A Game-Theoretic View on the Physical Layer Security of Cognitive Radio Networks

Ali Houjeij[1], Walid Saad[2], and Tamer Başar[1]

[1] Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, IL, USA, Emails: {houjeij2,basar1}@illinois.edu
[2] Electrical and Computer Engineering Department, University of Miami, Coral Gables, FL, USA, Email: walid@miami.edu

***Abstract*—In this paper, we investigate the problem of secure communication between secondary users (SUs) and their serving base station in the presence of multiple eavesdroppers and multiple primary users. We analyze the interactions between the SUs and eavesdroppers using the framework of noncooperative game theory. To solve the formulated game, we propose a novel secure channel selection algorithm that enables the SUs and eavesdroppers to take distributed decisions so as to reach a Nash equilibrium point. We study and analyze several properties of the equilibrium resulting from the proposed algorithm. Simulation results show that the proposed approach yields significant improvements of at least 32.7%, in terms of the average secrecy rate per SU, relative to a classical spectrum sharing scheme. Moreover, the results show that the proposed scheme enables the SUs to reach Nash equilibrium with up to 86.5% less computation than standard learning algorithms.**

I. Introduction

With the evolution of mobile and decentralized networks, implementing cryptographic techniques over large-scale wireless systems is becoming an increasingly complex task due to the associated computational overhead, especially in a resource constrained environment. Recently, physical layer (PHY) security has emerged as a promising solution for securing communication over the wireless medium. PHY security was first introduced in Wyner's seminal work [1] over the wire-tap channel and it was then extended to the wireless and mulit-user channels [2]. The main idea behind PHY security is to exploit the wireless channel characteristics, such as noise and fading, so as to improve the reliability of wireless transmission. This reliability is quantified through the notion of *secrecy rate*, which is defined as the rate of secret information sent from a node to its destination without being tapped in by malicious eavesdroppers.

The use of PHY security is of paramount importance for emerging wireless technologies such as cognitive radio networks (CR) which were introduced to boost the efficiency of spatial utilization of the radio spectrum [3]. In a CR network, a number of distributed, often ad hoc, unlicensed secondary users (SUs) are able to transmit over the licensed radio spectrum, when the associated channels are not being utilized by licensed primary users (PUs).

The decentralized nature of CR networks introduces numerous security issues that must be properly addressed [4]–[6]. For example, the authors in [4] study primary user emulation attacks by analyzing the equilibrium of a game between malicious and legitimate SUs. A second type of attack was considered in [5] where the authors address the problem of compromised SUs reporting false spectrum sensing results. The authors provide a solution technique to detect malicious SUs by assigning suspicious levels to each node. A comprehensive survey of CR security issues and solutions can be found in [6].

Clearly, while many aspects of security in cognitive radio have been studied [6], little has been done to analyze how the SUs' need to optimize their secrecy rates, in the presence of eavesdroppers, affects the spectrum sharing process. This becomes more challenging when addressing both the spectrum sharing and security aspects of the problem. In this case, the SUs must observe various parameters such as PUs' activity, mutual interference, and any potential or suspected eavesdropping, before choosing the transmission channel. To our knowledge, no work seems to have investigated how this potential presence of eavesdroppers can impact the channel selection strategies of the SUs in a cognitive network.

The main contribution of this paper is to introduce a novel scheme which enables the SUs to strategically decide on their preferred secure communication channel in a CR network, in the presence of eavesdroppers. To this end, we formulate a noncooperative game between the SUs and the eavesdroppers. This game consists of two levels of competition. On the one hand, the SUs need to choose their preferred channel so as to optimize the tradeoff between interference (due to channel congestion), availability (due to PUs' activity) and secrecy rate (due to the potential of being eavesdropped). On the other hand, the eavesdroppers are strategic and need to choose the channels that enable them to minimize the overall network's secrecy rate. We first study several properties of this game and characterize the resulting equilibrium. Then, we propose a distributed, low-complexity learning algorithm that can be adopted by the SUs and the eavesdroppers so as to reach an equilibrium of the game. Using simulations, we evaluate the performance of our algorithm and show that it yields significant performance improvements, in terms of the average secrecy rate per SU, compared to classical schemes.

The rest of the paper is organized as follows: Section II introduces the system model and describes the game formulation, and Section III provides the proposed game solution. Simulation results are analyzed in IV. Finally, conclusions are drawn in Section V.

II. System Model and Game Formulation

A. System Model

Consider a cognitive radio network composed of a set $\mathcal{M}$ of M licensed PUs or channels which can be accessed by

This research was supported in part by the U.S. National Science Foundation under Grant CNS-1253731, an AFOSR MURI Grant FA9550-10-1-0573, and Boeing and NSA through the Information Trust Institute at the University of Illinois

a set $\mathcal{N}$ of N unlicensed SUs, when they are not used for PU transmission. The objective of each SU is to communicate with a common base station (BS) by using one of the available PU channels. To model the activity of the primary users, we assume that each channel $m \in \mathcal{M}$ has a probability θ_m of being available, i.e., not used by its corresponding PU.

We consider a frequency selective Rayleigh fading channel so that the channel gain experienced by SU i on channel $m \in \mathcal{M}$ at the BS is given by $h_{i,m} = \alpha_m \cdot d_i^{-\mu}$. Here, μ denotes the path loss exponent, α_m represents the Rayleigh fading amplitude on channel m, while d_i represents the distance between SU i and the BS. Hereinafter, we consider a slowly varying channel with a long coherence time.

In essence, the SUs are interested in choosing the channel that provides the highest transmission rate. Since SUs share the available spectrum, mutual interference occurs when more than one SU chooses the same channel. The SINR perceived by an SU i when transmitting over a channel m is:

$$\gamma_{i,m} = \frac{h_{i,m}P_{i,m}}{\sigma^2 + \sum\limits_{j \in \mathcal{N}_m \setminus \{i\}} h_{j,m}P_{j,m}}, \tag{1}$$

where $P_{i,m}$ is the maximum transmit power of SU i on channel m, σ^2 is the variance of the Gaussian noise, and $\mathcal{N}_m$ is the set of SUs that are using channel m for transmission.

The capacity achieved by an SU i over an available channel m is thus given by:

$$C_i^m = \log(1 + \gamma_{i,m}), \tag{2}$$

where $\gamma_{i,m}$ is the SINR achieved by SU i on channel m as per (1). The capacity C_i^m is set to zero if the channel m is not available.

In this model, each SU tries to choose the channel which optimizes its capacity at the BS. Now, consider that a set $\mathcal{K}$ of K eavesdroppers is present in the network. Here, we consider practical, inexpensive eavesdropping devices which often have limited hardware and can only eavesdrop on a limited number of channels as discussed in [7] and the references therein. In the presence of eavesdroppers, the SUs aim at, not only maximizing their capacity, but also choosing a channel that can potentially lead to secure communication. To this end, each SU will seek to choose the available channel which can yield the highest secrecy rate. This leads to a competitive environment between the SUs, as well as between SUs and eavesdroppers. On the one hand, SUs compete to gain access to the available channels in order to maximize their secrecy rates. On the other hand, the objective of the eavesdroppers is to reduce the secrecy rate of the overall network or a subset of SUs which they are interested in, by choosing their optimal channels. We consider the case in which eavesdroppers want to reduce the overall social welfare of the network. Certainly, our approach can easily accommodate other eavesdropping models as well.

Given a set $\mathcal{K}_m$ of eavesdroppers active on a channel m, the secrecy rate achieved by an SU i is given by:

$$\tilde{C}_i^m = \left(C_i^m - \max_{k \in \mathcal{K}_m} C_{i,k}^m \right)^+, \tag{3}$$

where $a^+ := \max(a, 0)$ and C_i^m is given by (2). $C_{i,k}^m$ is the capacity of channel m between SU i and eavesdropper k as received by k and is given by:

$$C_{i,k}^m = \log\left(1 + \frac{g_{i,k,m}P_{i,m}}{\sigma^2 + \sum\limits_{j \in \mathcal{N}_m \setminus \{i\}} g_{j,k,m}P_{j,m}}\right), \tag{4}$$

where $g_{i,k,m} = \alpha_m \cdot d_{i,k}^{-\mu}$ represents the channel gain between SU i and any eavesdropper $k \in \mathcal{K}$ where $d_{i,k}$ is the distance between i and k.

It is clear from (3) that both channel congestion and eavesdropping decrease the overall secrecy rate of secondary users. Consequently, when an SU tries to maximize its secrecy rate in the presence of multiple eavesdroppers, there is an obvious tradeoff between choosing a crowded channel with better secrecy versus a less crowded one with more damaging eavesdroppers.

B. Game Formulation

We use the framework of noncooperative game theory to study the interactions between SUs and eavesdroppers [8]. This problem is game theoretic by nature since both SUs and eavesdroppers want to selfishly maximize their gains.

Denote by $\mathcal{P} = \mathcal{N} \bigcup \mathcal{K}$ the set of all players in this game, that is the set of SUs and eavesdroppers in the network. Players in $\mathcal{P}$ choose their actions from the same action space $\mathcal{M}_i = \mathcal{M}\ \forall i \in \mathcal{P}$ of size M representing the channels in the system. The action $m_i \in \mathcal{M}_i$ of an SU i represents the channel it chooses to transmit on, while the action $e_k \in \mathcal{M}_k$ of an eavesdropper k represents the channel it chooses to listen on. In this section, we define the capacities as functions of the channels, i.e., $C_i(m) := C_i^m$, $C_{i,k}(m) := C_{i,k}^m$ and $\tilde{C}_i(m) := \tilde{C}_i^m$.

We define the utility of the secondary users as the expected value, with respect to the PUs' activity, of the achieved secrecy rate, expressed in (3), when choosing a certain channel. Formally, the utility of an SU $i \in \mathcal{N}$ that selects an action $m_i \in \mathcal{M}_i$ is given by:

$$\begin{aligned} \phi(m_i, \boldsymbol{m}_{-i}, \boldsymbol{e}) &= \mathbb{E}\left[\tilde{C}_i(m_i)\right] \\ &= \theta_{m_i}\left(C_i(m_i) - \max_{\{k \in \mathcal{K}: e_k = m_i\}} C_{i,k}(m_i) \right)^+. \end{aligned} \tag{5}$$

Here, $\boldsymbol{m}_{-i}$ represents the vector of all actions taken by all other SUs in the set $\mathcal{N} \setminus \{i\}$, and $\boldsymbol{e}$ represents the vector of actions taken by all eavesdroppers in $\mathcal{K}$. Each SU aims at maximizing its achieved secrecy rate by choosing the channel that maximizes its utility function.

The utility of each eavesdropper is captured by its ability to decrease the secrecy rates of the SUs. Formally, the utility of an eavesdropper $k \in \mathcal{K}$ that chooses an action $e_k \in \mathcal{M}_k$ is

given by the expected value, with respect to the PUs' activity, of its eavesdropping effect on all SUs transmitting on channel e_k. Using (4), the utility is given by:

$$\psi(e_k, \boldsymbol{m}) = \theta_{e_k} \left(\sum_{i \in \mathcal{N}: e_k = m_k} C_{i,k}(e_k) \right). \quad (6)$$

Here, $\boldsymbol{m}$ represents the vector of actions taken by all SUs in $\mathcal{N}$. Hence, clearly, the eavesdroppers are mainly competing with the SUs, but not with one another. Each eavesdropper aims at maximizing its utility in order to increase the damage that it inflicts on the SUs.

Generally, let $a_i \in \mathcal{M}_i$ be the action of player $i \in \mathcal{P}$, i.e., $a_i = m_i$ if $i \in \mathcal{N}$ and $a_i = e_i$ if $i \in \mathcal{K}$. Let $\boldsymbol{a}_{-i}$ be the vector of actions taken by all players in the set $\mathcal{P} \setminus \{i\}$. Given the SUs' and eavesdroppers' utilities as expressed by (5) and (6), respectively, we define the general utility function as follows:

$$U_i(a_i, \boldsymbol{a}_{-i}) = \begin{cases} \phi(m_i, m_{-i}, \boldsymbol{e}) & \text{if } i \in \mathcal{N} \\ \psi(e_i, \boldsymbol{m}) & \text{if } i \in \mathcal{K} \end{cases} \quad (7)$$

Now, let $\boldsymbol{p}_i = \left[p_i^1, p_i^2, \cdots, p_i^M\right] \in \Lambda_i$ be the mixed strategy of player i $\forall i \in \mathcal{P}$. Each component p_i^m can be viewed as the frequency with which player i transmits on channel m, if $i \in \mathcal{N}$, or eavesdrops on channel m, if $i \in \mathcal{K}$. In other words, $p_i^m := \Pr(a_i = m)$. Λ_i represents the space of all possible mixed strategies for player i and it is defined as $\Lambda_i := \left\{\boldsymbol{p}_i \in [0,1]^M | \sum_{m \in \mathcal{M}_i} p_i^m = 1\right\}$. Let $\boldsymbol{p} = \{\boldsymbol{p}_i,\ i \in \mathcal{P}\}$; then, the expected utility of player i is given by

$$\bar{U}_i(\boldsymbol{p}_i, \boldsymbol{p_{-i}}) = \mathbb{E}_{\boldsymbol{p}}[U_i(a_i, \boldsymbol{a}_{-i})]$$

$$= \sum_{a_1 \in \mathcal{M}_1} \cdots \sum_{a_{N+K} \in \mathcal{M}_{N+K}} U_i(a_1, \cdots, a_{N+K}) \prod_{j=1}^{N+K} p_j^{a_j}, \quad (8)$$

where $\boldsymbol{p}_{-i}$ represents the vector of mixed strategies of all other players in $\mathcal{P} \setminus \{i\}$.

We now formulate a noncooperative game $\Gamma = \{\mathcal{P}, \mathcal{M}_{i\{i\in\mathcal{P}\}}, U_{i\{i\in\mathcal{P}\}}\}$ between N SUs and K eavesdroppers in the presence of M PUs. Our objective is to study and analyze the outcome from these interactions.

III. Game Solution

Here, we investigate the solution of the proposed finite noncooperative game Γ between SUs and eavesdroppers. Hereinafter, we use the term "player" to denote either an SU or an eavesdropper, unless an explicit distinction is needed.

A. Nash Equilibrium in Mixed Strategies and Fictitious Play

As a solution for the proposed game Γ, we use the concept of mixed-strategy Nash equilibrium defined as follows:

Definition 1. *A mixed strategy profile $\boldsymbol{p}^* = (\boldsymbol{p}_i^*, \boldsymbol{p}_{-i}^*)$ is said to be a* mixed strategy Nash equilibrium (MSNE) *if and only if it satisfies the following set of inequalities*

$$\bar{U}_i(\boldsymbol{p}_i^*, \boldsymbol{p}_{-i}^*) \geq \bar{U}_i(\boldsymbol{p}_i, \boldsymbol{p}_{-i}^*)\ \forall \boldsymbol{p}_i \in \Lambda_i\ \forall i \in \mathcal{P}. \quad (9)$$

The above definition implies that, whenever an MSNE is attained, no player has the incentive to unilaterally deviate and change its probability of channel selection. In other words, none of the SUs is capable of generating a higher secrecy rate by unilaterally altering its current probability distribution over the channels. Similarly, none of the eavesdroppers is capable of further decreasing the secrecy rate of SUs through unilateral action. It is well known that, for a finite noncooperative game, a Nash equilibrium in mixed strategies always exists [8].

Here, we consider that the locations of both SUs and eavesdroppers are known for all players in the network. This is commonly assumed in most physical layer security related literature such as in [2] and the references therein. In practice, this can be used to model a variety of scenarios. For example, this could correspond to a case in which SUs suspect the presence of eavesdroppers at a specific predetermined location (such as in the case of a battlefield).

To reach an MSNE, an algorithm based on fictitious play (FP) can be used. FP is a learning scheme in which players update their beliefs about their opponents by monitoring their actions. Since these actions are time dependent, we define $a_i(t)$ to be the the channel chosen by player i at time t. Let $p_i^{a_i}(t),\ a_i \in \mathcal{M}_i, i \in \mathcal{P}$, be the empirical frequency, defined as the frequency with which player i has chosen action a_i until time t. For any time t, the following recurrence holds:

$$p_i^{a_i}(t) = \frac{t-1}{t} \cdot p_i^{a_i}(t-1) + \frac{1}{t} \cdot \mathbb{1}_{\{a_i(t-1)=a_i\}}. \quad (10)$$

FP proceeds as follows: at time t, player i observes the actions of all other players at time $t-1$, and then updates its knowledge of the frequencies. Using (10), player i computes $p_j^{a_j}(t)\ \forall a_j \in \mathcal{M}_j, \forall j \in \mathcal{P} \setminus \{i\}$.

In FP, the channels chosen at time t are the ones that maximize the expected utility with respect to the updated empirical frequencies. To reach an MSNE, players' strategies need to converge to p_i^*, the mixed strategy equilibrium that maximizes the expected value of the utility $\bar{U}_i(p_i, p_{-i}^*)$ as expressed in (8). To do so, player i's action at each time step maximizes the expected utility $\bar{U}_i(a_i, \boldsymbol{p_{-i}}(t))$ over the set of actions:

$$a_i(t) = \arg \max_{a_i \in \mathcal{M}_i} \bar{U}_i(a_i, \boldsymbol{p}_{-i}(t)). \quad (11)$$

$\bar{U}_i(a_i, \boldsymbol{p_{-i}}(t))$ represents the expected utility at the current time t, and it is given by:

$$\bar{U}_i(a_i, \boldsymbol{p}_{-i}(t)) = \sum_{\boldsymbol{a}_{-i} \in \mathcal{M}_{-i}} U_i(a_i, \boldsymbol{a}_{-i}) \prod_{a_j \in \boldsymbol{a}_{-i}} p_j^{a_j}(t), \quad (12)$$

where $\boldsymbol{p}_{-i}(t)$ represents the vector of empirical frequencies pertaining to the actions selected by all other players in $\mathcal{P}\setminus\{i\}$ as calculated by player i at time t. $\mathcal{M}_{-i} := \times_{j \in \mathcal{P}\setminus\{i\}} \mathcal{M}_j$ represents the space of all possible actions taken by all players other than i.

Based on their observations, the players first update their empirical frequencies using (10), and then choose their actions as per (11).

B. Proposed Distributed Learning Algorithm

While FP can be used to find an MSNE, it often leads to extensive computational requirements especially when dealing

with large cognitive networks. This can be clearly seen from (12) and (11). In order to overcome this issue, we propose a novel distributed learning algorithm that can reach an MSNE of the game at a much lower computational complexity relative to the standard FP.

Our proposed approach is inspired from regret matching techniques and the so-called Joint Strategy Fictitious Play (JSFP) introduced in [9]. The main idea is to enable the players to update their actions based on the regret for not choosing this action in the past. At time t, each player i has an expectation of its utility, $\bar{U}_i^{a_i}(t)$, if it chooses a_i. This expected utility has the following update rule [9]:

$$\bar{U}_i^{a_i}(t) = \frac{t-1}{t} \cdot \bar{U}_i^{a_i}(t-1) + \frac{1}{t} \cdot U(a_i, \boldsymbol{a}_{-i}(t-1)), \quad (13)$$

where $\boldsymbol{a}_{-i}(t-1)$ represents the actions taken by all players other than i at time $t-1$ and $U(a_i, \boldsymbol{a}_{-i}(t-1))$ represents the utility of player i if it chose a_i at time $t-1$ and it can be computed using (7). By doing so, the players do not need to continuously calculate the expected utility as in (12), instead, they can update their expected utilities $\forall a_i \in \mathcal{M}_i$ as per (13).

Accordingly, the players update their actions at time t by maximizing their expectations of the utility over the action space:

$$a_i(t) = \arg \max_{a_i \in \mathcal{M}_i} \bar{U}_i^{a_i}(t). \quad (14)$$

Note that computing (11) has a worst-case complexity of $O\left(M^{N+K}\right)$ while computing (14) has a worst-case complexity of $O(M)$ only. Consequently, (13) and (14) can be readily computed even for large networks, unlike (11) and (12).

Based on this idea, we propose a Secure Channel Selection Algorithm (SCSA). SCSA is a low-complexity distributed learning algorithm that can be used by SUs and eavesdroppers to reach an equilibrium and it is divided into three main stages. In the first stage, both SUs and eavesdroppers choose the channels with equal probabilities as they do not have any observations on the state of the network initially.

The second stage is called fast learning. In this stage, the players learn about each others' decisions and choose their actions according to the update equations (13) and (14). Unlike classical regret matching such as in [9], our proposed approach allows the players to learn an MSNE not a pure strategy NE. Therefore, the players will keep observing and updating the frequencies as per (10).

When the difference between all the calculated frequencies in consecutive time instants is within a certain threshold τ, the players switch to the third and final stage of the algorithm. In this stage, the players use the standard fictitious play process starting from the beliefs obtained in stage 2 until they converge to an MSNE. This algorithm is summarized in Table I.

TABLE I
PROPOSED SECURE CHANNEL SELECTION ALGORITHM

SCSA Stage 1 - Initialization
Each player $i \in \mathcal{P}$ chooses a random action $a_i(0) \in \mathcal{M}_i$.
SCSA Stage 2 - Fast Learning
repeat
Each player $i \in \mathcal{P}$ observes the actions of other players $\boldsymbol{a}_{-i}(t-1)$ and updates its average utility as per (13).
Each player $i \in \mathcal{P}$ takes action $a_i(t)$ as per (14).
Each player $i \in \mathcal{P}$ updates his knowledge of empirical frequencies $\boldsymbol{p}_{-i}(t)$ as per (10).
until frequencies are within τ.
SCSA Stage 3 - Fictitious Play
As a starting point for FP, players use the probabilities obtained in SCSA Stage 2.
repeat
Each player $i \in \mathcal{P}$ observes the actions of other players $\boldsymbol{a}_{-i}(t-1)$ and updates its knowledge of empirical frequencies $\boldsymbol{p}_{-i}(t)$ as per (10).
Each player $i \in \mathcal{P}$ takes action $a_i(t)$ as per (11).
until convergence to a MSNE.

IV. Simulations and Results

For simulations, we set up the following network: the BS is located at the center of a 750m×750m square with SUs and eavesdroppers randomly placed in this area. The SUs' transmit power level $P_{i,m}$ is set to 10 mW. Unless otherwise specified, we consider a network of $M = 3$ channels. We set the noise level to $\sigma^2 = -90$ dBm, the path loss exponent to $\mu = 3$ and the path loss constant to 1. Finally, we set the SCSA threshold $\tau = 10^{-2}$. All the obtained results are averaged over random positions of SUs and eavesdroppers, channel gains, and channel availability θ_m.

To evaluate the performance of the proposed algorithm, we show, in Fig. 1, the average expected utility achieved by the SUs as the number N of SUs increases for a network with $K = 3$ eavesdroppers. The performance of our approach is compared to that of a classical spectrum sharing algorithm, in which SUs keep optimizing their capacities given by (2) until all channel selections converge. Also, SCSA is compared to standard FP and to an equiprobable channel selection algorithm, in which all SUs choose channels with equal probabilities. Fig. 1 shows that as the number N of SUs increases, the average utility per SU decreases for all four schemes. This is due to the fact that the SUs are utilizing the channels more, and hence the mutual interference between them is increasing. We can clearly see from Fig. 1 that the proposed algorithm and FP have comparable performances, while they both outperform the other two approaches. Fig. 1 shows that the proposed SCSA scheme yields a significant improvement, in terms of the average utility per SU, at all N. This improvement varies between 76.2% and 89.7% (at $N = 2$) to 25.4% and 32.7% (at $N = 6$), relative to equiprobable selection and classical spectrum sharing, respectively. Due to the presence of multiple MSNEs, FP and SCSA may converge to different equilibrium points with different average utilities.

Fig. 2 shows the average expected utility achieved by the SUs as the number K of eavesdroppers increases for a network with $N = 4$ SUs. We notice that as the number of eavesdroppers increases, the average utility per SU decreases for all four schemes. This is a result of the fact that an increase in the number of eavesdroppers will further decrease the overall secrecy rate of the SUs. In Fig. 2, we can see that SCSA and FP have a comparable performance while they both outperform the other two approaches. In this respect, Fig. 2 shows that the

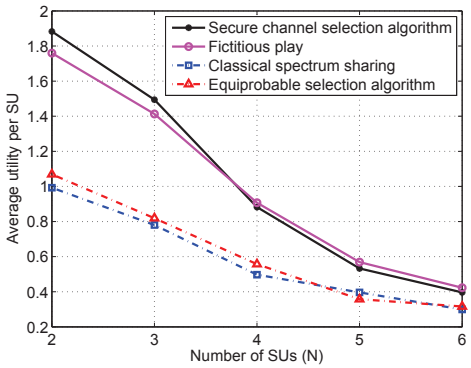

Fig. 1. Average utility per SU resulting from all selection algorithms as the number N of SUs varies for $K = 3$ eavesdroppers.

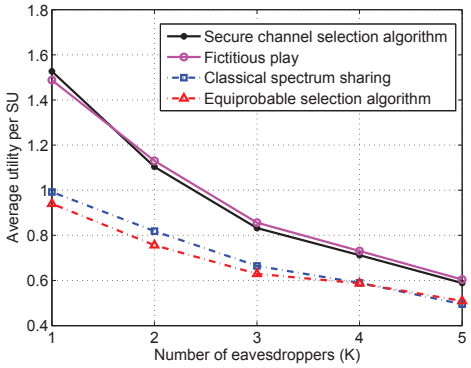

Fig. 2. Average utility per SU resulting from from all selection algorithms as the number K of eavesdroppers varies for $N = 4$ SUs.

proposed SCSA scheme yields a significant improvement, in terms of the average utility per SU, at all K. This improvement varies between 62.4% and 53.9% (at $K = 1$) to 15.6% and 18.8% (at $K = 5$), relative to equiprobable selection and classical spectrum sharing, respectively.

In Fig. 3 we show the computational performance of our proposed secure channel selection algorithm versus FP as the number of SUs, N, increases in the network. We assess the computational needs of both learning schemes in terms of the average number of utility computations, as per (7), performed per player in order to converge to an MSNE of the game. Fig. 3 shows that, as the number N of SUs in the network increases, the average number of utility computations done by each player increases exponentially in both algorithms. This is due to the fact that, as N increases, each SU i will have to consider a larger set of action space $\mathcal{M}_{-i}$ when calculating its expected utility. We note that the exponential increase in FP is due to the fact that computing (11) has a worst-case complexity of $O\left(M^{N+K}\right)$. The increase in complexity of the proposed SCSA is due to the use of FP at stage 3. Fig. 3 shows that the proposed SCSA achieves significant reductions in terms of computations as it requires 86.5% and 74.6% less computations than fictitious play at $N = 1$ and $N = 8$, respectively.

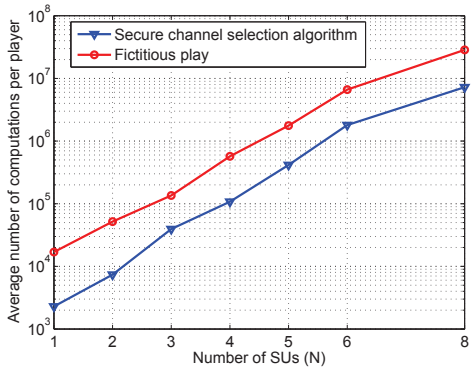

Fig. 3. Average number of computations per player resulting from both SCSA and FP as the number of SUs, N, varies for $K = 3$ eavesdroppers.

V. Conclusion

In this work, we have analyzed, using game theoretic techniques, the interactions between SUs and eavesdroppers in a cognitive radio network in the presence of multiple PUs. To this extent, we have formulated a game between the SUs and eavesdroppers and analyzed its equilibrium. In the proposed game, the objective of the SUs was to maximize their secrecy rates while the objective of eavesdroppers was to minimize the overall secrecy rate of the network by maximizing their eavesdropping capabilities. To solve this game, we have introduced a novel secure channel selection algorithm that enables the SUs and eavesdroppers to take distributed decisions that allows them to reach the equilibrium of the game. Simulation results have shown that the proposed approach yields significant improvements, in terms of the average secrecy rate per SU, when compared to classical spectrum sharing schemes.

References

[1] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[3] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, Feb 2005.

[4] H. Li and Z. Han, "Dogfight in spectrum: Jamming and anti-jamming in multichannel cognitive radio systems," in *Proc. of IEEE Global Communications Conference (GLOBECOM)*, New Orleans, Louisiana, USA, 2009.

[5] W. Wang, H. Li, Y. Sun, and Z. Han, "Catchit: detect malicious nodes in collaborative spectrum sensing," in *Proc. of IEEE Global Communications Conference (GLOBECOM)*, Honolulu, Hawaii, USA, 2009.

[6] T. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in *Proc. of the 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, Singapore, 2008.

[7] V. Aggarwal, L. Sankar, A. Calderbank, and H. Poor, "Information secrecy from multiple eavesdroppers in orthogonal relay channels," in *Proc. of IEEE International Symposium on Information Theory*, Seoul, Korea, 2009.

[8] T. Başar and G. Olsder, *Dynamic Noncooperative Game Theory*. SIAM Series in Classics in Applied Mathematics, Philadelphia, January 1999.

[9] J. Marden, G. Arslan, and J. Shamma, "Joint strategy fictitious play with inertia for potential games," *IEEE Transactions on Automatic Control*, vol. 54, no. 2, pp. 208–220, Feb 2009.