An Information Secrecy Game in Cognitive Radio Networks

Yongle Wu and K. J. Ray Liu, *Fellow, IEEE*

***Abstract*—Although cognitive radio technology improves efficiency of spectrum utilization, primary users usually do not gain from opening up the spectrum in the opportunistic spectrum access, and sometimes even suffer from collisions due to secondary users' imperfect spectrum sensing. However, in this paper, we show that if information secrecy is a concern, primary users could actually be better off by allowing secondary users to cooperatively share the spectrum. Specifically, we propose a new cooperation paradigm in cognitive radio networks that primary users improve secrecy with the help of trustworthy secondary users, in the presence of an intelligent and passive eavesdropper attempting to decode primary users' messages. After deriving the achievable pair of primary users' secrecy rate and secondary users' transmission rate under various circumstances, we model the interaction between primary users and secondary users as a Stackelberg game in which transmission power levels are the key to maximize data rates. Moreover, based on a 2-D representation of how achievable rates depend on power-level regions, we apply equilibrium analysis to understand the optimal strategy of primary and secondary users. Finally, simulation results are presented to verify the performance.**

***Index Terms*—Cognitive radio, equilibrium analysis, information-theoretic secrecy, protection against eavesdropping, Stackelberg game.**

I. Introduction

As demand for spectrum resources has kept growing dramatically during the last decades, cognitive radio technology [1] has become a promising way to increase the efficiency of spectrum utilization and has received intensive research interest. In a cognitive radio network, unlicensed users (secondary users) are allowed to access licensed bands on a noninterference or limited-interference basis to legacy spectrum holders (primary users). The first class of prototypes is the opportunistic spectrum access, where secondary users sense the environment for primary users' usage of the spectrum bands, and exploit the spectrum opportunity, also known as the "white spaces," when primary users are absent, e.g., [2], [3]. Spectrum trading models represent another class of cognitive radio networks involving cooperation between primary users and secondary users: primary users trade their temporarily unused spectrum for monetary gains, while secondary users pay for short-term spectrum rights to transmit their own messages. The trade is accomplished through market mechanisms and auctions, e.g., [4], [5].

In recent years, security issues in cognitive radio networks have received growing attention. For example, a malicious user might prevent secondary users from accessing the spectrum by mimicking a primary user, and defense strategies against this "primary user emulation attack" was investigated in [6]. In [7], denial-of-service attacks were considered and potential protection remedies were discussed. In [8], another kind of malicious behavior was considered where the attacker injected interference to jam the communication of secondary users. Although most works focused on attacks targeted at secondary users, in this paper, we consider one kind of security threats to primary users: a passive but *intelligent* eavesdropper [9] who knows all channel state information (CSI) and codebooks. This malicious attacker eavesdrops upon the communications of primary users and attempts to decode some confidential messages. In face of security threats, primary users may seek help from trustworthy secondary users, if such cooperation could potentially improve the secrecy level; in return, secondary users are granted spectrum opportunities for their own transmission. In order to know the maximal data rate that can be adopted by primary users without leaking any confidential information to the eavesdropper, we will investigate the information-theoretic secrecy [10] in this cooperative cognitive radio network with an eavesdropper.

The concept of information-theoretic secrecy dates back to Wyner's seminal paper [10]. In that work, the secrecy capacity of a wiretap channel was studied, where a single source-destination communication was eavesdropped on via a degraded channel, that is, when the eavesdropper observed a degraded version of the signal received by the intended receiver. Later, this formulation was generalized to nondegraded broadcast channels with confidential information in [11], and Gaussian wiretap channels were completely understood in [12]. Assume the transmitter encoded a confidential message w into a codeword x^n for broadcasting, and the intended receiver and the eavesdropper received noisy versions y^n and z^n, respectively. The level of ignorance that the eavesdropper had with respect to w given observation z^n, i.e., the conditional entropy $(1/n)h(w|z^n)$, was defined as the *equivocation rate*. When the equivocation rate was (asymptotically) equal to the information rate of the message w, the eavesdropper hardly knew anything about the message, and this was known as *perfect secrecy*. Just like the definition of channel capacity, a rate was *achievable* if there existed a coding scheme guaranteeing an arbitrarily small error probability for sufficiently long codewords, and the *secrecy capacity* was the maximum achievable rate with perfect

Manuscript received September 14, 2010; revised January 11, 2011; accepted April 11, 2011. Date of publication April 21, 2011; date of current version August 17, 2011. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Paul Prucnal.

Y. Wu is with the Qualcomm Incorporated, San Diego, CA 92121 USA (e-mail: yonglew@qualcomm.com).

K. J. R. Liu is with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA (e-mail: kjrliu@umd.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2011.2144585

secrecy. For Gaussian wiretap channels, the secrecy capacity was the difference of mutual information of two channels, i.e., $C_S = \max\{I(X;Y) - I(X;Z), 0\}$, and stochastic encoding could achieve perfect secrecy [12].

Building on these fundamental ideas, information-theoretic secrecy has gained a renewed research interest in recent years, thanks to fast developing wireless communications technologies. The secrecy capacity of fading channels was investigated in [13], when either full CSI or only the CSI of the intended receiver was available. In [14], secrecy capacity was studied for a particular multiple-input multiple-output (MIMO) system convertible to degraded channels. The authors in [15] modeled the secrecy of a deterministic interference channel into a non-cooperative game, in which two users competed for higher secrecy rates by choosing proper message-encoding strategies. In [16], the scenario was formed as a zero-sum game by modeling the environment as the opponent player, and information secrecy was studied under different assumptions about available channel state information. Information secrecy in cooperative communication systems was analyzed in [17], where relay nodes helped secure communications between source and destination.

Recent advancement has suggested that the secret communication may benefit from coordinated external "interference" generated by other transmitters, for example, in [9], [18], and [19], the secrecy rate was shown to increase by introducing interference in one form or another, e.g., noise or random codes. However, these schemes are not ready to directly apply to cognitive radio networks, because the special features have not been taken into consideration. First, primary users are prioritized in a cognitive radio network, because they own the spectrum band. Second, we cannot assume primary users and secondary users cooperate unconditionally with each other, since they have their own interests.

Therefore, in this paper, we study the information-theoretic secrecy in a cognitive radio network. We model and analyze the achievable secrecy for a primary user, when secondary users potentially help to defeat eavesdropping while acquiring spectrum opportunities. Moreover, we propose a game-theoretic framework to understand how primary and secondary users optimize their transmission power for higher data rates, and discuss the Nash equilibrium for this information secrecy game. Contributions of the paper are summarized as follows.

First, this paper suggests a new cooperative paradigm for cognitive radio networks, where cooperative simultaneous transmissions yield mutual benefits in the presence of an eavesdropper. In traditional opportunistic spectrum access, primary users in general do not benefit from opening up the spectrum, and sometimes their performance may degrade due to occasional collisions caused by secondary users' imperfect spectrum sensing. Spectrum trading mechanisms do award primary users monetary profits, but primary users have to give up short-term spectrum rights. However, when information secrecy is a concern, primary users may benefit from simultaneous transmissions of secondary users to increase the secrecy rate, and meanwhile secondary users also benefit from transmitting their own data. This lays the foundation of mutual cooperation.

Second, the primary user's secrecy is analyzed using the information-theoretic approach. Information theory has been applied to study cognitive radio networks, for example, see [20] and references therein. Our work extends [9] to the cognitive radio network scenario where secondary users serve as the helper; however, different from [9] in which the helper simply transmits interfering coded signals bearing no useful information and [21] in which the helper sends out white noise sequences, in our work, secondary users do transmit meaningful messages for their receivers to decode. This constitutes an interference channel similar to [15] to some extent, but the roles of primary users and secondary users are asymmetric.

Third, we describe a procedure of cooperation where the primary user has the upper hand, and model the interaction between primary users and secondary users as a Stackelberg game [22]. Since in cognitive radio networks primary users and secondary users usually do not belong to the same authority or serve a common goal, it is reasonable to assume they are selfish in nature; hence, game theory has been widely applied as a flexible and proper tool to model, study, and analyze their behavior [23]. In the proposed game, the players choose power levels to maximize their payoffs, and we further show that payoff functions are piece-wise defined so that the equilibrium can be easily found through a piece-by-piece search.

The remainder of this paper is organized as follows. In Section II, the system model is described. In Section III, the achievable secrecy rate for the primary user and the information rate for the secondary user are derived for fixed power levels. The interaction between the primary user and the secondary user is modeled as a game in Section IV, followed by Section V which presents some simulation results. Section VI concludes the paper.

II. System Models

In this paper, we consider a cognitive radio network consisting of a primary user, a trustworthy secondary user, and an eavesdropping malicious user who attempts to decode the primary user's message, as shown in Fig. 1. The primary user P wants to transmit some confidential messages from the transmitter to the receiver. The secondary user S also wants to transmit some messages from the transmitter to the receiver, but since he/she does not own the spectrum band, the transmission has to be approved by P when P is active. The malicious user M, attempting to decode P's message, is a passive eavesdropper with only a receiver. We further assume the malicious user is intelligent, in the sense that M knows P's and S's codebooks and all the CSI. We focus on the simple case where each transmitter and receiver is equipped with a single antenna. In this paper, we assume channels are slow fading, and hence users cannot take advantage of fast channel variations like [13] and [24].

When P and S simultaneously transmit signals, denoted by $x_{P,k}$ and $x_{S,k}$ at time k, their receivers receive the superposition of signals from two transmitters, i.e.,

$$\begin{aligned} y_{P,k} &= h_P x_{P,k} + h_{SP} x_{S,k} + v_{P,k} \\ y_{S,k} &= h_S x_{S,k} + h_{PS} x_{P,k} + v_{S,k}. \end{aligned} \tag{1}$$

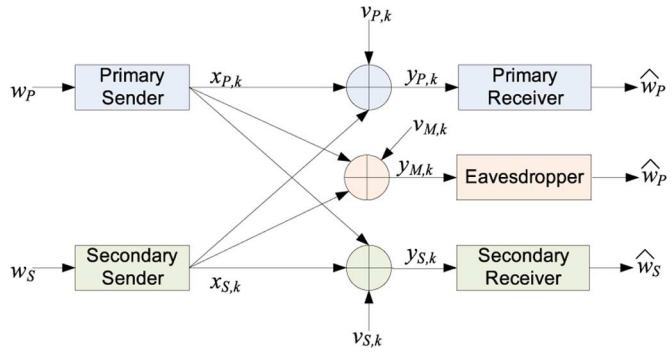

Fig. 1. Model of a cognitive radio network with an eavesdropper.

This can be viewed essentially as an interference channel [25], where h_P (or h_S) is the direct channel gain from P's (or S's) transmitter to the intended receiver, h_{SP} is the cross channel gain from S's transmitter to P's receiver, h_{PS} is from P's transmitter to S's receiver, and $v_{P,k}$ (or $v_{S,k}$) is the additive white Gaussian noise at P's (or S's) receiver. Similarly, the malicious user receives

$$y_{M,k} = h_{PM}x_{P,k} + h_{SM}x_{S,k} + v_{M,k} \tag{2}$$

where h_{PM} (or h_{SM}) is the channel gain from P's (or S's) transmitter to the eavesdropping receiver, and $v_{M,k}$ is the Gaussian noise, too. For convenience, we assume all noises have unit variances, i.e., $v_{P,k}$, $v_{S,k}$, $v_{M,k} \sim \mathcal{N}(0,1)$. In addition, we define $g_P = |h_P|^2$, $g_S = |h_S|^2$, $g_{PS} = |h_{PS}|^2$, $g_{SP} = |h_{SP}|^2$, $g_{PM} = |h_{PM}|^2$, and $g_{SM} = |h_{SM}|^2$.

The primary user encodes a confidential message $w_P \in \mathcal{W}_P$ into a n-length block codeword $x_P^n = (x_{P,1}, x_{P,2}, \ldots, x_{P,n})$ with a rate Q_P, and the secondary user encodes a message $w_S \in \mathcal{W}_S$ (w_S is independent of w_P) into $x_S^n = (x_{S,1}, x_{S,2}, \ldots, x_{S,n})$ with a rate R_S. The size of codebook $\mathcal{W}_P$ is 2^{nQ_P}, and the size of $\mathcal{W}_S$ is 2^{nR_S}. Both transmitters are power constrained, i.e.,

$$\begin{aligned} p_P &= \frac{1}{n}\sum_{k=1}^{n} |x_{P,k}|^2 \le p_P^M \\ p_S &= \frac{1}{n}\sum_{k=1}^{n} |x_{S,k}|^2 \le p_S^M. \end{aligned} \tag{3}$$

The primary user tries to recover w_P from observation, and the secondary user tries to recover w_S; an error is declared if recovered messages differ from original messages, $\hat{w}_P \neq w_P$ or $\hat{w}_S \neq w_S$. A joint encoding and decoding scheme of rate pair (Q_P, R_S) is desired such that Q_P can be made arbitrarily close to the equivocation rate $(1/n)h\left(w_P|y_M^n\right)$ and the average error probability can be made arbitrarily small, as long as n is sufficiently large. The achievable rate pair (Q_P, R_S) depends on power levels p_P and p_S.

When the secondary user is absent, the scenario reduces to the classical Gaussian wiretap channel [12], the secrecy capacity of which is known as

$$C_P\left(p_P^M\right) = \left(\gamma(g_P p_P^M) - \gamma(g_{PM} p_P^M)\right)_+ \tag{4}$$

where $\gamma(a) \triangleq (1/2)\log(1+a)$ and $(a)_+ \triangleq \max\{a, 0\}$. Note that the secrecy capacity is positive only if the eavesdropping channel has poorer quality, i.e., $g_{PM} < g_P$. With the help of a secondary user, the primary user may have a higher secrecy rate, which provides the incentive to share the spectrum band with the secondary user. The secondary user, on the other hand, is willing to join in cooperation because he/she needs such a spectrum opportunity to transmit his/her own data streams. This lays the incentive foundation of cooperation.

The potential cooperation can be established in the following procedure. The primary user first announces the power level p_P, and the secondary user responds by announcing his/her transmit power level p_S. Since the secrecy rate $C_P\left(p_P^M\right)$ is guaranteed without the secondary user's help, the primary user agrees to cooperate only when a higher secrecy rate is achievable. In this case, both users exchange necessary information (e.g., codebooks) and begin cooperative transmissions. Otherwise, the primary user rejects cooperation, and the secondary user is forbidden to use the spectrum band.

Since both users want to maximize rates of data transmission but the primary user has secrecy concerns, the primary user aims at maximizing the information secrecy rate Q_P and the secondary user aims at maximizing merely the information rate R_S. Moreover, because both users are able to manipulate transmit power levels for higher payoffs, this scenario forms a game where P and S are players, $p_P \in \left[0, p_P^M\right]$ and $p_S \in \left[0, p_S^M\right]$ are their actions, and achievable rates are their payoffs which depend on actions. We call it an *information secrecy game*, and will analyze it later.

III. Optimal Rates Under Fixed Power

In this section, we derive the achievable rate pair (Q_P, R_S) for fixed power levels (p_P, p_S). We first describe the nonsecrecy achievable rate region, and then show that the achievable secrecy rate is the difference between Pareto frontiers of two rate regions. Dividing the whole problem into four cases based on relative channel strengths, we further derive the specific expression for the optimal rate pair for each case under various conditions.

A. Achievable Rate Pairs

We first consider the interference channel without secrecy concerns. Note that the primary user can transmit with a higher rate R_P because the secrecy is not taken into account for the moment. The primary user receives the superposition of two transmitted signals, and is only interested in recovering his/her own messages. Because the primary user and the secondary user cooperate with each other and share their codebooks, the primary user can apply a joint decoding to obtain both users' messages, and then simply ignores the secondary user's message. This constitutes a multiple-access channel (MAC) [25], and the well-known capacity region is

$$\Re_P^{[\mathrm{MAC}]} = \left\{ (R_P, R_S) \middle| \begin{array}{c} 0 \le R_P \le \gamma(g_P p_P); \\ 0 \le R_S \le \gamma(g_{SP} p_S); \\ R_P + R_S \le \gamma_P. \end{array} \right\} \tag{5}$$

where $\gamma_P \triangleq \gamma(g_P p_P + g_{SP} p_S)$. When a rate R_S is too high to decode, the primary user can still attempt to decode w_P by treating the secondary user's signal as noise. The achievable rate region for this separate decoding (SD) is

$$\Re_P^{[\mathrm{SD}]} = \left\{ (R_P, R_S) \middle| \begin{array}{c} 0 \le R_P \le \gamma\left(\frac{g_P p_P}{1+g_{SP} p_S}\right); \\ R_S > \gamma(g_{SP} p_S) \end{array} \right\}. \tag{6}$$

In sum, as long as the rate pair falls into either region, the primary user is able to recover the message of interest.

Similar arguments apply to the secondary user, and the two regions are written as

$$\Re_S^{[\mathrm{MAC}]} = \left\{ (R_P, R_S) \middle| \begin{array}{c} 0 \le R_P \le \gamma(g_{PS} p_P); \\ 0 \le R_S \le \gamma(g_S p_S); \\ R_P + R_S \le \gamma_S. \end{array} \right\} \quad (7)$$

with $\gamma_S \triangleq \gamma(g_{PS} p_P + g_S p_S)$, and

$$\Re_S^{[\mathrm{SD}]} = \left\{ (R_P, R_S) \middle| \begin{array}{c} R_P > \gamma(g_{PS} p_P); \\ 0 \le R_S \le \gamma\left(\frac{g_S p_S}{1+g_{PS} p_P}\right) \end{array} \right\}. \quad (8)$$

Therefore, for any rate pair (R_P, R_S) inside the region

$$\Re^{[\mathrm{COOP}]} = \left\{ \Re_P^{[\mathrm{MAC}]} \cup \Re_P^{[\mathrm{SD}]} \right\} \cap \left\{ \Re_S^{[\mathrm{MAC}]} \cup \Re_S^{[\mathrm{SD}]} \right\} \quad (9)$$

both users are able to recover their own messages by either joint decoding or separate decoding.

Although the achievable rate region (9) is identical to the capacity region when $g_P \le g_{PS}$ and $g_S \le g_{SP}$ [26], it is worth pointing out that in general it is by no means the capacity of the interference channel which is still an open problem, and even not the best achievable rate region known to date. However, (9) can be achievable by simple encoding and decoding operations. A straightforward enlargement of a nonconvex rate region to its convex closure can be done by time sharing, but as shown later, time sharing will not help when secrecy is considered. Going beyond time sharing requires much more sophisticated coding methods such as the HK scheme [26], and hence we will focus on the principal achievable region (9) in this paper.

From the eavesdropper's point of view, who is only interested in the primary user's message, the decodable rate pair also has to fall into either the MAC region

$$\Re_M^{[\mathrm{MAC}]} = \left\{ (R_P, R_S) \middle| \begin{array}{c} 0 \le R_P < \gamma(g_{PM} p_P); \\ 0 \le R_S < \gamma(g_{SM} p_S); \\ R_P + R_S < \gamma_M. \end{array} \right\} \quad (10)$$

where $\gamma_M \triangleq \gamma(g_{PM} p_P + g_{SM} p_S)$, or the separate decoding region

$$\Re_M^{[\mathrm{SD}]} = \left\{ (R_P, R_S) \middle| \begin{array}{c} 0 \le R_P < \gamma\left(\frac{g_{PM} p_P}{1+g_{SM} p_S}\right); \\ R_S > \gamma(g_{SM} p_S). \end{array} \right\}. \quad (11)$$

In other words, correctly decoding messages with a rate pair outside the two regions is beyond the eavesdropper's capability.

Theorem 1: The rate pair (Q_P, R_S) is achievable if there exist rates $R_P > R_{PM} > 0$ such that

$$\begin{cases} Q_P = R_P - R_{PM}, \\ (R_P, R_S) \in \Re^{[\mathrm{COOP}]}, \\ (R_{PM}, R_S) \notin \left\{ \Re_M^{[\mathrm{MAC}]} \cup \Re_M^{[\mathrm{SD}]} \right\}. \end{cases} \quad (12)$$

Proof: The proof follows [9]. To achieve a rate pair (Q_P, R_S), both the primary user and the secondary user employ independent Gaussian random coding. Specifically, the secondary user uses a codebook with size 2^{nR_S}; the primary user generates 2^{nR_P} codewords and randomly groups them into 2^{nQ_P} bins. Each bin, associated with a unique confidential message $w_P \in \mathcal{W}_P$, contains $2^{nR_P - nQ_P} = 2^{nR_{PM}}$ codewords, and given a message w_P, one of the codewords will be randomly selected from the corresponding bin. Recall that $\Re^{[\mathrm{COOP}]}$ is the rate region that ensures both the primary user and the secondary user to decode their own messages correctly. For example, the primary user knows which exact codeword has been transmitted, and recovers the message from the index of the bin which the codeword falls into. Moreover, the third condition in (12) implies that deciding which codeword in the bin (the dummy information has a rate of R_{PM}) is already beyond the eavesdropper's capability, let alone the bin index that actually conveys real messages. Therefore, the primary user achieves a secrecy rate Q_P while the secondary user can transmit with the rate R_S. ■

Note that the achievable rate pairs given by Theorem 1 are not unique in general, and we need to find the "optimal" one from all candidates. Because the primary user has higher priority than the secondary user, it is reasonable to satisfy the primary user first. Denote the set of all achievable rate pairs satisfying constraints (12) as $\Re^{[\mathrm{SEC}]}$, and the optimal secrecy rate of the primary user can be found as

$$Q_P^\star = \max\left\{ Q_P \middle| (Q_P, R_S) \in \Re^{[\mathrm{SEC}]} \right\}. \quad (13)$$

Given $Q_P^\star$ for the primary user, the secondary user achieves the rate

$$R_S^\star = \max\left\{ R_S \middle| (Q_P^\star, R_S) \in \Re^{[\mathrm{SEC}]} \right\}. \quad (14)$$

The following proposition justifies our approach that excludes time sharing in the achievability scheme.

Proposition 1: Allowing time sharing in primary–secondary cooperation cannot help to improve the optimal rate pair $(Q_P^\star, R_S^\star)$.

Proof: See Appendix A. ■

B. Pareto Frontiers

Given a rate R_S, maximizing Q_P means maximizing the difference between R_P and R_{PM} $(R_P > R_{PM})$ according to (12). It requires moving R_P upwards to the Pareto frontier of the region $\Re^{[\mathrm{COOP}]}$ and moving R_{PM} downwards to approach the frontier of $\left\{ \Re_M^{[\mathrm{MAC}]} \cup \Re_M^{[\mathrm{SD}]} \right\}$. As a result, when the rate region is plotted in an R_P–R_S plane (R_S is the x-axis), $Q_P^\star$ can be viewed as the maximum vertical difference between these two frontiers, i.e., $Q_P^\star = \max_{R_S} Q_P(R_S)$, and

$$Q_P(R_S) = \left(f_C(R_S) - f_M(R_S)\right)_+ \quad (15)$$

where $f_M(R_S)$ denotes the frontier of $\left\{ \Re_M^{[\mathrm{MAC}]} \cup \Re_M^{[\mathrm{SD}]} \right\}$, and $f_C(R_S)$ denotes the frontier of $\Re^{[\mathrm{COOP}]}$.

It is easy to characterize $f_M(R_S)$ as a function of R_S

$$f_M(R_S) = \begin{cases} \gamma(g_{PM} p_P), & \text{if } 0 \le R_S < \gamma\left(\frac{g_{SM} p_S}{1+g_{PM} p_P}\right) \\ \gamma_M - R_S, & \text{if } \gamma\left(\frac{g_{SM} p_S}{1+g_{PM} p_P}\right) \le R_S < \gamma(g_{SM} p_S) \\ \gamma\left(\frac{g_{PM} p_P}{1+g_{SM} p_S}\right), & \text{if } R_S \ge \gamma(g_{SM} p_S) \end{cases} \quad (16)$$

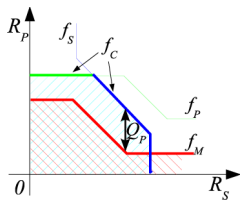

Fig. 2. Illustration of Pareto frontiers and the achievable secrecy rate.

which is a linear function with $f'_M(R_S) = -1$ in the central segment, and keeps constant elsewhere. We use $f'(\cdot)$ to denote the right derivative of $f(\cdot)$ throughout the paper. Similarly, the frontier of $\left\{\Re_P^{[\mathrm{MAC}]} \cup \Re_P^{[\mathrm{SD}]}\right\}$ is

$$f_P(R_S) = \begin{cases} \gamma(g_P p_P), & \text{if } 0 \le R_S < \gamma\left(\frac{g_{SP}p_S}{1+g_P p_P}\right) \\ \gamma_P - R_S, & \text{if } \gamma\left(\frac{g_{SP}p_S}{1+g_P p_P}\right) \le R_S < \gamma(g_{SP}p_S) \\ \gamma\left(\frac{g_P p_P}{1+g_{SP}p_S}\right), & \text{if } R_S \ge \gamma(g_{SP}p_S) \end{cases} \tag{17}$$

and the frontier of $\left\{\Re_S^{[\mathrm{MAC}]} \cup \Re_S^{[\mathrm{SD}]}\right\}$ is

$$f_S(R_S) = \begin{cases} +\infty, & \text{if } 0 \le R_S \le \gamma\left(\frac{g_S p_S}{1+g_{PS}p_P}\right) \\ \gamma_S - R_S, & \text{if } \gamma\left(\frac{g_S p_S}{1+g_{PS}p_P}\right) < R_S \le \gamma(g_S p_S) \\ 0, & \text{if } R_S > \gamma(g_S p_S). \end{cases} \tag{18}$$

Since $\Re^{[\mathrm{COOP}]}$ is the intersection of the two regions, $f_C(R_S)$ equals $\min(f_P(R_S), f_S(R_S))$, and its domain can be limited to $[0, \gamma(g_S p_S)]$ because $f_C(R_S) = 0$ when $R_S > \gamma(g_S p_S)$. It is easy to see that $f_C(R_S)$ is a nonincreasing function with $f'_C(R_S) = 0$ or -1 except discontinuous points; however, its specific form depends heavily on the channel conditions, and we discuss four cases according to relative channel strengths:

Case A) $g_P \le g_{PS}$ and $g_S \le g_{SP}$ (strong interference);
Case B) $g_P > g_{PS}$ and $g_S \le g_{SP}$ (P in a better position);
Case C) $g_P \le g_{PS}$ and $g_S > g_{SP}$ (S in a better position);
Case D) $g_P > g_{PS}$ and $g_S > g_{SP}$ (weak interference).

Fig. 2 illustrates the secrecy rate by an example of Case A, where the frontiers $f_M(R_S)$, $f_P(R_S)$, $f_S(R_S)$, and $f_C(R_S)$ are plotted. The shaded regions are $\Re^{[\mathrm{COOP}]}$ and $\left\{\Re_M^{[\mathrm{MAC}]} \cup \Re_M^{[\mathrm{SD}]}\right\}$. Then, the gap between the two Pareto frontiers in bold lines is the secrecy rate achievable by stochastic coding.

Proposition 2: The frontier of the cooperative rate region $f_C(R_S)$ defined on the interval $[0, \gamma(g_S p_S)]$ is specified for all four cases as follows:

$$f_C^A(R_S) = \begin{cases} \gamma(g_P p_P), & \text{if } R_S \le \min(\gamma_P, \gamma_S) - \gamma(g_P p_P) \\ \min(\gamma_P, \gamma_S) - R_S, & \text{if}^* \ R_S > \min(\gamma_P, \gamma_S) - \gamma(g_P p_P). \end{cases}$$

$$f_C^B(R_S) = \begin{cases} \gamma(g_P p_P), & \text{if } R_S \le \min\left(\gamma\left(\frac{g_{SP}p_S}{1+g_P p_P}\right), \gamma\left(\frac{g_S p_S}{1+g_{PS}p_P}\right)\right) \\ \gamma_P - R_S, & \text{if}^* \ \gamma\left(\frac{g_{SP}p_S}{1+g_P p_P}\right) < R_S \le \gamma\left(\frac{g_S p_S}{1+g_{PS}p_P}\right) \\ \gamma_S - R_S, & \text{if } R_S > \gamma\left(\frac{g_S p_S}{1+g_{PS}p_P}\right). \end{cases}$$

$$f_C^C(R_S) = \begin{cases} \gamma(g_P p_P), & \text{if } R_S < \gamma\left(\frac{g_{SP}p_S}{1+g_P p_P}\right) \\ \gamma_P - R_S, & \text{if } \gamma\left(\frac{g_{SP}p_S}{1+g_P p_P}\right) \le R_S < \gamma(g_{SP}p_S) \\ \gamma\left(\frac{g_P p_P}{1+g_{SP}p_S}\right), & \text{if } \gamma(g_{SP}p_S) \le R_S \le \\ & \gamma_S - \gamma\left(\frac{g_P p_P}{1+g_{SP}p_S}\right) \\ \gamma_S - R_S, & \text{if}^* \ R_S > \gamma_S - \gamma\left(\frac{g_P p_P}{1+g_{SP}p_S}\right). \end{cases}$$

$$f_C^D(R_S) = \begin{cases} \gamma(g_P p_P), & \text{if } R_S < \gamma\left(\frac{g_{SP}p_S}{1+g_P p_P}\right) \\ \gamma_P - R_S, & \text{if } \gamma\left(\frac{g_{SP}p_S}{1+g_P p_P}\right) \le R_S \\ & \le \min\left(\gamma(g_{SP}p_S), \gamma\left(\frac{g_S p_S}{1+g_{PS}p_P}\right)\right) \\ \gamma\left(\frac{g_P p_P}{1+g_{SP}p_S}\right), & \text{if}^* \ \gamma(g_{SP}p_S) \le R_S \le \\ & \max\left(\gamma\left(\frac{g_S p_S}{1+g_{PS}p_P}\right), \gamma_S - \gamma\left(\frac{g_P p_P}{1+g_{SP}p_S}\right)\right) \\ \gamma_S - R_S, & \text{if } R_S > \\ & \max\left(\gamma\left(\frac{g_S p_S}{1+g_{PS}p_P}\right), \gamma_S - \gamma\left(\frac{g_P p_P}{1+g_{SP}p_S}\right)\right). \end{cases}$$

The segments that may be missing under certain conditions are marked by "if*". For all cases, $f_C(R_S)$ is a nonincreasing function of R_S, and $f_C(R_S)$ is continuous within the interval $[0, \gamma(g_S p_S)]$ except a discontinuous point at $R_S = \gamma(g_S p_S/1 + g_{PS}p_P)$ in Case B and possibly Case D (when $p_S < (g_P/g_{PS} - 1)/g_{SP}$ or $p_S < p_P(g_P - g_{PS})/(g_S - g_{SP})$).

Proof: See Appendix B. ∎

C. Optimal Rate Pair

Recall that the primary user reserves the right not to cooperate with the secondary user unless cooperation yields a higher secrecy rate than the bottom line C_P given in (4). Therefore, the overall achievable rate pair is

$$(\overline{Q_P}, \overline{R_S}) = \begin{cases} (Q_P^\star, R_S^\star), & \text{if } Q_P^\star > C_P \\ (C_P, 0), & \text{otherwise} \end{cases} \tag{19}$$

which is always bounded below by C_P. We could relax the definition of Q_P without affecting rates $(\overline{Q_P}, \overline{R_S})$, e.g., by removing the nonnegative constraint. Slightly abusing the notations, we keep using the same notations after relaxation.

Proposition 3: Relaxing the definition of Q_P in (15) to $Q_P(R_S) \triangleq f_C(R_S) - \overline{f_M}(R_S)$ will not affect $(\overline{Q_P}, \overline{R_S})$, where $\overline{f_M}(R_S)$ inherits from $f_M(R_S)$ except extending the line segment $\gamma_M - R_S$ to the entire range $[0, \gamma(g_{SM}p_S)]$. Then, the optimal rate pair $(Q_P^\star, R_S^\star)$ defined in (13) and (14) is given by $Q_P^\star = Q_P(R_S^\star) = Q_P\left(R_S^\dagger\right)$ and $R_S^\star = \max\{R | Q_P(R) = Q_P^\star\}$, where the auxiliary variable $R_S^\dagger$ is

$$R_S^\dagger = \begin{cases} \gamma\left(\frac{g_S p_S}{(1+g_{PS}p_P)}\right), & (C1) \\ \min(\gamma(g_S p_S), \gamma(g_{SM}p_S)) & \text{otherwise} \end{cases}$$

with condition $(C1)$ being that $f_C(R_S)$ is discontinuous at $\gamma(g_S p_S/(1 + g_{PS}p_P))$ and $g_S/(1 + g_{PS}p_P) \le g_{SM}$. Furthermore, $R_S^\star$ differs from $R_S^\dagger$ only when $R_S^\dagger = \gamma(g_{SM}p_S)$ and $f'_C(\gamma(g_{SM}p_S)) = 0$.

Proof: See Appendix C. ∎

To sum up, $(Q_P^\star, R_S^\star)$ is first calculated from Proposition 3. If $Q_P^\star \leq C_P$, the primary user does not bother to cooperate, receiving a bottom line secrecy rate C_P; otherwise, the primary user has the incentive to cooperate, stochastically encoding using the scheme in Theorem 1 with $R_P = f_C(R_S^\star), R_{PM} = f_M(R_S^\star)$, and allowing the secondary user to transmit with the rate $R_S^\star$.

To obtain a more specific expression of $(Q_P^\star, R_S^\star)$, we need more subcases and branches within each case to deal with conditions in Proposition 3 and loose expressions like $\min(\cdot,\cdot)$ in Proposition 2. The results are summarized in Theorem 2. For conciseness, we define the following terms for common use:

$$\begin{aligned}
\gamma_{Q1} &= \gamma(g_P p_P) - \gamma\left(\frac{g_{PM}p_P}{(1+g_{SM}p_S)}\right)\\
\gamma_{Q2} &= \gamma(g_P p_P + g_{SP}p_S) - \gamma(g_{PM}p_P + g_{SM}p_S)\\
\gamma_{Q3} &= \gamma(g_{PS}p_P + g_S p_S) - \gamma(g_{PM}p_P + g_{SM}p_S)\\
\gamma_{Q4} &= \gamma\left(\frac{g_P p_P}{(1+g_{SP}p_S)}\right) - \gamma\left(\frac{g_{PM}p_P}{(1+g_{SM}p_S)}\right)\\
\gamma_{Q5} &= \gamma(g_P p_P) + \gamma(g_S p_S) - \gamma_M\\
\gamma_{Q6} &= \gamma(g_P p_P) + \gamma\left(\frac{g_S p_S}{(1+g_{PS}p_P)}\right) - \gamma_M\\
\gamma_{Q7} &= \gamma(g_S p_S) + \gamma\left(\frac{g_P p_P}{(1+g_{SP}p_S)}\right) - \gamma_M\\
\gamma_{Q8} &= \gamma\left(\frac{g_P p_P}{(1+g_{SP}p_S)}\right) + \gamma\left(\frac{g_S p_S}{(1+g_{PS}p_P)}\right)\\
&\quad - \gamma_M\\
\gamma_{R1} &= \gamma(g_{SM}p_S)\\
\gamma_{R2} &= \gamma(g_S p_S)\\
\gamma_{R3} &= \gamma\left(\frac{g_{SP}p_S}{(1+g_P p_P)}\right)\\
\gamma_{R4} &= \gamma\left(\frac{g_S p_S}{(1+g_{PS}p_P)}\right)\\
\gamma_{R5} &= \gamma_S - \gamma\left(\frac{g_P p_P}{(1+g_{SP}p_S)}\right)\\
\gamma_{R6} &= \gamma_S - \gamma(g_P p_P).
\end{aligned} \tag{20}$$

Theorem 2: The rate pair $(Q_P^\star, R_S^\star)$ takes one simple closed-form expression from the candidate list, i.e., (21) to (43) in what follows, depending on the channel gains and power levels.

Proof: It follows Proposition 3 straightforwardly by dealing with different conditions, and hence we omit the detailed proofs. ■

♢ **Case A)** $g_P \leq g_{PS}, g_S \leq g_{SP}$

Subcase A1) When $p_P \leq (g_{SP}/g_S - 1)/g_P$ and $p_S \leq (g_{PS}/g_P - 1)/g_S$.

If $g_{SM} \geq g_S$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q5}, \gamma_{R2}). \tag{21}$$

If $g_{SM} < g_S$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q1}, \gamma_{R2}). \tag{22}$$

Subcase A2) When $p_P > (g_{SP}/g_S - 1)/g_P$ and $(g_{PS} - g_P)p_P \geq (g_{SP} - g_S)p_S$.

If $p_P \leq (g_{SP}/g_{SM} - 1)/g_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q1}, \gamma_{R3}). \tag{23}$$

If $p_P > (g_{SP}/g_{SM} - 1)/g_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q2}, \min\{\gamma_{R1}, \gamma_{R2}\}). \tag{24}$$

Subcase A3) When $p_S > (g_{PS}/g_P - 1)/g_S$ and $(g_{SP} - g_S)p_S > (g_{PS} - g_P)p_P$.

If $g_{SM}p_S + g_P p_P + g_{SM}p_S g_P p_P \leq g_S p_S + g_{PS}p_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q1}, \gamma_{R6}). \tag{25}$$

If $g_{SM}p_S + g_P p_P + g_{SM}p_S g_P p_P > g_S p_S + g_{PS}p_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q3}, \min\{\gamma_{R1}, \gamma_{R2}\}). \tag{26}$$

♢ **Case B)** $g_P > g_{PS}, g_S \leq g_{SP}$

Subcase B1) When $g_S + g_P g_S p_P \leq g_{SP} + g_{SP}g_{PS}p_P$.

If $p_P \leq (g_S/g_{SM} - 1)/g_{PS}$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q1}, \gamma_{R4}). \tag{27}$$

If $p_P > (g_S/g_{SM} - 1)/g_{PS}$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q6}, \gamma_{R4}). \tag{28}$$

Subcase B2) When $g_S + g_P g_S p_P > g_{SP} + g_{SP}g_{PS}p_P$.

If $p_P \leq (g_{SP}/g_{SM} - 1)/g_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q1}, \gamma_{R3}). \tag{29}$$

If $p_P > (g_{SP}/g_{SM} - 1)/g_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q2}, \min\{\gamma_{R1}, \gamma_{R4}\}). \tag{30}$$

♢ **Case C)** $g_P \leq g_{PS}, g_S > g_{SP}$

Subcase C1) When $g_P + g_P g_S p_S \leq g_{PS} + g_{SP}g_{PS}p_S$.

If $g_{SM} < g_{SP}$ and $p_P \leq (g_{SP}/g_{SM} - 1)/g_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q1}, \gamma_{R3}). \tag{31}$$

If $g_{SM} < g_{SP}$ and $p_P > (g_{SP}/g_{SM} - 1)/g_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q2}, \gamma_{R1}). \tag{32}$$

If $g_{SP} \leq g_{SM} \leq g_S$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q4}, \gamma_{R2}). \tag{33}$$

If $g_{SM} > g_S$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q7}, \gamma_{R2}). \tag{34}$$

Subcase C2) When $g_P + g_P g_S p_S > g_{PS} + g_{SP}g_{PS}p_S$.

If $g_{SM} < g_{SP}$ and $p_P \leq (g_{SP}/g_{SM} - 1)/g_P$, the same as (31).

If $g_{SM} < g_{SP}$ and $p_P > (g_{SP}/g_{SM} - 1)/g_P$, the same as (32).

If $g_{SM} \geq g_{SP}$ and $(1 + g_{SP}p_S)(g_{PS}p_P + g_S p_S - g_{SM}p_S) \geq (1 + g_{SM}p_S)g_P p_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q4}, \gamma_{R5}). \tag{35}$$

If $g_{SM} \geq g_{SP}$ and $(1+g_{SP}p_S)(g_{PS}p_P + g_S p_S - g_{SM}p_S) < (1+g_{SM}p_S)g_P p_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q3}, \min\{\gamma_{R1}, \gamma_{R2}\}). \tag{36}$$

♢ **Case D)** $g_P > g_{PS}$, $g_S > g_{SP}$

Subcase D1) When $p_P < (g_S/g_{SP} - 1)/g_{PS}$ and $p_S < (g_P/g_{PS} - 1)/g_{SP}$.

If $g_{SM} < g_{SP}$ and $p_P \leq (g_{SP}/g_{SM} - 1)/g_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q1}, \gamma_{R3}). \tag{37}$$

If $g_{SM} < g_{SP}$ and $p_P > (g_{SP}/g_{SM} - 1)/g_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q2}, \gamma_{R1}). \tag{38}$$

If $g_{SM} \geq g_{SP}$ and $p_P \leq (g_S/g_{SM} - 1)/g_{PS}$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q4}, \gamma_{R4}). \tag{39}$$

If $g_{SM} \geq g_{SP}$ and $p_P > (g_S/g_{SM} - 1)/g_{PS}$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q8}, \gamma_{R4}). \tag{40}$$

Subcase D2) When $p_P \geq (g_S/g_{SP} - 1)/g_{PS}$ and $(g_P - g_{PS})p_P > (g_S - g_{SP})p_S$

If $p_P \leq (g_{SP}/g_{SM} - 1)/g_P$, the same as (37).

If $(g_{SP}/g_{SM} - 1)/g_P < p_P \leq (g_S/g_{SM} - 1)/g_{PS}$, the same as (38).

If $p_P > (g_S/g_{SM} - 1)/g_{PS}$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q2}, \gamma_{R4}). \tag{41}$$

Subcase D3) When $p_S \geq (g_P/g_{PS} - 1)/g_{SP}$ and $(g_S - g_{SP})p_S \geq (g_P - g_{PS})p_P$.

If $g_{SM} < g_{SP}$ and $p_P \leq (g_{SP}/g_{SM} - 1)/g_P$, the same as (37).

If $g_{SM} < g_{SP}$ and $p_P > (g_{SP}/g_{SM} - 1)/g_P$, the same as (38).

If $g_{SM} \geq g_{SP}$ and $(1+g_{SP}p_S)(g_S p_S + g_{PS}p_P - g_{SM}p_S) \geq (1+g_{SM}p_S)g_P p_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q4}, \gamma_{R5}). \tag{42}$$

If $g_{SM} \geq g_{SP}$ and $(1+g_{SP}p_S)(g_S p_S + g_{PS}p_P - g_{SM}p_S) < (1+g_{SM}p_S)g_P p_P$,

$$(Q_P^\star, R_S^\star) = (\gamma_{Q3}, \min\{\gamma_{R1}, \gamma_{R2}\}). \tag{43}$$

To sum up, $R_S^\star$ takes one of the six candidate forms $\{\gamma_{Rk}, k = 1, 2, \ldots, 6\}$ depending on the cases and subcases. Let us take a closer look at these candidate forms. $\gamma_{R1} = \gamma(g_{SM}p_S)$ is the critical rate that the malicious user could decode the secondary user's message in the ideal case; in general, transmitting a higher rate than γ_{R1} does not bring further difficulty to the eavesdropper's decoding, but instead affects the primary user's achievable rate. $\gamma_{R2} = \gamma(g_S p_S)$ is the highest possible rate for the secondary user, beyond which no message would be decodable even with perfect interference cancellation. γ_{R4} corresponds to condition (C1) in Proposition 3. The rest forms correspond to the situation where there are multiple R_S's that attains $Q_P^\star$, and thus the maximum R_S is selected as $R_S^\star$ according to (14), although the specific form varies case by case. $Q_P^\star$ is the difference of decodable rates of the primary user and the eavesdropper, i.e., $f_C(R_S^\star) - \overline{f_M}(R_S^\star)$ according to Proposition 3. Therefore, it takes the form of rate differences, i.e., one of the possible forms $\{\gamma_{Qk}, k = 1, 2, \ldots, 8\}$ depending on the specific condition.

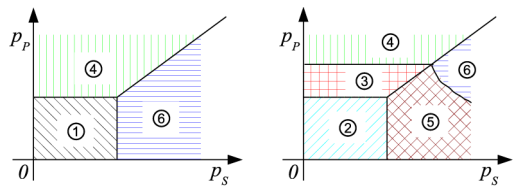

Fig. 3. Illustration of rate-pair regions on the p_P–p_S plane for Case A.

IV. Information Secrecy Game

We have derived achievable $(\overline{Q_P}, \overline{R_S})$ in Section III given fixed power levels p_P and p_S. However, both users have the freedom to select their power under the power constraint $p_P \in [0, p_P^M]$ and $p_S \in [0, p_S^M]$, and they have the incentive to manipulate power levels for a higher rate. We write down the achievable rates as functions of power levels, e.g., $\overline{Q_P}(p_P, p_S)$ and $\overline{R_S}(p_P, p_S)$, to emphasize the dependence.

In this section, we first demonstrate how rate pairs depend on power levels through a 2-D plane representation. Then, we model the cooperation between the primary user and the secondary user as a Stackelberg game, and discuss the game equilibrium in light of the 2-D representation. Finally, we extend the game to the multiuser case.

A. 2-D Representation

The payoff $(\overline{Q_P}(p_P, p_S), \overline{R_S}(p_P, p_S))$ is closely related to $(Q_P^\star(p_P, p_S), R_S^\star(p_P, p_S))$ whose expressions seem rather involved in Theorem 2, because of numerous cases, subcases, and additional branches. Although varying power levels will not change which case it belongs to (cases are divided purely by the CSI), different power combinations may activate different subcases and/or branches. To circumvent the difficulty, we "translate" the conditions of subcases and branches into the regions on a p_P–p_S plane, and visually show how $(Q_P^\star(p_P, p_S), R_S^\star(p_P, p_S))$ depends on power levels. Discussing the equilibrium on this 2-D plane is much easier.

For Case A, the p_P–p_S plane is divided into regions of different rate expressions, as shown in Fig. 3, where the left one corresponds to the scenario $g_{SM} \geq g_S$, and the right one is for $g_{SM} < g_S$. The equations of rate pair associated with each region are: ① ∼ (21); ② ∼ (22); ③ ∼ (23); ④ ∼ (24); ⑤ ∼ (25); ⑥ ∼ (26). We use circled numbers to denote the regions. The boundaries in the left figure are $p_P = (g_{SP}/g_S - 1)/g_P$ (between ① and ④), $p_S = (g_{PS}/g_P - 1)/g_S$ (between ① and ⑥), and $(g_{PS} - g_P)p_P = (g_{SP} - g_S)p_S$ (between ④ and ⑥). Two additional boundaries can be found in the right figure, $p_P = (g_{SP}/g_{SM} - 1)/g_P$ (between ③ and ④) and $g_{SM}p_S + g_P p_P + g_{SM}p_S g_P p_P = g_S p_S + g_{PS}p_P$ (between ⑤ and ⑥).

Fig. 4 shows the regions for Case B. The left figure holds when $g_{SM} > (g_P g_S - g_{SP}g_{PS})/(g_P - g_{PS})$, and the right one holds otherwise. The corresponding equations for each region are: ① ∼ (27); ② ∼ (28); ③ ∼ (29); ④ ∼ (30). The

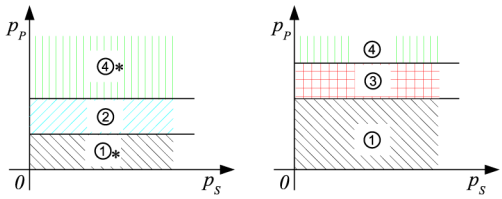

Fig. 4. Illustration of rate-pair regions on the p_P–p_S plane for Case B.

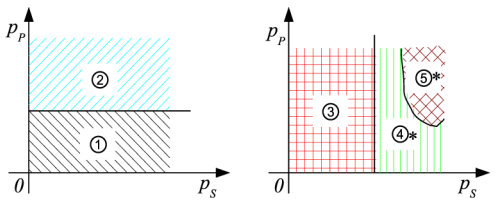

Fig. 5. Illustration of rate-pair regions on the p_P–p_S plane for Case C.

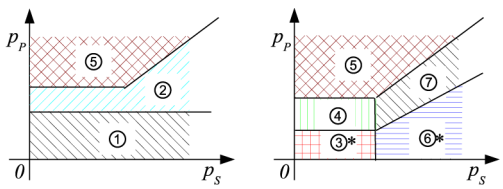

Fig. 6. Illustration of rate-pair regions on the p_P–p_S plane for Case D.

boundaries are $p_P = (g_{SP} - g_S)/(g_P g_S - g_{SP} g_{PS})$ (between ② and ④, or between ① and ③), $p_P = (g_S/g_{SM} - 1)/g_{PS}$ (between ① and ②), and $p_P = (g_{SP}/g_{SM} - 1)/g_P$ (between ③ and ④). Note that under certain conditions some regions may not exist and the corresponding boundaries are invalid (e.g., negative or infinity), and we mark such regions with a "*" in the figure.

Case C is illustrated in Fig. 5, where the mappings are ① $\sim$ (31); ② $\sim$ (32); ③ $\sim$ (33) when $g_{SP} \le g_{SM} \le g_S$ or (34) when $g_{SM} > g_S$; ④ $\sim$ (35); ⑤ $\sim$ (36). When $g_{SM} < g_{SP}$, the left figure applies, with the boundary $p_P = (g_{SP}/g_{SM} - 1)/g_P$. Otherwise, the right figure applies, with the boundary $p_S = (g_{PS} - g_P)/(g_P g_S - g_{SP} g_{PS})$, but when $g_P g_S \le g_{SP} g_{PS}$, the boundary is invalid and the entire plane is a single region. The boundary between ④ and ⑤, when existing, is $(1 + g_{SP} p_S)(g_{PS} p_P + g_S p_S - g_{SM} p_S) = (1 + g_{SM} p_S) g_P p_P$.

Finally, the regions for Case D are presented in Fig. 6 with corresponding equations: ① $\sim$ (37); ② $\sim$ (38); ③ $\sim$ (39); ④ $\sim$ (40); ⑤ $\sim$ (41); ⑥ $\sim$ (42); ⑦ $\sim$ (43). The left figure corresponds to $g_{SM} < g_{SP}$ whereas the right one corresponds to $g_{SM} \ge g_{SP}$. The boundaries are: $p_P = (g_{SP}/g_{SM} - 1)/g_P$ (between ① and ②), $(g_P - g_{PS}) p_P = (g_S - g_{SP}) p_S$ and $p_P = (g_S/g_{SM} - 1)/g_{PS}$ (between ② and ⑤), $p_P = (g_S/g_{SM} - 1)/g_{PS}$ (between ③ and ④), $(1 + g_{SP} p_S)(g_{PS} p_P + g_S p_S - g_{SM} p_S) = (1 + g_{SM} p_S) g_P p_P$ (between ⑥ and ⑦), $p_P = (g_S/g_{SP} - 1)/g_{PS}$ (between ④ and ⑤), $(g_P - g_{PS}) p_P = (g_S - g_{SP}) p_S$ (between ⑤ and ⑦), $p_S = (g_P/g_{PS} - 1)/g_{SP}$ (between ③④ and ⑥⑦).

B. Stackelberg Game

Recall that in the cooperation procedure, the primary user announces p_P first, the secondary user responds with p_S, and finally the primary user decides whether to cooperate. This can be modeled as a *Stackelberg game* with two *players*: the primary user is the *leader*, while the secondary user is the *follower*. Their *payoffs* are the secrecy rate $\overline{Q_P}(p_P, p_S)$ and the information rate $\overline{R_S}(p_P, p_S)$, respectively, which depend on their *actions* p_P and p_S. To understand the interaction between users, we discuss the *Nash equilibrium* of this information secrecy game based on the 2-D representation.

For a given p_P, a horizontal line segment can be drawn on the p_P–p_S plane with $p_S \in [0, p_S^M]$, which may remain in a single region or cross several regions. Depending on which regions have been passed through, $R_S^\star(p_P, p_S)$ and $Q_P^\star(p_P, p_S)$ may be piece-wise defined functions. The optimal power level $p_S^\star$ is a function of p_P

$$p_S^\star(p_P) = \arg\max_{p_S \in [0, p_S^M]} R_S^\star(p_P, p_S) \quad \text{s.t. } Q_P^\star(p_P, p_S) > C_P. \tag{44}$$

The constraint comes from that $\overline{R_S}(p_P, p_S) = R_S^\star(p_P, p_S)$ only when the primary user is willing to cooperate. Predicting that the secondary user will choose the optimal power $p_S^\star(p_P)$ for an announced power level p_P, the primary user is able to maximize the payoff by announce the power level $p_P^\star$ such that his/her own secrecy rate is maximized.

Searching for the maximum can be done piece by piece, and some monotonic properties are given in Propositions 4 and 5, with $a \overset{s}{\sim} b$ denoting that a and b have the same sign.

Proposition 4: With p_P fixed, the signs of first-order partial derivatives are as follows: $\partial\gamma_{Rj}/\partial p_S > 0$ for all $j = 1, 2, \ldots, 6$, $\partial\gamma_{Q1}/\partial p_S > 0$, and

$$\begin{aligned}
\frac{\partial\gamma_{Q2}}{\partial p_S} &\overset{s}{\sim} g_{SP}(1 + g_{PM} p_P) - g_{SM}(1 + g_P p_P) \\
\frac{\partial\gamma_{Q3}}{\partial p_S} &\overset{s}{\sim} \frac{\partial\gamma_{Q6}}{\partial p_S} \\
&\overset{s}{\sim} g_S(1 + g_{PM} p_P) - g_{SM}(1 + g_{PS} p_P) \\
\frac{\partial\gamma_{Q5}}{\partial p_S} &\overset{s}{\sim} g_S(1 + g_{PM} p_P) - g_{SM}.
\end{aligned}$$

All the above functions are monotonic when p_P is given. The rest functions share the same quadratic form, for $j = 4, 7, 8$

$$\frac{\partial\gamma_{Qj}}{\partial p_S} \overset{s}{\sim} F p_S^2 + 2(AC - BD) p_S + (AC - BD)(B + D) - BDF$$

where $F = B + D - A - C$, $A = (g_P p_P + 1)/g_{SP}$, $B = (g_{PM} p_P + 1)/g_{SM}$, $D = 1/g_{SP}$, and the parameter C is as follows: $C = 1/g_{SM}$ for γ_{Q4}, $C = 1/g_S$ for γ_{Q7}, and $C = (1 + g_{PS} p_P)/g_S$ for γ_{Q8}.

Proof: All can be proved through basic calculations and first-order derivatives, and we omit the details. ■

Proposition 5: With p_P fixed, $R_S^\star(p_P, p_S)$ is a strictly increasing function with regard to p_S.

Proof: See Appendix D. ■

Theorem 3: The power levels $(p_P^\star, p_S^\star(p_P^\star))$ are the Nash equilibrium of the proposed game, where

$$p_S^\star(p_P) = \max\left\{ p_S \in [0, p_S^M] \middle| Q_P^\star(p_P, p_S) > C_P \right\} \tag{45}$$

and

$$p_P^\star = \arg\max_{p_P \in [0, p_P^M]} Q_P^\star(p_P, p_S^\star(p_P)). \tag{46}$$

Proof: Using the property in Proposition 5, the optimization problem (44) reduces to an equivalent but simpler form, i.e., (45). Then, with the secondary user's best response known, the primary user chooses the optimal power level such that (46) is maximized. Therefore, $(p_P^\star, p_S^\star(p_P^\star))$ forms the Nash equilibrium of this Stackelberg game. ■

In a cognitive radio network, usually there are more than one secondary users. Intuitively, when there are more secondary users in the network, it is more likely that the primary user could find a secondary user in a good location to cooperate with, and hence the secrecy rate may increase. In this case, the primary user plays separate information secrecy games with each individual secondary user who needs to transmit information at the moment, and chooses to cooperate with the "best" secondary user who brings the highest secrecy rate. As expected, the achieved secrecy rate will improve with increasing numbers of secondary users participating in the game. We will show the performance through simulation results later.

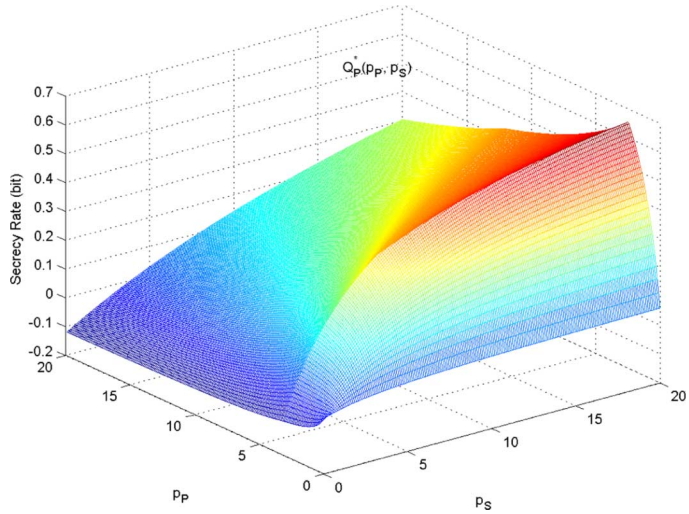

Fig. 7. Achievable secrecy rate $Q_P^*(p_P, p_S)$ with varying power levels p_P and p_S.

V. Simulation Results

In this section, some simulation results are presented. We first fix a channel realization to get some insight on the proposed cooperative transmission scheme, and then we show the average performance by generating thousands of independent channel realizations.

For illustrative purposes, we fix the channel as one realization of Case A: $g_P = g_S = 1$, $g_{PS} = 1.5$, $g_{SP} = 1.3$, $g_{SM} = 0.3$, and $g_{PM} = 1.2$. Note that under this setting $g_P < g_{PM}$, the primary user cannot transmit in secrecy at all without the secondary user's help, because $C_P = 0$ according to (4). In Fig. 7, we plot the achievable secrecy rate $Q_P^\star(p_P, p_S)$ when the transmit power levels take different values from $[0, 20] \times [0, 20]$. Some rates in the figure are negative, because $Q_P^\star(p_P, p_S)$ is the relaxed rate without considering the nonnegative constraint (the overall rate $\overline{Q_P}(p_P, p_S)$, however, is guaranteed to be nonnegative). As shown by the figure, the primary user does benefit from simultaneous transmissions of the secondary user. For example, within the power constraint, the primary user is able to reach a secrecy rate of 0.64 bit when $p_P = 2.5$ and $p_S = 20.0$. Moreover, as shown in the figure, it is not always beneficial to use full power; for example, when fixing $p_S = 20.0$, increasing p_P beyond 2.5 will reduce the secrecy rate. The reason is that the secrecy rate depends on the difference of the decoding capability of the primary receiver and the eavesdropper. It is possible that the decodable rate to the primary receiver grows with higher power but the eavesdropper may gain even more, which reduces the secrecy rate.

Next, we vary g_{PM} from 0.2 to 2, with all the other channel coefficients fixed as above. In Fig. 8, we compare the bottom line secrecy rate without cooperation and the optimal achievable secrecy rate at the Nash equilibrium of the proposed Stackelberg game, i.e., when users choose the optimal power levels according to (46). As expected, as the channel between the primary transmitter and the eavesdropper becomes better, the eavesdropper is more capable of decoding the primary user's message, and hence the secrecy rate without cooperation becomes lower, and further drops to zero when $g_{PM} > g_P$. When the primary user and the secondary user cooperate with each other, however, the

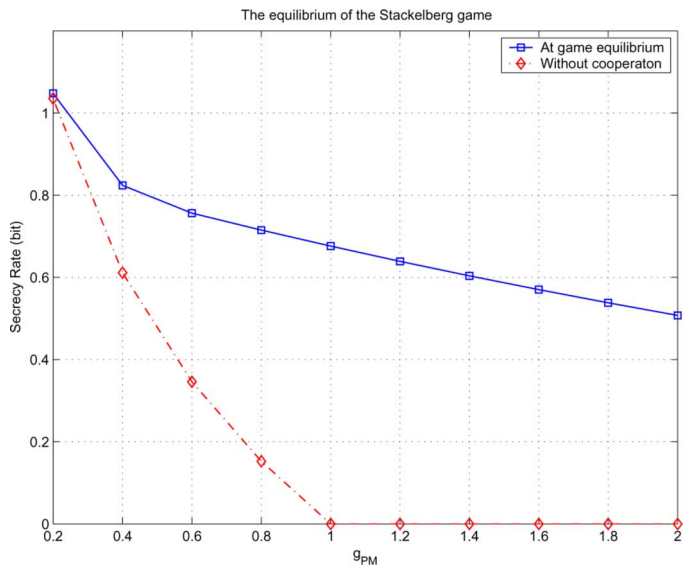

Fig. 8. Comparison of the optimal achievable secrecy rate at the game equilibrium and the secrecy rate without the secondary user's cooperation.

primary user may significantly enhance the secrecy of confidential messages, as shown in the figure. When g_{PM} is small, the eavesdropper receives very weak signals from the primary user, and the gain from a helper becomes limited.

In order to show the average performance of the proposed algorithm, we consider a scenario where all the users lie in a circular area with a radius 1000 m. The primary transmitter locates at the center of the circle, while the primary user's receiver, the eavesdropper, and the secondary transmitters/receivers are uniformly distributed in this circular area. We assume the channel gain merely depends on the distance from a transmitter to a receiver d, i.e.,

$$g = g_0 d^{-\alpha} \tag{47}$$

where the path loss exponent α is set to be 2 in the simulation, and g_0 is the channel gain at a reference point one meter away. We choose p_P^M, p_S^M, and g_0 in such a way that the signal-to-noise ratio (SNR) without considering interference is 15 dB when the distance is 300 m and the transmitter uses the maximum power. In the simulation,

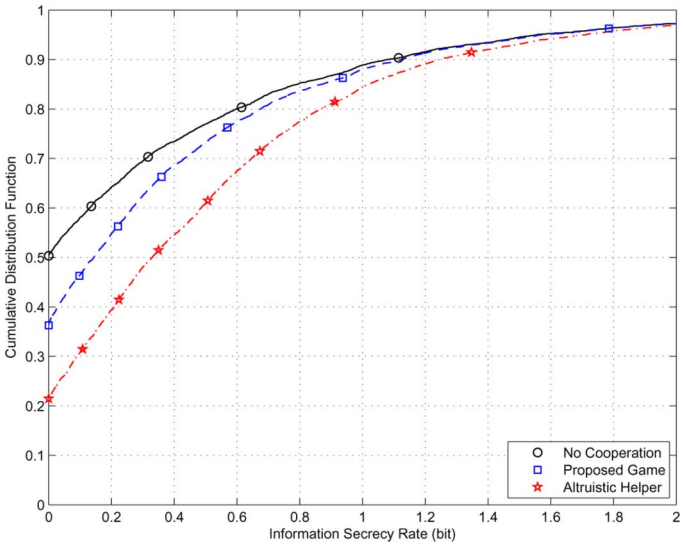

Fig. 9. Cumulative distribution functions of secrecy rates in scenarios with different levels of cooperation.

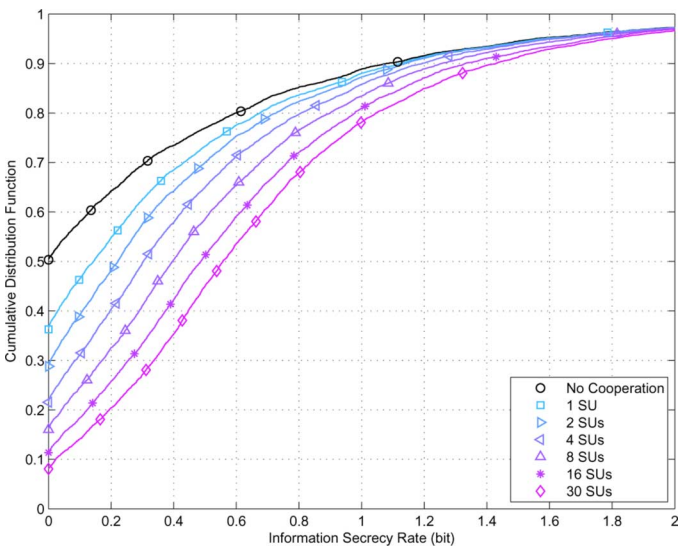

Fig. 10. Cumulative distribution functions of secrecy rates with different numbers of secondary users in the network.

we generate 5000 independent channel realizations. For each realization, we uniformly generate the location of users, calculate channel gains based on the distance, and find the equilibrium for this particular game with specific channel gains. The results from all independent realizations are plotted in the form of empirical cumulative distribution functions.

In Fig. 9, we compare the proposed scheme with the benchmark situation where there is no secondary user assisting the secrecy transmission, referred to as "no cooperation." Moreover, the scheme in [9] is also simulated, in which the helping interferer unconditionally cooperates and does not transmit his/her own useful information at all. Hence, we refer to this scheme as "altruistic helper." From the figure, it can be seen that the proposed game improves the information secrecy rate of the primary user while enabling the simultaneous transmission of a secondary user. The gap between our proposed game and the "altruistic helper" scheme is somewhat like the so-called "price of anarchy" in noncooperative game theory [23]. Because in our scheme, the secondary user has his/her own interest and transmits meaningful data to his/her own receiver, the game equilibrium takes both users' benefit into consideration. Therefore, from the primary user's point of view, the performance is suboptimal to the unconditional cooperation situation, and the cost is due to competition and compromise between two players in the game.

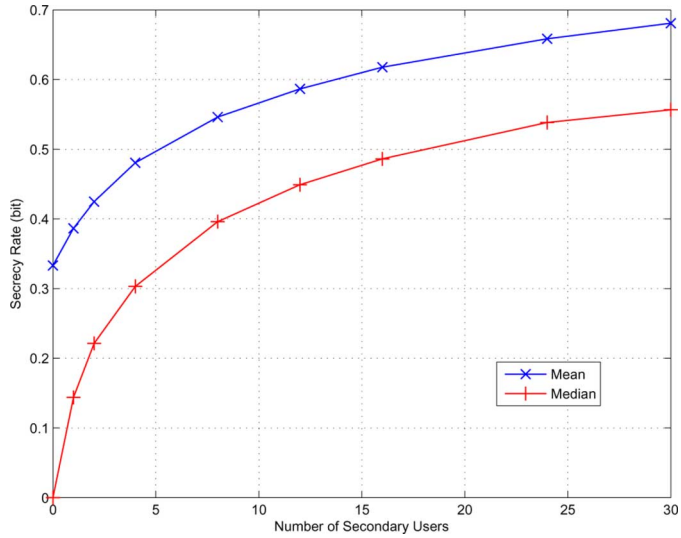

Fig. 11. Mean and median of secrecy rates with different numbers of secondary users in the network.

We have expected that the secrecy rate will improve when there are more secondary users in the network, because the primary user could pick up the best secondary user to cooperate with after playing a game with each individual secondary user separately. We verify this by simulation. Fig. 10 presents the cumulative distribution functions when the number of secondary users increases from 1 to 30, with the "no cooperation" curve provided as a benchmark. In Fig. 11, the mean and median values of secrecy rates are plotted versus different numbers of secondary users, and when the number of secondary users equals zero, it actually reduces to the "no cooperation" case. As illustrated by the two figures, secrecy rates are significantly improved by the proposed cooperation scheme, and higher rates are expected when there are more secondary users in the network.

VI. Conclusions

In this paper, we have modeled the cooperative transmission in a cognitive radio network as a Stackelberg game, where a secondary user helps a primary user to enhance secrecy against an intelligent and passive eavesdropper. Both the primary user and the secondary user want to maximize rates of data transmission, but the primary user has additional secrecy concerns. In order to learn what is the best achievable data rates for this system, we have applied information-theoretic approaches to derive the secrecy rate for the primary user and the information rate for the secondary user. In order to understand the incentive behind cooperation and predict the equilibrium behavior, we have applied game-theoretic approaches to characterize the Nash equilibrium in terms of how much power should be used in cooperative transmissions. Simulation results are presented to verify the performance.

APPENDIX A
PROOF OF PROPOSITION 1

Proof: The intelligent eavesdropper may comprehend the time sharing scheme when the primary user and the secondary user exchange this message. To realize the secrecy, the coding scheme is to encode according to multiple rate profiles $\left(R_P^1, R_{PM}^1, R_S^1\right), \left(R_P^2, R_{PM}^2, R_S^2\right), \ldots, (R_P^m, R_{PM}^m, R_S^m)$ in a time sharing way with a series of factors $\alpha^1, \alpha^2, \ldots, \alpha^m$ $\left(0 \le \alpha^j \le 1, \sum_j \alpha^j = 1\right)$ representing the fraction of time that each rate profile is used. Then, the secrecy rate is $Q_P = \sum_{j=1}^m \alpha^j \left(R_P^j - R_{PM}^j\right) \le \max_j (R_P^j - R_{PM}^j)$, with the equality hold if and only if $\alpha^j > 0$ implies $j \in \arg\max_{j'}(R_P^{j'} - R_{PM}^{j'})$. Therefore, $Q_P^\star$ cannot be increased by time sharing.

Similarly, assume an encoding strategy employs codes $\left(Q_P^\star, R_S^1\right), \left(Q_P^\star, R_S^2\right), \ldots, \left(Q_P^\star, R_S^m\right)$ in a time sharing manner with coefficients $\{\alpha^j, 1 \le j \le m\}$. Then, the secondary user's average rate $\sum_{j=1}^m \alpha^j R_S^j$ is bounded by $\max_j R_S^j$, which suggests $R_S^\star$ cannot be improved by time sharing either. ∎

APPENDIX B
PROOF OF PROPOSITION 2

Proof: $\Re^{[\mathrm{COOP}]}$ can be written as the union of four regions, $\Re^{[\mathrm{COOP}]} = \left\{\Re_P^{[\mathrm{MAC}]} \cap \Re_S^{[\mathrm{MAC}]}\right\} \cup \left\{\Re_P^{[\mathrm{MAC}]} \cap \Re_S^{[\mathrm{SD}]}\right\} \cup \left\{\Re_P^{[\mathrm{SD}]} \cap \Re_S^{[\mathrm{MAC}]}\right\} \cup \left\{\Re_P^{[\mathrm{SD}]} \cap \Re_S^{[\mathrm{SD}]}\right\}$. Depending on different cases, some of the regions may be empty, and the expression may be simplified.

For Case A, $\Re_P^{[\mathrm{MAC}]} \cap \Re_S^{[\mathrm{SD}]} = \emptyset$ and $\Re_P^{[\mathrm{SD}]} \cap \Re_S^{[\mathrm{SD}]} = \emptyset$, because $g_P \le g_{PS}$. Similarly, $\Re_P^{[\mathrm{SD}]} \cap \Re_S^{[\mathrm{MAC}]} = \emptyset$ because $g_S \le g_{SP}$. The region $\Re^{[\mathrm{COOP}]}$ reduces to $\Re_P^{[\mathrm{MAC}]} \cap \Re_S^{[\mathrm{MAC}]}$. For Case B, $\Re^{[\mathrm{COOP}]} = \Re_P^{[\mathrm{MAC}]} \cap \left\{\Re_S^{[\mathrm{MAC}]} \cup \Re_S^{[\mathrm{SD}]}\right\}$ because the other two regions are empty; Case C is similar, where the simplification yields $\Re^{[\mathrm{COOP}]} = \left\{\Re_P^{[\mathrm{MAC}]} \cup \Re_P^{[\mathrm{SD}]}\right\} \cap \Re_S^{[\mathrm{MAC}]}$. For Case D, however, none of the four regions is empty in general.

Finally, the frontier of the region can be derived after some manipulation, while monotonicity and continuity follow directly. ∎

APPENDIX C
PROOF OF PROPOSITION 3

Proof: Comparing the original and relaxed definitions of $Q_P(R_S)$, we find that the relaxed one removes the nonnegative constraint and reduces values for $R_S < \gamma(g_{SM}p_S/(1 + g_{PM}p_P))$. When $R_S < \gamma(g_{SM}p_S/(1 + g_{PM}p_P))$, $f_C(R_S)$ is nonincreasing and $f_M(R_S)$ is constant; hence, $f_C(R_S) - f_M(R_S) \le f_C(0) - f_M(0) = \gamma(g_P p_P) - \gamma(g_{PM}p_P) \le C_P$. Therefore, the relaxed definition only modifies segments that cannot exceed C_P, leaving $(\overline{Q_P}, \overline{R_S})$ unaltered.

When $R_S \ge \gamma(g_{SM}p_S)$, since $f_C(R_S)$ is nonincreasing and $\overline{f_M}(R_S)$ is constant, $Q_P(R_S) \le Q_P(\gamma(g_{SM}p_S))$; when $R_S < \gamma(g_{SM}p_S)$, $Q_P(R_S) = f_C(R_S) + R_S - \gamma_M$ is a nondecreasing function unless there is any discontinuous point (i.e., when the condition $(C1)$ holds), because $Q_P'(R_S) = f_C'(R_S) + 1 \ge 0$. If $(C1)$ holds, $Q_P(R_S)$ is maximized by $R_S^\dagger = \gamma(g_S p_S/(1 + g_{PS}p_P))$, because from piece-wise functions of $f_C(R_S)$ in Proposition 2, it is easy to check $f_C'(R_S) = -1$ after the discontinuous point, and thus the gap between two frontiers cannot be further increased. If $(C1)$ does not hold, $R_S^\dagger = \min(\gamma(g_{SM}p_S), \gamma(g_S p_S))$ is a maximizer to $Q_P(R_S)$. When there are multiple maximizers, the optimal one, $R_S^\star$, is selected according to (14). A necessary condition for $R_S^\star > R_S^\dagger$ is that f_C is continuous at $R_S^\dagger$ and $f_C'(R_S^\dagger) = \overline{f_M}'(R_S^\dagger)$. This excludes $R_S^\dagger = \gamma(g_S p_S)$ and $R_S^\dagger = \gamma(g_S p_S/(1 + g_{PS}p_P))$, and the condition reduces to $f_C'(R_S^\dagger) = \overline{f_M}'(R_S^\dagger) = 0$ with $R_S^\dagger = \gamma(g_{SM}p_S)$. ∎

APPENDIX D
PROOF OF PROPOSITION 5

Proof: In what follows, we will show that for all four possible cases, $R_S^\star(p_P, p_S)$ is a strictly increasing function of p_S, when p_P is fixed.

For Cases A and C, there is no discontinuous point in $f_C(R_S)$, and according to Proposition 3, the auxiliary variable $R_S^\dagger = \gamma(g_S p_S)$ (when $g_S \le g_{SM}$) or $\gamma(g_{SM}p_S)$ (when $g_S > g_{SM}$) is an increasing and continuous function in p_S. Note that $R_S^\star$ may be different from $R_S^\dagger$ under certain conditions stated in Proposition 3, but from the expression of $f_C^A(R_S)$ and $f_C^C(R_S)$ in Proposition 2, $R_S^\star(p_P, p_S)$ is still a strictly increasing function of p_S.

For Case B, as Fig. 4 shows that all boundaries in the 2-D representation are horizontal, when p_P is fixed, increasing p_S will not cross any boundary, and therefore, the expression of $R_S^\star(p_P, p_S)$ takes a sole form. According to Proposition 4, $R_S^\star(p_P, p_S)$ is an increasing and continuous function of p_S.

For Case D, we also need the 2-D representation given in Fig. 6. For any given p_P, a horizontal line segment can be drawn on the p_P–p_S plane with $p_S \in [0, p_S^M]$. It is possible that such a line crosses several regions and there are different rate expressions on each piece. Since each piece is a continuous and strictly increase function, it suffices to make sure that the value of function must not plummet when crossing any nonhorizontal boundary from the left to the right. For example, when $g_{SM} < g_{SP}$ (corresponding to the left figure in Fig. 6), if the given p_P is larger than $(g_S/g_{SM} - 1)/g_{PS}$, increasing p_S will possibly cross over the nonhorizontal boundary between ⑤ and ②. In region ⑤, $R_S^\star = \gamma(g_S p_S/(1 + g_{PS}p_P))$, and in region ②, $R_S^\star = \gamma(g_{SM}p_S)$. Since $p_P > (g_S/g_{SM} - 1)/g_{PS}$, $\gamma(g_S p_S/(1 + g_{PS}p_P)) < \gamma(g_{SM}p_S)$, which implies a jump at the boundary. Similarly, we can check that when $g_{SM} \ge g_{SP}$ (the right figure in Fig. 6), the value of rate does not change over the boundaries between ③ and ⑥ or between ⑥ and ⑦, while the value does jump up from region ④ (or region ⑤) to region ⑦. To sum up, $R_S^\star(p_P, p_S)$ is indeed a strictly increasing function of p_S, although it may be discontinuous between pieces. ∎

REFERENCES

[1] J. Mitola, III, "Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio," Ph.D. thesis, KTH Royal Institute of Technology, Stockholm, Sweden, 2000.

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

[3] S. Huang, X. Liu, and Z. Ding, "Opportunistic spectrum access in cognitive radio networks," in *Proc. IEEE Int. Conf. Computer Communications (Infocom)*, Phoenix, AZ, Apr. 2008, pp. 1427–1435.
[4] D. Niyato and E. Hossain, "Competitive spectrum sharing in cognitive radio networks: A dynamic game approach," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2651–2660, Jul. 2008.
[5] Y. Wu, B. Wang, K. J. R. Liu, and T. C. Clancy, "A scalable collusion-resistant multi-winner cognitive spectrum auction game," *IEEE Trans. Commun.*, vol. 57, no. 12, pp. 3805–3816, Dec. 2009.
[6] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 25–37, Jan. 2008.
[7] T. X. Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: A multi-dimensional analysis and assessment," *Mobile Netw. Appl.*, vol. 13, no. 5, pp. 516–532, Oct. 2008.
[8] B. Wang, Y. Wu, and K. J. R. Liu, "An anti-jamming stochastic game in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 877–889, Apr. 2011.
[9] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.
[10] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[11] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
[12] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
[13] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
[14] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.
[15] R. Berry and D. Tse, "Information theoretic games on interference channels," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Toronto, Canada, Jul. 2008, pp. 2518–2522.
[16] A. Garnaev and W. Trappe, "An eavesdropping game with SINR as an objective function," in *Proc. Security and Privacy in Communication Networks (SecureComm)*, Athens, Greece, Sep. 2009, vol. 19, pp. 142–162.
[17] E. Perron, S. Diggavi, and E. Telatar, "On cooperative wireless network secrecy," in *Proc. IEEE Int. Conf. Computer Communications (Infocom)*, Rio de Janeiro, Brazil, Apr. 2009, pp. 1935–1943.
[18] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.
[19] R. Liu, I. Marić, P. Spasojević, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–3507, Jun. 2008.
[20] A. Goldsmith, S. A. Jafar, I. Marić, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proc. IEEE*, vol. 97, no. 5, pp. 894–914, May 2009.
[21] Z. Han, N. Marina, M. Debbah, and A. Hjorungnes, "Physical layer security game: How to date a girl with her boyfriend on the same table," in *Proc. Int. Conf. Game Theory for Networks (GameNets)*, Istanbul, Turkey, May 2009, pp. 287–294.
[22] D. Fudenberg and J. Tirole, *Game Theory*. Cambridge, MA: MIT Press, 1993.
[23] B. Wang, Y. Wu, and K. J. R. Liu, "Game theory for cognitive radio networks: An overview," *Comput. Netw.*, vol. 54, no. 14, pp. 2537–2561, Oct. 2010.
[24] Z. Li, R. Yates, and W. Trappe, "Achieving secret communication for fast Rayliegh fading channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 9, pp. 2792–2799, Sep. 2010.
[25] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ: Wiley, 2006.
[26] T. S. Han and K. Kobayashi, "A new achievable rate region for the interference channel," *IEEE Trans. Inf. Theory*, vol. 27, no. 1, pp. 49–60, Jan. 1981.

Yongle Wu received the B.S. (with highest honor) and M.S. degrees in electronic engineering from Tsinghua University, Beijing, China, in 2003 and 2006, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Maryland, College Park, in 2010.

He is currently a senior engineer with Qualcomm Incorporated, San Diego, CA. His research interests are in the areas of wireless communications and networks, including cognitive radio techniques, dynamic spectrum access, network security, and MIMO-OFDM communication systems.

Dr. Wu received the Graduate School Fellowship from the University of Maryland in 2006, the Future Faculty Fellowship in 2009 and the Litton Industries Fellowship in 2010, both from A. James Clark School of Engineering, University of Maryland, and the Distinguished Dissertation Fellowship from Department of Electrical and Computer Engineering, University of Maryland, in 2011.

K. J. Ray Liu (F'03) is a Distinguished Scholar-Teacher of University of Maryland, College Park. He is Associate Chair, Graduate Studies and Research, Electrical and Computer Engineering Department, and leads the Maryland Signals and Information Group conducting research encompassing broad aspects of information science and technology including communications and networking, information forensics and security, multimedia signal processing, and biomedical engineering.

Dr. Liu is the recipient of numerous honors and awards, including best paper awards from the IEEE Signal Processing Society, the IEEE Vehicular Technology Society, and EURASIP; an IEEE Signal Processing Society Distinguished Lecturer, the EURASIP Meritorious Service Award, and the National Science Foundation Young Investigator Award. He also received various teaching and research recognitions from University of Maryland, including the university-level Invention of the Year Award; and Poole and Kent Senior Faculty Teaching Award and Outstanding Faculty Research Award, both from A. James Clark School of Engineering. He is a Fellow of AAAS. He was Vice President–Publications of the IEEE Signal Processing Society. He was the Editor-in-Chief of the *IEEE Signal Processing Magazine* and the founding Editor-in-Chief of the *EURASIP Journal on Applied Signal Processing*. His recent books include *Cooperative Communications and Networking* (Cambridge Univ. Press, 2008); *Resource Allocation for Wireless Networks: Basics, Techniques, and Applications* (Cambridge Univ. Press, 2008); *Ultra-Wideband Communication Systems: The Multiband OFDM Approach* (IEEE-Wiley, 2007); *Network-Aware Security for Group Communications* (Springer, 2007); *Multimedia Fingerprinting Forensics for Traitor Tracing* (Hindawi, 2005); *Handbook on Array Processing and Sensor Networks* (IEEE-Wiley, 2009).