2011

# Minimax Games for Cooperative Spectrum Sensing in a Centralized Cognitive Radio Network in the Presence of Interferers

Venkata Sriram Siddhardh Nadendla
*Syracuse University*, vnadendl@syr.edu

Hao Chen
*Boise State University*

Pramod Varshney
*Syracuse University*, varshney@syr.edu

# Minimax Games for Cooperative Spectrum Sensing in a Centralized Cognitive Radio Network in the Presence of Interferers

V. Sriram Siddhardh (Sid) Nadendla
Department of EECS
Syracuse University,
Syracuse, New York 13244.
Email: vnadendl@syr.edu

Hao Chen
Department of ECE
Boise State University,
Boise, Idaho 83725.
Email: haochen@boisestate.edu

Pramod K. Varshney
Department of EECS
Syracuse University,
Syracuse, New York 13244.
Email: varshney@syr.edu

***Abstract*—In this paper, we consider the problem of interference attacks for cooperative spectrum sensing in a centralized cognitive radio network comprising N cognitive radios (CRs) and one fusion center (FC) in the presence of a fixed interferer. The design metric chosen is the error probability. We prove the existence of a saddle-point in the minimax game between the interferer and the CR network. An optimal solution is found that maximizes the objective with respect to the interferer's parameters and minimizes the same with respect to the CR network's parameters. We show that the probability of error is a quasi-convex function with respect to the network's parameters and a monotone function with respect to the interferer's parameters. We also present numerical results that corroborate our theoretical results.**

## I. Introduction

Cognitive radio (CR) technology has received significant recent attention by many researchers due to the spectrum scarcity caused by growing demand. In order to accommodate upcoming applications, FCC started looking for practical solutions, one of which being the use of cognitive radios implemented over software-defined radios [1]. An important function of a cognitive radio is spectrum sensing where the radio scans the surrounding environment and finds the unused frequency bands of the licensed users (primary users) for use by secondary users. But since one radio is spatially limited while scanning the surroundings, in order to cope with the hidden terminal problem, cooperative spectrum sensing has been proposed [2]. Extensive research has been done in the literature regarding cooperative spectrum sensing, but security threats to this function have not been given much attention.

Security threats in CR networks can primarily be classified into two types - intrinsic and extrinsic attacks. *Intrinsic* attacks are the attacks on the network from within. Some of these attacks are Byzantine attacks and routing misbehavior attacks. Attacks from outside sources are called *extrinsic* attacks and examples include eavesdropping, jamming and primary-user emulation attacks (PUEAs). In this paper, we investigate the problem of interfering attacks over cooperative spectrum sensing in centralized CR networks. For more details on other possible attacks on CRs, the reader can refer to [3].

This work was supported in part by AFOSR Grants FA-9550-09-1-0064 and FA-9550-09-C-0146.

Interference attacks have always been focussed in the past as jamming attacks on one channel at a time and the problem has been solved in the context of minimax games [4] under different channel scenarios. Spread spectrum techniques have been offered as protection against jamming attacks [5], but seldom was this problem considered in the context of cognitive radio networks. PUEA is a special type of jamming where the attacker tries to emulate the primary user to disrupt the network. Li *et al.* [6] present this problem in a multiple channel framework, where the radio tries to move from one channel to another in order to evade jamming attacks as a one-stage minimax game as well as a multi-stage stochastic game. In this paper, we consider an interference attack which generalizes PUEAs by not just considering the source-sensor channel, but also the sensor-FC channel. This allows us to ensure better protection against interference threats in cooperative spectrum sensing.

We assume that the interferer has limited energy resources which it uses to disrupt or deteriorate the performance of the network. Specifically, we focus on two different channels in this paper, one being the target (PU) to spectrum sensor (CR) channel and the other being the transmission channel between the sensor and the fusion center which makes the global spectrum sensing decision. Therefore, the interferer tries to distribute its resources over the two available vulnerable options, while the network on the other hand, tries to protect itself from the interferer by manipulating its parameters which include the local quantizer threshold within the sensor and the threshold used in the fusion rule. Thus, we present a minimax formulation and prove the existence of a solution to this problem in this paper.

The remaining paper is organized as follows. We present some basic definitions and useful results from game theory in Section II. In Section III, we present the system model considered and the assumptions over which we build the minimax formulation. We also introduce the design metric used in this paper, the error probability of the network and

present how this can be analytically computed in terms of both the network's and interferer's parameters. Next, we formulate our minimax problem in Section IV. In Section V, we analyze the error probability as a function of both the network's and interferer's parameters and prove the existence of a solution to the formulation presented in Section IV. Furthermore, we present numerical results to corroborate our analytical results in Section VI. Finally, we conclude the paper with Section VII by summarizing the paper.

## II. Preliminaries

In this section, we introduce some basic definitions and theorems in game theory that are useful in this paper.

Let $(\mathbf{S}, \mathbf{u})$ denote a game played by $N$ players, where $\mathbf{S} = S_1 \times \cdots \times S_N$ is the space of strategy profiles and $\mathbf{u} = \{u_1(s_1), \cdots, u_N(s_N)\}$ be the payoff function corresponding to the strategy profile $\mathbf{s} = \{s_1, \cdots, s_N\} \in \mathbf{S}$ adopted by the N players. If $s_i$ is the strategy chosen by player-$i$, then we denote $\mathbf{s_{-i}} = \{s_1, \cdots, s_{i-1}, s_{i+1}, \cdots, s_N\}$ as the set of strategies chosen by the players other than player-$i$ in the game.

**Definition 1** (Normal-form game)**.** *A game $(\mathbf{S}, \mathbf{u})$ is said to be represented in its normal-form if it is presented in the form of a matrix.*

**Definition 2** (Finite Game)**.** *A game $(\mathbf{S}, \mathbf{u})$ is said to be finite if the strategy-profile space $\mathbf{S}$ is a finite set.*

**Definition 3** (Nash Equilibrium)**.** *Strategy $\mathbf{s} \in \mathbf{S}$ is a Nash Equilibrium for the game $(\mathbf{S}, \mathbf{u})$ if $u_i(\mathbf{s}) \geq u_i(\hat{s}_i, \mathbf{s_{-i}}), \forall \hat{s}_i \in \mathbf{S_i}$, $i = 1, \cdots, N$.*

In other words, Nash Equilibrium (NE) is a strategy profile where, no player can deviate unilaterally in order to increase his payoff. Nash's biggest contribution to game theory is the following theorem in his classic paper [7], where he proved the existence of a NE for a class of normal-form games.

**Theorem 1 (Nash, [7]).** *Every finite game in normal form has a NE in either mixed or pure strategies.*

In the case of continuous games, the existence of a NE has been proved for some special cases such as games with convex-concave utility functions. The following theorem is a useful generalization to the Nash's equilibrium theorem for continuous games, where the saddle point is proved under the assumption of quasi-concave-convexity.

**Theorem 2 (Nikaido, [8]).** *Let $X$ and $Y$ be any two compact sets. If $K(x, y)$ is any function that is quasi-concave in $x \in X$ and quasi-convex in $y \in Y$, then there exists a unique $(x, y) \in X \times Y$ such that*

$$\max_{x \in X} \min_{y \in Y} K(x, y) = \min_{y \in Y} \max_{x \in X} K(x, y). \tag{1}$$

## III. System Model

We consider a CR network model with $N$ CRs (or spectrum sensors), each indexed as $i \in \{1, 2, \cdots, N\}$ and one fusion center FC trying to detect whether a Primary User (PU) T is transmitting ($H_1$ hypothesis ) or not ( $H_0$). Let the prior probabilities of the hypotheses be $P(H_0) = p_0$ and $P(H_1) = p_1 = 1 - p_0$. Also, we assume that a stationary interferer is present at distances $d_{J,i}$, $d_{J,fc}$ from the $i^{th}$ CR and the FC respectively which jams both the CR (sensing channel) and FC (communication channel) receptions by injecting noise-like signals. These individual jamming signals are denoted as $w_s$ and $w_{fc}$ respectively, where $w_s \sim \mathcal{N}(0, \sigma^2_{W_s})$ and $w_{fc} \sim \mathcal{N}(0, \sigma^2_{W_{fc}})$. We also assume that the attacker has a reasonable total power constraint over its transmissions, given by $\sigma^2_{W_s} + \sigma^2_{W_{fc}} \leq P_J$. Therefore, the interferer would choose its attack by optimizing the power distribution of noise-like signals over the N different CRs' and the FC's receptions.

Without any loss of generality, we assume that the transmitting power of the PU is $A = 1$ under hypothesis $H_1$ or $A = 0$ under $H_0$. Hence, the signal received at the CR is given by

$$r_i = h_i A + n_i + h_{J_i} w_s \tag{2}$$

where $h_i$ is the channel gain for the corresponding target-to-$i^{th}$ CR channel, $h_{J_i}$ is the channel gain for the interferer-to-$i^{th}$ CR channel and $n_i \sim \mathcal{N}(0, \sigma^2_s)$. The CR sends its received signal (raw data) to the fusion center through a communication channel. Therefore, the received signal $r_{fc}$ is given by

$$r_{fc} = \sum_{i=1}^{N} g_i . r_i + n_{fc} + g_J w_{fc} \tag{3}$$

where $g_i$ is the path-loss coefficient for the corresponding $i^{th}$ CR-to-FC channel, $g_J$ is the path-loss coefficient for the interferer-to-FC channel and $n_{fc} \sim \mathcal{N}(0, \sigma^2_{fc})$. In this paper, all the path-loss coefficients are assumed to be known to both the attacker and FC.

The optimal fusion rule is given by the likelihood ratio rule as follows.

$$\frac{p(r_{fc}|H_1)}{p(r_{fc}|H_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \frac{p_0}{p_1} \tag{4}$$

In order to find the optimal fusion rule, we evaluate the conditional probability distributions, $p(r_{fc}|H_1)$ and $p(r_{fc}|H_0)$. Note that, the CR receptions $\mathbf{r} = \{r_1, \cdots, r_N\}$ are dependent on each other because of the presence of the common interference signal $w_s$. Since $w_s, n_1, n_2, \cdots, n_N$ are independent Gaussian noises, it is easy to show from Equation (2) that the conditional joint distribution of $\mathbf{r}$ is normally distributed. Therefore, we have $r_{fc}|H_k \sim \mathcal{N}(\mu_k, \sigma^2)$, $k = 0, 1$, where

$$\mu_0 = \mathbb{E}(r_{fc}|H_0) = 0 \tag{5a}$$

$$\mu_1 = \mathbb{E}(r_{fc}|H_1) = \sum_{i=1}^{N} g_i h_i \tag{5b}$$

and

$$\begin{aligned} \sigma^2 &= Var(r_{fc}|H_0) \\ &= \sigma^2_{fc} + g_J^2 \sigma^2_{W_{fc}} + \left(\sum_{i=1}^{N} g_i\right)^2 \sigma^2_s + \left(\sum_{i=1}^{N} g_i h_{J_i}\right)^2 \sigma^2_{W_s} \end{aligned} \tag{6}$$

Hence, the likelihood ratio fusion rule, given by Equation (4), can be reduced to

$$r_{fc} \underset{H_0}{\overset{H_1}{\gtrless}} \lambda \tag{7}$$

Note that, the optimal $\lambda$ also depends on the choice of attacker's parameters, $\sigma_{W_s}$ and $\sigma_{W_{fc}}$. Therefore, we treat $\lambda$ as the parameter that determines network's strategy.

In this paper, we consider the probability of error, $P_E$, as the performance metric (utility function of the minimax game), which is given as follows.

$$P_E = p_0 Q_F + p_1(1 - Q_D). \tag{8}$$

where,

$$Q_F = P(r_{fc} \geq \lambda | H_0) \tag{9a}$$

$$Q_D = P(r_{fc} \geq \lambda | H_1) \tag{9b}$$

Now, we investigate the impact of interferer's strategy (choice of $\sigma_{W_s}$ and $\sigma_{W_{fc}}$, that maximizes $P_E$) and the best possible counter-attack from the network's perspective through an optimal choice of the threshold $\lambda$ that minimizes $P_E$.

## IV. Problem Formulation

In this section, we formulate a minimax game framework where, the interferer on the one hand, optimizes its attack within the available resources, while the network, on the other hand, chooses an optimal strategy (design) to improve its performance. The solution to this minimax game between the network and the attacker is the Nash equilibrium (NE), which is a saddle point in the design metric, $P_E$.

Thus, our problem formulation is as follows.

**Problem Statement.** *Prove the existence of NE and find* $\{\lambda, \sigma_{W_s}, \sigma_{W_{fc}}\}$ *such that*

$$\min_{\lambda} \max_{\underline{\sigma}} P_E = \max_{\underline{\sigma}} \min_{\lambda} P_E$$

*under the constraint*

$$\sigma^2_{W_s} + \sigma^2_{W_{fc}} \leq P_J \tag{10}$$

where $\underline{\sigma} = \{\sigma_{W_s}, \sigma_{W_{fc}}\}$.

In the next section, we present some analytical results that allow us to find the optimal minimax strategies for the above mentioned formulation.

## V. Equilibrium Analysis

In the minimax game between the centralized CR network and the interferer, the network has one strategy parameter, $\lambda$, while the interferer has control on $\sigma_{w_s}$ and $\sigma_{w_{fc}}$. Nash-Equilibrium (NE) to a game exists if there exists a saddle-point in the performance metric considered (in our case, error probability) which is a function of both network's and attacker's strategies, as given by Equation (8).

In this context, it is easy to show that the expressions for $Q_F$ and $Q_D$ in Equations (9a) and (9b) are as follows.

$$Q_F = Q\left(\frac{\lambda}{\sigma}\right) \tag{11a}$$

$$Q_D = Q\left(\frac{\lambda - \cdot \sum_{i=1}^{N} g_i \cdot h_i}{\sigma}\right) \tag{11b}$$

So, we investigate the behavior of the performance metric (error probability) as a function of network's and interferer's strategies. We first present the behavior of $P_E$ with respect to network's strategy parameter, $\lambda$.

**Lemma 1.** *For a given* $\sigma_{w_s}$ *and* $\sigma_{w_{fc}}$, $P_E$ *is a quasiconvex function of* $\lambda$.

*Proof:* Treating $\sigma_{w_s}$ and $\sigma_{w_{fc}}$ as constants, we differentiate $P_E$ with respect to $\lambda$ and simplify the expression as follows.

$$\begin{aligned} \frac{\partial P_E}{\partial \lambda} &= p_0 \frac{\partial Q_F}{\partial \lambda} - p_1 \frac{\partial Q_D}{\partial \lambda} \\ &= r_1(\lambda) \cdot \{p_1 \cdot r_2(\lambda) - p_0\} \end{aligned} \tag{12}$$

where

$$r_1(\lambda) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{\lambda^2}{2\sigma^2}\right), \tag{13a}$$

$$r_2(\lambda) = \exp\left(\frac{2 \cdot \sum_{i=1}^{N} g_i h_i \cdot \lambda - \sigma^2}{2\sigma^2}\right) \tag{13b}$$

Note that $r_1(\lambda) \geq 0$. Therefore, the value of $r_2(\lambda)$ decides the behavior of $P_E$. One can easily observe that $r_2(\lambda)$ is an exponential function of $\lambda$ and is, therefore, a monotonic function of $\lambda$. Hence, there is only one value of $\lambda = \lambda_0$ at which $r_2(\lambda) = 0$. This implies that $\frac{\partial P_E}{\partial \lambda} \geq 0$, if $\lambda \geq \lambda_0$, and $\frac{\partial P_E}{\partial \lambda} < 0$, otherwise. In other words, $P_E$ is a quasi-convex function of $\lambda$. ■

Similarly, we investigate the behavior of $P_E$ with respect to the interferer's strategies in the following lemma.

**Lemma 2.** *For any given CR network with fixed* $\lambda$, *such that* $0 \leq \lambda \leq \sum_{i=1}^{N} g_i h_i$ *(under a limiting constraint on* $P_J$*),* $P_E$ *is a monotonic function of* $\sigma_{w_{fc}}$, *given* $\sigma_{w_s}$. *Similarly,* $P_E$ *is a monotonic function of* $\sigma_{w_s}$, *given* $\sigma_{w_{fc}}$.

*Proof:* When $\lambda \in \left[0, \sum_{i=1}^{N} g_i h_i\right]$, it is straightforward to show that $Q_F$ ($Q_D$) is a monotonic increasing (decreasing) function of $\sigma^2$. The lemma follows from the definition of $\sigma^2$ (Eqn. (6)).

It is easy to show that, given $\sigma^2$, the optimal $\lambda$ is of the

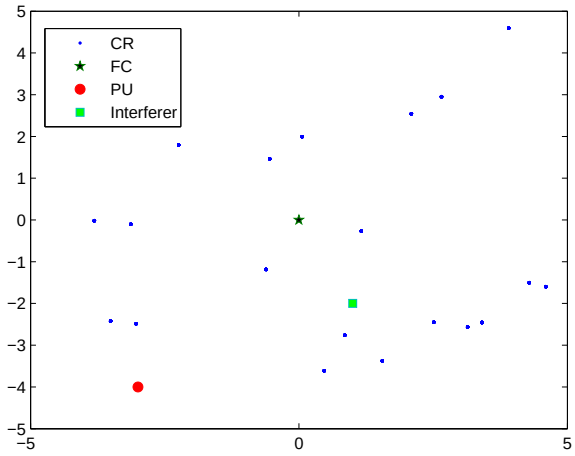



Fig. 1: CR Network for $p_0 = 0.5$ case

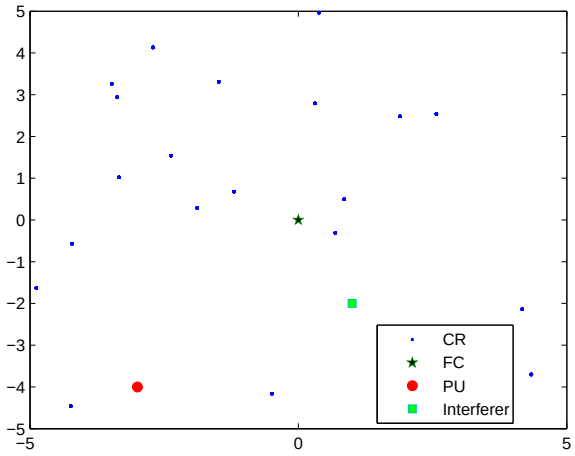



Fig. 2: CR Network for $p_0 = 0.8$ case

following form.

$$\lambda_{opt} = \frac{1}{2}\sum_{i=1}^{N} g_i h_i + \frac{\sigma^2}{\sum_{i=1}^{N} g_i h_i} \ln \frac{p_0}{p_1} \tag{14}$$

Since the contribution of thermal noise is usually small, an appropriate limiting constraint on $P_J$ results in a reasonably smaller value of $\sigma$. Then, from Equation (14), $0 \leq \lambda_{opt} \leq \sum_{i=1}^{N} g_i h_i$ and hence $P_E$ is a monotonic increasing function of $\sigma_{w_s}$, given $\sigma_{w_{fc}}$ and similarly, vice versa. ■

Note that $P_E$ is still a quasi-concave function of both $\sigma_{w_s}$ and $\sigma_{w_{fc}}$, as monotonicity is a special case of quasi-concavity. Therefore, by Theorem 2, a unique saddle-point (Nash Equilibrium) exists in the minimax game formulated between the CR network and the interferer.

## VI. Numerical Results

We obtain this NE numerically in this paper for the 20-node CR network shown in Figures 1 and 2. We assume that the FC is centered at origin ($\mathbf{x_{fc}} = 0$), PU is located at $\mathbf{x_t} = (-3, -4)$, interferer is at $\mathbf{x_j} = (1, -2)$ and CRs are randomly deployed in the $10 \times 10$ grid centered around origin. We assume $\sigma_s = 0.1$, $\sigma_{fc} = 0.1$ and $P_J = 0.5$. Also, we consider free-space path loss shadowing with any path loss coefficient defined in the form $\sqrt{\frac{1}{(1+d_{\{\cdot\}}^2)}}$ where $d_{\{\cdot\}}$ is the propagation distance between the transmitter node and the receiver node in the above mentioned system-model.

First, in Figure 3, we present error probability as a function of $\lambda$, $\sigma_{W_{fc}}$ and $\sigma_{W_s}$ for the CR network shown in Figure 1. In this case, we let $p_0 = 0.5$, which is the worst case performance scenario of the network. The plots depict clearly both quasiconvexity with respect to $\lambda$ and monotonicity with respect to the attacker's parameters, $\sigma_{W_{fc}}$ and $\sigma_{W_s}$, whenever $\lambda \geq 0$. In this case,

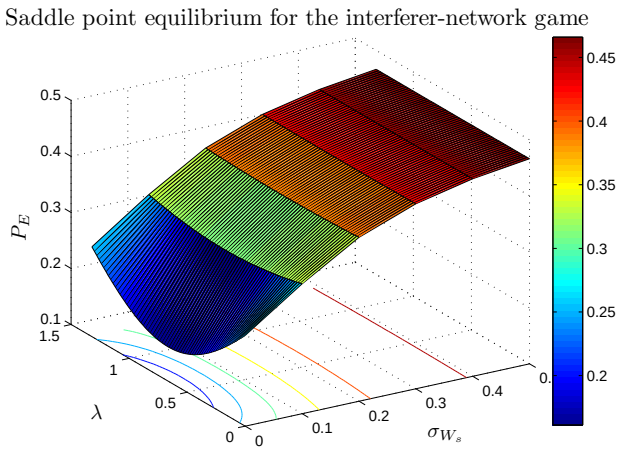
$$\lambda_{opt} = \frac{\sum_{i=1}^{N} g_i h_i}{2}.$$

Figure 4, on the other hand, presents the error probability as a function of $\lambda$, $\sigma_{W_{fc}}$ and $\sigma_{W_s}$ for $p_0 = 0.8$. We particularly present these results because $p_0 = 0.8$ is found in practice as pointed out by the FCC's survey on spectrum utilization of licensed bands [1]. One can clearly note that the NE of the game from the network's perspective has now moved away from $\lambda = 0$ due to the bias in the prior probabilities.

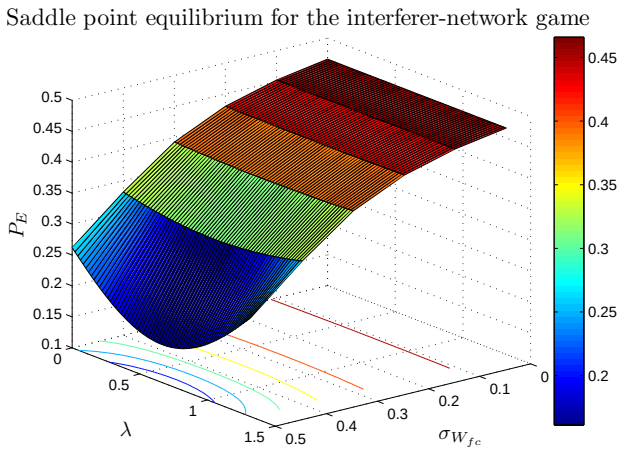
One can also note from Figures 3 and 4 that in both the scenarios considered, the optimal attack for the interferer is to degrade the individual CRs' performance by allocating all the available power to the sensing channel's noise-like signal ($\sigma_{W_s} = 1$). This corroborates our argument for the case when the attacker is close to the CR in [9], where we presented our analysis of a interfering attack on a given CR network. This can also be justified intuitively because the interferer would invest more energy in interfering the most vulnerable channel available (one with maximum information about the spectrum availability) in order to give maximal impact on the network performance. Therefore, the PU-CR channel, which carries maximum information about the true state of the channel availability, is the most vulnerable wireless link available for the interferer to attack and have maximal impact on the network performance as a whole. Another important observation is that, the figure-pairs 3a-3b and 4a-4b are mirror-images of each other with respect to $\sigma_{W_{fc}}$ and $\sigma_{W_s}$, indicating that the interferer is spending a total of $P_J$ units of energy, where $\sigma_{W_{fc}} = P_J - \sigma_{W_s}$.

## VII. Conclusion

In this paper, we have proved the existence of a solution to the minimax problem for cooperative spectrum sensing in a

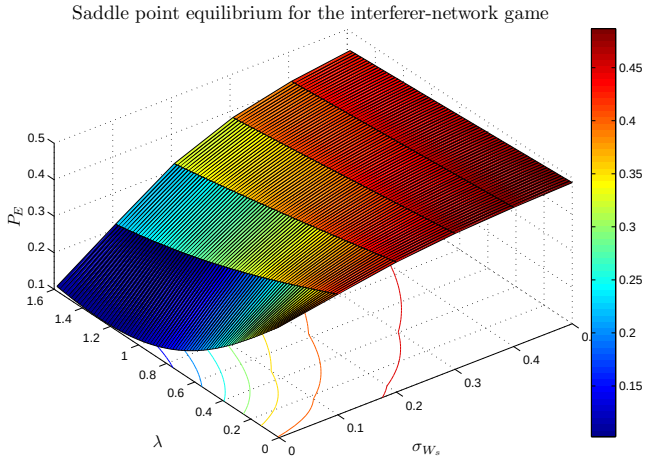



(a) Error Probability in terms of $\lambda$ and $\sigma^2_{W_s}$

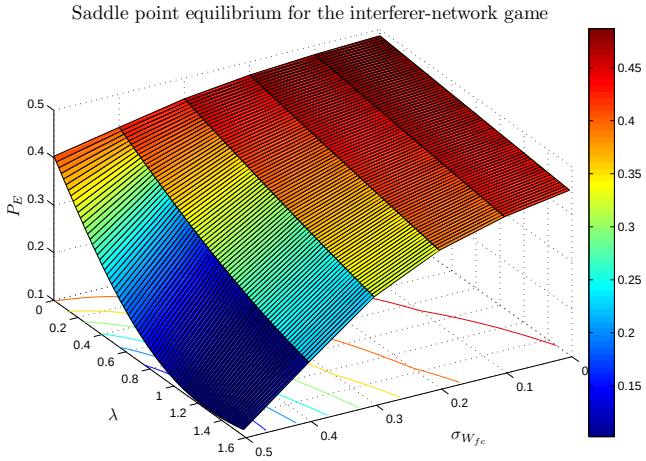



(b) Error Probability in terms of $\lambda$ and $\sigma^2_{W_{fc}}$

Fig. 3: Performance of the CR network for $p_0 = 0.5$




(a) Error Probability in terms of $\lambda$ and $\sigma^2_{W_s}$




(b) Error Probability in terms of $\lambda$ and $\sigma^2_{W_{fc}}$

Fig. 4: Performance of the CR network for $p_0 = 0.8$

centralized cognitive radio network in the presence of a fixed interferer by showing that the error probability is a quasi-convex function with respect to the network's parameters and a monotonic function (quasiconcave) with respect to the interferer's parameters. We found the optimal solution numerically in our simulation results that maximizes the objective function with respect to the interferer's parameters and minimizes the same with respect to the CR network's parameters.

## REFERENCES


[1] Q. Zhao and B. M. Sadler, "A survey of dynamic spectrum access," *IEEE Signal Process. Mag.*, vol. 24, no. 3, pp. 79–89, 2007.

[2] Z. Quan, S. Cui, H. Poor, and A. Sayed, "Collaborative wideband sensing for cognitive radios," *IEEE Signal Process. Mag.*, vol. 25, no. 6, pp. 60–73, 2008.

[3] J. L. Burbank, "Security in cognitive radio networks: The required evolution in approaches to wireless network security," in *Proc. 3rd Int. Conf. Cognitive Radio Oriented Wireless Networks and Communications CrownCom 2008*, 2008, pp. 1–7.

[4] T. Basar, "The gaussian test channel with an intelligent jammer," *IEEE Trans. Inf. Theory*, vol. 29, no. 1, pp. 152–157, 1983.

[5] R. Pickholtz, D. Schilling, and L. Milstein, "Theory of spread-spectrum communications–a tutorial," *IEEE Trans. Commun.*, vol. 30, no. 5, pp. 855–884, 1982.

[6] H. Li and Z. Han, "Dogfight in spectrum: Jamming and anti-jamming in multichannel cognitive radio systems," in *Proc. IEEE Global Telecommunications Conf. GLOBECOM 2009*, 2009, pp. 1–6.

[7] J. Nash, "Non-cooperative games," *Annals of Mathematics*, vol. 54, no. 2, pp. 286–295, September 1951.

[8] H. Nikaido, "On von neumann's minimax theorem," *Pacific Journal of Mathematics*, vol. 4, no. 1, pp. 65–72, 1954.

[9] V. S. S. Nadendla, H. Chen, and P. K. Varshney, "On jamming models against collaborative spectrum sensing in a simple cognitive radio network," in *2010 Conference Record of the 44th Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, November 2010.