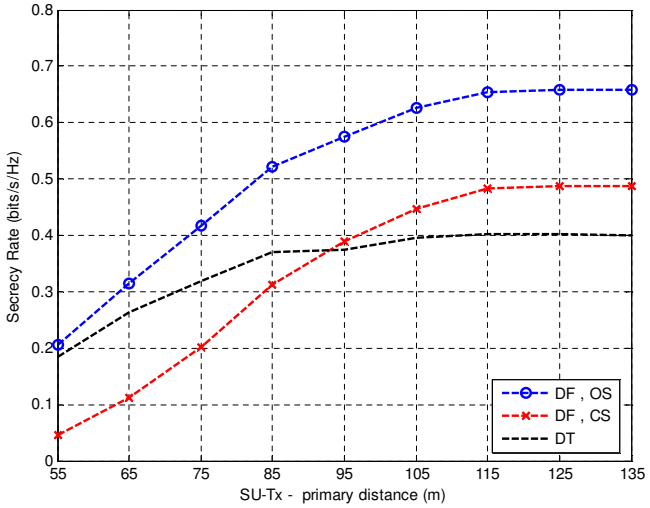

Figure 3: Secrecy rate versus distance between SU-Tx and PU.

In figure 4 we test the impact of the eavesdropper's location on the achieved secrecy rate. The power of SU-Tx is fixed at 10 dB. The location of the eavesdroppers is moved from (55,0) up to (135,0). This reflects the importance (effect) of the location of the eavesdropper relative to the location of the SU-Tx.

Figure 5 shows the secrecy rate for different values of interference temperature Γ. In this figure, the location of the $N = 4$ relays at (15,0), (10,0), (17,0) and (30,0), $P_R = P_s = 10$ dB, eavesdropper's location is (60,0). We note from figure 5 that when Γ increases, the secrecy rate increases, and then becomes stable at Γ values larger than 0 dB.

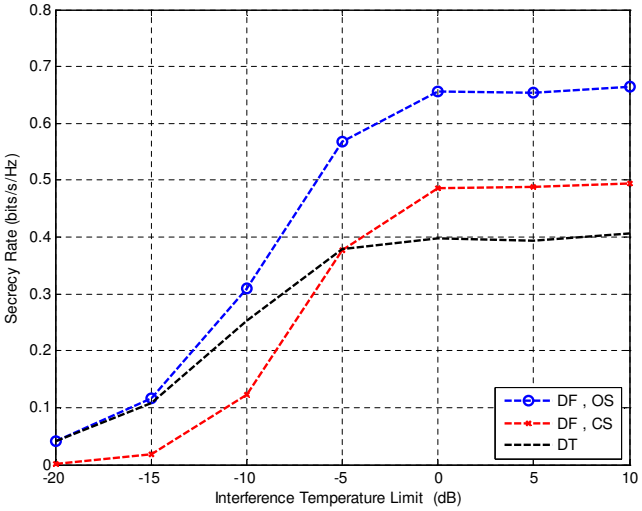

Figure 5: Secrecy rate versus different values of Γ.

The secrecy outage probability is the second performance metric that is used to verify the effectiveness of the proposed scheme. Figure 6, shows the secrecy outage probability versus transmitted power at SU-Tx. The target secrecy rate is equal to 0.1 bits/s/Hz. From this figure, we can see that the robustness of the proposed scheme and the improvement in the secrecy outage probability are achieved.

Figure 7, depicts the effect of the primary user location on the secrecy outage probability for the DT, OS and CS. It can be seen that if the primary user is far away from SU-Tx, the secrecy outage probability improves.

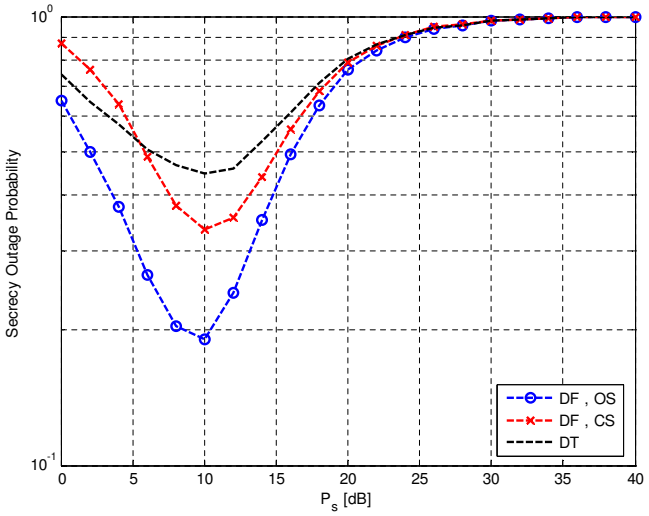

Figure 6: Secrecy outage probability versus power at SU-Tx.

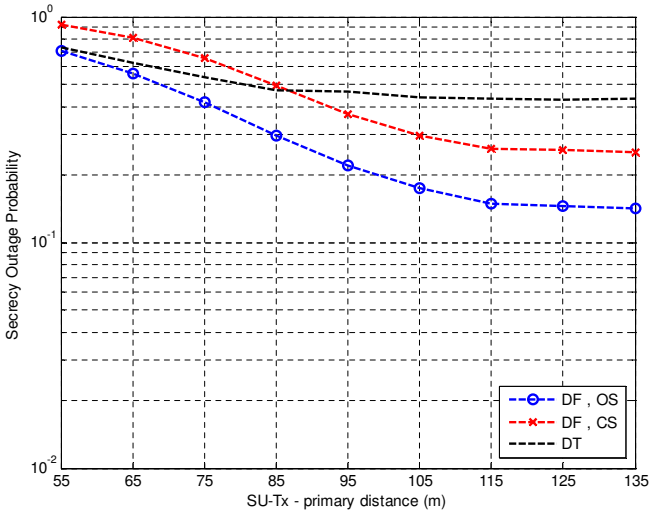

Figure 7: Secrecy outage probability versus SU-Tx to primary distance.

VII. Conclusion

In this paper, we have proposed a relay selection scheme for secrecy-aware cognitive radio networks. The proposed scheme improves the secrecy rate of such systems, taking into account the interference temperature. In the proposed scheme, one relay is selected in the second phase to enhance the security against the eavesdropper subject to the interference temperature constraints at the primary user. Simulation results show that the proposed selection scheme can significantly improve the system performance in terms of both the achievable secrecy rate and the secrecy outage probability.

References

[1] F. C. Commission, "Spectrum policy task force report." FCC Document ET Docket No. 02-135, November 2002.

[2] J. Mitola, *Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio*. PhD thesis, KTH, Stockholm, Sweden, 2000.

[3] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, pp. 201–220, February 2005.

[4] P. Kolodzy, "Interference temperatue : a metric for dynamic spectrum utilization," *International Journal of Network Management*, vol. 16, pp. 103–113, April 2006.

[5] H. Delfs and H. Knebl, *Introduction to Cryptography: Principles and Applications*. 2nd ed. Springer, 2007.

[6] A. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, October 1975.

[7] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transaction of Information Theory*, vol. 24, pp. 451–456, July 1978.

[8] Y. Pei, Y. Liang, K. Teh, and K. Li, "Secure communication over miso cognitive radio channels," *IEEE Transaction on Wireless Communications*, vol. 9, pp. 1494–1502, April 2010.

[9] Y. Pei, Y. Liang, K. Teh, and K. Li, "Secure communication in multiantenna cognitive radio networks with imperfect channel state information," *IEEE Transactions on Signal Processing*, vol. 59, pp. 1683–1693, April 2011.

[10] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Transaction on Information Theory*, vol. 54, pp. 4005–4019, September 2008.

[11] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *IEEE International Symposium on Information Theory*, July 2006.

[12] I. Krikidis, J. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Transactions on Wireless Communications*, vol. 8, pp. 5003–5011, October 2009.