Secrecy Games over the Cognitive Channel

Elizabeth Toher, O. Ozan Koyluoglu, Hesham El Gamal
Department of Electrical and Computer Engineering
The Ohio State University, Columbus, OH 43210
Email: {tohere, koyluogo, helgamal}@ece.osu.edu

***Abstract*—A secure communication game is considered for the cognitive channel with a confidential primary message, where the primary user is interested in maximizing its secure rate with lowest possible power consumption and the utility of the cognitive user is a weighted sum of the primary secrecy rate and the cognitive rate (corresponds to a spectrum law in favor of the legacy owners of the spectrum). An achievable rate region is derived for the channel with message splitting at the cognitive radio and noise forwarding. The game considers the case with no common message, but shows that even this limited scenario can still be beneficial. The established Nash Equilibrium (NE) shows that the cognitive user *trades noise for bits*. The results are also interesting in the sense that *both* users can benefit (by playing the distributed game) compared to their throughput resulting from the non-cooperative scenario.**

I. Introduction

Cognitive radios can maximize the utilization of a limited bandwidth by allowing additional (cognitive) users to share a frequency spectrum dedicated to primary users. In a two-user setting, the cognitive radio channel can be defined as an interference channel, but with additional assumptions and/or constraints on the cognitive nodes. For example, there are many works in the literature that assume the existence of the primary message at cognitive radios (see, e.g., [1] [2]). In addition, some information theoretical constraints for cognitive radio were established in [2]: 1) The primary user experiences no decrease in rate, 2) the primary user is oblivious to the presence of the cognitive radio, i.e., the primary user does not need to change the single-user encoding/decoding scheme. However, the security constraint has not been extensively studied in the literature.

Secrecy from an eavesdropper as defined by Wyner's wire-tap model ([3]) has been applied to many scenarios recently. In the cognitive setting, a scenario in which the message of the cognitive transmitter has to be kept secret at the primary receiver is considered in [4]. A slightly modified channel model, where the primary message has to be decoded at both users, is studied in [5] with and without secrecy constraints. However, as the primary users are the legacy owners of the spectrum, one should consider the confidentiality of the primary message as well.

This paper explores the case in which the message of primary transmitter must be kept secret at the cognitive receiver. Here, the cognitive radio can support the primary receiver as a "deaf helper" (as described in [6]) by jamming the channel. We present an achievable rate region (inner bound), where we also utilize message splitting at the cognitive user. Then, a game formulation for this setup is given, where the primary user is penalized with the power consumption and the utility of the cognitive user is made proportional to the primary secure communication rate. The former is the self-desire of the primary node, whereas the latter can be considered as a spectrum law in favor of the primary users (set by spectrum authorities, such as FCC). The unique Nash Equilibrium (NE), where the cognitive radio allocates power to its jamming signal in addition to its message codeword, is established. The result is interesting in the sense that the cognitive radio trades noise for bits. Furthermore, the analysis provides a motivation for the primary users to accommodate cognitive radios: the secure throughput of the primary node can be increased in some cases compared to the wiretap channel rate.

II. Problem Statement

We consider a two-user discrete memoryless interference channel and the two-user Gaussian interference channel.

The discrete memoryless interference channel is defined by transmitted signals X_1, X_2, received signals Y_1 and Y_2, and transition probabilities $p(y_1, y_2|x_1, x_2)$, $x_1 \in \mathcal{X}_1$, $x_2 \in \mathcal{X}_2$, $y_1 \in \mathcal{Y}_1$ and $y_2 \in \mathcal{Y}_2$, for some finite sets $\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}_1, \mathcal{Y}_2$.

We assume that each transmitter $k \in \{1, 2\}$ has a secret message W_k which is to be transmitted to the respective receiver in n channel uses. In addition, W_1 needs to be secured from the receiver 2. In this setting, an $(n, M_1, M_2, P_{e,1}, P_{e,2})$ secret codebook has the following components:

1) The message set $\mathcal{W}_k = \{1, ..., M_k\}$; $k = 1, 2$.

2) A stochastic encoding function $f_k(.)$ at transmitter k which maps the secret messages to the transmitted symbols: $f_k : w_k \to \mathbf{X}_k$ for each $w_k \in \mathcal{W}_k$; $k = 1, 2$.

3) Decoding function $\phi_k(.)$ at receiver k which maps the received symbols to an estimate of the message: $\phi_k(\mathbf{Y}_k) = \hat{w}_k$; $k = 1, 2$.

The reliability of transmission is measured by the following probabilities of error

$$P_{e,k} = \frac{1}{M_1 M_2} \sum_{(w_1,w_2)\in\mathcal{W}_1\times\mathcal{W}_2} \Pr\Big\{\phi_k(\mathbf{Y}_k) \neq w_k \,|(w_1, w_2) \text{ is sent}\Big\},$$

for $k = 1, 2$. The secrecy is measured by the information leakage rate to the cognitive receiver

$$\frac{1}{n} I\left(W_1; \mathbf{Y}_2\right).$$

We say that the rate tuple (R_1, R_2) is achievable for the cognitive channel with confidential primary message, if, for any given $\epsilon > 0$, there exists an $(n, M_1, M_2, P_{e,1}, P_{e,2})$ secret codebook such that,

$$\begin{aligned} \frac{1}{n}\log(M_1) &= R_1 \\ \frac{1}{n}\log(M_2) &= R_2, \\ \max\{P_{e,1}, P_{e,2}\} &\leq \epsilon, \end{aligned}$$

and

$$\frac{1}{n} I\left(W_1; \mathbf{Y}_2\right) \leq \epsilon \tag{1}$$

for sufficiently large n. The capacity region of this channel is the closure of the set of all achievable rate pairs (R_1, R_2) and is denoted as $\mathbb{C}$.

In its standard form, the two user Gaussian interference channel is given by

$$Y_1 = X_1 + \sqrt{c_{21}} X_2 + N_1 \tag{2}$$

$$Y_2 = \sqrt{c_{12}} X_1 + X_2 + N_2, \tag{3}$$

where $N_r \sim \mathcal{N}(0,1)$ is the noise at each receiver $r = 1, 2$ and the average power constraints are $\frac{1}{n}\sum_{t=1}^{n}(X_k(t))^2 \leq P_k$ for $k = 1, 2$. The capacity region of this channel under the above reliability and secrecy constraints will be denoted as $\mathbb{C}^G$.

We denote the secret communication rate of the primary users when the cognitive transmitter does not transmit as R_1^{wt} (the wiretap rate) [3]:

$$R_1^{wt} \triangleq \left[\frac{1}{2}\log\left(1 + P_1\right) - \frac{1}{2}\log\left(1 + c_{12}P_1\right)\right]^+ \tag{4}$$

III. Information Theoretic Results

A. Main Result for the Discrete Memoryless Channel

Theorem 1: An inner bound of the achievable region is given by

$$\mathcal{R} \triangleq \text{the closure of } \left\{\bigcup_{p\in\mathcal{P}} \mathcal{R}(p)\right\} \subset \mathbb{C}, \tag{5}$$

where $\mathcal{P}$ is the set of probability distributions $p(.)$ that factor as

$$p(q, v_1, v_{2c}, v_{2p}, x_1, x_2) =$$

$$p(q)p(v_1|q)p(x_1|v_1, q)p(v_{2c}|q)p(v_{2p}|v_{2c}, q)p(x_2|v_{2c}, v_{2p}, q),$$

and, for any $p \in \mathcal{P}$, $\mathcal{R}(p)$ is the set of (R_1, R_2) pairs for which non-negative rate tuples (R_1, R_{2c}, R_{2p}) satisfy

$$\begin{aligned} R_1 &< I(V_1; Y_1|V_{2c}, Q) - I(V_1; Y_2|V_{2c}, V_{2p}, Q) \\ R_{2c} &< I(V_{2c}; Y_1|V_1, Q) \\ R_1 + R_{2c} &< I(V_1, V_{2c}; Y_1|Q) - I(V_1; Y_2|V_{2c}, V_{2p}, Q) \\ R_{2p} &< I(V_{2p}; Y_2|V_{2c}, Q) \\ R_{2c} + R_{2p} &< I(V_{2c}, V_{2p}; Y_2|Q) \\ R_2 &= R_{2c} + R_{2p} \end{aligned}$$

Proof: Please refer to Appendix A. ∎

We note that the capacity region of this model remains open.

B. The Gaussian Channel

Here we specialize the results obtained in the previous section to the Gaussian scenario. Towards this end, we first define the power allocation and joint distribution sets for the model.

Consider a probability mass function on the time sharing parameter denoted by $p(q)$. Let $\mathcal{A}(p(q))$ denote the set of all possible power allocations, i.e.,

$$\begin{aligned} \mathcal{A}(p(q)) \triangleq \Bigg\{ & P_1(q), P_{2c}(q), P_{2p}(q), P_{2j}(q) | \sum_{q\in Q} P_1(q)p(q) \leq P_1 \\ & \sum_{q\in Q} (P_{2c}(q) + P_{2p}(q) + P_{2j}(q))p(q) \leq P_2 \Bigg\} \end{aligned} \tag{6}$$

We then define a set of joint distributions $\mathcal{P}^G$ for the Gaussian case as follows.

$$\begin{aligned} \mathcal{P}^G \triangleq \Bigg\{ & p | p \in \mathcal{P}, (P_1(q), P_{2c}(q), P_{2p}(q), P_{2j}(q)) \in \mathcal{A}(p(q)), \\ & V_1(q) \sim \mathcal{N}(0, P_1(q)), \\ & V_{2c}(q) \sim \mathcal{N}(0, P_{2c}(q)), V_{2p}(q) \sim \mathcal{N}(0, P_{2p}(q)) \\ & J_2(q) \sim \mathcal{N}(0, P_{2j}(q)), \\ & X_1(q) = V_1(q), X_2(q) = V_{2c}(q) + V_{2p}(q) + J_2(q), \Bigg\} \end{aligned}$$

where the Gaussian model above gives $p(y_1, y_2|x_1, x_2)$.

We have the following corollary.

Corollary 2:

$$\mathcal{R}^G \triangleq \text{the closure of } \left\{\bigcup_{p\in\mathcal{P}^G} \mathcal{R}(p)\right\} \subset \mathbb{C}^G$$

We will consider the following subregion of Corollary 2, where we set Q to be deterministic. In the special case of the Gaussian channel as described, our main theorem reduces to the following acheiveable rate region:

Corollary 3: The set of (R_1, R_2) pairs, with $R_2 = R_{2c} + R_{2p}$, for which non-negative rate tuples (R_1, R_{2c}, R_{2p}) satisfy

$$\begin{aligned} R_1 &< \frac{1}{2}\log\left(1 + \frac{P_1}{1 + c_{21}P_{2p} + c_{21}P_{2j}}\right) \\ &\quad -\frac{1}{2}\log\left(1 + \frac{c_{12}P_1}{1 + P_{2j}}\right) \end{aligned} \tag{7}$$

$$R_{2c} < \frac{1}{2}\log\left(1 + \frac{c_{21}P_{2c}}{1 + c_{21}P_{2p} + c_{21}P_{2j}}\right) \tag{8}$$

$$\begin{aligned} R_1 + R_{2c} &< \frac{1}{2}\log\left(1 + \frac{P_1 + c_{21}P_{2c}}{1 + c_{21}P_{2p} + c_{21}P_{2j})}\right) \\ &\quad -\frac{1}{2}\log\left(1 + \frac{c_{12}P_1}{1 + P_{2j}}\right) \end{aligned} \tag{9}$$

$$R_{2p} < \frac{1}{2}\log\left(1 + \frac{P_{2p}}{1 + c_{12}P_1 + P_{2j}}\right) \tag{10}$$

$$R_{2c} + R_{2p} < \frac{1}{2}\log\left(1 + \frac{P_{2c} + P_{2p}}{1 + c_{12}P_1 + P_{2j}}\right) \tag{11}$$

are achievable.

IV. Secure Communication Game

In our game setup, we assume that the primary transmitter and receiver employ single-user wiretap channel encoder and decoder, respectively. Hence, the cognitive transmitter can not utilize W_{2c}, as any such information can not be decoded at the primary user. Even in this simplified game we show that *trading noise for bits* at the cognitive radio can motivate cooperation between primary and cognitive users. Future work will investigate the more general case.

We model the strategy of the cognitive transmitter as power allocation on P_{2p} (the cognitive message) and P_{2j} (the noise signal). For a given $\gamma \in [0,1]$, we set $P_{2p} = \gamma P_2$ and $P_{2j} = (1-\gamma)P_2$. We assume that the cognitive user sets $P_2 = P_2^{max}$. Then, the primary and cognitive transmitter have the following power control strategies.

$$s_1 = P_1 \text{ such that } P_1 \in [0, P_1^{max}] \quad (12)$$

$$s_2 = \gamma \text{ such that } \gamma \in [0,1] \quad (13)$$

We assume that the primary user is penalized by the power it uses. For some $\alpha > 0$, we consider the following utility function for the primary link:

$$\begin{aligned} u_1 &= R_1 - \alpha P_1 \\ &= \frac{1}{2}\log\left(1+\frac{P_1}{1+c_{21}P_2}\right) \\ &\quad -\frac{1}{2}\log\left(1+\frac{c_{12}P_1}{1+(1-\gamma)P_2}\right) - \alpha P_1 \end{aligned}$$

For the utility of the cognitive user, we consider a penalty term $\beta(R_1^{wt} - R_1)$ for some $\beta > 0$. This penalty term corresponds to a desired protection of the legacy owners of the spectrum by the FCC. As R_1^{wt} is a constant, we consider

$$\begin{aligned} u_2 &= R_2 + \beta R_1 \\ &= \frac{1}{2}\log\left(1+\frac{\gamma P_2}{1+c_{12}P_1+(1-\gamma)P_2}\right) \\ &\quad +\beta\left(\frac{1}{2}\log\left(1+\frac{P_1}{1+c_{21}P_2}\right)\right. \\ &\quad \left.-\frac{1}{2}\log\left(1+\frac{c_{12}P_1}{1+(1-\gamma)P_2}\right)\right) \end{aligned}$$

Essentially, rather than penalize the cognitive pair for interference, the utility function instead includes a reward for a high primary rate, R_1. We have the following result:

Theorem 4: There is a unique NE at $s_1 = P_1^*$, $s_2 = \gamma^*$, where

$$P_1^* = \frac{1+kP_2}{\beta c_{21}}, \quad (14)$$

and

$$\gamma^* = 1-k, \quad (15)$$

if

$$\beta \geq \frac{1+kP_2}{c_{12}P_1^{max}} \quad (16)$$

and

$$\alpha 2\ln 2 = \frac{\beta c_{12}}{1+\beta c_{12}(1+c_{21}P_2)+kP_2} \quad (17)$$

for any $k \in (0,1)$.

Proof: Please refer to Appendix B. ∎

Using (37) for γ, the negative term in R_1 is reduced to a constant:

$$\frac{1}{2}\log\left(1+\frac{c_{12}P_1}{1+(1-\gamma)P_2}\right) = \frac{1}{2}\log\left(\frac{\beta+1}{\beta}\right) \quad (18)$$

We make the following observations:

1) An increase in P_2 may increase the first term in u_2 but will **only decrease** the second term. Thus, depending on the choice of constants, for some games $P_2 < P_2^{max}$ may be the optimal power allocation at the cognitive transmitter. This is interesting as the cognitive radio can refrain from using its full resources while maximizing its utility.
2) For some channel gains, we observe that $R_1 > R_1^{wt}$. For instance, when $c_{12} > 1$, the primary channel can achieve a non-zero secure rate (which is not possible in the non-cooperative scenario). We expect message-splitting to improve this rate even further.

V. Conclusion

A secure communication game is considered for the cognitive channel, where the primary user is interested in maximizing its secure rate with lowest possible power consumption and the utility of the cognitive user is proportional to the primary secrecy rate in addition to its own rate. The established Nash Equilibrium (NE) shows that the cognitive user *trades noise for bits*. Furthermore, the secure throughput of the primary node can be increased in some cases compared to the wiretap channel rate (a motivation for the primary users to accommodate cognitive radios). Further investigations will consider more general cases, the fading case with message splitting, a utility function for the primary transmitter that optimizes secrecy rate per power, and quality of service limitations for the cognitive transmitter (e.g., the primary transmitter **must** achieve a minimum rate).

Appendix A
Proof of Theorem 1

Fix some $p(q)$, $p(v_1|q)$, $p(x_1|v_1,q)$, $p(v_{2c}|q)$, $p(v_{2p}|v_{2c},q)$, $p(x_2|v_{2c},v_{2p},q)$, for the given channel $p(y_1,y_2|x_1,x_2)$. Generate a random typical sequence $\mathbf{q}^n$, where $p(\mathbf{q}^n) = \prod_{t=1}^{n} p(q(t))$ and each entry is chosen i.i.d. according to $p(q)$. Every node knows the sequence $\mathbf{q}^n$.

Codebook Generation:

Each codebook in the ensemble is constructed as follows. We first split the message W_2, which is to be decoded at the receiver 2, as $W_2 = \{W_{2c}, W_{2p}\}$, where W_{2c} and W_{2p} are referred to as the common and the private messages of transmitter 2.

$$W_{2c} = [1,2,\cdots,2^{nR_{2c}}] \quad (19)$$

$$W_{2p} = [1,2,\cdots,2^{nR_{2p}}] \quad (20)$$

Generate $2^{n(R_1+R_1')}$ codewords $\mathbf{v_1}(w_1,w_1')$ i.i.d. according to $\prod_{t=1}^{n} p(v_1(t)|q(t))$, and distribute them uniformly into 2^{nR_1}

bins, where $w_1 \in \{1, \cdots, 2^{nR_1}\}$ is the bin index and and $w_1' \in \{1, \cdots, 2^{nR_1'}\}$ is the codeword index per bin. Generate $2^{nR_{2c}}$ codewords $\mathbf{v_{2c}}(w_{2c})$ i.i.d. according to $\prod_{t=1}^{n} p(v_{2c}(t)|q(t))$. For each w_{2c}, generate $2^{nR_{2p}}$ codewords $\mathbf{v_{2p}}(w_{2c}, w_{2p})$ i.i.d. according to $\prod_{t=1}^{n} p(v_{2p}(t)|v_{2c}(t), q(t))$.

Encoding:

Encoder 1, to transmit w_1, will randomly select a codeword from the bin w_1 according to a uniform distribution, where the codeword index is w_1' and the codeword is $\mathbf{v_1}(w_1, w_1')$. The channel input at the transmitter, $\mathbf{x_1}(w_1, w_1')$ is generated according to $\prod_{t=1}^{n} p(x_1(t)|v_1(t), q(t))$.

Encoder 2, to transmit w_2, first finds corresponding indices w_{2c} and w_{2p} over the sets W_{2c} and W_{2p} to perform the message splitting. Then, the channel input at the transmitter 2, $\mathbf{x_2}(w_{2c}, w_{2p})$ is generated according to $\prod_{t=1}^{n} p(x_2(t)|v_{2c}(t), v_{2p}(t), q(t))$.

Decoding:

Decoder 1, given $\mathbf{y_1}$, looks for unique tuple (w_1, w_1', w_{2c}) such that

$$(\mathbf{v_1}(w_1, w_1'), \mathbf{v_{2c}}(w_{2c}), \mathbf{y_1}, \mathbf{q}) \in \mathcal{A}_\epsilon^{(n)}(V_1, V_{2c}, Y_1, Q).$$

If there is no such found, it declares an error. If there is more than one such tuple, one of them is selected. The decoded estimate is set to $\hat{w}_1$.

Decoder 2 tries to obtain the estimates (w_{2c}, w_{2p}) such that

$$(\mathbf{v_{2c}}(w_{2c}), \mathbf{v_{2p}}(w_{2c}, w_{2p}), \mathbf{y_2}, \mathbf{q}) \in \mathcal{A}_\epsilon^{(n)}(V_{2c}, V_{2p}, Y_2, Q).$$

If there is no such found, it declares an error. If there is more than one such tuple, one of them is selected. Decoded message indices are represented by the tuple $(\hat{w}_{2c}, \hat{w}_{2p})$, from which the message estimate $(\hat{w}_2)$ is obtained.

Error Probability Analysis:

Without loss of generality and by the symmetrical property of the ensemble it suffices to consider $w_1 = w_{2c} = w_{2p} = 1$ is transmitted. We also assume that the first codeword in the bin is chosen at encoder 1 (w_1' above). We first focus on error probability $P_{e,1}^{(n)}$. We consider the following events.

$$\begin{aligned}
E_1 &: (\mathbf{v_1}(1,1), \mathbf{v_{2c}}(1)) \text{ does not satisfy} \\
&\quad (\mathbf{v_1}(1,1), \mathbf{v_{2c}}(1), \mathbf{y_1}, \mathbf{q}) \in \mathcal{A}_\epsilon^{(n)}(V_1, V_{2c}, Y_1, Q) \\
E_2 &: (\mathbf{v_1}(i_1, i_1'), \mathbf{v_{2c}}(i_{2c})) \text{ satisfies} \\
&\quad (\mathbf{v_1}(i_1, i_1'), \mathbf{v_{2c}}(i_{2c}), \mathbf{y_1}, \mathbf{q}) \in \mathcal{A}_\epsilon^{(n)}(V_1, V_{2c}, Y_1, Q) \\
&\quad \text{for some } (i_1, i_1', i_{2c}) \neq (1,1,1)
\end{aligned}$$

By asymptotic equipartition property (AEP) we have that $Pr\{E_1\} \to 0$ as n gets large. It remains to show the conditions for which $Pr\{E_2|E_1^c\} \to 0$ as $n \to \infty$, as $P_{e,1}^{(n)} \leq Pr\{E_1\} + Pr\{E_2|E_1^c\}$ by the union bound for probabilities. We first define the following event

$$\begin{aligned}
E_2(\mathbf{i}) &= \{(\mathbf{v_1}(i_1, i_1'), \mathbf{v_{2c}}(i_{2c}), \mathbf{y_1}, \mathbf{q}) \\
&\quad \in \mathcal{A}_\epsilon^{(n)}(V_1, V_{2c}, Y_1, Q)|E_1^c\}
\end{aligned}$$

where the index vector is given by $\mathbf{i} = (i_1, i_1', i_{2c})$. Then, using the union bound, we have

$$\begin{aligned}
Pr\{E_2|E_1^c\} &= Pr\{\bigcup_{(i_1,i_1',i_{2c})\neq(1,1,1)} E_2(\mathbf{i})\} && (21) \\
&\leq \sum_{(i_1,i_1')\neq(1,1),i_{2c}=1} Pr\{E_2(\mathbf{i})\} && (22) \\
&\quad + \sum_{(i_1,i_1')=(1,1),i_{2c}\neq 1} Pr\{E_2(\mathbf{i})\} && (23) \\
&\quad + \sum_{(i_1,i_1')\neq(1,1),i_{2c}\neq 1} Pr\{E_2(\mathbf{i})\} && (24)
\end{aligned}$$

Here, we observe that once the rates satisfy the following equations, $Pr\{E_2|E_1^c\}$ vanishes for sufficiently large n.

$$\begin{aligned}
R_1 + R_1' &< I(V_1; V_{2c}, Y_1|Q) \\
&= I(V_1; Y_1|V_{2c}, Q) && (25) \\
R_{2c} &< I(V_{2c}; Y_1|V_1, Q) && (26) \\
R_1 + R_1' + R_{2c} &< I(V_1, V_{2c}; Y_1|Q) && (27)
\end{aligned}$$

where (25) is due to the independence of V_1 and V_{2c} given Q.

We now focus on error probability $P_{e,2}^{(n)}$. We consider the following events.

$$\begin{aligned}
E_3 &: (\mathbf{v_{2c}}(1), \mathbf{v_{2p}}(1,1)) \text{ does not satisfy} \\
&\quad (\mathbf{v_{2c}}(1), \mathbf{v_{2p}}(1,1), \mathbf{y_2}, \mathbf{q}) \in \mathcal{A}_\epsilon^{(n)}(V_{2c}, V_{2p}, Y_2, Q) \\
E_4 &: (\mathbf{v_{2c}}(i_{2c}), \mathbf{v_{2p}}(i_{2c}, i_{2p}), \mathbf{y_2}) \text{ satisfies} \\
&\quad (\mathbf{v_{2c}}(i_{2c}), \mathbf{v_{2p}}(i_{2c}, i_{2p}), \mathbf{y_2}, \mathbf{q} \in \mathcal{A}_\epsilon^{(n)}(V_{2c}, V_{2p}, Y_2, Q) \\
&\quad \text{with } (i_{2c}, i_{2p}) \neq (1,1)
\end{aligned}$$

Similar to above, $P_{e,2}^{(n)} \leq Pr\{E_3\} + Pr\{E_4|E_3^c\}$ and the first term can be arbitrarily made small as $n \to \infty$ due to AEP. To analyze the second term, we define $E_4(\mathbf{i}) = \{\mathbf{v_{2c}}(i_{2c}), \mathbf{v_{2p}}(i_{2c}, i_{2p}), \mathbf{y_2}) \in \mathcal{A}_\epsilon^{(n)}(V_{2c}, V_{2p}, Y_2)|E_3^c\}$ where the index vector is given by $\mathbf{i} = (i_{2c}, i_{2p})$. Then, using the union bound, we have

$$\begin{aligned}
Pr\{E_4|E_3^c\} &= Pr\{\bigcup_{(i_{2c},i_{2p})\neq(1,1)} E_4(\mathbf{i})\} && (28) \\
&\leq \sum_{i_{2c}\neq 1, i_{2p}=1} Pr\{E_4(\mathbf{i})\} && (29) \\
&\quad + \sum_{i_{2c}=1, i_{2p}\neq 1} Pr\{E_4(\mathbf{i})\} && (30) \\
&\quad + \sum_{i_{2c}\neq 1, i_{2p}\neq 1} Pr\{E_4(\mathbf{i})\} && (31)
\end{aligned}$$

Here, once the rates satisfy the following equations, $Pr\{E_4|E_3^c\}$ vanishes for sufficiently large n.

$$\begin{aligned}
R_{2c} &< I(V_{2c}, V_{2p}; Y_2|Q) && (32) \\
R_{2p} &< I(V_{2p}; Y_2|V_{2c}, Q) && (33) \\
R_{2c} + R_{2p} &< I(V_{2c}, V_{2p}; Y_2|Q) && (34)
\end{aligned}$$

The first equation is redundant here.

Equivocation Computation:

We bound the conditional entropy as follows:

$$\begin{aligned} H(W_1|\mathbf{Y_2}) &\geq H(W_1|\mathbf{Y_2},\mathbf{V_{2c}},\mathbf{V_{2p}},\mathbf{Q}) \\ &= H(W_1) - I(W_1;\mathbf{Y_2},\mathbf{V_{2c}},\mathbf{V_{2p}}|\mathbf{Q}) \\ &= H(W_1) - I(W_1,W_1';\mathbf{Y_2},\mathbf{V_{2c}},\mathbf{V_{2p}}|\mathbf{Q}) \\ &\quad +I(W_1';\mathbf{Y_2},\mathbf{V_{2c}},\mathbf{V_{2p}}|W_1,\mathbf{Q}) \\ &\overset{(a)}{\geq} H(W_1) - I(\mathbf{V_1};\mathbf{Y_2},\mathbf{V_{2c}},\mathbf{V_{2p}}|\mathbf{Q}) \\ &\quad +H(W_1'|W_1,\mathbf{Q}) \\ &\quad -H(W_1'|\mathbf{Y_2},\mathbf{V_{2c}},\mathbf{V_{2p}},W_1,\mathbf{Q}) \\ &\overset{(b)}{\geq} H(W_1) + n(R_1' - I(V_1;Y_2,V_{2c},V_{2p}|Q)) \\ &\quad -n(\epsilon_1+\epsilon_2), \end{aligned}$$

where in (a) we used the fact that, given $\mathbf{Q}$, $(W_1, W_1') \rightarrow \mathbf{V_1} \rightarrow (\mathbf{Y_2},\mathbf{V_{2c}},\mathbf{V_{2p}})$ forms a Markov chain; and (b) follows due to the following:

1) $I(\mathbf{V_1};\mathbf{Y_2},\mathbf{V_{2c}},\mathbf{V_{2p}}|\mathbf{Q}) \leq nI(V_1;Y_2,V_{2c},V_{2p}|Q) + n\epsilon_1$ with $\epsilon_1 \rightarrow 0$ as $n \rightarrow \infty$
2) Fano's inequality and the binning codebook construction implies that $\frac{1}{n}H(W_1'|\mathbf{Y_2},\mathbf{V_{2c}},\mathbf{V_{2p}},W_1,\mathbf{Q}) \leq \epsilon_2$ with some $\epsilon_2 \rightarrow 0$ as $n \rightarrow \infty$ once we set

$$R_1' = I(V_1;Y_2|V_{2c},V_{2p},Q) \tag{35}$$

Now, using the above, we obtain that

$$\frac{1}{n}I(W_1;\mathbf{Y_2}) \leq \epsilon \text{ with some } \epsilon \rightarrow 0 \text{ as } n \rightarrow \infty.$$

Therefore, the secrecy and reliability constraints are satisfied if (25), (26), (27), (33), (34), and (35) are satisfied. Combining these equations with $R_2 = R_{2c} + R_{2p}$ completes the proof.

Appendix B
Proof of Theorem 4

The function u_2 is concave with respect to γ, if

$$\gamma_{min} \triangleq \frac{1+P_2^{max}}{P_2^{max}} + \frac{c_{12}P_1}{P_2^{max}(1-\sqrt{\frac{\beta+1}{\beta}})} < \gamma. \tag{36}$$

If (36) is satisfied, we find the optimal operating point for u_2 given P_1, solving $\frac{\delta u_2}{\delta \gamma} = 0$:

$$\gamma^* = 1 + \frac{1-\beta c_{12}P_1}{P_2^{max}} \tag{37}$$

Here $\beta > 0$ implies $\gamma^* > \gamma_{min}$, which implies that this γ^* is the optimal response. Now, assuming that the NE will occur at $s_2 = \gamma^*$, we derive the optimal response of the primary user.

$$\begin{aligned} u_1(P_1,\gamma^*) &= \frac{1}{2}\log\left(1+\frac{P_1}{1+c_{21}P_2^{max}}\right) \\ &\quad -\frac{1}{2}\log\left(\frac{1+\beta}{\beta}\right) - \alpha P_1 \end{aligned} \tag{38}$$

$$\frac{\delta u_1}{\delta P_1} = \frac{1}{2\ln 2}\frac{1}{1+c_{21}P_2^{max}+P_1} - \alpha \tag{39}$$

$$\frac{\delta^2 u_1}{\delta P_1^2} = \frac{1}{2\ln 2}\frac{-1}{(1+c_{21}P_2^{max}+P_1)^2} \tag{40}$$

The second derivative test shows that u_1 is concave everywhere on $[0, P_1^{max}]$, and thus the maximum for γ^* is

$$P_1^* = \frac{1}{\alpha 2\ln 2} - c_{21}P_2 - 1 \tag{41}$$

with

$$\frac{1}{\alpha 2\ln 2} > c_{21}P_2 + 1 \tag{42}$$

to guarantee $P_1^* > 0$. Now, we have

$$\gamma^* = 1 + \frac{1-\beta c_{12}(\frac{1}{\alpha 2\ln 2} - c_{21}P_2 - 1)}{P_2} \tag{43}$$

We would like to satisfy $\gamma^* \in [0,1]$.

$$0 \leq \gamma^* \leq 1 \tag{44}$$

$$0 \leq 1 + \frac{1-\beta c_{12}(\frac{1}{\alpha 2\ln 2} - c_{21}P_2 - 1)}{P_2} \leq 1, \tag{45}$$

which reduces to

$$\frac{\beta c_{12}}{2\ln 2(1+\beta c_{12}(1+c_{21}P_2)+P_2)} \leq \alpha \tag{46}$$

and

$$\alpha \leq \frac{\beta c_{12}}{2\ln 2(1+\beta c_{12}(1+c_{21}P_2))}. \tag{47}$$

For some $k \in (0,1)$, we set

$$\alpha 2\ln 2 = \frac{\beta c_{12}}{1+\beta c_{12}(1+c_{21}P_2)+kP_2} \tag{48}$$

to satisfy (47) and (46). As a result $\gamma^* = 1-k$. Note that if (47) holds, then

$$\alpha 2\ln 2 \leq \frac{\beta c_{12}}{(1+\beta c_{12}(1+c_{21}P_2))} < \frac{1}{(1+c_{21}P_2)}.$$

Hence, (47) guarantees (42). Additionally, to guarantee $P_1^* \leq P_1^{max}$ we require (from (41)):

$$\frac{1+kP_2}{\beta c_{12}} \leq P_1^{max} \tag{49}$$

Thus, we obtain the unique NE at $s_1 = P_1^*$ and $s_2 = \gamma^*$.

References

[1] N. Devroye, P. Mitran, and V. Tarokh, "Achievable rates in cognitive radio channels," IEEE Trans. Inf. Theory, vol. 52, no. 5, pp. 1813-1827, May 2006.

[2] A. Jovicic and P. Viswanath, "Cognitive Radio: An Information-Theoretic Perspective," IEEE Trans. Inf. Theory, vol. 55, no. 9, pp 3945-3958, Sept. 2009.

[3] A. D. Wyner, "The Wire-Tap Channel," The Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[4] L. Zhang, Y. Xin, Y.-C. Liang, and X. Wang, "Achievable rate regions of cognitive radio channels with a confidential message," in Proc. 2009 IEEE International Conference on Communications (ICC 2009), 2009.

[5] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdu, "Capacity of cognitive interference channels with and without secrecy," IEEE Trans. Inf. Theory, vol. 55, no. 2, pp. 604-619, Feb. 2009.

[6] L. Lai and H. El Gamal, "The Relay-Eavesdropper Channel: Cooperation for Secrecy," IEEE Trans. Inf. Theory, vol. 54, no. 9, pp. 4005-4019, Sept. 2008.

[7] R. Liu, I. Maric, P. Spasojevic, 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. 2493-2507, Jun. 2008.